**SPECYFIKACJA WARUNKÓW ZAMÓWIENIA**

**(dalej: SWZ)**

Znak sprawy: BZP.272.93.2023

**ZAMAWIAJĄCY**

Powiat Wołomiński

ul. Prądzyńskiego 3, 05-200 Wołomin

**REGON:** 013269344 **NIP:** 125-09-40-609

**tel.:** (22) 787-43-01

**Adres strony internetowej prowadzonego postępowania:** <https://platformazakupowa.pl/pn/powiat_wolominski>

Na tej stronie udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia

Adres platformy zakupowej: <https://platformazakupowa.pl/pn/powiat_wolominski>

Adres poczty elektronicznej: bzp@powiat-wolominski.pl

**Nazwa zamówienia:**

**Dostawa zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem w ramach zadania „Zakup urządzeń sieciowych klasy UTM, urządzeń komputerowych, oprogramowania biurowego, macierzy oraz dysków i pamięci serwerowych na potrzeby Starostwa Powiatowego w Wołominie”**

Wartość zamówienia **nie przekracza** progów unijnych określonych na podstawie art. 3 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (t.j.: Dz.U. z 2022 r. poz.1710 z późn. zm.).

**Spis treści:**

**Rozdział I** –Informacje ogólne

1. **Tryb udzielenia zamówienia**
2. **Wykonawcy/podwykonawcy/podmioty trzecie udostępniające wykonawcy swój potencjał**
3. **Komunikacja w postępowaniu**
4. **Wizja lokalna**
5. **Podział zamówienia na części**
6. **Oferty wariantowe**
7. **Katalogi elektroniczne**
8. **Umowa ramowa**
9. **Aukcja elektroniczna**
10. **Zamówienia, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp**
11. **Rozliczenia w walutach obcych**
12. **Zwrot kosztów udziału w postępowaniu**
13. **Zaliczki na poczet udzielenia zamówienia**
14. **Unieważnienie postępowania**
15. **Pouczenie o środkach ochrony prawnej**
16. **Ochrona danych osobowych zebranych przez zamawiającego w toku postępowania**

 **Rozdział II** – Wymagania stawiane wykonawcy

1. **Przedmiot zamówienia**
2. **Rozwiązania równoważne**
3. **Wymagania w zakresie zatrudniania przez wykonawcę lub podwykonawcę osób na podstawie stosunku pracy**
4. **Wymagania w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2 ustawy Pzp**
5. **Informacja o przedmiotowych środkach dowodowych**
6. **Termin wykonania zamówienia**
7. **Informacja o warunkach udziału w postępowaniu o udzielenie zamówienia**
8. **Podstawy wykluczenia**
9. **Wykaz podmiotowych środków dowodowych**
10. **Wymagania dotyczące wadium**
11. **Sposób przygotowania ofert**
12. **Opis sposobu obliczenia ceny**

 **Rozdział III** –Informacje o przebiegu postępowania

1. **Sposób porozumiewania się zamawiającego z wykonawcami**
2. **Sposób oraz termin składania ofert; Termin otwarcia ofert**
3. **Termin związania ofertą**
4. **Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert**
5. **Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do umowy w sprawie zamówienia publicznego**
6. **Zabezpieczenie należytego wykonania umowy**
7. **Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego**
8. **Informacje ogólne**
9. **Tryb udzielenia zamówienia**

Tryb podstawowy bez negocjacji, o którym mowa w art. 275 pkt 1 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (t.j.: Dz.U. z 2022 r. poz.1710 z późn. zm.) – dalej: ustawa Pzp.

1. **Wykonawcy/podwykonawcy/podmioty trzecie udostępniające wykonawcy swój potencjał**
2. **Wykonawcą** jest osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która oferuje na rynku wykonanie robót budowlanych lub obiektu budowlanego, dostawę produktów lub świadczenie usług lub ubiega się o udzielenie zamówienia, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego.
3. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 ustawy Pzp, tj. mających status zakładu pracy chronionej, spółdzielnie socjalne oraz innych wykonawców, których głównym celem lub głównym celem działalności ich wyodrębnionych organizacyjnie jednostek, które będą realizowały zamówienie, jest społeczna i zawodowa integracja osób społecznie marginalizowanych.
4. Zamówienie może zostać udzielone wykonawcy, który:

– spełnia warunki udziału w postępowaniu opisane w rozdziale II podrozdziale 7 SWZ,

– nie podlega wykluczeniu na podstawie art. 108 ust. 1, art. 109 ust. 1 pkt 4 i 7 ustawy Pzp oraz 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.

– złożył ofertę niepodlegającą odrzuceniu na podstawie art. 226 ust. 1 ustawy Pzp.

1. **Wykonawcy** **mogą wspólnie ubiegać się o udzielenie zamówienia**.

W takim przypadku:

* Wykonawcy występujący wspólnie są zobowiązani do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy w sprawie przedmiotowego zamówienia publicznego.
* Wszelka korespondencja będzie prowadzona przez zamawiającego wyłącznie z pełnomocnikiem.
1. **Potencjał podmiotu trzeciego**

W celu potwierdzenia spełnienia warunków udziału w postępowaniu, wykonawca może polegać na potencjale podmiotu trzeciego na zasadach opisanych w art. 118–123 ustawy Pzp. Podmiot trzeci, na potencjał którego wykonawca powołuje się w celu wykazania spełnienia warunków udziału w postępowaniu, nie może podlegać wykluczeniu na podstawie art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4 i 7 ustawy Pzp oraz 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.

1. **Podwykonawstwo**

Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych zadań.

1. **Komunikacja w postępowaniu**

Komunikacja w postępowaniu o udzielenie zamówienia odbywa się przy użyciu środków komunikacji elektronicznej, za pośrednictwem platformy zakupowej pod adresem <https://platformazakupowa.pl/pn/powiat_wolominski>, zwanej dalej **Platformą**. Szczegółowe informacje dotyczące przyjętego w postępowaniu sposobu komunikacji, znajdują się w rozdziale III podrozdziale 1 niniejszej SWZ.

Uwaga!Przed przystąpieniem do składania oferty, wykonawca jest zobowiązany zapoznać się z Instrukcją korzystania z Platformy zakupowej Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>

1. **Wizja lokalna**

Zamawiający nie wymaga odbycia przez wykonawcę wizji lokalnej.

1. **Podział zamówienia na części**

Zamawiający nie dokonuje podziału zamówienia na części. Tym samym zamawiający nie dopuszcza składania ofert częściowych, o których mowa w art. 7 pkt 15 ustawy Pzp.

**Powody niedokonania podziału:**

Zamówienie jednorodne.

1. **Oferty wariantowe**

Zamawiający:

– nie dopuszcza możliwości,

– nie wymaga

złożenia oferty wariantowej, o której mowa w art. 92 ustawy Pzp tzn. oferty przewidującej odmienny sposób wykonania zamówienia niż określony w niniejszej SWZ.

1. **Katalogi elektroniczne**

Zamawiający:

– nie wymaga złożenia ofert w postaci katalogów elektronicznych.

1. **Umowa ramowa**

Zamawiający nie przewiduje zawarcia umowy ramowej, o  której mowa w art. 311–315 ustawy Pzp.

1. **Aukcja elektroniczna**

Zamawiający **nie przewiduje** przeprowadzenia aukcji elektronicznej, o  której mowa w art. 308 ust. 1 ustawy Pzp.

1. **Zamówienia, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp**

Zamawiający nie przewiduje udzielenie udzielania zamówień na podstawie art. 214 ust. 1 pkt 7 i 8 ustawy Pzp/zamówienia polegającego na powtórzeniu podobnych usług lub robót budowlanych, zamówienia na dodatkowe dostawy.

1. **Rozliczenia w walutach obcych**

Zamawiający nie przewiduje rozliczenia w walutach obcych.

1. **Zwrot kosztów udziału w postępowaniu**

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

1. **Zaliczki na poczet udzielenia zamówienia**

Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.

1. **Unieważnienie postępowania**

Poza możliwością unieważnienia postępowania o udzielenie zamówienia na podstawie art. 255 ustawy Pzp, zamawiający przewiduje możliwość unieważnienia postępowania, jeżeli środki publiczne, które zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostaną mu przyznane.

1. **Pouczenie o środkach ochrony prawnej**

Wykonawcom, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy, przysługują środki ochrony prawnej na zasadach przewidzianych w dziale IX ustawy Pzp (art. 505–590).

1. **Ochrona danych osobowych zebranych przez zamawiającego w toku postępowania**
2. Zamawiający oświadcza, że spełnia wymogi określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z  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 4 maja 2016 r.), dalej: RODO, tym samym dane osobowe podane przez wykonawcę  będą przetwarzane zgodnie z RODO oraz zgodnie z przepisami krajowymi.

Dane osobowe wykonawcy będą przetwarzane na podstawie art. 6 ust. 1 lit. c RODO
w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego pn. Dostawa zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem ramach zadania „Zakup urządzeń sieciowych klasy UTM, urządzeń komputerowych, oprogramowania biurowego, macierzy oraz dysków i pamięci serwerowych na potrzeby Starostwa Powiatowego w Wołominie”

Odbiorcami przekazanych przez wykonawcę danych osobowych będą osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania zgodnie z art. 8 oraz art. 96 ust. 3 ustawy Pzp, a także art. 6 ustawy z 6 września 2001 r. o dostępie do informacji publicznej.

1. Dane osobowe wykonawcy zawarte w protokole postępowania będą przechowywane przez okres 4 lat, od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy.
2. Klauzula informacyjna, o której mowa w art. 13 ust. 1 i 2 RODO znajduje się **w załączniku nr 1 do SWZ.**
3. Zamawiający nie planuje przetwarzania danych osobowych wykonawcy w celu innym niż cel określony w lit. b powyżej. Jeżeli administrator będzie planował przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane (tj. cel określony w lit. b powyżej), przed takim dalszym przetwarzaniem poinformuje on osobę, której dane dotyczą, o tym innym celu oraz udzieli jej wszelkich innych stosownych informacji, o których mowa w art. 13 ust. 2 RODO.
4. Wykonawca jest zobowiązany, w związku z udziałem w przedmiotowym postępowaniu, do wypełnienia wszystkich obowiązków formalno-prawnych wymaganych przez RODO i związanych z udziałem w przedmiotowym postępowaniu o udzielenie zamówienia. Do obowiązków tych należą:
* obowiązek informacyjny przewidziany w art. 13 RODO względem osób fizycznych, których dane osobowe dotyczą i od których dane te wykonawca bezpośrednio pozyskał i przekazał zamawiającemu w treści oferty lub dokumentów składanych na żądanie zamawiającego;
* obowiązek informacyjny wynikający z art. 14 RODO względem osób fizycznych, których dane wykonawca pozyskał w sposób pośredni, a które to dane wykonawca przekazuje zamawiającemu w treści oferty lub dokumentów składanych na żądanie zamawiającego.
1. W celu zapewnienia, że wykonawca wypełnił ww. obowiązki informacyjne oraz ochrony prawnie uzasadnionych interesów osoby trzeciej, której dane zostały przekazane w związku z udziałem w postępowaniu, wykonawca składa oświadczenia o wypełnieniu przez niego obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO – treść oświadczenia została zawarta **w załączniku nr 1 do SWZ 🡪 Informacje dotyczące wykonawcy.**
2. Zamawiający informuje, że:
* Zamawiający udostępnia dane osobowe, o których mowa w art. 10 RODO (dane osobowe dotyczące wyroków skazujących i czynów zabronionych) w celu umożliwienia korzystania ze środków ochrony prawnej, o których mowa w dziale IX ustawy Pzp, do upływu terminu na ich wniesienie.
* Udostępnianie protokołu i załączników do protokołu ma zastosowanie do wszystkich danych osobowych, z wyjątkiem tych, o których mowa w art. 9 ust. 1 RODO (tj. danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby), zebranych w toku postępowania o udzielenie zamówienia.
* W przypadku korzystania przez osobę, której dane osobowe są przetwarzane przez zamawiającego, z uprawnienia, o którym mowa w art. 15 ust. 1–3 RODO (związanych z prawem wykonawcy do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jego dotyczące, prawem wykonawcy do bycia poinformowanym o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem jego danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz prawem otrzymania przez wykonawcę od administratora kopii danych osobowych podlegających przetwarzaniu), zamawiający może żądać od osoby występującej z żądaniem wskazania dodatkowych informacji, mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.
* Skorzystanie przez osobę, której dane osobowe dotyczą, z uprawnienia, o którym mowa w art. 16 RODO (z uprawnienia do sprostowania lub uzupełnienia danych osobowych), nie może naruszać integralności protokołu postępowania oraz jego załączników.
* W postępowaniu o udzielenie zamówienia zgłoszenie żądania ograniczenia przetwarzania, o którym mowa w art. 18 ust. 1 RODO, nie ogranicza przetwarzania danych osobowych do czasu zakończenia tego postępowania.
* W przypadku gdy wniesienie żądania dotyczącego prawa, o którym mowa w art. 18 ust. 1 RODO spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole postępowania lub załącznikach do tego protokołu, od dnia zakończenia postępowania o udzielenie zamówienia zamawiający nie udostępnia tych danych, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 rozporządzenia 2016/679.

**Do spraw nieuregulowanych w SWZ mają zastosowanie przepisy ustawy z 11 września 2019 r. – Prawo zamówień publicznych (t.j.: Dz.U. z 2022 r., poz. 1710 ze zm.).**

1. **Wymagania stawiane wykonawcy**
2. **Przedmiot zamówienia**

**Dostawa zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem ramach zadania „Zakup urządzeń sieciowych klasy UTM, urządzeń komputerowych, oprogramowania biurowego, macierzy oraz dysków i pamięci serwerowych na potrzeby Starostwa Powiatowego w Wołominie”**

Kod CPV:

**32420000-3**

**32427000-2**

Szczegółowy opis przedmiotu zamówienia:

* **UTM TYP1 – 2 sztuki**

|  |
| --- |
| **ARCHITEKTURA SYSTEMU** |
| 1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności co najmniej Active-Passive, o specyfikacji opisanej poniżej
2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
 |
| 1. Metalowa obudowa typu desktop.
2. Możliwość zastosowania redundantnego zasilania, z wykorzystaniem zewnętrznego zasilacza.
3. Obsługa nielimitowanej ilości hostów w sieci chronionej.
4. Minimalna liczba i typ interfejsów fizycznych:

•System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/2500•System realizujący funkcję Firewall musi dysponować minimum 1 interfejsem optycznym 1 GbE (SFP)•Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.1. Minimalna liczba nowych połączeń na sekundę: 20 000
2. Minimalna liczba jednoczesnych połączeń: 300 000
3. Minimalna przepustowość Firewall: 4 Gbps
4. Minimalna przepustowość IPS: 2 Gbps
5. Minimalna przepustowość Threat Protection: 500 Mbps
6. Minimalna przepustowość IPSec VPN: 1 Gbps
7. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania lub musi istnieć możliwość wykorzystania karty SD do celów logowania i raportowania.
 |

|  |
| --- |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** |
| **Zarządzanie i utrzymanie** | 1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.
2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping
3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego
7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników.
8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP
10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3
11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie.
12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
 |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | 1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.
2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia
3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading.
5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking).
7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
8. Rozwiązanie musi zapewniać obsługę routingu statycznego.
9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP).
10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP.
11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay.
12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP.
13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP.
15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe .
16. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.
17. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
18. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług.
19. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
20. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
 |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | 1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia.
2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
 |
| **Autoryzacja użytkowników** | 1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 100 kont.
2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP
3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory
4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
 |
| **Samoobsługowy portal dla użytkowników** | 1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android
3. Rozwiązanie musi umożliwiać zmianę hasła.
 |
| **Podstawowe opcje VPN** | System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)
2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
 |
| **OCHRONA SIECI** |
| **IPS** | 1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur.
2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS.
3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.
4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur
5. System musi generować alerty w przypadku wykrycia ataku.
6. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów
 |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** |
| **Ochrona i kontrola Web** | 1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.
3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym poprzez komercyjny antywirus.
4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów.
5. System musi filtrować pliki na podstawie MIME.
6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
7. Rozwiązanie musi zawierać przynajmniej 65 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.
8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS.
9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
 |
| **Ochrona i kontrola aplikacji** | 1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.
2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook)
3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
 |
| **Kształtowanie pasma dla Web i Aplikacji** | 1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download.
2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
 |
| **OCHRONA ANTYWIRUSOWA** |
| **Ochrona i kontrola Email** | 1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy
2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń.
5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników.
6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL.
7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email.
8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
 |
| **OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY** |
| **On-cloud Sandboxing** | Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe
2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf.
3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf.
4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab
5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
 |
| **LOGOWANIE I RAPORTOWANIE** |
|  | 1. System musi umożliwiać składowanie oraz archiwizację logów.
2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.
3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
5. Rozwiązanie musi generować raporty w HTML i CSV.
6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog.
7. System musi zapewniać podgląd wykorzystania łącza internetowego.
8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP
9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
 |

* **UTM TYP2 – 3 sztuki**

|  |
| --- |
| **ARCHITEKTURA SYSTEMU** |
| 1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności co najmniej Active-Passive, o specyfikacji opisanej poniżej
2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
 |
| 1. Metalowa obudowa typu desktop.
2. Możliwość zastosowania redundantnego zasilania, z wykorzystaniem zewnętrznego zasilacza.
3. Obsługa nielimitowanej ilości hostów w sieci chronionej.
4. Minimalna liczba i typ interfejsów fizycznych:

•System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/2500•System realizujący funkcję Firewall musi dysponować minimum 1 interfejsem optycznym 1 GbE (SFP)•Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.1. Minimalna liczba nowych połączeń na sekundę: 25 000
2. Minimalna liczba jednoczesnych połączeń: 400 000
3. Minimalna przepustowość Firewall: 8 Gbps
4. Minimalna przepustowość IPS: 4 Gbps
5. Minimalna przepustowość Threat Protection: 1 Gbps
6. Minimalna przepustowość IPSec VPN: 2 Gbps
7. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania lub musi istnieć możliwość wykorzystania karty SD do celów logowania i raportowania.
 |

|  |
| --- |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** |
| **Zarządzanie i utrzymanie** | 1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.
2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping
3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego
7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników.
8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP
10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3
11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie.
12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
 |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | 1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.
2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia
3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading.
5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking).
7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
8. Rozwiązanie musi zapewniać obsługę routingu statycznego.
9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP).
10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP.
11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay.
12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP.
13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP.
15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe .
16. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.
17. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
18. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług.
19. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
20. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
 |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | 1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia.
2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
 |
| **Autoryzacja użytkowników** | 1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 100 kont.
2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP
3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory
4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
 |
| **Samoobsługowy portal dla użytkowników** | 1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android
3. Rozwiązanie musi umożliwiać zmianę hasła.
 |
| **Podstawowe opcje VPN** | System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)
2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
 |
| **OCHRONA SIECI** |
| **IPS** | 1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur.
2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS.
3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.
4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur
5. System musi generować alerty w przypadku wykrycia ataku.
6. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów
 |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** |
| **Ochrona i kontrola Web** | 1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.
3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym z wykorzystaniem komercyjnego antywirusa.
4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów.
5. System musi filtrować pliki na podstawie MIME.
6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
7. Rozwiązanie musi zawierać przynajmniej 65 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.
8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS.
9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
 |
| **Ochrona i kontrola aplikacji** | 1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.
2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook)
3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
 |
| **Kształtowanie pasma dla Web i Aplikacji** | 1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download.
2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
 |
| **OCHRONA ANTYWIRUSOWA** |
| **Ochrona i kontrola Email** | 1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy
2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń.
5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników.
6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL.
7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email.
8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
 |
| **OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY** |
| **On-cloud Sandboxing** | Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe
2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf.
3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf.
4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab
5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
 |
| **LOGOWANIE I RAPORTOWANIE** |
|  | 1. System musi umożliwiać składowanie oraz archiwizację logów.
2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.
3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
5. Rozwiązanie musi generować raporty w HTML i CSV.
6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog.
7. System musi zapewniać podgląd wykorzystania łącza internetowego.
8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP
9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
 |

* **UTM TYP 3 – 1 sztuka**

|  |
| --- |
| **ARCHITEKTURA SYSTEMU** |
| 1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności conajmniej Active-Passive, o specyfikacji opisanej poniżej
2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
 |
| 1. Metalowa obudowa o wysokości max. 1U przeznaczona do montażu w szafie RACK 19’’
2. Podwójne, redundantne, zintegrowane zasilanie.
3. Obsługa nielimitowanej ilości hostów w sieci chronionej.
4. Minimalna liczba i typ interfejsów fizycznych:

•System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 2,5 Gbps•System realizujący funkcję Firewall musi dysponować minimum 2 interfejsami optycznymi 1GbE (SFP)•System realizujący funkcję Firewall musi umożliwiać rozbudowę dostępnych interfejsów •Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.1. Minimalna liczba nowych połączeń na sekundę: 30 000
2. Minimalna liczba jednoczesnych połączeń: 600 000
3. Minimalna przepustowość Firewall: 10 Gbps
4. Minimalna przepustowość IPS: 5 Gbps
5. Minimalna przepustowość Threat Protection: 1,3 Gbps
6. Minimalna przepustowość IPSec VPN: 2,5 Gbps
7. Minimalna liczba tuneli SSL VPN: 150
8. Minimalna liczba tuneli IPSEC VPN: 1000
9. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania
 |

|  |
| --- |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** |
| **Zarządzanie i utrzymanie** | 1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.
2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping
3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego
7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników.
8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP
10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3
11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie.
12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
 |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | 1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.
2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia
3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading.
5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking).
7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
8. Rozwiązanie musi zapewniać obsługę routingu statycznego.
9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP).
10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP.
11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay.
12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP.
13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP.
15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe .
16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.
18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług.
20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
 |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | 1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia.
2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
 |
| **Autoryzacja użytkowników** | 1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.
2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP
3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory
4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
 |
| **Samoobsługowy portal dla użytkowników** | 1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android
3. Rozwiązanie musi umożliwiać zmianę hasła.
 |
| **Podstawowe opcje VPN** | System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)
2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
 |
| **OCHRONA SIECI** |
| **IPS** | 1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur.
2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS.
3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.
4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur
5. System musi generować alerty w przypadku wykrycia ataku.
6. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów
 |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** |
| **Ochrona i kontrola Web** | 1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.
3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym z wykorzystaniem komercyjnego antywirusa.
4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów.
5. System musi filtrować pliki na podstawie MIME.
6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
7. Rozwiązanie musi zawierać przynajmniej 65 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.
8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS.
9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
 |
| **Ochrona i kontrola aplikacji** | 1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.
2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook)
3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
 |
| **Kształtowanie pasma dla Web i Aplikacji** | 1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download.
2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
 |
| **OCHRONA ANTYWIRUSOWA** |
| **Ochrona i kontrola Email** | 1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy
2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń.
5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników.
6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL.
7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email.
8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
 |
| **OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY** |
| **On-cloud Sandboxing** | Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe
2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf.
3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf.
4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab
5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
 |
| **LOGOWANIE I RAPORTOWANIE** |
|  | 1. System musi umożliwiać składowanie oraz archiwizację logów.
2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.
3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
5. Rozwiązanie musi generować raporty w HTML i CSV.
6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog.
7. System musi zapewniać podgląd wykorzystania łącza internetowego.
8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP
9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
 |

* **UTM TYP 4 – 1 sztuka**

|  |
| --- |
| **ARCHITEKTURA SYSTEMU** |
| 1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności conajmniej Active-Passive, o specyfikacji opisanej poniżej
2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
 |
| 1. Metalowa obudowa o wysokości max. 1U przeznaczona do montażu w szafie RACK 19’’
2. Podwójne, redundantne, zintegrowane zasilanie.
3. Obsługa nielimitowanej ilości hostów w sieci chronionej.
4. Minimalna liczba i typ interfejsów fizycznych:

•System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 2,5 Gbps•System realizujący funkcję Firewall musi dysponować minimum 2 interfejsami optycznymi 10GbE (SFP+)•System realizujący funkcję Firewall musi umożliwiać rozbudowę dostępnych interfejsów do minimum 6 interfejsów optycznych 10GbE (SFP+) lub 4 interfejsów elektrycznych 10 Gbps lub 16 interfejsów 2.5 Gbps.•Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.1. Minimalna liczba nowych połączeń na sekundę: 50 000
2. Minimalna liczba jednoczesnych połączeń: 1 000 000
3. Minimalna przepustowość Firewall: 18 Gbps
4. Minimalna przepustowość IPS: 10 Gbps
5. Minimalna przepustowość Threat Protection: 3 Gbps
6. Minimalna przepustowość IPSec VPN: 4 Gbps
7. Minimalna liczba tuneli SSL VPN: 300
8. Minimalna liczba tuneli IPSEC VPN: 1000
9. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania
 |

|  |
| --- |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** |
| **Zarządzanie i utrzymanie** | 1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.
2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping
3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego
7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników.
8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP
10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3
11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie.
12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
 |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | 1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.
2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia
3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading.
5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking).
7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
8. Rozwiązanie musi zapewniać obsługę routingu statycznego.
9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP).
10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP.
11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay.
12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP.
13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP.
15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe .
16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.
18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług.
20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
 |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | 1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia.
2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
 |
| **Autoryzacja użytkowników** | 1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.
2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP
3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory
4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
 |
| **Samoobsługowy portal dla użytkowników** | 1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android
3. Rozwiązanie musi umożliwiać zmianę hasła.
 |
| **Podstawowe opcje VPN** | System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)
2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
 |
| **OCHRONA SIECI** |
| **IPS** | 1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur.
2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS.
3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.
4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur
5. System musi generować alerty w przypadku wykrycia ataku.
6. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów
 |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** |
| **Ochrona i kontrola Web** | 1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.
3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym z wykorzystaniem komercyjnego antywirusa.
4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów.
5. System musi filtrować pliki na podstawie MIME.
6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
7. Rozwiązanie musi zawierać przynajmniej 65 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.
8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS.
9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
 |
| **Ochrona i kontrola aplikacji** | 1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.
2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook)
3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
 |
| **Kształtowanie pasma dla Web i Aplikacji** | 1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download.
2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
 |
| **OCHRONA ANTYWIRUSOWA** |
| **Ochrona i kontrola Email** | 1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy
2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń.
5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników.
6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL.
7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email.
8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
 |
| **OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY** |
| **On-cloud Sandboxing** | Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe
2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf.
3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf.
4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab
5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
 |
| **LOGOWANIE I RAPORTOWANIE** |
|  | 1. System musi umożliwiać składowanie oraz archiwizację logów.
2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.
3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
5. Rozwiązanie musi generować raporty w HTML i CSV.
6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog.
7. System musi zapewniać podgląd wykorzystania łącza internetowego.
8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP
9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
 |

* **WYMAGANIA WSPÓLNE DLA UTM: TYP 1, TYP2, TYP3 i TYP 4**

|  |
| --- |
| **POZOSTAŁE** |
| **Certyfikaty**  | Urządzenie musi posiadać:- certyfikat Common Criteria;- certyfikat ICSA Labs dla funkcji VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE; |
| **GWARANCJA I SERWIS** |
| Wymagania ogólne dla dostarczanych rozwiązań : |
| * Dostarczone urządzenia musza być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji.
* Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki,
* Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu,
* Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta,
* Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.
 |
| Warunki gwarancji i serwisu : |
| * Na dostarczany sprzęt musi być udzielona **min. 12-miesięczna gwarancja**; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań,
* Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę),
 |
| Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:* bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji
* dostęp do dokumentacji sprzętu i oprogramowania,
* dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
* dostęp do pomocy technicznej producenta.

Zamawiający w momencie odbioru otrzyma:* licencje obejmujące wszystkie wymagane moduły na okres **min. 12 miesięcy**
* możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.
 |

* **WDROŻENIE**

Wykonawca w ramach realizacji Przedmiotu Umowy dokona wdrożenia i uruchomienia systemu w stanie kompletnym.

Osoba realizująca usługi wdrożenia i uruchomienia systemu musi być ekspertem w obszarze

związanym z technologią bezpieczeństwa sieci oraz legitymować się ważnym i aktualnym

certyfikatem technicznym oferowanym w ramach certyfikacji Producenta oferowanego rozwiązania Next Generation Firewall oraz musi posiadać dostęp do bazy wiedzy tego Producenta.

W ramach wdrożenia Zamawiający wymaga co najmniej następujących czynności:

1. Wykonawca zapewni obecność w miejscu instalacji Urządzeń wykwalifikowanej osoby

(inżyniera) podczas wdrożenia i uruchomienia systemu przynajmniej przez 5 dni.

2. Montaż urządzeń zostanie wykonany w:

* Wołomin, ul.Prądzyńskiego 3;
* Wołomin, ul.Powstańców 8/10;
* Wołomin, ul.Kobyłkowska 1A;
* Wołomin, ul.Sasina 15;
* Zagościniec, ul.Asfaltowa 1;
* Radzymin, ul.Komunalna 8;
* Tłuszcz, ul.Warszawska 10;

3. Wykonawca przeprowadzi analizę infrastruktury sieciowej (optymalizacja zgodna z aktualnymi trendami panującymi w sferze zagrożeń sieciowych i możliwościami systemu)

4. Wykonawca przygotuje środowisko: rejestracja i uruchomienie urządzeń, instalacja licencji, aktualizacja oprogramowania.

5. Wykonawca dokona konfiguracji Urządzeń co najmniej według poniższych wytycznych:

a. konfiguracja zarządzania, skomunikowanie z siecią Zamawiającego z wykorzystaniem wskazanych adresów IP dla interfejsów;

c. analiza polityki bezpieczeństwa na produkcyjnej zaporze sieciowej i konfiguracja wdrażanego systemu odpowiednich reguł dotyczących:

* Konfiguracja sieci (interfejsy i routing).
* Konfiguracja firewalla (limit reguł – 40).
* Konfiguracja NAT (limit reguł – 10).
* Konfiguracja IPS – zgodnie z wymaganiami klienta.
* Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy.
* Integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników).
* Konfiguracja dostawców Internetu (maksymalnie 3 dostawców).
* Instruktaż konfiguracji transparentnej autoryzacji w Active Directory

Konfiguracja VPN:

* IPSec Site-to-Site (limit 5 tuneli)
* SSL VPN (na kliencie pod windows) Client-to-Site (limit 5 tuneli)
* przekazanie Zamawiającemu wszystkich haseł do systemu.

6. Kopia bezpieczeństwa konfiguracji wdrożonych urządzeń.

7. Instruktarz obsługi urządzenia z wykorzystaniem GUI.

8. Przygotowanie i przekazanie zamawiającemu procedury zgłaszania problemów do

serwisu.

Wszystkie wymagania określone w dokumentach wskazanych powyżej stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne. Niespełnienie ww. wymagań minimalnych będzie skutkować odrzuceniem oferty jako niezgodnej z warunkami zamówienia na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp.

1. **Rozwiązania równoważne**

Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez zamawiającego. W takim przypadku, wykonawca załącza do oferty wykaz rozwiązań równoważnych wraz z jego opisem lub normami.

1. **Wymagania w zakresie zatrudniania przez wykonawcę lub podwykonawcę osób na podstawie stosunku pracy**

Nie dotyczy.

1. **Wymagania w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2 ustawy Pzp**

Nie dotyczy.

1. **Informacja o przedmiotowych środkach dowodowych**

Nie dotyczy.

1. **Termin wykonania zamówienia**

Max. 30 dni od dnia podpisania umowy – termin określony jako kryterium oceny ofert.

1. **Informacja o warunkach udziału w postępowaniu o udzielenie zamówienia i dokumenty składane na wezwanie**

Na podstawie art. 112 ustawy Pzp, zamawiający określa warunek/warunki udziału w postępowaniu **dotyczący/-e:**

|  |  |  |
| --- | --- | --- |
| **WARUNKI UDZIAŁU** **W POSTĘPOWANIU** | ***Warunki szczegółowe*** | **WYMAGANE DOKUMENTY**  |
| **zdolności do występowania w obrocie gospodarczym** | *-* | - |
| **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów** | *-* | - |
| **sytuacji ekonomicznej lub finansowej** | - | - |
| **zdolności technicznej lub zawodowej** | Potwierdzenie wykonania minimum dwóch dostaw polegających na dostawie sprzętu komputerowego bądź urządzeń peryferyjnych realizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane, oraz załączeniem dowodów określających czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze usługodawca nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert. | - wykaz dostaw wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy; |
| ***brak podstaw wykluczenia*** | - |  - oświadczenie wykonawcy o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z 16.02.2007 r. o ochronie konkurencji i konsumentów z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej. |

Zgodnie z art. 274 ust. 1 ustawy Pzp, zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, ww. podmiotowych środków dowodowych.

Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

Wykonawca składa podmiotowe środki dowodowe aktualne na dzień ich złożenia.

1. **Podstawy wykluczenia**

Zamawiający **wykluczy** z postępowania wykonawców, wobec których zachodzą podstawy wykluczenia, o których mowa w art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4 i 7 ustawy Pzp oraz 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.

1. **Wykaz podmiotowych środków dowodowych**
2. **DOKUMENTY SKŁADANE RAZEM Z OFERTĄ**
3. Oferta składana jest pod rygorem nieważności **w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**
4. Wykonawca dołącza do oferty oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu w zakresie wskazanym w rozdziale II podrozdziałach 7 i 8 SWZ. Oświadczenie to stanowi dowód potwierdzający brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu, na dzień składania ofert, tymczasowo zastępujący wymagane podmiotowe środki dowodowe, wskazane w rozdziale II podrozdziale 9 pkt 2 SWZ.
5. Oświadczenie składane jest pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym.
6. Oświadczenie składają **odrębnie**:
* wykonawca/każdy spośród wykonawców wspólnie ubiegających się o udzielenie zamówienia. W takim przypadku oświadczenie potwierdza brak podstaw wykluczenia wykonawcy oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu;
* podmiot trzeci, na którego potencjał powołuje się wykonawca celem potwierdzenia spełnienia warunków udziału w postępowaniu. W takim przypadku oświadczenie potwierdza brak podstaw wykluczenia podmiotu oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim podmiot udostępnia swoje zasoby wykonawcy;
* podwykonawcy, na których zasobach wykonawca nie polega przy wykazywaniu spełnienia warunków udziału w postępowaniu. W takim przypadku oświadczenie potwierdza brak podstaw wykluczenia podwykonawcy.
1. **Samooczyszczenie** – w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2, 5 i 6 lub art. 109 ust. 1 pkt 2–10 ustawy Pzp, wykonawca nie podlega wykluczeniu jeżeli udowodni zamawiającemu, że spełnił **łącznie** następujące przesłanki:

1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;

2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania lub zamawiającym;

3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:

a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,

b) zreorganizował personel,

c) wdrożył system sprawozdawczości i kontroli,

d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,

e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

**Zamawiający ocenia, czy podjęte przez wykonawcę czynności są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, a jeżeli uzna, że nie są wystarczające, wyklucza wykonawcę.**

1. Do oferty wykonawca załącza również:
2. **Pełnomocnictwo**
* Gdy umocowanie osoby składającej ofertę nie wynika z dokumentów rejestrowych, wykonawca, który składa ofertę za pośrednictwem pełnomocnika, powinien dołączyć do oferty dokument pełnomocnictwa obejmujący swym zakresem umocowanie do złożenia oferty lub do złożenia oferty i podpisania umowy.
* W przypadku wykonawców ubiegających się wspólnie o udzielenie zamówienia wykonawcy zobowiązani są do ustanowienia pełnomocnika. Dokument pełnomocnictwa, z treści którego będzie wynikało umocowanie do reprezentowania w postępowaniu o udzielenie zamówienia tych wykonawców należy załączyć do oferty.

Pełnomocnictwo powinno być załączone do oferty i powinno zawierać w szczególności wskazanie:

* postępowania o zamówienie publiczne, którego dotyczy,
* wszystkich wykonawców ubiegających się wspólnie o udzielenie zamówienia wymienionych z nazwy z określeniem adresu siedziby,
* ustanowionego pełnomocnika oraz zakresu jego umocowania.

**Wymagana forma:**

Pełnomocnictwo powinno zostać złożone w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym.

Dopuszcza się również przedłożenie elektronicznej kopii dokumentu poświadczonej za zgodność z oryginałem przez notariusza, tj. podpisanej kwalifikowanym podpisem elektronicznym osoby posiadającej uprawnienia notariusza.

1. **Oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia**
* Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, spośród których tylko jeden spełnia warunek dotyczący uprawnień, są zobowiązani dołączyć do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.
* Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z wykonawców, którzy wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane. W takiej sytuacji wykonawcy są zobowiązani dołączyć do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.

**Wymagana forma:**

Wykonawcy składają oświadczenia w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

1. **Zobowiązanie podmiotu trzeciego**
* Zobowiązanie podmiotu udostępniającego zasoby lub inny podmiotowy środek dowodowy potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
* zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
* sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
* czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

**Wymagana forma:**

Zobowiązanie musi być złożone w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

1. **Wykaz rozwiązań równoważnych –** wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez zamawiającego. W takim przypadku wykonawca załącza do oferty wykaz rozwiązań równoważnych z jego opisem lub normami.

**Wymagana forma:**

Wykaz musi być złożony w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

1. **Zastrzeżenie tajemnicy przedsiębiorstwa** – w sytuacji, gdy oferta lub inne dokumenty składane w toku postępowania będą zawierały tajemnicę przedsiębiorstwa, wykonawca, wraz z przekazaniem takich informacji, zastrzega, że nie mogą być one udostępniane, oraz wykazuje, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.

**Wymagana forma:**

Dokument musi być złożony w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

1. **Wymagania dotyczące wadium**

Nie dotyczy.

1. **Sposób przygotowania ofert**

**Zasady obowiązujące podczas przygotowywania ofert**

1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem w przypadku zamówień o wartości równej lub przekraczającej progi unijne, w przypadku zamówień o wartości niższej od progów unijnych Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym. W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu[[1]](#footnote-2) (**opcja rekomendowana** przez[**platformazakupowa.pl**](https://platformazakupowa.pl/strona/1-regulamin)).
2. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
3. Oferta powinna być:
	1. sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
	2. złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem [platformazakupowa.pl](https://platformazakupowa.pl/),
	3. podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione
4. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać “Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku”.
5. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.
6. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
7. Wykonawca, za pośrednictwem [platformazakupowa.pl](https://platformazakupowa.pl/) może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem:

<https://platformazakupowa.pl/strona/45-instrukcje>

1. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje podlegać będzie odrzuceniu.
2. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
3. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
4. Zgodnie z definicją dokumentu elektronicznego z art.3 ustęp 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
5. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
6. **Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z** “OBWIESZCZENIEM PREZESA RADY MINISTRÓW z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych”.
7. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) **ze szczególnym wskazaniem na .pdf**
8. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:
	1. .zip
	2. .7Z
9. Wśród formatów powszechnych a **NIE występujących** w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. **Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.**
10. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
11. Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.
12. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
13. Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
14. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
15. Zaleca się, aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza “Wyślij wiadomość do zamawiającego”, nie za pośrednictwem adresu email.
16. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
17. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
18. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
19. Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
20. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
21. Zamawiający zaleca aby **nie** wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.
22. **Opis sposobu obliczenia ceny**
	* + 1. Rozliczenia będą prowadzone w złotych polskich z dokładnością do dwóch miejsc po przecinku.

UWAGA! Jeden grosz jest najmniejszą jednostką monetarną w systemie pieniężnym RP i nie jest możliwe wyliczenie ceny końcowej, jeśli komponenty ceny (ceny jednostkowe) są określone za pomocą wielkości mniejszych niż 1 grosz.

Wartości kwotowe ujęte jako wielkości matematyczne znajdujące się na trzecim i kolejnym miejscu po przecinku, w odniesieniu do nieistniejącej wielkości w polskim systemie monetarnym powodują, że tak wyrażona cena usługi dla powszechnego obrotu gospodarczego jest niemożliwa do wypłacenia. Nie można kogoś realnie zobowiązać do zapłaty na jego rzecz kwoty niższej niż jeden grosz.

Tym samym, ceny jednostkowe, stanowiące podstawę do obliczenia ceny oferty, muszą być podane z dokładnością do dwóch miejsc po przecinku. **Jeżeli oferta będzie zawierała ceny jednostkowe wyrażone jako wielkości matematyczne znajdujące się na trzecim i kolejnym miejscu po przecinku, zostanie odrzucona na podstawie art. 226 ust. 1 pkt 4 i 5 ustawy Pzp.**

* + - 1. Wykonawca zobowiązany jest zastosować stawkę VAT zgodnie z obowiązującymi przepisami ustawy z 11 marca 2004 r. o podatku od towarów i usług.
			2. Cenę oferty/ceny jednostkowe należy obliczyć, uwzględniając całość wynagrodzenia wykonawcy za prawidłowe wykonanie umowy. Wykonawca jest zobowiązany skalkulować cenę na podstawie wszelkich wymogów związanych z realizacją zamówienia.
			3. Cena ofertowa/ceny jednostkowe muszą obejmować wszystkie koszty związane z realizacją przedmiotu zamówienia, wszystkie inne koszty oraz ewentualne upusty i rabaty a także wszystkie potencjalne ryzyka ekonomiczne, jakie mogą wystąpić przy realizacji przedmiotu umowy, wynikające z okoliczności, których nie można było przewidzieć w chwili zawierania umowy.
			4. Wykonawcy ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty.
			5. W formularzu oferty wypełnianym za pośrednictwem Platformy wykonawca poda wyłącznie cenę oferty, która uwzględnia całkowity koszt realizacji zamówienia w okresie obowiązywania umowy, obliczoną zgodnie z powyższymi dyspozycjami.
			6. Zgodnie z art. 225 ustawy Pzp jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z 11 marca 2004 r. o podatku od towarów i usług, dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W takiej sytuacji wykonawca ma obowiązek:

1) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;

2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;

3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;

4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

* + - 1. Informację w powyższym zakresie wykonawca składa w załączniku nr 1 do SWZ 🡪 Informacja o wykonawcy. Brak złożenia ww. informacji będzie postrzegany jako brak powstania obowiązku podatkowego u zamawiającego.
1. **Informacje o przebiegu postępowania**
2. **Sposób porozumiewania się zamawiającego z wykonawcami**
3. Osobą uprawnioną do kontaktu z Wykonawcami jest:

- Sylwia Perzanowska - bzp@powiat-wolominski.pl

2) Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem [platformazakupowa.pl](https://platformazakupowa.pl/) pod adresem: <https://platformazakupowa.pl/pn/powiat_wolominski>

3) W celu skrócenia czasu udzielenia odpowiedzi na pytania preferuje się, aby komunikacja między zamawiającym a wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane są w formie elektronicznej za pośrednictwem [platformazakupowa.pl](http://platformazakupowa.pl) i formularza „Wyślij wiadomość do zamawiającego”.

Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem [platformazakupowa.pl](http://platformazakupowa.pl) poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego” po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

1. Zamawiający będzie przekazywał wykonawcom informacje w formie elektronicznej za pośrednictwem [platformazakupowa.pl](http://platformazakupowa.pl). Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji “Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem [platformazakupowa.pl](http://platformazakupowa.pl) do konkretnego wykonawcy.
2. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
3. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 31 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na [platformazakupowa.pl](https://platformazakupowa.pl/), tj.:
	1. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
	2. komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
	3. zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
	4. włączona obsługa JavaScript,
	5. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
	6. Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
	7. Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
4. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
	1. akceptuje warunki korzystania z [platformazakupowa.pl](https://platformazakupowa.pl/) określone w Regulaminie zamieszczonym na stronie internetowej [pod linkiem](https://platformazakupowa.pl/strona/1-regulamin) w zakładce „Regulamin" oraz uznaje go za wiążący,
	2. zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej [pod linkiem](https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view).
5. **Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z** [**platformazakupowa.pl**](http://platformazakupowa.pl), w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego”).
Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 Ustawy Prawo Zamówień Publicznych.
6. Zamawiający informuje, że instrukcje korzystania z [platformazakupowa.pl](http://platformazakupowa.pl) dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu [platformazakupowa.pl](http://platformazakupowa.pl) znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>
7. **Sposób oraz termin składania ofert. Termin otwarcia ofert**
	1. Ofertę należy złożyć w terminie do dnia 11.07.2023 r. do godz. 10:00
	2. Sposób składania ofert:
* za pośrednictwem Platformy: <https://platformazakupowa.pl/pn/powiat_wolominski>
	1. Otwarcie ofert nastąpi w dniu 11.07.2023 r. o godz. 10:10 poprzez odszyfrowanie wczytanych na Platformie ofert.
	2. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
	3. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:

1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej bądź miejscach zamieszkania wykonawców, których oferty zostały otwarte;

*2)* cenach lub kosztach zawartych w ofertach.

1. **Termin związania ofertą**

Wykonawca pozostaje związany ofertą **do dnia 09.08.2023 r.**

Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

1. **Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert**

Przy wyborze najkorzystniejszej oferty zamawiający będzie kierował się następującymi kryteriami i odpowiadającymi im znaczeniami oraz w następujący sposób będzie oceniał spełnienie kryteriów:

|  |  |  |
| --- | --- | --- |
| Lp. | Opis kryterium oceny | Znaczenie (%) |
| 1. |  Cena (koszt) | 60% |
| 2. | Termin dostawy i wdrożenia | 40% |
|  | **Razem** | **100%** |

Oferty będą oceniane przez komisję przetargową metodą punktową w skali 100-punktowej.

**I kryterium: Cena za wykonanie zadania – 60 punktów**

Cenę należy ustalić, jako cenę brutto w oparciu o przedstawiony formularz ofertowy.

Zamawiający, Ofercie o najniżej cenie przyzna 60 punktów, a każdej następnej zostanie przyporządkowana liczba punktów proporcjonalnie mniejsza, według wzoru:

 Najniższa cena oferty

PC = --------------------------------------- x 100 x 60%

 Cena badanej oferty

**II kryterium: Termin dostawy i wdrożenia – 40 punktów**

W ramach kryterium ,,Termin dostawy i wdrożenia” porównana będzie ilość dni potrzebnych dostawcy na dostawę urządzeń do siedziby zamawiającego oraz czas na konfigurację i wdrożenie.

Oferta z najkrótszym terminem uzyska maksymalna liczbę punktów (40 pkt.)

Punktacja za termin wykonania zamówienia odbędzie się wg wzoru:

30 dni – 0 punktów

21 dni – 20 punktów

14 dni – 40 punktów

**Za najkorzystniejszą zostanie uznana oferta Wykonawcy, który spełni wszystkie postawione w niniejszej SIWZ warunki oraz uzyska łącznie największą liczbę punktów (P) stanowiących sumę punktów przyznanych w ramach każdego z podanych kryteriów, wyliczoną zgodnie z poniższym wzorem:**

**P = PC + PG**

**gdzie:**

**PC - liczba punktów przyznana ofercie ocenianej w kryterium „Cena”**

**PG - liczba punktów przyznana ofercie ocenianej w kryterium „Termin dostawy i wdrożenia”.**

1. **Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do umowy w sprawie zamówienia publicznego**

Projektowane postanowienia umowy stanowią załącznik nr 3 do SWZ.

**Złożenie oferty jest jednoznaczne z akceptacją przez wykonawcę projektowanych postanowień umowy.**

1. **Zabezpieczenie należytego wykonania umowy**

Nie dotyczy.

1. **Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego**
2. Zamawiający poinformuje wykonawcę, któremu zostanie udzielone zamówienie, o miejscu i terminie zawarcia umowy.
3. Wykonawca przed zawarciem umowy:
	* poda wszelkie informacje niezbędne do wypełnienia treści umowy na wezwanie zamawiającego,
	* wniesie zabezpieczenie należytego wykonania umowy.

Jeżeli zostanie wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zamawiający będzie żądał przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych wykonawców, w której m.in. zostanie określony pełnomocnik uprawniony do kontaktów z zamawiającym oraz do wystawiania dokumentów związanych z płatnościami, przy czym termin, na jaki została zawarta umowa, nie może być krótszy niż termin realizacji zamówienia.

Niedopełnienie powyższych formalności przez wybranego wykonawcę będzie potraktowane przez zamawiającego jako niemożność zawarcia umowy w sprawie zamówienia publicznego z przyczyn leżących po stronie wykonawcy i zgodnie z art. 98 ust. 6 pkt 3 ustawy Pzp, będzie skutkowało zatrzymaniem przez zamawiającego wadium wraz z odsetkami.

**Ewentualne zmiany umowy:**

Nie dotyczy.

 ……………………………………………………..

Podpis kierownika zamawiającego

lub osoby upoważnionej

Załącznik nr 1

BZP.272.93.2023

**OFERTA**

Zamawiający:

**Powiat Wołomiński**

**ul. Prądzyńskiego 3**

**05-200 Wołomin**

Nawiązując do ogłoszenia o zamówieniu w postępowaniu prowadzonym w trybie podstawowym na: **Dostawa zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem ramach zadania „Zakup urządzeń sieciowych klasy UTM, urządzeń komputerowych, oprogramowania biurowego, macierzy oraz dysków i pamięci serwerowych na potrzeby Starostwa Powiatowego w Wołominie”**

My niżej podpisani:

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

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

działający w imieniu i na rzecz…................................................................................................................................................

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

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

 (należy podać pełną nazwę Wykonawcy i adres)

tel.: …………….……………………. e-mail: ………………………………………

* 1. **Oferujemy realizację powyższego przedmiotu zamówienia, zgodnie z zapisami**

SWZ za kwotę: ………………………… PLN brutto

**słownie**…...................................................................................................................................

w tym obowiązujący podatek VAT.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| l.p. | Nazwa | Ilośćszt. | Cena jednostkowa netto | Cena jednostkowa brutto | Wartośćnetto | Wartość brutto |
| 1. | UTM TYP1 | 2 |  |  |  |  |
| 2. | UTM TYP2 | 3 |  |  |  |  |
| 3. | UTM TYP3 | 1 |  |  |  |  |
| 4. | UTM TYP4 | 1 |  |  |  |  |
| 5. | Wdrożenie | 1 |  |  |  |  |

1. Oświadczamy, że termin dostawy i wdrożenia wynosi ……………..\* dni (14,21,30 dni)

\*w przypadku nie wskazania wartości Zamawiający uzna, iż termin wynosi 30 dni.

1. Oświadczamy, że zapoznaliśmy się ze specyfikacją, nie wnosimy do jej treści zastrzeżeń i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
2. Oświadczamy, że zapoznaliśmy się z postanowieniami umowy, która stanowi załącznik do specyfikacji. Zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na określonych w niej warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.
3. Uważamy się za związanych niniejszą ofertą na czas wskazany w specyfikacji.
4. Zamówienie zrealizujemy przy udziale podwykonawców, którzy będą realizować wymienione części zamówienia:

a)....................................................................................

b)....................................................................................

1. Wykonawca oświadcza, że wyraża zgodę\*/nie wyraża zgody\* na bezpośrednią zapłatę podwykonawcy z wynagrodzenia należnego wykonawcy.

(\* niepotrzebne skreślić)

1. Akceptujemy warunki płatności 30 dni od daty dostarczenia prawidłowo wystawionej faktury do siedziby Zamawiającego.
2. Oświadczamy, iż tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, które nie mogą być udostępnione innym uczestnikom postępowania stanowią informacje zawarte w ofercie na stronach nr/w pliku:
3. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*
4. Oświadczamy, że jesteśmy:

mikroprzedsiębiorstwem\*

małym przedsiębiorstwem\*

średnim przedsiębiorstwem\*

prowadzimy jednoosobową działalność gospodarczą\*

osobą fizyczną nieprowadzącą działalności gospodarczej\*

inny rodzaj……………………………………..……………\*.

\*niepotrzebne skreślić

1. Osobą upoważnioną do kontaktów z Zamawiającym w sprawach dotyczących realizacji umowy jest: …………………………………………………………………………………………

tel.: ………………………………..…. e-mail: …………………………..………………………

1. Załącznikami do niniejszej oferty, stanowiącymi jej integralną część są:
2. .............................................................................................
3. .............................................................................................

.................., dn. ......................................

.....................................................

(podpis i pieczątka wykonawcy)

Załącznik Nr 2

BZP.272.93.2023

**Zamawiający:**

**Powiat Wołomiński**

**ul. Prądzyńskiego 3**

**05-200 Wołomin**

**Wykonawca:**

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

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

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

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

**Oświadczenie wykonawcy**

**składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.**

 **Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

**DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU I NIE PODLEGANIA WYKLUCZENIU**

Na potrzeby postępowania o udzielenie zamówienia publicznego
pn. **Dostawa zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem ramach zadania „Zakup urządzeń sieciowych klasy UTM, urządzeń komputerowych, oprogramowania biurowego, macierzy oraz dysków i pamięci serwerowych na potrzeby Starostwa Powiatowego w Wołominie”**, prowadzonego przez Powiat Wołomiński*,* oświadczam, co następuje:

* + Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w ogłoszeniu o zamówieniu i Specyfikacji Warunków Zamówienia*.*
	+ Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie
	art. 108 i art. 109 ust. 1 pkt 4 i 7 ustawy Pzp;
	+ Oświadczam, że 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.

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

 …………………………………………

*(podpis)*

Załącznik nr 3

BZP.272.93.2023

**§ 1**

Zamawiający powierza, a Wykonawca przyjmuje do realizacji „Dostawa zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem na potrzeby Starostwa Powiatowego w Wołominie”

**§ 2**

1. Zakres przedmiotu umowy obejmuje dostawę zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem na potrzeby Starostwa Powiatowego w Wołominie, wg opisu przedmiotu zamówienia stanowiącego załącznik nr 1 do niniejszej umowy.
2. Urządzenia dostarczone w ramach niniejszej umowy to sprzęt nowy, wyprodukowany nie wcześniej niż w roku 2022 (wymóg ten dotyczy także poszczególnych podzespołów).
3. Wykonawca zobowiązuje się do:
4. sprzedaży i dostarczenia Zamawiającemu: urządzeń zgodnie z niniejszą umową, opisem przedmiotu zamówienia, certyfikatów CE (lub świadectw zgodności), instrukcji obsługi i konserwacji w języku polskim, nośników ze sterownikami i oprogramowaniem,
5. serwisu gwarancyjnego świadczonego u Zamawiającego.
6. Wykonawca dostarczy urządzenia, o których mowa w ust. 1 do siedziby Zamawiającego, transportem własnym, na własny koszt (tj. w ramach wynagrodzenia umownego).

**§ 3**

1. Termin zakończenia wykonania przedmiotu umowy: ……… dni od daty podpisania umowy.
2. Miejsce dostawy: siedziba Zamawiającego ul. Prądzyńskiego 3, 05-200 Wołomin
(w godzinach urzędowania Starostwa Powiatowego w Wołominie).

**§ 4**

1. Za wykonanie przedmiotu umowy Wykonawca otrzyma wynagrodzenie w wysokości netto: ……………………………… + podatek VAT, co stanowi wynagrodzenie brutto: …………………………………………… zł. Wynagrodzenie zostało ustalone na podstawie oferty Wykonawcy z dnia ………… stanowiącej załącznik nr 2 do niniejszej umowy.
2. Wynagrodzenie obejmuje całość kosztów związanych z realizacją zadania określonego w § 2 (koszt sprzedaży, dostawy, konfiguracji oraz serwisu gwarancyjnego). Cena jest wiążąca i niezmienna do końca realizacji przedmiotu umowy.
3. Zapłata za wykonanie przedmiotu umowy nastąpi po dokonaniu dostawy i odbioru przedmiotu umowy, w terminie ……….. dni od daty dostarczenia prawidłowej faktury
do siedziby Zamawiającego, przelewem na konto Wykonawcy.
4. Za dzień zapłaty strony uznają dzień złożenia polecenia przelewu z rachunku Zamawiającego.
5. Zamawiający oświadcza, że będzie dokonywało płatności za przedmiot umowy
z zastosowaniem mechanizmu podzielonej płatności.
6. Wykonawca oświadcza, że wskazany w fakturze rachunek bankowy (nr rachunku bankowego…………) jest rachunkiem rozliczeniowym służącym wyłącznie do celów rozliczeń z tytułu prowadzonej przez niego działalności gospodarczej.
7. Wykonawca nie może dokonać cesji żadnych praw i roszczeń oraz przeniesienia obowiązków wynikających z umowy na rzecz osoby trzeciej bez uprzedniej pisemnej zgody Zamawiającego.

**§ 5**

1. Ustala się jednorazowy odbiór końcowy przedmiotu umowy, który nastąpi
po dostawie wszystkich urządzeń, konfiguracji, wdrożeniu, przeprowadzeniu próby ich działania, wydaniu Zamawiającemu kart gwarancyjnych, certyfikatów, instrukcji obsługi i konserwacji.
2. W dniu odbioru Wykonawca przekaże Zamawiającemu podpisany protokół zdawczo-odbiorczy i dokumenty wymienione w ust. 1. Niedostarczenie jakiegokolwiek dokumentu,
o którym mowa w niniejszym ustępie jest uważane jako niezakończenie wykonania umowy
i powoduje niepodpisanie protokołu zdawczo-odbiorczego.
3. Bezusterkowy odbiór przedmiotu umowy potwierdzi podpisany przez obie strony protokół zdawczo-odbiorczy przygotowany wcześniej przez Wykonawcę. W przypadku stwierdzenia przy odbiorze wad lub usterek przedmiotu umowy Zamawiający wyznaczy Wykonawcy stosowny termin na ich usunięcie, określając kolejną datę odbioru. W przypadku nie przedstawienia protokołu zdawczo-odbiorczego przez Wykonawcę Zamawiający jest uprawniony, lecz nie zobowiązany, do samodzielnego sporządzenia protokołu.

**§ 6**

1. Wykonawca udziela gwarancji jakości na dostarczony sprzęt na okres gwarancji ……… miesięcy. W ramach gwarancji Wykonawca zapewnia obsługę transportu wadliwego sprzętu od Zamawiającego do miejsca naprawy i z powrotem.
2. Bieg terminu gwarancji rozpoczyna się w dniu zakończenia bezusterkowego odbioru.
3. Niezależnie od gwarancji Zamawiający zastrzega sobie prawo do wykonania uprawnień z tytułu rękojmi.

**§ 7**

1. Wszelkie wady i usterki związane z funkcjonowaniem dostarczonego sprzętu zgłaszane będą Wykonawcy telefonicznie, e-mailem lub faksem, w dni robocze w godz.: poniedziałek 8:00 – 17:00, wtorek – czwartek 08:00 – 16:00, piątek 8:00 – 15.00. Wykonawca wskazuje następujące dane kontaktowe:
2. Telefon: ……………………………
3. E-mail: ……………………………..
4. Fax: ………………………………….
5. Wykonawca zapewni nieodpłatne przeprowadzenie skutecznej naprawy wszystkich urządzeń nie później niż w terminie 14 dni od dnia zgłoszenia usterki. Za zgłoszenie usterki strony odpowiednio uznają chwile telefonicznego zgłoszenia, wysłania faxu lub maila.

**§ 8**

1. Wykonawca zobowiązany jest do zapłacenia Zamawiającemu następujących kar umownych:
2. odstąpienia od umowy w całości lub w części z przyczyn zależnych od Wykonawcy –
w wysokości 15% wynagrodzenia brutto wskazanego w §4 ust. 1 umowy;
3. zwłoki w wykonaniu przedmiotu umowy – w wysokości 1% wynagrodzenia brutto wskazanego w § 4 ust. 1 umowy, za każdy rozpoczęty dzień zwłoki wykraczający poza termin zakończenia wykonania przedmiotu umowy, o którym mowa w § 3 ust. 1;
4. zwłoki w usunięciu wad przedmiotu umowy stwierdzonych przy odbiorze, ujawnionych w okresie gwarancji lub rękojmi – w wysokości 1% wynagrodzenia brutto wskazanego w § 4 ust. 1 umowy za każdy rozpoczęty dzień zwłoki, liczony od upływu terminu wyznaczonego przez Zamawiającego na usunięcie wad i usterek.
5. Zamawiający zapłaci Wykonawcy karę umowną za odstąpienie od umowy z przyczyn zawinionych przez Zamawiającego w wysokości 15% wynagrodzenia brutto wskazanego
 w § 4 ust. 1 umowy.
6. W przypadku, gdy wysokość zastrzeżonych kar nie pokryje rzeczywiście poniesionej szkody, Zamawiający ma prawo dochodzić odszkodowania uzupełniającego na ogólnych zasadach kodeksu cywilnego.
7. Wykonawca wyraża zgodę na potrącenie naliczonych kar umownych z przysługującego mu wynagrodzenia umownego.

**§ 9**

* 1. Zamawiający może odstąpić od umowy w całości lub części w następujących przypadkach:
1. dostarczenia wadliwego lub niekompletnego przedmiotu umowy;
2. gdy przedmiot umowy odbiega od opisu zamówienia w całości lub w jakiejkolwiek części;
3. zaistnienia okoliczności powodującej, iż wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy,
4. wydania sądowego nakazu zajęcia majątku Wykonawcy,
5. wykonawca przekroczył o 3 dni termin realizacji zamówienia, o którym mowa
w § 3 ust. 1,
6. powierzenia wykonania umowy w całości lub części podwykonawcom.
	1. Wykonawcy przysługuje prawo odstąpienia od umowy, jeżeli Zamawiający bez podania przyczyny odmawia odbioru prawidłowego i kompletnego przedmiotu umowy,
	2. Oświadczenie o odstąpieniu od umowy powinno zostać złożone w terminie 30 dni
	od dnia, w którym strona dowiedziała się o przyczynie odstąpienia.
	3. Odstąpienie od umowy przez Zamawiającego na podstawie którejkolwiek z przyczyn wskazanych w ust. 1, z wyjątkiem przypadku, gdy realizacja umowy nie leży w interesie publicznym, uznawane będzie za odstąpienie z przyczyn zależnych od Wykonawcy.
	4. Postanowienia niniejszego paragrafu nie wykluczają uprawnień Zamawiającego
	do odstąpienia od umowy, wynikających z obowiązujących w tym zakresie przepisów prawa oraz naliczania w takich przypadkach kar umownych, jeżeli przyczyny odstąpienia leżeć będą po stronie Wykonawcy.

**§ 10**

* 1. Wykonawca oświadcza, że znany jest mu fakt, iż treść niniejszej umowy,
	a w szczególności dane go identyfikujące przedmiot umowy i wysokość wynagrodzenia, stanowią informację publiczną w rozumieniu art. 1 ust. 1 ustawy z dnia 6 września 2001r.
	o dostępie do informacji publicznej, która podlega udostępnieniu w trybie przedmiotowej ustawy.
	2. Wykonanie niniejszej umowy nie wiąże się z przetwarzaniem danych w rozumieniu Rozporządzenia 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/W (Dz. Urz. U. E. z dnia 4.05.2016 r., L 119) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018r poz. 1000) dla których Administratorem jest Starosta Wołomiński, a co za tym idzie nie wiąże się z dostępem do zasobów informatycznych Starostwa Powiatowego w Wołominie, z zastrzeżeniem zawartym w zdaniu drugim. Starostwo Powiatowe w Wołominie oświadcza, iż realizuje obowiązki Administratora danych osobowych, określone w przepisach RODO, w zakresie danych osobowych Wykonawca,
	w sytuacji, w której jest on osobą fizyczną (w tym osobą fizyczną prowadzącą działalność gospodarczą) a także danych osobowych osób, które Wykonawca wskazał ze swojej strony
	do realizacji niniejszej umowy.

**§11**

Strony wskazują osoby uprawnione do wzajemnych kontaktów, w tym podpisania protokołu zdawczo-odbiorczego (każda samodzielnie):

1. ze strony Zamawiającego:
2. ………………
3. ………………
4. ze strony Wykonawcy:
5. ………………
6. ………………

**§12**

* + 1. Ewentualne spory rozstrzygać będzie sąd właściwy dla siedziby Zamawiającego.
		2. Wszelkie zmiany i uzupełnienia treści niniejszej umowy, wymagają formy pisemnej
		w postaci aneksów do umowy, pod rygorem nieważności.
		3. W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie właściwe przepisy prawa.
		4. Umowa została sporządzona w 3 jednobrzmiących egzemplarzach, z czego 2 egz. przeznaczone są dla Zamawiającego, 1 egz. dla Wykonawcy.

Załącznik Nr 4

…………………………………………………………

…………………………………………………………

 nazwa oferenta

…………………………………………………………

…………………………………………………………

 adres

 BZP.272.93.2023

**WYKAZ DOSTAW**

Nazwa wykonawcy...............................................................................................................

Adres wykonawcy...............................................................................................................

Miejscowość ................................................ Data .........................

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Odbiorca \* | Wartość. | Przedmiot wyk. dostaw | Data dostawy |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

\* Do wykazu należy dołączyć dokumenty potwierdzające, że w/w dostawy zostały wykonane należycie.

 ...........................................................................

(podpis osoby upoważnionej do składania oświadczeń woli w imieniu Wykonawcy)

BZP.272.93.2023 Załącznik nr 5

**OŚWIADCZENIE**

**o przynależności Wykonawcy do grupy kapitałowej**

....................................................................................................................................................

(Nazwa i adres Wykonawcy)

....................................................................................................................................................

składając ofertę w trybie podstawowym na:

Dostawa zintegrowanych systemów bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń, gwarancją i wdrożeniem ramach zadania „Zakup urządzeń sieciowych klasy UTM, urządzeń komputerowych, oprogramowania biurowego, macierzy oraz dysków i pamięci serwerowych na potrzeby Starostwa Powiatowego w Wołominie”

oświadczam(y), że:

1. Nie należymy do grupy kapitałowej**\***

2. Należymy do grupy kapitałowej **\***

Miejscowość .................................................. dnia ....................................... roku

 .......................................................................

(podpis osoby uprawnionej

do składania oświadczeń woli w imieniu wykonawcy)

\* Niepotrzebne skreślić

1. Rozporządzenie Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych. [↑](#footnote-ref-2)