UNIWERSYTET SZCZECIŃSKI

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

A-ZP.381.23.2024.WB

Dotyczy postępowania prowadzonego w trybie podstawowym pn.:

Modernizacja systemu zabezpieczającego dostęp do infrastruktury sieciowej oraz jej monitorowania w zakresie bezpieczeństwa oraz zakup usługi rocznego serwisu i subskrypcji bezpieczeństwa dla posiadanych przez Uniwersytet Szczeciński urządzeń firmy Fortinet

Spis treści

ROZDZIAŁ 1
INSTRUKCJA DLA WYKONAWCÓW

DZIAŁ I Dane Zamawiającego

UNIWERSYTET SZCZECIŃSKI
al. Papieża Jana Pawła II 22a
70-453 SZCZECIN
NIP: 851-020-80-05

- adres strony internetowej: https://usz.edu.pl
- adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia: https://platformazakupowa.pl/pn/usz
- adres poczty elektronicznej: przetargi@usz.edu.pl
- numery telefonów:
  - +48 91 444 11 72 (sekretariat Rektora)
  - +48 91 444 11 05 (sekretariat Kanclerza)
  - +48 91 444 11 51 (Dział Zamówień Publicznych)

Adres do korespondencji:
UNIWERSYTET SZCZECIŃSKI
DZIAŁ ZAMÓWIEŃ PUBLICZNYCH
al. Papieża Jana Pawła II 31 (pok. 205)
70-453 SZCZECIN
Adres e-mail: przetargi@usz.edu.pl

DZIAŁ II Tryb udzielenia zamówienia

1. Postępowanie prowadzone jest na podstawie przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r., poz. 1605 ze zm.) – dalej PZP.
2. Postępowanie prowadzone jest w trybie podstawowym (art. 275 – 296 PZP).
3. Zamawiający **nie przewiduje** możliwości prowadzenia negocjacji.
4. Do udzielenia przedmiotowego zamówienia stosuje się przepisy dotyczące zamówień klasycznych na usługi o wartości mniejszej niż progi unijne[1].
5. Zamawiający informuje, iż w odniesieniu do przedmiotowego zamówienia **nie prowadzono wstępnych konsultacji rynkowych**.

DZIAŁ III Opis przedmiotu zamówienia

1. **Przedmiotem zamówienia jest modernizacja systemu zabezpieczającego dostęp do infrastruktury sieciowej oraz jej monitorowania w zakresie bezpieczeństwa oraz zakup usługi rocznego serwisu i subskrypcji bezpieczeństwa dla posiadanych przez Uniwersytet Szczeciński urządzeń firmy Fortinet.**

[1] Przez progi unijne należy rozumieć kwoty wartości zamówień lub konkursów określone w art. 4 i art. 13 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE (Dz. Urz. UE L 94 z 28.03.2014, str. 65, z późn. zm.), zwanej dalej „dyrektywą 2014/24/UE"

2. Główne miejsce lub lokalizacja realizacji usług: obiekty Zamawiającego na terenie Miasta Szczecin (główny kod NUTS PL424 Miasto Szczecin).
3. Nazwy i kody Wspólnego Słownika Zamówień (CPV):

	Numer	Nazwa
Główny kod CPV	**72611000-6**	**Usługi w zakresie wsparcia technicznego**

	Numer	Nazwa
Dodatkowy kod CPV	**72000000-5**	**Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia**

4. Zamawiający informuje o niedokonaniu podziału zamówienia na części. Każdy Wykonawca przedłoży tylko jedną ofertę, sam lub jako reprezentant spółki czy konsorcjum. Złożenie więcej niż jednej oferty przez jednego Wykonawcę spowoduje odrzucenie wszystkich jego ofert.
5. Powody niedokonania podziału zamówienia na części:
   1) brak podziału na części nie wpływa na konkurencję;
   2) brak podziału na części związany jest z koniecznością zapewnienia spójnej usługi wsparcia jednolitego systemu bezpieczeństwa danych.
6. Zamawiający nie dopuszcza możliwości złożenia oferty wariantowej.
7. Zamawiający nie wymaga złożenia oferty w postaci katalogu elektronicznego.
8. Zamawiający **nie zastrzega** by o udzielenie zamówienia mogli ubiegać się wyłącznie Wykonawcy mający status zakładu pracy chronionej, spółdzielnie socjalne oraz inni Wykonawcy, których głównym celem lub głównym celem działalności ich wyodrębnionych organizacyjnie jednostek, które będą realizowały zamówienie, jest społeczna i zawodowa integracja osób społecznie marginalizowanych.
9. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7 PZP.
10. Nie dopuszcza się składania ofert równoważnych.
11. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.
12. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
13. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań, o których mowa w art. 60 i art. 121 PZP.
14. Szczegółowy opis przedmiotu zamówienia, zawarty jest w Rozdziale 2 niniejszej SWZ.

DZIAŁ IV Informacja o przedmiotowych środkach dowodowych

1. W celu wykazania, że oferowane usługi spełniają określone przez zamawiającego w Rozdziale 2 niniejszej SWZ wymagania, cechy lub kryteria, Zamawiający żąda złożenia wraz z ofertą następujących przedmiotowych środków dowodowych:
   1) w celu potwierdzenia zgodności oferowanych usług z wymaganiami zamawiającego określonymi w SWZ, które nie podlegają ocenie w ramach kryteriów oceny ofert:
      a. **Szczegółowy opis oferowanego rozwiązania potwierdzający spełnienie wymagań określonych w SWZ wraz z wymienionymi dokumentami w opisie.**
      b. **W przypadku istnienia wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca zobowiązany jest załączyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania**

międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2023 r. poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

c. **W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej centrum serwisowego, Wykonawca winien przedłożyć dokument wystawiony przez producenta, który wskazuje podmiot uprawniony do realizowania usługi gwarancyjnej na terenie Rzeczpospolitej Polskiej.**

d. **oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych (vide: Rozdział 2 SWZ)**.

2. Jeżeli wykonawca nie złożył przedmiotowych środków dowodowych, o których mowa w pkt 1 ppkt 1, lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
3. Przepisu pkt. 2 nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania**.**

DZIAŁ V Termin wykonania zamówienia

1. Wymagany termin realizacji niniejszego zamówienia**: do 30 dni kalendarzowych od dnia zawarcia umowy (modernizacja systemu zabezpieczającego dostęp do infrastruktury sieciowej oraz jej monitorowania w zakresie bezpieczeństwa oraz dostarczenie i zainstalowanie licencji zapewniających roczny serwis i subskrypcję bezpieczeństwa - odnowienie licencji oprogramowania).**
2. **Wykonawca gwarantuje Zamawiającemu odnowienie licencji, o których mowa w pkt 1 na okres 12 miesięcy od dnia wygaśnięcia aktualnie obowiązującej umowy.**

DZIAŁ VI Podstawy wykluczenia

1. Z postępowania o udzielenie zamówienia Zamawiający wykluczy wykonawcę:

PRZESŁANKI WYKLUCZENIA, O KTÓRYCH MOWA W ART. 108 PZP

1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
   a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego (Dz. U. z 2022 r. poz. 1138) – dalej KK,
   b) handlu ludźmi, o którym mowa w art. 189a KK,
   c) o którym mowa w art. 228–230a, art. 250a KK, w art. 46–48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2022 r. poz. 1599) lub w art. 54 ust. 1–4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. z 2022 r. poz. 2555),
   d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a KK, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 KK,
   e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 KK, lub mające na celu popełnienie tego przestępstwa,
   f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy

cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2021 r. poz. 1745),

g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 KK, przestępstwo oszustwa, o którym mowa w art. 286 KK, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d KK, lub przestępstwo skarbowe,

h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2021 r. poz. 1745),

lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;

3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

5) jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2023 r. poz. 1689), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

6) jeżeli, w przypadkach, gdy Wykonawca lub podmiot, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2023 r. poz. 1689), doradzał lub w inny sposób był zaangażowany w przygotowanie postępowania o udzielenie tego zamówienia i doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2023 r. poz. 1689), chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia;

PRZESŁANKI WYKLUCZENIA, O KTÓRYCH MOWA W ART. 109 PZP
(art. 109 ust. 1 pkt 4, 5, 7, 8, 9 oraz 10 PZP)

7) w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;

8) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co Zamawiający jest w stanie wykazać za pomocą stosownych dowodów;

9) który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy

koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;

10) który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził Zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez Zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;
11) który bezprawnie wpływał lub próbował wpływać na czynności Zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
12) który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez Zamawiającego w postępowaniu o udzielenie zamówienia.

PRZESŁANKI WYKLUCZENIA, O KTÓRYCH MOWA W ART. 7 USTAWY Z DNIA 13 KWIETNIA 2022 R. O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO

13) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz. 185);
14) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2023 r. poz. 185);
15) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2023 r. poz. 120) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2023 r. poz.185),

2. Wykluczenie Wykonawcy następuje:
   1) w przypadkach, o których mowa w pkt. 1 ppkt 1 lit. a–g i ppkt 2 - na okres 5 lat od dnia uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia;
   2) w przypadkach, o których mowa w:
      pkt. 1 ppkt 1 lit. h i ppkt 2, gdy osoba, o której mowa w tych przepisach, została skazana za przestępstwo wymienione w pkt. 1 ppkt 1 lit. h,
      w przypadku, o którym mowa w pkt. 1 ppkt 6 - w postępowaniu o udzielenie zamówienia, w którym zaistniało zdarzenie będące podstawą wykluczenia,

w przypadku, o którym mowa w pkt. 1 ppkt 7 - na okres 3 lat od zaistnienia zdarzenia będącego podstawą wykluczenia,

3) w przypadkach, o których mowa w pkt. 13-15 - na okres trwania okoliczności określonych w tych punktach.

3. Osoba lub podmiot podlegające wykluczeniu w przypadkach, o których mowa w pkt. 13-15, które w okresie tego wykluczenia ubiegają się o udzielenie zamówienia publicznego lub dopuszczenie do udziału w konkursie lub biorą udział w postępowaniu o udzielenie zamówienia publicznego lub w konkursie, podlegają karze pieniężnej. Karę pieniężną, o której mowa w zdaniu poprzednim, nakłada Prezes Urzędu Zamówień Publicznych, w drodze decyzji, w wysokości do 20 milionów zł.
4. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w pkt 1 ppkt pkt 1, 2, 5 i 7-12 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.
5. Zamawiający ocenia, czy podjęte przez Wykonawcę czynności, o których mowa w pkt. 4, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez Wykonawcę czynności, o których mowa w pkt. 4, nie są wystarczające do wykazania jego rzetelności, Zamawiający wyklucza wykonawcę.
6. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.

DZIAŁ VII Informacja o warunkach udziału w postępowaniu o udzielenie zamówienia

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu, na zasadach określonych w Rozdziale 1, Dział VI SWZ, oraz spełniają poniżej określone przez Zamawiającego warunki udziału w postępowaniu.
2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące:
   1) **zdolności do występowania w obrocie gospodarczym:**
      Zamawiający nie stawia warunku w powyższym zakresie.
   2) **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:**
      Zamawiający nie stawia warunku w powyższym zakresie.
   3) **sytuacji ekonomicznej lub finansowej:**
      Zamawiający nie stawia warunku w powyższym zakresie.
   4) **zdolności technicznej lub zawodowej:**
      a) Zamawiający uzna, że Wykonawca posiada wymagane zdolności techniczne lub zawodowe zapewniające należyte wykonanie zamówienia, jeżeli Wykonawca wykaże, że w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest

krótszy – ***w tym okresie, wykonał co najmniej dwa zamówień polegających na wdrożeniu sprzętowo – programowych systemów bezpieczeństwa wewnętrznych sieci komputerowych, zawierających co najmniej 500 stanowisk***

b) Zamawiający wymaga, aby Wykonawcy składający ofertę wykazali, że dysponują lub będą dysponować podczas realizacji zamówienia zespołem osób składającym się **co najmniej** z **dwóch osób posiadających po dwa imienne certyfikaty autoryzacyjne producenta (zgodne z aktualną i przyjętą przez producenta polityką certyfikacyjną) poświadczające kompetencje inżynierów dokonujących rejestracji oferowanych serwisów..**

UWAGA:

- **Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które usługi wykonają poszczególni wykonawcy; wzór oświadczenia zawarty jest w formularzu oferty – zał. nr 1 do SWZ;**
- **W odniesieniu do warunku dotyczącego doświadczenia wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane.**

DZIAŁ VIII Wykaz podmiotowych środków dowodowych

1. **Dokumenty wymagane na etapie składania ofert:**
   1) Do oferty Wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert oświadczenie wstępne o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu według wzoru stanowiącego **Załącznik nr 2 do SWZ**.
   Oświadczenie wstępne, **składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, lub podpisem zaufanym lub podpisem osobistym**. Oświadczenie, stanowi dowód potwierdzający brak podstaw wykluczenia, spełnianie warunków udziału w postępowaniu, tymczasowo zastępujący wymagane przez Zamawiającego podmiotowe środki dowodowe. W przypadku składania oferty wspólnej ww. oświadczenie składa każdy z Wykonawców składających ofertę wspólną. W przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, wraz z ww. oświadczeniem, Wykonawca składa także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.
   2) Wykonawca, który powołuje się na zasoby innych podmiotów na zasadach określonych w art. 118 PZP w celu potwierdzenia spełniania warunków udziału w postępowaniu, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. Zobowiązanie podmiotu udostępniającego zasoby musi potwierdzać, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określać 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 usługi, których wskazane zdolności dotyczą.
2. **Dokumenty wymagane przed udzieleniem zamówienia:**
   1. **Zamawiający przed udzieleniem zamówienia wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni,**

terminie aktualnych na dzień złożenia następujących podmiotowych środków dowodowych:

- **a)** odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 PZP, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
- **b)** oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 PZP, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego w Dziale VI SWZ **(załącznik 5);**
- **c)** **wykazu usług 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 usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi 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 (***Załącznik nr 4***);
- **d)** **wykazu osób**, skierowanych przez Wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami (***Załącznik nr 3***).

UWAGA:

3. **Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast:**
   1) odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w pkt 2 ppkt 1 lit. a) – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury. wystawione nie wcześniej niż 3 miesiące przed ich złożeniem.
   2) Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt. 3 ppkt. 1) zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy.
4. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 pkt 4 PZP, a także bada,

czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy. W związku z powyższym, Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów przedstawienia w odniesieniu do tych podmiotów:

1) odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 PZP, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
2) oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 PZP, w zakresie podstaw wykluczenia z postępowania wskazanych przez Zamawiającego, o których mowa w art. 108 ust. 1 pkt 1-6 PZP, oraz w art. 109 ust. 1 pkt 5, 7-10 PZP.

Postanowienia pkt. 3 stosuje się odpowiednio.

5. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 poz. 346), o ile Wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 PZP, dane umożliwiające dostęp do tych środków.
6. Okresy wyrażone w latach lub miesiącach, o których mowa w pkt 1-4, liczy się wstecz od dnia w którym upływa termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu.
7. Jeżeli Wykonawca powołuje się na doświadczenie w realizacji usług, wykonywanych wspólnie z innymi Wykonawcami, wykaz, o którym mowa w pkt 2 ppkt 1 lit. c) i d), dotyczy usług, w których wykonaniu Wykonawca ten bezpośrednio uczestniczył, a w przypadku świadczeń powtarzających się lub ciągłych, w których wykonywaniu bezpośrednio uczestniczył lub uczestniczy.
8. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
9. Wykonawca nie może, po upływie terminu składania ofert powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

DZIAŁ IX Informacje o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami

1. W przedmiotowym postępowaniu komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu następujących środków komunikacji elektronicznej:
   1) **platformy** do obsługi postępowań przetargowych, dostępnej pod adresem: https://platformazakupowa.pl/pn/usz;
   2) poczty elektronicznej: przetargi@usz.edu.pl

   - z zastrzeżeniem, iż oferta wraz z załącznikami oraz podmiotowe i przedmiotowe środki dowodowe mogą zostać przekazane wyłącznie za pomocą powyższej Platformy.

DZIAŁ X Wskazanie osób uprawnionych do komunikowania się z Wykonawcami. Informacje o sposobie komunikowania się Zamawiającego z Wykonawcami oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

1. Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami jest: Wojciech Bereszko tel.: +48 91 444 11 51; e-mail: przetargi@usz.edu.pl
2. Komunikacja między Zamawiającym, a Wykonawcami odbywa się przy użyciu platformy zakupowej przy użyciu środków komunikacji elektronicznej. (**https://platformazakupowa.pl/pn/usz**).
3. W sytuacjach awaryjnych np. w przypadku braku działania platformy zakupowej **https://platformazakupowa.pl/pn/usz** Zamawiający może również komunikować się z wykonawcami za pomocą poczty elektronicznej - przetargi@usz.edu.pl.
4. 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 i formularza „Wyślij wiadomość do zamawiającego".
5. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.
6. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń, o których mowa w niniejszej SWZ, składane są przez Wykonawcę za pośrednictwem **https://platformazakupowa.pl/pn/usz**
7. Maksymalny rozmiar jednego pliku przesyłanego przy komunikacji wynosi 500 MB.
8. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu **Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. 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. poz. 2452)** oraz rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. poz. 2415).
9. Wykonawcy mogą zwracać się do Zamawiającego o wyjaśnienie treści SWZ, zgodnie z art. 284 ust. 1 PZP, kierując swoje zapytania do Zamawiającego, ze wskazaniem numeru postępowania określonego w SWZ. Zapytania winny być składane w sposób określony w pkt. 2, a w przypadku braku działania platformy zakupowej https://platformazakupowa.pl/pn/usz za pomocą poczty elektronicznej na adres przetargi@usz.edu.pl.
10. 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.
11. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 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, tj.:
    - stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
    - 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,
    - zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
    - włączona obsługa JavaScript,
    - zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,

- Platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
- 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.

12. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
13. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w pkt 12, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert.
14. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ, o którym mowa w pkt 12.
15. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w pkt. 12, zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
16. Treść zapytań wraz z wyjaśnieniami zamawiający udostępnia na stronie internetowej prowadzonego postępowania.
17. Wszelkie wyjaśnienia i modyfikacje, w tym zmiany terminów stają się integralną częścią specyfikacji istotnych warunków zamówienia i są wiążące dla Zamawiającego i Wykonawców.

DZIAŁ XI Termin związania ofertą

1. Wykonawca jest związany ofertą nie dłużej niż **30 dni** od dnia upływu terminu składania ofert, **tj. do dnia 06.07.2024 r.,** przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w pkt. 1, Zamawiający przed upływem terminu związania ofertą, zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w pkt. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. W przypadku gdy Zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, którym mowa w pkt. 2, następuje wraz z przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

DZIAŁ XII Opis sposobu przygotowywania oferty oraz innych dokumentów wymaganych w postępowaniu

1. Treść oferty musi odpowiadać treści SWZ.
2. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty, **w tym koszty poniesione z tytułu nabycia kwalifikowanego podpisu elektronicznego, bądź poniesione w związku z nabyciem lub korzystaniem z podpisu zaufanego lub podpisu osobistego.**
3. Wykonawca zobowiązany jest do zdobycia wszelkich informacji, które mogą być konieczne do przygotowania oferty oraz podpisania umowy.
4. Wykonawca składa ofertę wraz z załącznikami za pośrednictwem platformy zakupowej pod adresem: https://platformazakupowa.pl/pn/usz.
5. Korzystanie z platformy zakupowej przez Wykonawcę jest bezpłatne.

6. Celem prawidłowego złożenia oferty Zamawiający zamieścił na stronie platformy zakupowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje plik pn. **Pełna instrukcja tekstowa składania ofert, wysyłania wiadomości w Ogłoszeniu o Zamówieniu (UE/PL).**
7. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   - akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej https://platformazakupowa.pl/strona/1-regulamin oraz uznaje go za wiążący,
   - zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem https://platformazakupowa.pl/strona/45-instrukcje.
8. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z 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.
9. 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.
10. Formaty plików wykorzystywanych przez Wykonawcę 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".
11. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) ze szczególnym wskazaniem na .pdf. Wśród formatów powszechnych a niewymienionych w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.
12. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:
    - .zip
    - .7Z
13. **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.**
14. 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.
15. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
16. 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.
17. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
18. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
19. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert.
20. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.

21. Jeśli Wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.

22. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.

23. 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.

24. Ofertę sporządza się w języku polskim się na Formularzu Ofertowym – zgodnie z **Załącznikiem nr 1 do SWZ**. Wraz z ofertą Wykonawca jest zobowiązany złożyć:

- **a) oświadczenie, o którym mowa w Rozdziale 1, Dział VIII pkt. 1 ppkt 1 SWZ;**
- **b) zobowiązanie innego podmiotu oraz jego oświadczenie, o których mowa w Rozdziale 1 Dział VIII pkt. 1 ppkt 1 i 2 SWZ (jeżeli dotyczy);**
- **c) przedmiotowe środki dowodowe, o których mowa w Rozdziale I, Dział IV SWZ;**
- **d) dokumenty, z których wynika prawo do podpisania oferty; odpowiednie pełnomocnictwa (jeżeli dotyczy).**

25. Po wypełnieniu Formularza składania oferty i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk ***„Przejdź do podsumowania”***.

26. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem https://platformazakupowa.pl/pn/usz, Wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust 1 oraz ust. 2 PZP, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust.1 PZP sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Na stronie platformy zakupowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje znajduje się plik: **Pigułka wiedzy na temat podpisów osobistych i zaufanych**. Zamawiający zaleca zapoznanie się z dokumentem.

27. 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”.

28. W przypadku wykorzystania formatu podpisu XAdES zewnętrznego. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.

29. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.

30. Każdy Wykonawca przedłoży tylko jedną ofertę, sam lub jako reprezentant spółki czy konsorcjum. Złożenie więcej niż jednej oferty przez jednego Wykonawcę spowoduje odrzucenie wszystkich jego ofert.

31. Wykonawca, za pośrednictwem 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.

32. Formularz oferty oraz wszystkie załączniki zostaną podpisane przez upełnomocnionego przedstawiciela Wykonawcy. Pełnomocnictwo do podpisania oferty winno być dołączone do oferty, o ile nie wynika ono z ustawy albo z innych dokumentów załączonych do oferty.

33. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, może dokonać również notariusz.

34. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio

Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 PZP lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, **zostały wystawione przez upoważnione podmioty** inne niż Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „upoważnionymi podmiotami", jako dokument elektroniczny, przekazuje się ten dokument.

35. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania, **zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej**, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym lub podpisem zaufanym, lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej w przypadku:

- podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
- przedmiotowych środków dowodowych – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
- innych dokumentów – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.

36. Podmiotowe środki dowodowe, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, **niewystawione przez upoważnione podmioty oraz pełnomocnictwo** przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym lub podpisem zaufanym, lub podpisem osobistym.

37. W przypadku gdy podmiotowe środki dowodowe, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, **niewystawione przez upoważnione podmioty lub pełnomocnictwo**, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, lub podpisem zaufanym, lub podpisem osobistym poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej dokonuje w przypadku:

- podmiotowych środków dowodowych – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;
- przedmiotowego środka dowodowego lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
- pełnomocnictwa – mocodawca.

38. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego składają jeden lub kilka dokumentów tak, aby wspólnie udokumentować spełnianie warunków podmiotowych, brak podstaw do wykluczenia oraz dotyczących przedmiotu zamówienia. Wymagane oświadczenia należy złożyć w sposób wyraźnie wskazujący, iż oświadczenie składają wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego. Nadto, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Stosowne pełnomocnictwo musi zostać opatrzone kwalifikowanym podpisem elektronicznym lub podpisem zaufanym, lub podpisem osobistym. **Wspólnicy spółki cywilnej traktowani są jak Wykonawcy ubiegający się wspólnie o udzielenie zamówienia publicznego.**

39. W przypadku załączania do oferty dokumentów lub oświadczeń sporządzonych w języku obcym, z zastrzeżeniem postanowień Rozdziału 1, Dział IV SWZ należy je złożyć wraz z tłumaczeniem na język polski.

40. Zamawiający zaleca wykorzystanie formularzy załączonych do SWZ. Dopuszcza się złożenie załączników opracowanych przez Wykonawców pod warunkiem, że będą one zgodne co do treści z formularzami określonymi przez Zamawiającego.

41. Oferty będą oceniane według kryteriów i zasad określonych w rozdziale 1, Dział XV SWZ. Wykonawcy przedstawią oferty zgodnie z wymaganiami SWZ.

42. Ofertę wraz z załącznikami należy złożyć za pośrednictwem platformy zakupowej pod adresem: **https://platformazakupowa.pl/pn/usz** w terminie najpóźniej do dnia **07.06.2024 r. do godziny 11:30.**

DZIAŁ XIII Termin otwarcia ofert

1. Otwarcie ofert nastąpi w dniu **07.06.2024 r. o godz. 12:00** i realizowane będzie przy użyciu systemu teleinformatycznego.
2. W przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii. W takim przypadku Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
3. Bezpośrednio przed otwarciem ofert Zamawiający udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje pod adresem: https://platformazakupowa.pl/pn/usz
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.
5. Zamawiający przekazuje Prezesowi Urzędu informację o złożonych ofertach, nie później niż w terminie 7 dni od dnia otwarcia ofert albo unieważnienia postępowania.

DZIAŁ XIV Sposób obliczenia ceny

1. Wykonawca określi ceny brutto na formularzu oferty. W kalkulacji należy uwzględnić wszystkie koszty związane z wykonaniem usługi.
2. Wszystkie elementy oferty powinny zawierać w sobie ewentualne upusty stosowane przez Wykonawcę, tzn. muszą być one wkalkulowane w cenę oferty.
3. Cena powinna zostać wyrażona cyfrowo.
4. Cenę należy obliczyć na podstawie szczegółowego opisu przedmiotu zamówienia zawartego w Rozdziale 2 SWZ.
5. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2023 r. poz. 1570), dla celów zastosowania kryterium ceny Zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. Wykonawca w takim przypadku 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.

6. Rozliczenia będą prowadzone w walucie: PLN.

DZIAŁ XV Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami i ich wagami oraz w następujący sposób będzie oceniał spełnianie kryteriów:
   - **cena brutto - 60%**
   - **termin płatności - 40%**
2. Sposób oceny ofert według przyjętych kryteriów (1%=1pkt):
   Kryterium 1 będzie obliczone za pomocą następującego wzoru:
   maksymalnie można uzyskać 60 pkt
   Cena brutto (C) = [(Cn : Cb) x 60 %] x 100
   gdzie:
   Cn - cena najniższa (brutto)
   Cb - cena wynikająca z oferty badanej (brutto)

Kryterium 2 obliczone zostanie w następujący sposób:
Termin płatności (T) - waga kryterium 40 % (maksymalnie można uzyskać 40 pkt)
Wykonawca w formularzu oferty (Załącznik nr 1 do SWZ) zadeklaruje oferowany termin płatności. Punkty zostaną przyznane w następujący sposób:
Liczba punktów = T, gdzie:

a) T - termin płatności do 30 dni od dnia podpisania umowy – 40 pkt.
b) T - termin płatności do 21 dni od dnia podpisania umowy – 20 pkt.
c) T - termin płatności do 14 dni od dnia podpisania umowy – 0 pkt.

Uwaga: termin płatności nie może być krótszy niż 14 dni kalendarzowych, licząc od dnia doręczenia faktury Zamawiającemu. W przypadku oferowania terminu płatności krótszego niż 14 dni oferta zostanie odrzucona. W przypadku, gdy Wykonawca w ofercie nie wskaże oferowanego terminu płatności, Zamawiający uzna, iż wynosi on 14 dni i przyzna w kryterium 0 pkt.

Wynik oferty = C+T.

3. W wyniku komisyjnej analizy i oceny otrzymanych ofert, stosując kryteria ustawowe i określone w SWZ dokonany zostanie wybór najkorzystniejszej oferty.
4. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
5. Zgodnie z art. 223 ust. 2 PZP Zamawiający poprawi w treści oferty:
   1) oczywiste omyłki pisarskie,
   2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, oraz
   3) inne omyłki polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty,

niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.

6. W przypadku, o którym mowa w pkt. 5 pkt 3, Zamawiający wyznacza Wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.

DZIAŁ XVI Informacja o podstawie odrzucenia ofert

1. Zamawiający odrzuca ofertę, jeżeli:
   1) została złożona po terminie składania ofert;
   2) została złożona przez Wykonawcę:

a) podlegającego wykluczeniu z postępowania lub niespełniającego warunków udziału w postępowaniu, lub
b) który nie złożył w przewidzianym terminie oświadczenia, o którym mowa w art. 125 ust. 1 PZP, lub podmiotowego środka dowodowego, potwierdzających brak podstaw wykluczenia lub spełnianie warunków udziału w postępowaniu, przedmiotowego środka dowodowego, lub innych dokumentów lub oświadczeń,

3) jest niezgodna z przepisami ustawy;
4) jest nieważna na podstawie odrębnych przepisów;
5) jej treść jest niezgodna z warunkami zamówienia;
6) nie została sporządzona lub przekazana w sposób zgodny z wymaganiami technicznymi oraz organizacyjnymi sporządzania lub przekazywania ofert przy użyciu środków komunikacji elektronicznej określonymi przez Zamawiającego;
7) została złożona w warunkach czynu nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
8) zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia;
9) zawiera błędy w obliczeniu ceny lub kosztu;
10) Wykonawca w wyznaczonym terminie zakwestionował poprawienie omyłki, o której mowa w art. 223 ust. 2 pkt 3 PZP;
11) Wykonawca nie wyraził pisemnej zgody na przedłużenie terminu związania ofertą;
12) Wykonawca nie wyraził pisemnej zgody na wybór jego oferty po upływie terminu związania ofertą;
13) w przypadku, gdy Zamawiający żądał wniesienia wadium - Wykonawca nie wniósł wadium, lub wniósł w sposób nieprawidłowy lub nie utrzymywał wadium nieprzerwanie do upływu terminu związania ofertą lub złożył wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 PZP;
14) jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób;
15) obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 poz. 1369), stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe;

DZIAŁ XVII Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawrze umowę w sprawie zamówienia publicznego z Wykonawcą, którego oferta zostanie uznana za najkorzystniejszą, w terminach określonych w art. 264 PZP.
2. Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, będzie zobowiązany przed podpisaniem umowy do wniesienia zabezpieczenia należytego wykonania umowy (jeżeli jego wniesienie było wymagane) w wysokości i formie określonej w Rozdziale 1, Dział XIX SWZ.
3. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający zastrzega sobie prawo żądania przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców.
4. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.
5. Wykonawca będzie zobowiązany do podpisania umowy w terminie wskazanym przez Zamawiającego.

DZIAŁ XVIII Wadium

Zamawiający nie wymaga wniesienia wadium.

DZIAŁ XIX Zabezpieczenie należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy

DZIAŁ XX Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy

1. Odwołanie przysługuje na:
   1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania Wykonawców lub konkursie, w tym na projektowane postanowienie umowy;
   2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania Wykonawców lub konkursie, do której Zamawiający był obowiązany na podstawie ustawy;
   3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że Zamawiający był do tego obowiązany
2. Odwołanie wnosi się do Prezesa Izby w terminie:
   1) 5 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
   2) 10 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w ppkt 1;
   3) odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie: 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub zamieszczenia dokumentów zamówienia na stronie internetowej;
   4) odwołanie w przypadkach innych niż określone w ppkt 1-3 wnosi się w terminie: 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
3. Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
4. Domniemywa się, że Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
5. Odwołanie zawiera:
   1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);
   2) nazwę i siedzibę Zamawiającego, numer telefonu oraz adres poczty elektronicznej Zamawiającego;
   3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;
   4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku – numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;
   5) określenie przedmiotu zamówienia;
   6) wskazanie numeru ogłoszenia w Biuletynie Zamówień Publicznych;

7) wskazanie czynności lub zaniechania czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, lub wskazanie zaniechania przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy;
8) zwięzłe przedstawienie zarzutów;
9) żądanie co do sposobu rozstrzygnięcia odwołania;
10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;
11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;
12) wykaz załączników.

6. Do odwołania dołącza się:
   1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;
   2) dowód przekazania odpowiednio odwołania albo jego kopii Zamawiającemu;
   3) dokument potwierdzający umocowanie do reprezentowania odwołującego.
7. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 PZP stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
8. Skargę wnosi się do Sądu Okręgowego w Warszawie – sądu zamówień publicznych, zwanego dalej „sądem zamówień publicznych".
9. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 PZP, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe jest równoznaczne z jej wniesieniem.
10. Skarga powinna czynić zadość wymaganiom przewidzianym dla pisma procesowego oraz zawierać oznaczenie zaskarżonego orzeczenia, ze wskazaniem, czy jest ono zaskarżone w całości, czy w części, przytoczenie zarzutów, zwięzłe ich uzasadnienie, wskazanie dowodów, a także wniosek o uchylenie orzeczenia lub o zmianę orzeczenia w całości lub w części, z zaznaczeniem zakresu żądanej zmiany.

DZIAŁ XXI Pozasądowe rozwiązywanie sporów

1. W sprawie majątkowej, w której zawarcie ugody jest dopuszczalne, każda ze stron umowy, w przypadku sporu wynikającego z zamówienia, może złożyć wniosek o przeprowadzenie mediacji lub inne polubowne rozwiązanie sporu do Sądu Polubownego przy Prokuratorii Generalnej Rzeczypospolitej Polskiej, wybranego mediatora albo osoby prowadzącej inne polubowne rozwiązanie sporu.
2. Umowa może zawierać postanowienia o mediacji lub innym polubownym rozwiązaniu sporu. Umowa o mediację lub inne polubowne rozwiązanie sporu może być zawarta także przez wyrażenie przez stronę zgody na mediację lub inne polubowne rozwiązanie sporu, gdy druga strona złożyła wniosek, o którym mowa w pkt. 1
3. Zawarcie ugody nie może prowadzić do naruszenia przepisów działu VII rozdziału 3 PZP.

DZIAŁ XXII Jawność postępowania. Informacja dotycząca przetwarzania danych osobowych

1. Zamawiający informuje, iż zgodnie z art. 18 ust. 1 PZP postępowanie o udzielenie zamówienia jest jawne.
2. Protokół wraz załącznikami jest jawny i udostępniany na wniosek. Oferty wraz z załącznikami udostępnia się na wniosek niezwłocznie po otwarciu ofert, nie później jednak niż w terminie 3 dni od dnia otwarcia ofert. W przypadku gdy wniesienie żądania dotyczącego prawa, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, 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.

3. Zgodnie z art. 13 ust. 1 i 2 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/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:
   - administratorem Pani/Pana danych osobowych jest Uniwersytet Szczeciński, al. Papieża Jana Pawła II 22a 70-453 Szczecin.
   - Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z ww. postępowaniem o udzielenie zamówienia publicznego
   - odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o przepisy PZP;
   - Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, 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;
   - obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z PZP;
   - w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
   - posiada Pani/Pan:
     4) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
     5) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
     6) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
     7) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
   - nie przysługuje Pani/Panu:
     - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
     - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
     - **na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO**.
4. Udostępnianie, o którym mowa w pkt 2 ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, zebranych w toku postępowania o udzielenie zamówienia. Ograniczenia zasady jawności, o których mowa w pkt 17 i art. 18 ust. 3–6 PZP, stosuje się odpowiednio.
5. W przypadku korzystania przez osobę, której dane osobowe są przetwarzane przez Zamawiającego, z uprawnienia, o którym mowa w art. 15 ust. 1–3 rozporządzenia 2016/679, Zamawiający może żądać od osoby występującej z żądaniem wskazania dodatkowych informacji, mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.
6. Skorzystanie przez osobę, której dane osobowe są przetwarzane, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 rozporządzenia 2016/679, nie może naruszać integralności protokołu postępowania oraz jego załączników.
7. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone

informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 PZP.

8. Przez tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2020 r. poz. 1913) rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującymi się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzenia nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich poufności, tzn. składając ofertę zastrzegł, iż nie mogą być one udostępnione innym uczestnikom postępowania oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać załączone na platformie zakupowej zgodnie z instrukcją składania oferty dla Wykonawcy.
9. Ujawnienie niezastrzeżonej treści ofert dokonywane będzie wg poniższych zasad:
   1) osoba zainteresowana zobowiązana jest wystąpić do Zamawiającego o udostępnienie treści protokołu lub/i załączników do protokołu,
   2) Zamawiający ustali, z uwzględnieniem złożonego w ofercie zastrzeżenia o tajemnicy przedsiębiorstwa, zakres informacji, które mogą być udostępnione,
   3) po przeprowadzeniu powyższych czynności Zamawiający niezwłocznie udostępni wnioskodawcy protokół lub/i załączniki do protokołu.

ROZDZIAŁ 2
SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

WYMAGANIA SZCZEGÓŁOWE:

I. Modernizacja systemu zabezpieczającego dostęp do infrastruktury sieciowej oraz jej monitorowania w zakresie bezpieczeństwa obejmuje następujące jego elementy:

- Firewall_A – obecnie 2 x FortiGate 1500D – pracujący w trybie HA, pełniący funkcje kontrolera Wi-Fi (260+ AP)
- Firewall_B – obecnie 2 x FortiGate 500E – pracujący w trybie HA, podstawowy koncentrator połączeń VPN dla ponad 1500 użytkowników
- WAF – obecnie 2 x FortiWeb 1000D – pracujący w trybie HA
- centralny system składkowania i analizy logów - 1 x FortiAnalyzer 400E

Modernizacja Firewall_A

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę minimum 6 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Parametry fizyczne systemu:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 GE
   - 4 gniazdami SFP+ 10 GE.
   - 4 gniazdami SFP28 10/25 GE.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall posiada min 1 dedykowany port HA
4. System Firewall posiada min 1 dedykowany management port niezależny od portu konsoli
5. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
6. System jest wyposażony w redundantne zasilanie min 2x AC.
7. Obudowa urządzenia o wysokości 1U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 15 mln. jednoczesnych połączeń oraz 700 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 160 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 70 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 256 nie mniej niż 50 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 25 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 20 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 15 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Funkcje kontrolera sieci bezprzewodowych

- Maksymalna liczba obsługiwanych AP – nie mniej niż 512
- Maksymalna liczba obsługiwanych AP w trybie tunelowania - nie mniej niż 128
- Maksymalna liczba obsługiwanych SSID – nie mniej niż 128
- Zarządzanie punktami dostępowymi FortiAP (Zamawiający posiada ponad 260 szt.)

Ochrona przed malware

Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

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

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Jeżeli do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje to powinny być zawarte w ofercie:

a. Kontrola Aplikacji,
b. IPS,
c. Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),
d. Analiza typu Sandbox cloud, Antyspam, Web Filtering,
e. bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Minimalne wymagania odnośnie dostarczonych licencji:

<u>AntiVirus (AV) - Moduł Antywirusowy parametry:</u>

- skanowanie protokołów HTTP, POP3, IMAP, FTP, SMTP,
- baza sygnatur dopasowana do aktualnych zagrożeń,
- blokowanie połączeń do znanych serwerów kontrolujących botnety,
- kwarantanna na dysk twardy,
- wykrywanie plików typu „Spyware”, „Grayware",

- blokowanie plików danego typu,
- automatyczne uaktualnianie sygnatur baz wirusów,

AntiSpam - Moduł Antyspamowy:

- filtrowanie po adresie IP, mail, słowach kluczowych,
- sprawdzanie zwrotnego DNS'u, serwerów RBL,
- możliwość usuwania wiadomości tylko przy SMTP,
- dodatkowe sprawdzanie adresu IP nadawcy i linków URL w treści wiadomości,
- filtrowanie wiadomości email na podstawie list RBL,
- filtrowanie wiadomości email na podstawie baz ORDB,
- filtrowanie wiadomości email na bazie białych oraz czarnych list,
- blokowanie wiadomości email na podstawie słów kluczowych,
- wsparcie dla protokołu RevDNS,
- funkcja sprawdzania nagłówków MIME wiadomości.

Web Filtering - Filtrowanie WWW:

- filtrowanie na podstawie adresu URL, słowie kluczowym,
- filtrowanie Applet JAVA, ActiveX, Cookies,
- możliwość blokowania stron z wybranej kategorii,
- możliwość filtrowania wyników wyszukiwania najpopularniejszych wyszukiwarek internetowych (tzw. bezpieczne wyszukiwanie - *Safe Search*),
- możliwość dodawania własnych stron (adresów URL) do kategorii.

Parametry systemu wykrywania i zapobiegania włamaniom [IPS/IDS+AP]:

- wykrywanie połączeń typu „**Peer-to-Peer**”,
- wykrywania anomalii sieciowych oraz ataków,
- możliwość definiowania sygnatur ataków,
- przyporządkowanie priorytetów oraz określenie podatności sygnatur ataków do określonych systemów operacyjnych,
- logowanie, blokowanie oraz informowanie o atakach,
- rozpoznawanie i kontrola aplikacji sieciowych,
- automatyczne aktualizowanie „sygnatur ataków”, **Automated Attack Signature Updates.**

Dodatkowe akcesoria dla klastra:

- 2 x DAC SFP+ 1m
- 4 x SFP28 SR MM Duplex LC
- 4 x SFP28 LR SM Duplex LC
- 8 x SFP+ LRM Duplex LC
- 12 X SFP SR MM Duplex LC
- 4 X SFP LR SM Duplex LC

Modernizacja Firewall_B

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę minimum 6 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

- W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- Monitoring stanu realizowanych połączeń VPN.
- System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
- System ma pracować w postaci redundantnego klastra.

Parametry fizyczne systemu:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
    - 16 portami Gigabit Ethernet RJ-45.
    - 8 gniazdami SFP 1 Gbps.
    - 8 gniazdami SFP+ 10 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall posiada min 1 dedykowany port HA
4. System Firewall posiada min 1 dedykowany management port niezależny od portu konsoli
5. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
6. System jest wyposażony w redundantne zasilanie min 2x AC.
7. Obudowa urządzenia o wysokości 1U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Parametry wydajnościowe:

- W zakresie Firewall'a obsługa nie mniej niż 7.2 mln jednoczesnych połączeń oraz 480 tys. nowych połączeń na sekundę.
- Przepustowość Stateful Firewall: nie mniej niż 76 Gbps dla pakietów 512 B.
- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps.
- Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 256 nie mniej niż 50 Gbps.
- Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 11 Gbps.
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 9 Gbps.
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7.2 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

- Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
- Kontrola Aplikacji.
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
- Ochrona przed malware.
- Ochrona przed atakami - Intrusion Prevention System.
- Kontrola stron WWW.
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
- Zarządzanie pasmem (QoS, Traffic shaping).
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
- Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
- Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
- Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

- Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
  1. Translację jeden do jeden oraz jeden do wielu.
  2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
- W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
- Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
- Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
- Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
  1. Amazon Web Services (AWS).
  - Microsoft Azure.
  - Cisco ACI.
  - Google Cloud Platform (GCP).
  - OpenStack.
  - VMware NSX.
  - Kubernetes.

Połączenia VPN

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

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

- Routingu statycznego.
- Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
- Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
- ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
- BFD (Bidirectional Forwarding Detection).
- Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

- System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
- SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

- System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- System daje możliwość określania pasma dla poszczególnych aplikacji.
- System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
- System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

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

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
    - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

- Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
- Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
- Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
- System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

- System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
- Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
- Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

- Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
- W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
- Możliwość włączenia logowania per reguła w polityce firewall.
- System zapewnia możliwość logowania do serwera SYSLOG.
- Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

- Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Jeżeli do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje to powinny być zawarte w ofercie:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Minimalne wymagania odnośnie dostarczonych licencji:

AntiVirus (AV) - Moduł Antywirusowy parametry:

- skanowanie protokołów HTTP, POP3, IMAP, FTP, SMTP,
- baza sygnatur dopasowana do aktualnych zagrożeń,
- blokowanie połączeń do znanych serwerów kontrolujących botnety,
- kwarantanna na dysk twardy,
- wykrywanie plików typu „Spyware", „Grayware",
- blokowanie plików danego typu,
- automatyczne uaktualnianie sygnatur baz wirusów,

AntiSpam - Moduł Antyspamowy:

- filtrowanie po adresie IP, mail, słowach kluczowych,
- sprawdzanie zwrotnego DNS'u, serwerów RBL,
- możliwość usuwania wiadomości tylko przy SMTP,
- dodatkowe sprawdzanie adresu IP nadawcy i linków URL w treści wiadomości,
- filtrowanie wiadomości email na podstawie list RBL,
- filtrowanie wiadomości email na podstawie baz ORDB,
- filtrowanie wiadomości email na bazie białych oraz czarnych list,
- blokowanie wiadomości email na podstawie słów kluczowych,
- wsparcie dla protokołu RevDNS,
- funkcja sprawdzania nagłówków MIME wiadomości.

Web Filtering - Filtrowanie WWW:

- filtrowanie na podstawie adresu URL, słowie kluczowym,
- filtrowanie Applet JAVA, ActiveX, Cookies,
- możliwość blokowania stron z wybranej kategorii,
- możliwość filtrowania wyników wyszukiwania najpopularniejszych wyszukiwarek internetowych (tzw. bezpieczne wyszukiwanie - *Safe Search*),
- możliwość dodawania własnych stron (adresów URL) do kategorii.

Parametry systemu wykrywania i zapobiegania włamaniom [IPS/IDS+AP]:

- wykrywanie połączeń typu „**Peer-to-Peer**”,
- wykrywania anomalii sieciowych oraz ataków,
- możliwość definiowania sygnatur ataków,
- przyporządkowanie priorytetów oraz określenie podatności sygnatur ataków do określonych systemów operacyjnych,
- logowanie, blokowanie oraz informowanie o atakach,
- rozpoznawanie i kontrola aplikacji sieciowych,
- automatyczne aktualizowanie „sygnatur ataków”, **Automated Attack Signature Updates.**

Dodatkowe akcesoria dla klastra:

- 2 x DAC SFP+ 1m
- 4 x SFP+ LR Duplex LC
- 4 x SFP+ SR Duplex LC
- 12 X SFP SR MM Duplex LC
- 4 X SFP LR SM Duplex LC

Modernizacja Web Application Firewall

System ochrony aplikacji webowych oraz API, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. Powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej dla której producent zapewnia pełne wsparcie techniczne dla wszystkich jej elementów.

Architektura systemu

1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się, aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3. Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4. Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web.
5. Powinna istnieć możliwość zdefiniowania co najmniej 10 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
6. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.
7. System ma pracować w postaci redundantnego klastra.

Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi dysponować minimum:
   - 6 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. Powierzchnia dyskowa - minimum 2 x 480 GB typu SSD.
3. Redundantne zasilanie z sieci 230V/50Hz.
4. Obudowa urządzenia o wysokości do 2U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Parametry wydajnościowe

1. Przepustowość dla ruchu http - min 2,5 Gbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1. Obsługa protokołów: - http 1.1, http 2.0, FTP.

2. System musi posiadać możliwość automatycznego uczenia się działania aplikacji w zakresie:
   - obserwacji i budowania profilu dla URL, parametrów, metod http, sesji https. Obserwacje powinny uczyć model matematyczny normalnych zachowań, który następnie umożliwi wykrywanie anomalii
   - Wyuczony model matematyczny wykrywa odstępstwa od normy w obserwowanych elementach
   - System automatycznie wykrywa zmiany po stronie aplikacji lub zachowania użytkowników i ponawia proces uczenia.
   - Możliwe jest zdefiniowanie wyjątków, które nie będą brały udziału w uczeniu modelu matematycznego
   - Musi istnieć możliwość strojenia czułości modelu wykrywającego anomalie przez administratora systemu. Poziom czułości musi być ustawiany globalnie dla aplikacji jak i na poziomie pojedynczych parametrów.
3. System musi posiadać funkcje ochrony komunikacji API wspieraną technologią uczenia maszynowego. Zakres wsparcia nie może być mniejszy niż:
   - Uczenie modelu matematycznego w oparciu o widziany faktyczny ruch REST API
   - Budowanie automatyczne schematu struktury API w oparciu o obserwowany ruch
   - Ruch niezgodny z wyuczonym profilem uznawany jest za atak
4. System ochrony aplikacji musi być wyposażony w mechanizm wykrywania komunikacji pochodzącej od internetowych bot'ów. Wykrywanie musi być oparte co najmniej o następujące mechanizmy:
   - Uczenie maszynowe: powinno działać w trybie nauki modelu matematycznego standardowego zachowania użytkowników. Po zebraniu informacji system powinien przejść do trybu ochrony, gdzie wykrycie zachowania odbiegającego od normy powinno skutkować uznaniem źródła za automat.
5. Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
   - Round Robin,
   - Weighted Round Robin,
   - Least Connection,
6. Wsparcie dla mechanizmów session persistence:
   - Source IP
   - HTTP Header
   - URL parameter
   - Insert Cookie
   - Rewrite Cookie
   - Persistent Cookie
   - Embedded Cookie
   - ASP Session ID
   - PHP Session ID
   - JSP Session ID
   - SSL Session ID
7. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3.
8. Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa.
9. Ochrona aplikacji www przed takimi zagrożeniami jak:
   - SQL and OS Command Injection.
   - Cross Site Scripting (XSS).
   - Cross Site Request Forgery.
   - Outbound Data Leakage.
   - HTTP Request Smuggling.
   - Buffer Overflow.
   - Encoding Attacks.
   - Cookie Tampering / Poisoning.
   - Session Hijacking.

- Broken Access Control.
- Forceful Browsing /Directory Traversal.
- Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP.
- DoS w warstwie aplikacji.
- Ochrona przed atakami typu Brute force.
- Ochrona przed atakami clickjacking.
- Ochrona przed credential stuffing.

10. Mechanizmy ochrony przed wyciekiem informacji poufnych.
11. Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację.
12. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
13. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.
14. Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy.
15. Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only".
16. Content routing na bazie parametrów http oraz certyfikatów X.509.
17. Ochrona przed Web Scraping.
18. Wsparcie dla kompresji danych oraz cache.
19. Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos).
20. Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
21. Ochrona przed atakami typu SLOW (Slowloris i podobne).
22. Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie wielu parametrów:
    - Metoda HTTP.
    - IP klienta.
    - Host.
    - URI.
    - Cały URL.
    - Parametr.
    - Cookie.
    - http Header
    - JSON Elements
23. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For".
24. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
25. Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.
26. Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload'u HTML.
27. Wsparcie dla walidacji OpenAPI, JSON i XML.
28. Blokowania „Illegal XML Format" oraz „Illegal JSON Format".
29. Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy.
30. Przydzielanie różnych certyfikatów dla różnych nazw domenowych.
31. Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate.
32. URL Encryption.

Wymagane funkcje dodatkowe

1. Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
2. Skaner aplikacji WWW realizowany bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.

3. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.
4. Dekodowanie Base64 oraz CSS.
5. Domyślne szablony ochrony dla Exchange, SharePoint i WordPress.
6. Uwierzytelnianie użytkowników w oparciu o protokół SAML.
7. Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji.
8. Wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników.
9. Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa.
10. Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day.
11. Możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez urządzenie w celu późniejszej ich analizy.
12. Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych.
13. Cross-Origin Resource Sharing (CORS) protection.
14. Integracja z Lets's encrypt pozwalająca na automatyczne generowanie certyfikatów.

Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.
2. Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
4. Możliwość przechowywania lokalnie na urządzeniu do 10 plików konfiguracyjnych.

Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2. Możliwość logowania do zewnętrznego serwera syslog i SIEM.
3. Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

Sygnatury, subskrypcje

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
   - Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 12 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Dodatkowe akcesoria dla klastra:

- 4 x SFP+ SR MM Duplex LC
- 4 x SFP LR SM Duplex LC
- 4 x SFP SR MM Duplex LC

Modernizacja urządzenia do składowania i analizy logów

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej.

Parametry fizyczne systemu:

1. System musi dysponować co najmniej:
   - 4 portami Gigabit Ethernet RJ-45.

- 2 gniazdami SFP 1 Gbps.

2. Rozwiązanie musi dysponować powierzchnią dyskową min. 16 TB.
3. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0, 1, 5, 10.
4. Obudowa urządzenia o wysokości 1U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 200 GB logów na dzień.
2. System musi być w stanie przeanalizować minimum 4000 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 800 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
   a) Listę najczęściej wykrywanych ataków.
   b) Listę najbardziej aktywnych użytkowników.
   c) Listę najczęściej wykorzystywanych aplikacji.
   d) Listę najczęściej odwiedzanych stron www.
   e) Listę krajów, do których nawiązywane są połączenia.
   f) Listę najczęściej wykorzystywanych polityk Firewall.
   g) Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
7. System powinien bez żadnych dodatkowych ograniczeń kolekcjonować przesyłane logi z pozostałych urządzeń objętych tym zamówieniem oraz umożliwiać ich pełną analitykę.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.

- Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać definiowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Dodatkowe akcesoria:

- 2 x SFP SR MM Duplex LC

Odnowienia wsparcia producenta (serwis i subskrypcja) dla posiadanego sprzętu

1. **FortiGuard dla urządzenia FortiGate 60F - licencje aktywacyjne (subskrypcja) dla funkcji bezpieczeństwa na okres 12 miesięcy zapewniające**:
   a) ochronę przed atakami – systemy wykrywania i zapobiegania włamaniom – *Intrusion Prevention System* [IPS/IDS],
   b) ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, http, FTP, IM),
   c) kontrolę treści – *Web Filter* [WF]
   d) kontrolę aplikacji – *Application Control* [AP]
   e) kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
2. **Forticare dla urządzenia FortiGate 60F**
   f) Przedłużenie serwisu producenta w zakresie naprawy lub wymiany sprzętu w przypadku awarii, uaktualnienia oprogramowania wewnętrznego urządzenia (firmware) oraz wsparcie techniczne przez producenta w trybie 24x7 obejmujące dostęp przez telefon, web, chat na okres 12 miesięcy w niżej wymienionym urządzeniu firmy Fortinet będących w posiadaniu Zamawiającego:

FortiGate 60F s/n: FGT60FTK21030829, okres obecnego wsparcia do **2024-08-21**

Wyżej wymienione urządzenie jest na gwarancji i pracuje w systemie ciągłym (tj. 24 godziny na dobę, 7 dni w tygodniu) zabezpieczając sieć komputerową oraz urządzenia i usługi sieciowe świadczone przez Uniwersytet Szczeciński.

Wykonawca dostarczy i zainstaluje licencje (subskrypcje) producenta dla w/w sprzętu i modułów o minimalnych parametrach:

AntiVirus (AV) – Moduł Antywirusowy parametry:

- skanowanie protokołów http, POP3, IMAP, FTP, SMTP,
- baza sygnatur dopasowana do aktualnych zagrożeń,
- blokowanie połączeń do znanych serwerów kontrolujących Botnety,
- kwarantanna na dysk twardy,
- wykrywanie plików typu „Spyware", „Grayware",
- blokowanie plików danego typu,
- automatyczne uaktualnianie sygnatur baz wirusów,

AntiSpam – Moduł Antyspamowy z usługa FortiGuard:

- filtrowanie po adresie IP, mail, słowach kluczowych,
- sprawdzanie zwrotnego DNS'u, serwerów RBL,
- możliwość usuwania wiadomości tylko przy SMTP,
- dodatkowe sprawdzanie adresu IP nadawcy i linków URL w treści wiadomości,
- filtrowanie wiadomości email na podstawie list RBL,
- filtrowanie wiadomości email na podstawie baz ORDB,
- filtrowanie wiadomości email na bazie białych oraz czarnych list,
- blokowanie wiadomości email na podstawie słów kluczowych,

- wsparcie dla protokołu RevDNS,
- funkcja sprawdzania nagłówków MIME wiadomości.

Web Filtering – Filtrowanie WWW z usługa FortiGuard:

- filtrowanie na podstawie adresu URL, słowie kluczowym,
- filtrowanie Applet JAVA, ActiveX, Cookies,
- możliwość blokowania stron z wybranej kategorii,
- możliwość filtrowania wyników wyszukiwania najpopularniejszych wyszukiwarek internetowych (tzw. Bezpieczne wyszukiwanie – *Safe Search*),
- możliwość dodawania własnych stron (adresów URL) do kategorii.

Parametry systemu wykrywania i zapobiegania włamaniom [IPS/IDS+AP]:

- wykrywanie połączeń typu „**Peer-to-Peer**”,
- wykrywania anomalii sieciowych oraz ataków,
- możliwość definiowania sygnatur ataków,
- przyporządkowanie priorytetów oraz określenie podatności sygnatur ataków do określonych systemów operacyjnych,
- logowanie, blokowanie oraz informowanie o atakach,
- rozpoznawanie i kontrola aplikacji sieciowych,
- automatyczne aktualizowanie „sygnatur ataków”, **Automated Attack Signature Updates.**

Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Warunki dodatkowe (dla całości)

1. W przypadku istnienia wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), **Wykonawca** zobowiązany jest załączyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2023 r. poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. *Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.*
3. Wykonawca musi przedłożyć wykaz minimum dwóch osób posiadających po dwa imienne certyfikaty autoryzacyjne producenta (zgodne z aktualną i przyjętą przez producenta polityką certyfikacyjną) poświadczające kompetencje inżynierów dokonujących rejestracji oferowanych serwisów.
4. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej centrum serwisowego wykonawca winien przedłożyć dokument wystawiony przez producenta który wskazuje podmiot uprawniony do realizowania usługi gwarancyjnej na terenie Rzeczpospolitej Polskiej.
5. Do czasu pełnego wdrożenia rozwiązania oraz aktywacji licencji wykonawca zapewni ciągłość ochrony systemów zabezpieczających Zamawiającego.
6. Wykonawca wykona projekt wdrożenia i konfiguracji dostarczanego rozwiązania, który zostanie zaakceptowany przez przedstawiciela Zamawiającego. Uruchomienie dostarczanego rozwiązania odbędzie się w oparciu o projekt konfiguracji oraz projekt polityki bezpieczeństwa wraz z integracją z istniejącymi rozwiązaniami wykorzystywanymi przez Zamawiającego.
7. Wykonawca zapewni usługę wdrożenia nowego rozwiązania polegającą w szczególności na:
   - instalacji i uruchomieniu urządzeń w infrastrukturze Zamawiającego
   - migracji obecnej konfiguracji, w szczególności polityk i zasad zabezpieczeń (w odniesieniu do WAF dotyczy także wykluczeń i wyjątków stosowanych dla predefiniowanych sygnatur)

- konfiguracji, optymalizacji i uruchomieniu posiadanych przez urządzenie dostępnych funkcji bezpieczeństwa (takich jak AV, IPS, Anty-spam etc.)
- podłączeniu i konfiguracji innych urządzeń współpracujących z nowo instalowanymi (migracja i podłączenie AP do nowego kontrolera WiFi)
- wsparcia technicznego w obsłudze nowych urządzeń

8. Wykonawca zapewni przeszkolenie z dostarczanego rozwiązania dla minimum trzech osób od strony Zamawiającego przeprowadzone przez certyfikowanego inżyniera producenta. Szkolenie swoim zakresem będzie obejmowało konfigurację oraz administrację urządzeniem. Szkolenie musi być przeprowadzone w języku polskim.

ROZDZIAŁ 3 – Wzór umowy
Umowa nr A-ZP.383….2024

zawarta w dniu ..... w Szczecinie pomiędzy:

Uniwersytetem Szczecińskim, z siedzibą przy ul. Papieża Jana Pawła II nr 22a, 70-453 Szczecin, NIP 851-020-80-05, reprezentowanym przez:
- .....
- .....

zwanym dalej w treści umowy ***Zamawiającym,***

a.....
reprezentowanym przez:
.....
zwanym dalej w treści umowy ***Wykonawcą.***

W wyniku przeprowadzonego postępowania nr **A-ZP.381.23.2024.WB** w trybie podstawowym, zgodnie z Ustawą z dnia 11 września 2019 r. Prawo Zamówień Publicznych (Dz. U. z 2023 r., poz. 1605) – dalej PZP, zawarta została umowa następującej treści:

§ 1

1. Przedmiotem niniejszej umowy jest modernizacja systemu zabezpieczającego dostęp do infrastruktury sieciowej oraz jej monitorowania w zakresie bezpieczeństwa oraz zakup usługi rocznego serwisu i subskrypcji bezpieczeństwa dla posiadanych przez Uniwersytet Szczeciński urządzeń firmy Fortinet zgodnie z Rozdziałem 2 SWZ oraz złożoną ofertą (odpowiednio załącznik nr 1 oraz 2 do umowy) wraz z instalacją na pracującym sprzęcie ***Zamawiającego*.**
2. Wykonawca zapewni usługę wdrożenia nowego rozwiązania polegającą w szczególności na:
   1) instalacji i uruchomieniu urządzeń w infrastrukturze Zamawiającego
   2) migracji obecnej konfiguracji, w szczególności polityk i zasad zabezpieczeń (w odniesieniu do WAF dotyczy także wykluczeń i wyjątków stosowanych dla predefiniowanych sygnatur)
   3) konfiguracji, optymalizacji i uruchomieniu posiadanych przez urządzenie dostępnych funkcji bezpieczeństwa (takich jak AV, IPS, Anty-spam etc.)
   4) podłączeniu i konfiguracji innych urządzeń współpracujących z nowo instalowanymi (migracja i podłączenie AP do nowego kontrolera WiFi)
   5) wsparcia technicznego w obsłudze nowych urządzeń
3. Wykonawca nieodpłatnie zapewni, w terminie uzgodnionym przez Strony, nie później jednak niż do 30.09.2024 r., przeszkolenie z dostarczanego rozwiązania dla minimum trzech osób od strony Zamawiającego przeprowadzone przez certyfikowanego inżyniera producenta.

Szkolenie swoim zakresem będzie obejmowało konfigurację oraz administrację urządzeniem. Szkolenie musi być przeprowadzone w języku polskim.

4. Zakres rzeczowy przedmiotu umowy oraz warunki gwarancji określa Rozdział 2 SWZ oraz oferta ***Wykonawcy*** (odpowiednio załącznik nr 1 oraz 2 do umowy).
5. ***Wykonawca*** gwarantuje wykonanie przedmiotu zamówienia o którym mowa w ust. 1 w terminie do 30 dni kalendarzowych od podpisania umowy.
6. Przed przystąpieniem do wykonania przedmiotu zamówienia, Wykonawca wykona i przedstawi Zamawiającemu w formie pisemnej lub elektronicznej projekt wdrożenia i konfiguracji dostarczanego rozwiązania, który zostanie zaakceptowany przez przedstawiciela Zamawiającego. Uruchomienie dostarczanego rozwiązania odbędzie się w oparciu o projekt konfiguracji oraz projekt polityki bezpieczeństwa wraz z integracją z istniejącymi rozwiązaniami firewall Zamawiającego.
7. Zamawiający w terminie 7 dni od daty otrzymania przedmiotu umowy, o którym mowa w ust. 1 dokona jego weryfikacji, w szczególności w zakresie kompletności i zapewnienia bezpieczeństwa i ochrony sieci komputerowej. Zamawiający może złożyć oświadczenie stwierdzające wady lub braki przedmiotu umowy, o którym mowa w ust. 1, powstałe z przyczyn leżących po stronie Wykonawcy lub złoży oświadczenie o braku uwag do przekazanego przedmiotu umowy.
8. W razie wystąpienia wad lub braków, o których mowa w ust. 7 ich usunięcie przez Wykonawcę nastąpi w terminie 2 dni od daty otrzymania przez Wykonawcę zawiadomienia w tej sprawie od Zamawiającego. Zamawiający dokona ponownej weryfikacji poprawionego przedmiotu Umowy zgodnie z zapisami ust. 4, przy czym Wykonawca zobowiązany jest w celu ponownej weryfikacji przekazać przedmiot umowy na własny koszt, niezależnie od ilości ponownych weryfikacji.
9. ***Wykonawca*** gwarantuje ***Zamawiającemu*** odnowienie licencji, o których mowa w ust. 1 na okres **12 miesięcy od dnia wygaśnięcia aktualnie obowiązującej umowy.**

§ 2

1. Przedmiot umowy określony w § 1 ust. 1 dostarczony, zainstalowany i wdrożony będzie ***Zamawiającemu*** na koszt i ryzyko ***Wykonawcy.*** Potwierdzeniem realizacji przedmiotu umowy określonego w § 1 ust. 1 będzie dostarczenie, montaż i konfiguracja sprzętu potwierdzona obustronnie podpisanym protokołem odbioru oraz stosownego dokumentu potwierdzającego odnowienie licencji oprogramowania i licencji serwisowych.
2. W okresie obowiązywania licencji ***Wykonawca*** zobowiązuje się do świadczenia niezbędnej asysty technicznej na rzecz ***Zamawiającego.***
3. Potwierdzeniem należytego wykonania umowy w zakresie § 1 ust. 1 jest podpisanie obustronnie protokołu odbioru bez uwag.

§ 3

1. Całkowite wynagrodzenie Wykonawcy za wykonanie przedmiotu umowy, wynosi …….. zł netto (słownie netto: ……..), powiększone o podatek VAT w stawce obowiązującej, tj. …….. zł brutto (słownie brutto: …….).
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty związane z realizacją przedmiotu umowy. Wykonawcy nie przysługuje zwrot od Zamawiającego jakichkolwiek kosztów, opłat i podatków poniesionych przez Wykonawcę w związku z realizacją przedmiotu umowy.
3. ***Wykonawca*** nie ma prawa zbywania wierzytelności wynikających z niniejszej umowy osobom trzecim bez zgody ***Zamawiającego*** wyrażonej na piśmie.

§ 4

Zamawiający zobowiązany jest do zapłaty ceny przelewem, na konto ***Wykonawcy*** w banku: **…….** na rachunek: **…….** w terminie **…. dni** od daty otrzymania faktury oraz obustronnie podpisanymi protokołami odbioru. Wykonawca uprawniony jest do wystawienia faktury po wykonaniu całości przedmiotu określonego w § 1 ust. 1.

§ 5

W sprawach związanych z realizacją niniejszej umowy ***Zamawiającego*** reprezentować będzie:

- **mgr Rafał Skorasiński tel. 91 444 11 79, kom. 512 053 887**
- **mgr inż. Rafał Mikulak tel. 91 444 10 15, kom. 571 601 170**

Wykonawcę reprezentować będzie:

- …….. **tel.** ……..…….

§ 6

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   1) w przypadku, gdy Wykonawca dopuszcza się zwłoki w terminowym wykonaniu obowiązków określonych w § 1 ust. 3, 5 lub 7 Umowy − w wysokości 0,2 % całkowitego wynagrodzenia netto określonego w § 3 ust. 1 Umowy za każdy dzień zwłoki, przy czym kara umowna będzie naliczana odrębnie za każdy przypadek zwłoki, nie więcej jednak niż 50% całkowitego wynagrodzenia netto, o którym mowa w § 3 ust. 1 umowy;
   2) z tytułu odstąpienia od umowy przez ***Zamawiającego*** z powodu okoliczności, o których mowa w § 7 ust. 1 lub rozwiązania umowy z przyczyn leżących po stronie ***Wykonawcy*** (niezależnych od ***Zamawiającego),*** w wysokości 10% całkowitego wynagrodzenia netto określonego w § 3 ust. 1;
   3) w przypadku odstąpienia od umowy przez ***Wykonawcę*** z przyczyn niezależnych od ***Zamawiającego,*** w wysokości 10% całkowitego wynagrodzenia netto, o którym mowa w § 3 ust. 1.
2. Kary umowne stają się wymagalne w pierwszym dniu kiedy możliwe jest ich naliczenie, a w przypadku kar za zwłokę z każdym dniem.
3. Łączna maksymalna wysokość kar umownych, które Zamawiający może naliczyć Wykonawcy ograniczona jest do 50% całkowitego wynagrodzenia netto określonego w § 3 ust. 1.
4. W przypadku poniesienia szkody przewyższającej karę umowną Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego.
5. Naliczoną karę umowną Zamawiający może potrącić z wynagrodzenia określonego w § 3 ust. 1, informując o tym Wykonawcę na piśmie, na co Wykonawca wyraża zgodę.

§ 7

1. ***Zamawiający*** może odstąpić od umowy jeżeli ***Wykonawca*** nie wykonuje lub nienależycie wykonuje umowę. W takiej sytuacji ***Zamawiający*** przed odstąpieniem od umowy wzywa ***Wykonawcę*** do zmiany sposobu realizacji umowy wyznaczając mu odpowiedni termin, z zastrzeżeniem, że po upływie wyznaczonego terminu odstąpi od umowy. ***Zamawiający*** odstąpi od umowy w ciągu 14 dni od bezskutecznego upływu wyznaczonego ***Wykonawcy*** terminu.
2. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
3. W przypadku odstąpienia od umowy przez Zamawiającego z powodu okoliczności, o których mowa w ust. 1 Wykonawca może żądać wyłącznie wynagrodzenia należnego mu z tytułu wykonania części umowy, bez prawa dochodzenia odszkodowania z tego tytułu.

§ 8

Strony podają jako adresy do korespondencji adresy wskazane we wstępie do niniejszej umowy. Każda ze Stron zobowiązana jest do powiadomienia drugiej strony o zmianie adresu. W przypadku zaniechania zawiadomienia, skuteczne jest skierowanie oświadczenia na ostatni znany drugiej stronie adres.

§ 9

1. Wszelkie zmiany warunków niniejszej Umowy wymagają formy pisemnej, pod rygorem nieważności.
2. W sprawach nie uregulowanych postanowieniami niniejszej Umowy zastosowanie mają odpowiednie przepisy PZP oraz *Kodeksu Cywilnego.*
3. Wszelkie ewentualne spory mogące wyniknąć na tle niniejszej Umowy, których nie będzie można rozstrzygnąć polubownie, rozpatrywane będą przez właściwy rzeczowo sąd powszechny według siedziby Zamawiającego.
4. Załączniki do niniejszej Umowy stanowiącej integralną część.
5. Umowa niniejsza podlega prawu polskiemu.
6. Umowa została sporządzona w formie elektronicznej.

Signature Not Verified
Dokument podpisany przez Wojciech Jerzy Bereszko
Data: 2024.05.22 09:54:37 CEST

.....

/Dział Zamówień Publicznych/

Specyfikację warunków zamówienia zatwierdzam.

Andrzej Stanisław Jakubowski

Elektronicznie podpisany przez Andrzej Stanisław Jakubowski
Data: 2024.05.22 14:04:19 +02'00'

Szczecin, ...

.....

/Zamawiający/