KOMENDA GŁÓWNA STRAŻY GRANICZNEJ
BIURO FINANSÓW
ZAMÓWIENIA PUBLICZNE
00-463 Warszawa, ul. Podchorążych 38
tel. +48 22 5004372, +48 22 5004387, +48 22 5004436
fax: +48 22 5004782, +48 22 5004707

Numer sprawy 14/BF/BŁiI/17

„ZATWIERDZAM"
ZASTĘPCA DYREKTORA
Biura Finansów
Komendy Głównej Straży Granicznej
płk SG Jarosław KORLAK
04.05.2017r
Komendant Główny
Straży Granicznej

KOMENDA GŁÓWNA
STRAŻY GRANICZNEJ
BIURO FINANSÓW
Nr 1794
Wpłynęło 2017 - 05
Zał. 7 Str. 128

S P E C Y F I K A C J A
ISTOTNYCH WARUNKÓW ZAMÓWIENIA
(SIWZ)

D o t y c z y: **Przetargu nieograniczonego**
dla zamówienia o wartości powyżej 135 000 euro
ogłoszonego przez Komendanta Głównego Straży Granicznej
na realizację zamówienia pn:

„Rozbudowa systemu telekomunikacyjnego
Straży Granicznej"

Warszawa – 2017r.

Komendant Główny Straży Granicznej zaprasza do udziału w postępowaniu prowadzonym w trybie przetargu nieograniczonego na realizację zamówienia pn: **„Rozbudowa systemu telekomunikacyjnego Straży Granicznej"**. Wykonawca wyłoniony w procedurze przetargu nieograniczonego zrealizuje zamówienie w sposób zgodny z wymaganiami Zamawiającego określonymi w niniejszej Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej SIWZ.

I. INFORMACJE OGÓLNE:

1. Do udzielenia przedmiotowego zamówienia stosuje się przepisy ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (tekst jednolity Dz. U. z 2015 r. poz. 2164 z późn. zm.), zwanej dalej ustawą Pzp oraz akty wykonawcze wydane na jej podstawie.
2. Do czynności podejmowanych przez Zamawiającego i Wykonawców w postępowaniu o udzielenie zamówienia publicznego stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (tekst jednolity Dz. U. z 2017 r. poz. 459 z późn. zm.), jeżeli przepisy ustawy Pzp nie stanowią inaczej.
3. Postępowanie o udzielenie zamówienia publicznego prowadzi się w języku polskim (art. 9 ust. 2 ustawy Pzp).
4. Realizacja zamówienia będzie odbywać się zgodnie z przepisami prawa obowiązującymi na terytorium Rzeczpospolitej Polskiej.
5. Niniejsze zamówienie objęte jest postanowieniami Porozumienia w sprawie zamówień rządowych (Government Procurement Agreement – GPA) zawartego w ramach Światowej Organizacji Handlu (World Trade Organization – WTO).
6. Zgodnie z art. 9 ust. 3 ustawy Pzp Zamawiający dopuszcza złożenie oferty zawierającej terminologię w języku angielskim w zakresie, w jakim została ona użyta przez Zamawiającego w Opisie Przedmiotu Zamówienia (OPZ) tzn. przy użyciu określeń zastosowanych przez Zamawiającego lub określeń równoważnych.

II. NAZWA I ADRES ZAMAWIAJĄCEGO:

KOMENDA GŁÓWNA STRAŻY GRANICZNEJ
02-514 Warszawa, Al. Niepodległości 100
REGON: 013008431
NIP: PL 5212921032, jako podatnika VAT UE

Adres do korespondencji:

Komenda Główna Straży Granicznej
Biuro Finansów - Zamówienia Publiczne
00-463 Warszawa, ul. Podchorążych 38

tel. +48 225004372, +48 225004387, +48 225004436;
faks: +48 225004782, +48 225004707

Informacje związane z przedmiotowym postępowaniem objęte ustawowym wymogiem zamieszczania na stronie internetowej Zamawiającego będą udostępniane pod adresem: www.strazgraniczna.pl

III. TRYB UDZIELENIA ZAMÓWIENIA:

Postępowanie prowadzone jest w trybie przetargu nieograniczonego, w którym w odpowiedzi na publiczne ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy.

IV. OPIS PRZEDMIOTU ZAMÓWIENIA:

1. Przedmiotowe zamówienie jest podzielone na dwie części, **przy czym w ramach realizacji części 1 zamówienia Zamawiający przewiduje możliwość skorzystania z prawa opcji**.
2. **Wykonawca może złożyć ofertę na jedną lub dwie części zamówienia**.
3. **Część 1 zamówienia składa się z**:
   1) **zamówienia podstawowego**, które będzie realizowane w dwóch etapach,

      przy czym:

      a) **Etap pierwszy** będzie obejmował dostawę urządzeń sieciowych (wraz z oprogramowaniem, licencjami i gwarancją) do jednostek organizacyjnych Straży Granicznej (w tym wdrożenie niektórych z dostarczonych urządzeń w Bieszczadzkim Oddziale Straży Granicznej) oraz przeprowadzenie szkoleń z obsługi tych urządzeń.

      Wykaz jednostek organizacyjnych objętych Etapem pierwszym zamówienia wraz informacją na temat rodzajów urządzeń, które będą dostarczone do tych jednostek w ramach realizacji tego etapu zamówienia określono w punkcie **1** Załącznika nr 1 do OPZ.

      b) **Etap drugi** będzie obejmował dostawę urządzeń sieciowych (wraz z oprogramowaniem, licencjami i gwarancją) do jednostek organizacyjnych Straży Granicznej oraz przeprowadzenie szkoleń z obsługi tych urządzeń.

      Wykaz jednostek organizacyjnych objętych Etapem drugim zamówienia wraz z informacją na temat rodzajów urządzeń, które będą dostarczane do tych jednostek w ramach realizacji tego etapu zamówienia określono w punkcie **2** Załącznika nr 1 do OPZ.

   2) **zamówienia objętego prawem opcji** – które będzie realizowane przez Wykonawcę wyłącznie w przypadku skorzystania przez Zamawiającego z prawa opcji. Zamówienie to będzie obejmowało dostawę urządzeń sieciowych (wraz z oprogramowaniem, licencjami i gwarancją) do jednostek organizacyjnych Straży Granicznej oraz przeprowadzenie szkoleń z obsługi tych urządzeń.

      Wykaz jednostek organizacyjnych, do których będą dostarczane urządzenia w ramach realizacji zamówienia objętego prawem opcji wraz z informacją na temat rodzajów urządzeń, które będą dostarczane do tych jednostek w ramach realizacji prawa opcji określono w punkcie **3** Załącznika nr 1 do OPZ

   Dostarczone w ramach realizacji części 1 zamówienia urządzenia, oprogramowanie i licencje muszą być objęte co najmniej 48 miesięczną gwarancją,

   przy czym:

   - gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach realizacji Etapu pierwszego zamówienia rozpocznie swój bieg od dnia podpisania przez Strony Protokółu Odbioru urządzeń (oprogramowania, licencji) dostarczonych do tej jednostki organizacyjnej;
   - gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach realizacji Etapu drugiego zamówienia rozpocznie swój bieg od dnia podpisania przez Strony Protokółu Odbioru urządzeń (oprogramowania, licencji) dostarczonych do tej jednostki organizacyjnej;

- gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach zamówienia objętego prawem opcji rozpocznie swój bieg od dnia podpisania przez Strony Protokółu Odbioru urządzeń (oprogramowania, licencji) dostarczonych do tej jednostki organizacyjnej.

Gwarancja musi zapewniać m. in. wymianę uszkodzonego sprzętu, a także pobieranie poprawek i aktualizacji oprogramowania (zarówno update jak i upgrade) oraz aktualnych sygnatur dla urządzeń IPS w okresie trwania umowy.

Długość okresu gwarancji udzielonej na dostarczone urządzenia stanowi jedno z kryteriów oceny ofert w części 1 zamówienia.

Szczegółowe informacje dotyczące warunków realizacji **części 1 zamówienia** zawarto **w punkcie A OPZ** stanowiącego Załącznik nr 1 do SIWZ.

2. **Część 2 zamówienia obejmuje**:

   1) świadczenie przez Wykonawcę przez okres 36 miesięcy gwarancji na wskazane przez Zamawiającego urządzenia, licencje i oprogramowanie obecnie eksploatowane przez Straż Graniczną.

      Wykaz sprzętu, który zostanie przez Wykonawcę objęty gwarancją producenta zawarto w Załączniku nr **3** do OPZ.

   2) świadczenie przez Wykonawcę przez okres 36 miesięcy zaawansowanego wsparcia technicznego dla jednostek organizacyjnych Zamawiającego przy rozwiązywaniu problemów i administrowaniu systemem telekomunikacyjnym Straży Granicznej;

   3) przeprowadzenie szkoleń dla pracowników Zamawiającego.

   Szczegółowe informacje dotyczące warunków realizacji **części 2 zamówienia** zawarto **w punkcie B OPZ** stanowiącego Załącznik nr 1 do SIWZ.

3. Wykonawca wyłoniony w trakcie procedury udzielenia zamówienia publicznego zobowiązany jest do realizacji przedmiotu zamówienia zgodnie z wymaganiami określonymi w niniejszej SIWZ (stosownie do zakresu przedmiotowego złożonej przez niego oferty).

4. Przedmiot zamówienia został oznaczony we Wspólnym Słowniku Zamówień następującymi kodami CPV:

   dotyczy części **1** zamówienia

   32.52.20.00 – 8 – sprzęt telekomunikacyjny
   32.52.30.00 – 5 – urządzenia telekomunikacyjne
   50.00.00.00 – 5 – usługi naprawcze i konserwacyjne
   50.33.00.00 – 7 – usługi w zakresie konserwacji sprzętu telekomunikacyjnego
   50.33.20.00 – 1 – usługi w zakresie konserwacji infrastruktury telekomunikacyjnej
   80.53.12.00 – 7 – usługi szkolenia technicznego
   48.00.00.00 – 8 – pakiety oprogramowania i systemy informatyczne

   dotyczy części **2** zamówienia

   50.00.00.00 – 5 – usługi naprawcze i konserwacyjne
   50.33.00.00 – 7 – usługi w zakresie konserwacji sprzętu telekomunikacyjnego

50.33.20.00 – 1 – usługi w zakresie konserwacji infrastruktury telekomunikacyjnej
72.22.00.00 – 3 – usługi doradcze w zakresie systemów i doradztwo techniczne
72.00.00.00 – 5 – usługi konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia
79.63.20.00 – 3 – szkolenie pracowników

5. **Zamawiający nie dopuszcza składania ofert wariantowych**.

6. Jeżeli w niniejszej SIWZ użyto parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę i mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych w stosunku do opisanych w SIWZ, pod warunkiem, że będą one posiadały, co najmniej takie same lub lepsze parametry techniczne i funkcjonalne i nie obniżą standardów określonych w SIWZ. Wykonawca powołujący się na rozwiązania równoważne do opisywanych przez Zamawiającego, zobowiązany jest załączyć do oferty dokładny opis oferowanych rozwiązań/produktów i/lub inne dokumenty, z których wynikać będzie zachowanie warunków równoważności. Zaproponowane rozwiązania/produkty równoważne muszą być opisane na tyle szczegółowo, żeby Zamawiający przy ocenie oferty mógł ocenić spełnienie wymagań dotyczących parametrów technicznych oferowanych rozwiązań oraz rozstrzygnąć, czy zaproponowane rozwiązania/produkty są równoważne. Zgodnie z art. 30 ust. 5 ustawy Pzp na Wykonawcy spoczywa obowiązek wykazania, że zaoferowane przez niego rozwiązania/produkty są równoważne w stosunku do opisanych przez Zamawiającego.

7. Jeżeli Wykonawca przewiduje udział podwykonawców w realizacji zamówienia wówczas jest on zobowiązany do wskazania w ofercie zakresu zamówienia (w ramach części zamówienia objętej ofertą Wykonawcy), którego wykonanie powierzy podwykonawcom oraz firm tych podwykonawców (art. 36b ust. 1 ustawy Pzp). W przypadku powierzenia podwykonawcy do realizacji określonego zakresu zamówienia, Wykonawca ponosi odpowiedzialność za działania podwykonawcy jak za własne.

   Jeżeli Wykonawca nie zamieści w ofercie ww. informacji wówczas Zamawiający uzna, że Wykonawca zrealizuje zamówienie bez udziału podwykonawców.

V. INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 67 UST. 1 PKT 6 i 7 USTAWY PZP

Zamawiający nie przewiduje możliwości udzielenia zamówienia na podstawie art. 67 ust. 1 pkt 6 i 7 ustawy Pzp.

VI. TERMIN I MIEJSCE WYKONANIA ZAMÓWIENIA:

1. **Część 1 zamówienia** zostanie zrealizowana przez Wykonawcę w następujących terminach:

   1) zamówienie podstawowe:

      a) Etap pierwszy – w terminie do dnia **11.12.2017r**.
      b) Etap drugi – w terminie do dnia **28.09.2018r**.

   2) zamówienie objęte prawem opcji:

      W przypadku skorzystania z prawa opcji Zamawiający przekaże Wykonawcy stosowne oświadczenie w formie pisemnej do dnia 31.01.2018r.
      Wówczas Wykonawca zrealizuje zamówienie objęte prawem opcji do dnia **28.09.2018r**.

Zamawiający zastrzega sobie prawo do wielokrotnego złożenia oświadczenia o skorzystaniu z prawa opcji z tym, że całkowita liczba dostarczonych w ramach opcji urządzeń nie przekroczy ilości wskazanych w punkcie 3 Załącznika nr 1 do OPZ.

Szczegółowe zasady korzystania z prawa opcji określono w projekcie umowy stanowiącym Załącznik nr 3 do SIWZ.

3) Miejsce realizacji zamówienia:

a) Etap pierwszy:
- Nadodrzański Oddział Straży Granicznej,
- Bieszczadzki Oddział Straży Granicznej,
- Karpacki Oddział Straży Granicznej,
- Komenda Główna Straży Granicznej,

b) Etap drugi:
- Śląski Oddział Straży Granicznej,
- Podlaski Oddział Straży Granicznej,
- Ośrodek Szkoleń Specjalistycznych Straży Granicznej w Lubaniu,
- Nadwiślański Oddział Straży Granicznej,
- Komenda Główna Straży Granicznej (Centralny Węzeł Teleinformatycznego (CWT),
- Centralny Ośrodek Szkolenia Straży Granicznej,

c) zamówienie objęte prawem opcji:
- Warmińsko-Mazurski Oddział Straży Granicznej,
- Morski Oddział Straży Granicznej,
- Nadbużański Oddział Straży Granicznej,

przy czym adresy jednostek organizacyjnych do których będą realizowane dostawy zawarto w Załączniku nr 2 do OPZ.

2. **Część 2 zamówienia** zostanie zrealizowana przez Wykonawcę w następujących terminach:

1) Wykonawca w terminie do 14 dni od daty zawarcia umowy dostarczy zaświadczenie producenta o objęciu gwarancją wskazanych przez Zamawiającego urządzeń, licencji i oprogramowania obecnie eksploatowanych przez Straż Graniczną;

2) Wykonawca będzie realizował wsparcie techniczne dla systemu telekomunikacyjnego Straży Granicznej, a także będzie świadczył gwarancję dla wskazanych przez Zamawiającego urządzeń przez okres 36 miesięcy licząc od dnia przekazania Zamawiającemu zaświadczenia o wykupieniu przez Wykonawcę gwarancji producenta, o której mowa w punkcie 1);

3) Wykonawca przeprowadzi szkolenia zgodnie z harmonogramem szkoleń, który zostanie przekazany Zamawiającemu w terminie 14 dni od daty zawarcia umowy;

4) Miejscem realizacji zamówienia w zakresie wsparcia technicznego będzie CWT, natomiast szkolenia muszą być przeprowadzone na terenie Warszawy w centrach szkoleniowych autoryzowanych przez producenta urządzeń posiadanych przez Zamawiającego.

VII. PODSTAWY WYKLUCZENIA I WARUNKI UDZIAŁU W POSTĘPOWANIU:

1. **dotyczy wszystkich Wykonawców**

O udzielenie zamówienia może ubiegać się Wykonawca, który nie podlega wykluczeniu z postępowania, w okolicznościach, o których mowa w:

1) art. 24 ust. 1 pkt 12) – 23) ustawy Pzp;
2) art. 24 ust. 5 pkt 1), 2) i 4) ustawy Pzp, przy czym wykluczeniu na tej podstawie podlega Wykonawca:
   a) w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015r. – Prawo restrukturyzacyjne (Dz. U. z 2015r. poz. 978, 1259, 1513, 1830 i 1844 oraz z 2016r. poz. 615) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003r. – Prawo upadłościowe (Dz. U. z 2015r. poz. 233, 978, 1166, 1259 i 1844 oraz z 2016r. poz. 615),
   b) 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 środków dowodowych,
   c) który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z Zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4 ustawy Pzp, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania.

Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16–20, lub ust. 5 pkt 1, 2 i 4 ustawy Pzp może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu Wykonawcy.

Przedstawienie dowodów nie ma zastosowania wobec Wykonawcy, będącego podmiotem zbiorowym, wobec którego orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.

2. **dotyczy wyłącznie Wykonawców ubiegających się o udzielenie części 2 zamówienia**

O udzielenie zamówienia może się ubiegać Wykonawca, który spełnia określony poniżej warunek udziału w postępowaniu dotyczący zdolności technicznej/zawodowej:

Minimalny poziom wymaganych zdolności:

Zamawiający uzna, że Wykonawca posiada wymagane zdolności techniczne/zawodowe zapewniające należyte wykonanie zamówienia, jeżeli Wykonawca wykaże, że:

dysponuje lub będzie dysponował co najmniej **trzema** inżynierami Network Consulting Engineer Cisco Advanced Services, którzy będą odpowiedzialni w trakcie realizacji zamówienia za świadczenie wsparcia technicznego dla systemu telekomunikacyjnego Straży Granicznej,

w tym:

- jednym inżynierem producenta z certyfikatem co najmniej Cisco Certified Internetwork Expert – CCIE Routing&Switching lub równoważnym,
- jednym inżynierem producenta ze stopniem certyfikacji dla bezpieczeństwa co najmniej Cisco Certified Internetwork Expert – CCIE Security lub równoważnym,
- jednym inżynierem producenta z certyfikatem co najmniej Cisco Certified Internetwork Expert – CCIE Voice lub równoważnym.

Jednocześnie Zamawiający wymaga, aby ww. inżynierowie mieli bezpośredni dostęp do wewnętrznych baz danych producenta oraz do ekspertów technicznych w celu zapewnienia skutecznej diagnostyki sieci oraz szybkiej reakcji na awarie, a w szczególności muszą oni posiadać:

1) bezpośredni dostęp do zasobów stanowiących własność intelektualną producenta, przy czym zakres dostępu musi obejmować co najmniej wewnętrzną bazę wiedzy producenta na temat konfiguracji, wewnętrzną bazę danych na temat błędów w oprogramowaniu, bazę wiedzy producenta (Technical Knowledge Library),
2) możliwość bezpośredniej zmiany priorytetów i kolejkowania zgłoszeń serwisowych,
3) dostęp pozwalający na uzupełnianie i zmianę numerów seryjnych urządzeń w bazach danych producenta

Ponadto każda z ww. osób musi posiadać poświadczenie bezpieczeństwa lub pisemne upoważnienie do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone" wydane przez kierownika jednostki organizacyjnej Wykonawcy, jeżeli osoba nie posiada poświadczenia bezpieczeństwa oraz zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych i ochrony danych osobowych.

Potencjał podmiotu trzeciego:

1) Wykonawca może w celu potwierdzenia spełniania ww. warunku udziału w postępowaniu, polegać na zdolnościach technicznych/zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2) Wykonawca, który polega na zdolnościach innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.
3) W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi, do realizacji których te zdolności są wymagane.

Ocena spełnienia wymagań określonych w punktach 1 i 2 niniejszego rozdziału SIWZ zostanie dokonana zgodnie z formułą spełnia/nie spełnia w oparciu o treść dokumentów i oświadczeń dostarczonych przez Wykonawcę. **W przypadku nie spełnienia ww. wymagań, Wykonawca zostanie wykluczony z postępowania, a jego oferta zostanie odrzucona zgodnie z art. 89 ust. 1 pkt 5 ustawy Pzp.**

VIII. WYKAZ OŚWIADCZEŃ I DOKUMENTÓW POTWIERDZAJĄCYCH BRAK PODSTAW DO WYKLUCZENIA WYKONAWCY ORAZ SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU JAKIE MUSZĄ DOSTARCZYĆ WYKONAWCY

Na podstawie art. 24aa ustawy Pzp Zamawiający dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

1. W celu wstępnego potwierdzenia, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu, **Wykonawca jest zobowiązany do dostarczenia wraz z ofertą**:

   1) aktualnego na dzień składania ofert **oświadczenie w formie jednolitego dokumentu** sporządzonego zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust. 3 dyrektywy 2014/25/UE, zwanego dalej **Jednolitym Europejskim Dokumentem Zamówienia lub „JEDZ"**;

      Zamawiający informuje, że Instrukcję wypełnienia „**JEDZ**" oraz edytowalną wersję formularza „**JEDZ**" można znaleźć pod adresem:

      https://www.uzp.gov.pl/baza-wiedzy/jednolity-europejski-dokument-zamowienia

      przy czym,

      - w przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, „**JEDZ**" składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu lub brak podstaw wykluczenia,
      - Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec tych podmiotów podstaw wykluczenia oraz spełniania przez te podmioty warunków udziału w postępowaniu, w zakresie w jakim Wykonawca powołuje się na ich zasoby, jest zobowiązany do złożenia „**JEDZ**"-**ów** dotyczących tych podmiotów,
      - Wykonawca może wykorzystać w „**JEDZ**" nadal aktualne informacje zawarte w innym „**JEDZ**" złożonym w odrębnym postępowaniu o udzielenie zamówienia prowadzonym przez Zamawiającego. W takim przypadku Wykonawca wskazuje w formularzu oferty: numer i nazwę oraz datę wszczęcia tego postępowania oraz zakres informacji do wykorzystania,
      - ww. oświadczenia („**JEDZ**"/„**JEDZ**"-e) należy złożyć w oryginale

   2) zobowiązania podmiotu trzeciego do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia – jeżeli Wykonawca będzie polegał na zasobach innych podmiotów w celu potwierdzenia spełniania warunku udziału w postępowaniu, określonego w rozdziale VII pkt 2 niniejszej SIWZ,

przy czym:

- ww. oświadczenie musi być złożone w formie oryginału lub kopii poświadczonej notarialnie;

Przykładowy wzór zobowiązania podmiotu trzeciego do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia wskazano w Załączniku nr 4 do niniejszej SIWZ.

3) odpowiednich pełnomocnictw – jeżeli mają zastosowanie zapisy zawarte w rozdziale XII pkt 12 SIWZ i w rozdziale XII pkt 14 niniejszej SIWZ w związku z art. 23 ust. 2 ustawy Pzp,

przy czym:

- ww. oświadczenia muszą być złożone w formie oryginału lub kopii poświadczonej notarialnie;

2. **Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni, aktualnych na dzień złożenia**:

1) **oświadczeń i dokumentów na potwierdzenie, że Wykonawca nie podlega wykluczeniu z postępowania z powodów określonych w rozdziale VII pkt 1 niniejszej SIWZ, tj.**:

a) **informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy Pzp** - wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert

przy czym,

- w przypadku wspólnego ubiegania się Wykonawców o zamówienie ww. informację składa każdy z Wykonawców składających ofertę wspólną
- ww. dokument należy złożyć w oryginale lub kopii potwierdzonej za zgodność z oryginałem

b) **oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienie publiczne**

przy czym,

- w przypadku składania oferty wspólnej ww. informację składa każdy z Wykonawców składających ofertę wspólną
- ww. oświadczenie należy złożyć w oryginale
- wzór ww. oświadczenia stanowi Załącznik nr 5 do niniejszej SIWZ;

c) **oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne** albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności

przy czym,

- w przypadku składania oferty wspólnej ww. dokumenty składa każdy z Wykonawców składających ofertę wspólną
- ww. oświadczenie należy złożyć w oryginale
- wzór ww. oświadczenia stanowi Załącznik nr 6 do niniejszej SIWZ

d) **odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej**, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw do wykluczenia na podstawie **art. 24 ust. 5 pkt 1** ustawy Pzp

przy czym,

- w przypadku wspólnego ubiegania się Wykonawców o zamówienie ww. odpis składa każdy z Wykonawców składających ofertę wspólną;
- ww. dokument należy złożyć w oryginale lub kopii potwierdzonej za zgodność z oryginałem

Jeżeli Wykonawca, w celu potwierdzenia spełniania warunku udziału w postępowaniu określonego w rozdziale VII pkt 2 niniejszej SIWZ, polega na zasobach innych podmiotów, wówczas Zamawiający wymaga od Wykonawcy przedstawienia w odniesieniu do tych podmiotów dokumentów, o których mowa w rozdziale VIII pkt 2 ppkt 1 lit. a), b), c) i d).

2) **oświadczeń i dokumentów na potwierdzenie, że Wykonawca spełnia warunek udziału w postępowaniu określony w rozdziale VII pkt 2 niniejszej SIWZ, tj.**:

a) wykazu osób, które zostaną skierowane przez Wykonawcę do realizacji zamówienia odpowiedzialnych za świadczenie usługi wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami

przy czym

- ww. oświadczenie (wykaz) należy złożyć w oryginale
- wzór ww. wykazu zawarto w Załączniku nr 7 do SIWZ.
- **ww. oświadczenie (wykaz) składają wyłącznie Wykonawcy ubiegający się o część 2 zamówienia**.

3. **Ponadto Wykonawca jest zobowiązany do złożenia w terminie 3 dni od dnia zamieszczenia przez Zamawiającego na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy Pzp „Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy z dnia 29 stycznia 2004r. – Prawo zamówień publicznych**",

przy czym:

- w przypadku składania oferty wspólnej ww. oświadczenie składa każdy z Wykonawców składających ofertę wspólną;
- ww. oświadczenie należy złożyć w oryginale
- wzór ww. oświadczenia zostanie zamieszczony na stronie internetowej Zamawiającego wraz z informacją, o której mowa w art. 86 ust. 5 ustawy Pzp.

Wykonawca składa powyższe oświadczenie na potwierdzenie, że nie podlega on wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 23 ustawy Pzp. W przypadku przynależności do tej samej grupy kapitałowej Wykonawca może złożyć wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym Wykonawcą, który złożył ofertę w przedmiotowym postępowaniu, nie prowadzą do zakłócenia konkurencji w postępowaniu.

4. **Zgodnie z § 7 Rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia** (**Dz. U. z 2016 r. poz. 1126**):

   1) **Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej**:

      a) zamiast dokumentów, o których mowa w rozdziale VIII pkt 2 ppkt 1) lit. a) niniejszej SIWZ składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy Pzp;

         Dokumenty te powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

      b) zamiast dokumentu, o którym mowa w rozdziale VIII pkt 2 ppkt 1) lit. d) niniejszej SIWZ składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości.

         Dokumenty te powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

   Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w punktach a) i b), zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy lub miejsce zamieszkania tej osoby.

   Dokument ten powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

   W przypadku wątpliwości co do treści dokumentu złożonego przez ww. Wykonawcę, Zamawiający może zwrócić się do właściwych organów odpowiednio kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

   2) **Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej**, której dotyczy dokument wskazany w rozdziale VIII pkt 2 ppkt 1) lit. a) niniejszej SIWZ, składa dokument, o którym mowa w rozdziale VIII pkt 4 ppkt 1) lit. a) niniejszej SIWZ, w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 ustawy Pzp. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby.

Dokument ten powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

W przypadku wątpliwości co do treści dokumentu złożonego przez tego Wykonawcę, Zamawiający może zwrócić się do właściwych organów kraju, w którym miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

5. **Wymagana forma składanych dokumentów**:
   1) oświadczenia dotyczące Wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 22a ustawy Pzp oraz dotyczące podwykonawców, składane są w oryginale;
   2) dokumenty inne niż oświadczenia, o których mowa w pkt. 1) składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem;
   3) poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą;
   4) poświadczenie za zgodność z oryginałem następuje w formie pisemnej;
   5) dokumenty sporządzone w języku obcym należy złożyć wraz z ich tłumaczeniem na język polski.
6. **Zasady dotyczące składania oświadczeń i dokumentów**:
   a) w przypadku wskazania przez Wykonawcę dostępności dokumentów, o których mowa w Rozdziale VIII SIWZ, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobierze samodzielnie z tych baz danych wskazane przez Wykonawcę dokumenty,
   b) w przypadku, o którym mowa w pkt a) Zamawiający będzie żądał od Wykonawcy przedstawienia tłumaczenia na język polski wskazanych przez Wykonawcę i pobranych samodzielnie przez Zamawiającego dokumentów,
   c) jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów,
   d) jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 25a ust. 1 ustawy Pzp, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy Pzp, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich złożenia, uzupełnienia, lub poprawienia lub do udzielenia wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy będzie podlegać odrzuceniu albo konieczne będzie unieważnienie postępowania,
   e) jeżeli Wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, Zamawiający wezwie do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlegać będzie odrzuceniu albo konieczne będzie unieważnienie postępowania,

f) w przypadku wątpliwości Zamawiający wezwie, w wyznaczonym przez siebie terminie, do złożenia wyjaśnień dotyczących oświadczeń i dokumentów, o których mowa w art. 25 ust. 1 ustawy Pzp,

g) jeżeli Wykonawca, którego oferta została oceniona jako najkorzystniejsza, będzie uchylał się od zawarcia umowy lub nie wniesie wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający będzie mógł zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu Wykonawca, który złożył ofertę najwyżej ocenioną spośród pozostałych ofert.

IX. OSOBY UPRAWNIONE DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI ORAZ INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI I PRZEKAZYWANIA OŚWIADCZEŃ ORAZ DOKUMENTÓW:

1. Osoby uprawnione przez Zamawiającego do porozumiewania się z Wykonawcami:
   - Jolanta Górzyńska-Gortat – Biuro Finansów KGSG - Zamówienia Publiczne - tel. 22 5004476 .
2. Zamawiający urzęduje w dni robocze, od poniedziałku do piątku w godzinach 8^{15}-16^{15}.
3. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawca przekazują **pisemnie**, z zastrzeżeniem pkt 4.
4. Zamawiający dopuszcza porozumiewanie się za pomocą:
   1) faksu, przy przekazywaniu następujących dokumentów:
      a) pytania Wykonawców i wyjaśnienia Zamawiającego dotyczące treści SIWZ,
      b) wezwanie Wykonawcy do wyjaśnienia treści oferty i odpowiedź Wykonawcy,
      c) wezwanie kierowane do Wykonawców na podstawie art. 26 ustawy Pzp,
      d) wezwanie do udzielenia wyjaśnień dotyczących elementów oferty mających wpływ na wysokość ceny oraz odpowiedź Wykonawcy,
      e) informacja o poprawieniu oferty na podstawie art. 87 ust. 2 ustawy Pzp,
      f) oświadczenie Wykonawcy w kwestii wyrażenia zgody na poprawienie innych omyłek na podstawie art. 87 ust. 2 pkt 3 ustawy Pzp,
      g) wezwanie skierowane przez Zamawiającego do Wykonawcy o wyrażenie zgody na przedłużenie terminu związania ofertą oraz odpowiedź Wykonawcy,
      h) oświadczenie Wykonawcy o przedłużeniu terminu związania ofertą,
      i) zawiadomienie o wyborze najkorzystniejszej oferty, zgodnie z art. 92 ust. 1 ustawy Pzp,
      j) zawiadomienie o unieważnieniu postępowania,
      k) informacje i zawiadomienia kierowane do Wykonawców na podstawie art. 181, 184 i 185 ustawy Pzp;
   2) Jeżeli Zamawiający lub Wykonawca przekazują ww. oświadczenia, wnioski, zawiadomienia oraz informacje faksem, każda ze Stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania. W przypadku przekazywania dokumentów faksem dowód transmisji danych oznacza, że Wykonawca otrzymał korespondencję w momencie jej przekazania przez Zamawiającego, niezależnie od ewentualnego potwierdzenia faktu jej otrzymania. Zamawiający nie ponosi odpowiedzialności za niesprawne działanie urządzeń Wykonawcy.
5. Zamawiający wymaga, aby wszelkie pisma związane z postępowaniem były kierowane wyłącznie na adres do korespondencji wskazany na pierwszej stronie niniejszej SIWZ.

6. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ. Zamawiający udzieli odpowiedzi na wszelkie pytania związane z prowadzonym postępowaniem niezwłocznie, jednak nie później niż **na 6 dni** przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
7. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu, o którym mowa w pkt. 6, lub będzie dotyczył udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
8. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w pkt. 6.
9. W uzasadnionych przypadkach, Zamawiający może przed upływem terminu składania ofert zmienić treść SIWZ. Dokonana zmianę treści SIWZ Zamawiający udostępni na stronie swojej internetowej.
10. Treść pytań wraz z wyjaśnieniami Zamawiający przekaże Wykonawcom, którym przekazał SIWZ, bez ujawniania źródła zapytania, a także zamieści je na swojej stronie internetowej (www.strazgraniczna.pl).

X. WYMAGANIA DOTYCZĄCE WADIUM:

1. Przystępując do przetargu Wykonawca, który składa ofertę na **dwie części przedmiotu zamówienia** zobowiązany jest wnieść **wadium w kwocie 419 000, 00 zł** (słownie: czterysta dziewiętnaście tysięcy zł 00/100) zaznaczając cel wpłaty.
2. W przypadku częściowego składania ofert wadium należy wnieść w kwotach podanych poniżej:
   a) składając ofertę na **część 1 zamówienia** – wadium należy wnieść w kwocie wynoszącej **340 000, 00 zł** (słownie: trzysta czterdzieści tysięcy zł 00/100),
   b) składając ofertę na **część 2 zamówienia** – wadium należy wnieść w kwocie wynoszącej **79 000, 00 zł** (słownie: siedemdziesiąt dziewięć tysięcy zł 00/100).
3. Wadium wnoszone w pieniądzu Wykonawca wpłaca przelewem na podany poniżej rachunek bankowy Zamawiającego (kserokopię dokumentu potwierdzającego dokonanie przelewu Wykonawca powinien dołączyć do oferty).

Komenda Główna Straży Granicznej
Narodowy Bank Polski Oddział Okręgowy w Warszawie
SWIFT: NBP LP LPW 12 1010 1010 0043 2713 9120 0000
z dopiskiem:
„Rozbudowa systemu telekomunikacyjnego Straży Granicznej" –
numer sprawy: 14/BF/BŁiI/17 – dotyczy części .....* zamówienia

* należy wpisać numer części zamówienia, na którą Wykonawca składa ofertę

Wadium musi być złożone lub wpłynąć na rachunek Zamawiającego przed upływem terminu składania ofert. Decyduje moment wpływu środków do Zamawiającego.

4. **Wadium** wnoszone w formie: poręczenia bankowego lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej (z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym), gwarancji bankowej, gwarancji ubezpieczeniowej lub poręczenia udzielanego przez Polską Agencję Rozwoju Przedsiębiorczości, **należy złożyć w formie oryginału w Kancelarii Biura Finansów KGSG** mieszczącej się w Warszawie przy ul. Podcho-

rążych 38, budynek nr 5, pokój nr 118, tel. +48 225004372, +48 22 5004387, +48 22 5004436 (w dniach od poniedziałku do piątku, w godz. 9^{00}-15^{00}).

Nie należy załączać oryginału dokumentu wadialnego do oferty.

5. Gwarancja, o której mowa w pkt. 4 musi być podpisana przez przedstawiciela Gwaranta. Podpis winien być sporządzony w sposób umożliwiający identyfikację osoby, która złożyła podpis np. wraz z imienną pieczątką lub czytelnie (z podaniem imienia i nazwiska). Z treści gwarancji winno wynikać bezwarunkowe zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust. 4a i 5 ustawy Pzp na każde pisemne żądanie zgłoszone przez Zamawiającego w terminie związania ofertą.
6. W przypadku, gdy Wykonawca wnosi wadium w formie gwarancji bankowej, gwarancji ubezpieczeniowej lub poręczenia:
   1) dokument gwarancji/poręczenia sporządzony w języku obcym należy złożyć wraz z tłumaczeniem na język polski,
   2) gwarancje/poręczenia podlegać muszą prawu polskiemu, a wszystkie spory odnośnie gwarancji/poręczeń będą rozstrzygane zgodnie z prawem polskim i poddane jurysdykcji sądów polskich.
7. **Oferta Wykonawcy, który nie zabezpieczy złożonej oferty wadium w wymaganej formie, zostanie odrzucona na podstawie art. 89 ust. 1 pkt 7b) ustawy Pzp**.
8. Zamawiający dokona zwrotu wadium niezwłocznie, jeżeli zostaną spełnione warunki określone w art. 46 ust. 1, 1a i 2 ustawy Pzp.
9. Zamawiający zażąda ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium na podstawie art. 46 ust. 1 ustawy Pzp, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta zostanie wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez Zamawiającego.
10. Zamawiający zatrzymuje wadium w przypadkach określonych w art. 46 ust. 4a i 5 ustawy Pzp.
11. Zgodnie z:
   - art. 46 ust. 4a ustawy Pzp Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 i 3a, z przyczyn leżących po jego stronie, nie złożył oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1, oświadczenia, o którym mowa w art. 25a ust. 1, pełnomocnictw lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3, co spowodowało brak możliwości wybrania oferty złożonej przez Wykonawcę jako najkorzystniejszej.
   - art. 46 ust. 5 ustawy Pzp Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca, którego oferta została wybrana:
     1) odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie;
     2) nie wniósł wymaganego zabezpieczenia należytego wykonania umowy;
     3) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.

XI. TERMIN ZWIĄZANIA OFERTĄ

Termin związania ofertą wynosi 60 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

XII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY ORAZ FORMY SKŁADANYCH DOKUMENTÓW:

1. Wykonawca zobowiązany jest do złożenia oryginału swojej oferty zgodnie z wymaganiami określonymi w SIWZ. Dodatkowo zaleca się złożenie 1 kopii oferty wykonanej z oryginału oferty.
2. Wykonawcy przedstawią ofertę zgodnie z wymaganiami określonymi w SIWZ.
3. Wykonawca zobowiązany jest do złożenia oferty na wypełnionym i podpisanym formularzu ofertowym, który winien być sporządzony zgodnie ze wzorem stanowiącym załącznik nr 2 i/lub załącznik 2a (stosownie do zakresu przedmiotowego składanej oferty).
4. Oferta wraz ze wszystkimi załącznikami - pod rygorem jej odrzucenia - musi być sporządzona w języku polskim (zgodnie z art. 9 ust. 2 ustawy Pzp) w trwałej i czytelnej technice (np. przy użyciu maszyny do pisania, komputera lub w inny sposób).
5. Wykonawca może złożyć tylko jedną ofertę.
6. Oferta i załączniki do oferty (oświadczenia Wykonawcy oraz inne dokumenty sporządzone przez Wykonawcę) muszą być podpisane przez upoważnionych przedstawicieli Wykonawcy w sposób umożliwiający identyfikację osób, które złożyły podpisy w imieniu Wykonawcy (np. wraz z imiennymi pieczątkami tych osób).
7. Zamawiający zaleca, by każda strona oferty (wraz z załącznikami do oferty) była ponumerowana.
8. Zamawiający zaleca, aby oferta wraz z załącznikami była zestawiona w sposób uniemożliwiający jej samoistną dekompletację (bez udziału osób trzecich) oraz uniemożliwiający zmianę jej zawartości bez widocznych śladów naruszenia (np. całą ofertę Wykonawca może przesznurować, a końce sznurka trwale zabezpieczyć lub zszyć wszystkie strony, na co najmniej dwie zszywki, itp.).
9. Wszelkie poprawki lub zmiany w treści oferty (w tym w załącznikach do oferty) muszą być parafowane (lub podpisane) własnoręcznie przez osobę(y) upoważnioną(e). Parafka (podpis) winna być naniesiona w sposób umożliwiający identyfikację osoby, która złożyła parafkę np. wraz z imienną pieczątką osoby sporządzającej parafkę.
10. Wykonawca ma prawo zastrzec informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji (np. w formularzu ofertowym). Zgodnie z art. 8 ust. 3 ustawy Pzp nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz **wykazał**, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp.
11. Wszelkie czynności Wykonawcy związane ze złożeniem wymaganych dokumentów (w tym m. in.: polegające na złożeniu oświadczeń woli w imieniu Wykonawcy, poświadczaniu kserokopii dokumentów za zgodność z oryginałem) muszą być dokonywane przez upoważnionych przedstawicieli Wykonawcy.
12. W przypadku dokonywania czynności związanych ze złożeniem oferty lub innych wymaganych dokumentów przez osobę(y) nie wymienioną(e) w dokumencie rejestracyjnym Wykonawcy do oferty należy dołączyć odpowiednie pełnomocnictwo (ciąg pełnomocnictw) w formie oryginału lub kopii poświadczonej notarialnie za zgodność z oryginałem.

13. Poświadczenie za zgodność z oryginałem winno być sporządzone w sposób umożliwiający identyfikację osoby, która dokonała czynności poświadczenia (np. wraz z pieczątką imienną osoby poświadczającej kopię dokumentu za zgodność z oryginałem).
14. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia (np. w formie konsorcjum). W takim przypadku zastosowanie mają przepisy określone w art. 23 ustawy Pzp, a Wykonawcy ci muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo, o którym mowa wyżej należy dołączyć do oferty. Wszelka korespondencja prowadzona będzie wyłącznie z pełnomocnikiem. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wypełniając formularz ofertowy, jak również inne wymagane dokumenty, w miejscu „Nazwa i adres Wykonawcy" muszą wpisać dane dotyczące pełnomocnika.
15. Oferta składana przez spółkę cywilną zostanie potraktowana przez Zamawiającego jako oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego.
16. Wykonawcy ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty. Wykonawcy zobowiązują się nie podnosić jakichkolwiek roszczeń z tego tytułu względem Zamawiającego, z zastrzeżeniem art. 93 ust. 4 ustawy Pzp.
17. Zgodnie z art. 96 ust. 3 ustawy Pzp protokół postępowania wraz z załącznikami jest jawny, z zastrzeżeniem art. 8 ust. 3 ustawy Pzp. Załączniki do protokołu udostępnia się po dokonaniu wyboru najkorzystniejszej oferty lub po unieważnieniu postępowania, z tym że oferty udostępnia się od chwili ich otwarcia.

XIII. MODYFIKACJA I WYCOFANIE OFERTY:

1. Wykonawca może wprowadzić zmiany oraz wycofać złożoną przez siebie ofertę przed terminem składania ofert, przy czym:
   1) w przypadku wycofania oferty, Wykonawca składa pisemne oświadczenie, że ofertę swą wycofuje, w zamkniętej kopercie zaadresowanej jak w Rozdziale XIV pkt 2 niniejszej SIWZ z dopiskiem „**Wycofanie**",
   2) w przypadku zmiany oferty, Wykonawca składa pisemne oświadczenie, że ofertę swą zmienia, określając zakres i rodzaj tych zmian, a jeśli oświadczenie o zmianie oferty pociąga za sobą konieczność wymiany czy też przedłożenia nowych dokumentów Wykonawca musi takie dokumenty złożyć. Powyższe oświadczenie i ewentualne dokumenty należy umieścić w kopercie wewnętrznej i zewnętrznej, oznaczonych jak w Rozdziale XIV pkt 2 niniejszej SIWZ, przy czym koperta zewnętrzna powinna zostać opatrzona dopiskiem „**Zmiany**".
2. Wykonawca nie może wprowadzić zmian do oferty oraz wycofać jej po upływie terminu składania ofert.
3. Zamawiający zawiadomi niezwłocznie Wykonawcę o złożeniu przez niego oferty po terminie oraz zwróci ofertę po upływie terminu do wniesienia odwołania.

Uwaga: do składanego oświadczenia (o zmianie lub o wycofaniu oferty) należy dołączyć stosowny dokument potwierdzający prawo osoby podpisującej oświadczenie do występowania w imieniu Wykonawcy.

XIV. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT:

1. Zaleca się, aby ofertę wraz ze wszystkimi podpisanymi załącznikami umieścić w dwóch kopertach, z których każda zostanie zamknięta przez Wykonawcę w sposób gwarantujący zachowanie poufności jej treści oraz zapewniający jej nienaruszalność do terminu otwarcia ofert.
2. Koperta zewnętrzna musi być zaadresowana i opisana według poniższego wzoru:

Komenda Główna Straży Granicznej Biuro Finansów - Zamówienia Publiczne Postępowanie nr 14/BF/BŁiI/17 - oferta na realizację zamówienia pn.: „**Rozbudowa systemu telekomunikacyjnego Straży Granicznej**" - dotyczy części .....* zamówienia – nie otwierać przed ..... (wpisać termin i godzinę otwarcia ofert)

* **należy wpisać numer części zamówienia, na którą Wykonawca składa ofertę**

Uwaga: przesyłka zawierająca ofertę, przekazywana za pośrednictwem poczty kurierskiej, musi być oznakowana (opisana) zewnętrznie w sposób określony powyżej.

Koperta wewnętrzna poza oznakowaniem jak powyżej powinna być opatrzona dokładną nazwą i adresem Wykonawcy.

3. **Ofertę należy złożyć do dnia 19.06.2017 r. do godz. 10^{00}** w **Kancelarii Biura Finansów KGSG** w Warszawie przy ul. Podchorążych 38, budynek nr 5, pokój nr 118, w godz. 8^{30} – 15^{30} (od poniedziałku do piątku), tel. kontaktowy – po linii miejskiej: +48 225004372, +48 225004387 lub +48 225004436, z biura prze-pustek – po linii resortowej 76604372, 766043 87 lub 76604436.
4. Wykonawca (na żądanie) otrzyma pisemne potwierdzenie złożenia oferty.
5. Konsekwencje złożenia oferty niezgodnie z ww. opisem (np. potraktowanie oferty jako zwykłej korespondencji i nie dostarczenie jej na miejsce składania ofert w terminie określonym w SIWZ) ponosi Wykonawca.
6. **Publiczna sesja otwarcia ofert odbędzie się w siedzibie Zamawiającego w Warszawie przy ul. Podchorążych 38, budynek nr 5, w dniu 19.06.2017r. o godz. 11^{00}**.
7. Bezpośrednio przed otwarciem ofert Zamawiający poda do publicznej wiadomości kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia. Następnie Zamawiający poda informacje, o których mowa w art. 86 ust. 4 ustawy Pzp.
8. Niezwłocznie po otwarciu ofert Zamawiający zamieści na stronie internetowej informacje dotyczące:
   1) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;
   2) firm oraz adresów Wykonawców, którzy złożyli oferty w terminie;
   3) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

XV. OPIS SPOSOBU OBLICZENIA CENY:

1. Przez cenę ofertową należy rozumieć cenę w rozumieniu art. 3 ust. 1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz. U. poz. 915).

2. Cena ofertowa musi obejmować wszystkie koszty, które zostaną poniesione przez Wykonawcę w związku z wykonaniem przedmiotu zamówienia, **a w przypadku Wykonawcy spoza wspólnego obszaru celnego Unii Europejskiej również opłaty celne na warunkach DDP miejsca realizacji zamówienia**.
3. Jeżeli w postępowaniu złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazując ich wartość bez kwoty podatku.
4. Rozliczenia pomiędzy Zamawiającym i Wykonawcą dokonywane będą w złotych polskich.

   Uwaga: cenę ofertową należy określić w złotych polskich z dokładnością do dwóch miejsc po przecinku.

XVI. OPIS KRYTERIÓW Z PODANIEM ICH ZNACZENIA I SPOSOBU OCENY OFERT

1. **Kryteria oceny ofert <u>w części 1 zamówienia</u>:**

   Oferty będą oceniane na podstawie kryteriów opisanych poniżej:

Nazwa kryterium	Ranga (%)	Sposób oceny
cena (P_1)	60	minimalizacja
okres udzielonej gwarancji (P_2) <u>(w miesiącach)</u>	30	punkty będą przyznawane według zasad określonych w pkt 2)
czas wymiany uszkodzonego sprzętu (P_3)	10	punkty będą przyznawane według zasad określonych w pkt 3)

Sposób przyznawania punktów w poszczególnych kryteriach:

1) punkty za kryterium „<u>cena</u>" (**P_1**) zostaną obliczone wg wzoru:

$$P_1 = \frac{\text{cena minimalna}}{\text{cena oferty}} \times 60$$ (maksymalna liczba punktów do uzyskania - 60)

<u>gdzie:</u>

cena minimalna - łączna cena brutto oferty najtańszej
cena oferty - łączna cena brutto oferty badanej

2) punkty za kryterium „<u>okres udzielonej gwarancji</u>" (**P_2**) zostaną przyznane w następujący sposób:

0 pkt – 48 – 53 miesięcy
15 pkt – 54 – 59 miesięcy,
30 pkt – 60 miesięcy i więcej

3) punkty za kryterium „czas wymiany uszkodzonego sprzętu" (P_3) - zostaną przyznane w następujący sposób:

0 pkt – zgłoszenie awarii w dniu roboczym do godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii; zgłoszenie awarii w dniu roboczym po godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej w ciągu dwóch dni roboczych licząc od dnia zgłoszenia awarii,

10 pkt – zgłoszenie awarii w dniu roboczym o dowolnej godzinie – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenie awarii.

ŁĄCZNA OCENA PUNKTOWA OFERTY

Łączna liczba punktów przyznanych ofercie (P) stanowi sumę punktów przyznanych za kryterium „cena" (P_1), kryterium „okres udzielonej gwarancji" (P_2) i kryterium „czas wymiany uszkodzonego sprzętu" (P_3) .

$$P = P_1 + P_2 + P_3$$

2. **Kryteria oceny ofert w części 2 zamówienia**:

Oferty będą oceniane na podstawie kryteriów opisanych poniżej:

Nazwa kryterium	Ranga (%)	Sposób oceny
cena (P_1)	60	minimalizacja
czas wymiany uszkodzonego sprzętu (P_2)	40	punkty będą przyznawane według zasad określonych w pkt 2)

Sposób przyznawania punktów w poszczególnych kryteriach opisano poniżej:

1) punkty za kryterium „**cena**" (P_1) zostaną obliczone wg wzoru:

$$P_1 = \frac{\text{cena minimalna}}{\text{cena oferty}} \times 60 \text{ (maksymalna liczba punktów do uzyskania - 60)}$$

gdzie:

cena minimalna - łączna cena brutto oferty najtańszej
cena oferty - łączna cena brutto oferty badanej

2) punkty za kryterium „**czas wymiany uszkodzonego sprzętu**" (P_2) - zostaną przyznane w następujący sposób:

0 pkt – zgłoszenie awarii w dniu roboczym do godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii; zgłoszenie awarii w dniu roboczym po godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej w ciągu dwóch dni roboczych licząc od dnia zgłoszenia awarii,

40 pkt – zgłoszenie awarii w dniu roboczym o dowolnej godzinie – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenie awarii

ŁĄCZNA OCENA PUNKTOWA OFERTY

Łączna liczba punktów przyznanych ofercie (P) stanowi sumę punktów przyznanych za kryterium „cena" (P_1) i kryterium „czas wymiany uszkodzonego sprzętu" (P_2)

$$P = P_1 + P_2$$

2. Zasady wyboru oferty i udzielenia zamówienia:
   1) W toku oceny ofert Zamawiający może żądać od Wykonawcy pisemnych wyjaśnień dotyczących treści złożonej oferty. Wykonawca będzie zobowiązany do przedstawienia pisemnych wyjaśnień w terminie określonym przez Zamawiającego;
   2) Zamawiający poprawi w tekście oferty omyłki określone w art. 87 ust. 2 ustawy Pzp, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona. Zamawiający odrzuci ofertę Wykonawcy, który w terminie 3 dni od dnia doręczenia mu zawiadomienia o poprawieniu omyłki, o której mowa w art. 87 ust. 2 pkt 3 ustawy Pzp nie zgodzi się na jej poprawienie;
   3) W przypadku wystąpienia błędów w ofercie w obliczeniu łącznej ceny za realizację części 1 zamówienia Zamawiający uzna, że prawidłowo podano ceny jednostkowe i dokona obliczenia łącznej ceny ofertowej.
   4) Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie oceniona jako najkorzystniejsza w oparciu o podane w niniejszym rozdziale kryteria wyboru oraz spełni wszystkie wymagania określone w ustawie i SIWZ.
   5) Umowa z Wykonawcą, którego ofertę wybrano zostanie zawarta po zakończeniu postępowania o zamówienie publiczne (zgodnie z przepisami ustawy Pzp). Umowa dotycząca realizacji zamówienia zostanie podpisana wyłącznie na warunkach określonych w projekcie umowy stanowiącym załącznik do SIWZ.

XVII. INFORMACJA O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO:

1. O terminie i miejscu zawarcia umowy Zamawiający poinformuje Wykonawcę, którego oferta została wybrana.
2. Przed podpisaniem umowy Zamawiający może zażądać przedłożenia umowy regulującej współpracę Wykonawców wspólnie ubiegających się o udzielenie zamówienia.
3. W przypadku, gdy w postępowaniu zostanie wybrana oferta Wykonawcy prowadzącego działalność w formie spółki z ograniczoną odpowiedzialnością, a wartość złożonej przez niego oferty przekroczy dwukrotność kapitału zakładowego spółki, wówczas przed podpisaniem umowy Wykonawca ten na żądanie Zamawiającego przedłoży dokument wymagany treścią art. 230 ustawy z dnia 15 września 2000r. – Kodeks spółek handlowych (tekst jednolity Dz.U. z 2013r. poz. 1030 z późn. zm.).
4. Wykonawcy wspólnie ubiegający się o zamówienie publiczne, których oferta została wybrana i zawiera pełnomocnictwo (o którym mowa w art. 23 ust. 2 ustawy Pzp) nieobejmujące swym zakresem czynności podpisywania umowy, przedłożą stosowne pełnomocni ctwo przed podpisaniem umowy w sprawie zamówienia publicznego.
5. Jeżeli Wykonawca, którego oferta została oceniona jako najkorzystniejsza, uchyla się od zawarcia umowy lub nie wniesie wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu Wykonawca, który złożył ofertę najwyżej ocenioną spośród pozostałych ofert.

XVIII. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Poniższy wymóg dotyczy wyłącznie Wykonawców składających ofertę na część 1 zamówienia.

1. Wykonawca, którego oferta zostanie wybrana zobowiązany będzie przed podpisaniem umowy do wniesienia zabezpieczenia należytego wykonania umowy w wysokości 2% ceny całkowitej podanej w ofercie.
2. Zabezpieczenie może być wnoszone w następujących formach:
   - pieniądzu,
   - poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym,
   - gwarancjach bankowych,
   - gwarancjach ubezpieczeniowych,
   - poręczeniach udzielanych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości
3. Gwarancja musi być podpisana przez przedstawiciela Gwaranta. Podpis winien być sporządzony w sposób umożliwiający identyfikację osoby, która złożyła podpis, np. wraz z imienną pieczątką lub podpis czytelny (z podaniem imienia i nazwiska). Z treści gwarancji (bankowej, ubezpieczeniowej) winno wynikać bezwarunkowe i nieodwołalne zobowiązanie Gwaranta do wypłaty Zamawiającemu kwoty zabezpieczenia należytego wykonania umowy na każde pisemne żądanie zgłoszone przez Zamawiającego.
4. Zamawiający dokona zwrotu zabezpieczenia należytego wykonania umowy oraz roszczeń z tytułu udzielonej rękojmi za wady w następujący sposób:
   a) 70% wartości zabezpieczenia zostanie zwrócone w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane tj. od dnia zakończenia realizacji zamówienia podstawowego – potwierdzonego kompletem protokołów odbiorowych z poszczególnych jednostek organizacyjnych SG objętych zamówieniem podstawowym, a w przypadku skorzystania przez Zamawiającego z prawa opcji – od dnia zakończenia realizacji całości zamówienia (obejmującego zamówienie podstawowe i zamówienie objęte prawem opcji) – potwierdzonego kompletem protokołów odbiorowych z poszczególnych jednostek organizacyjnych SG objętych zamówieniem podstawowym i zamówieniem opcjonalnym,
   b) 30% wartości zabezpieczenia, zatrzymane przez Zamawiającego na zabezpieczenie roszczeń z tytułu rękojmi za wady, zostanie zwrócone nie później niż w 15 dniu po upływie okresu rękojmi za wady dla urządzeń objętych ostatnią dostawą w ramach realizacji zamówienia.

XIX. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWARTEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

Zamawiający podpisze z wybranym Wykonawcą umowę zgodnie z projektem umowy stanowiącym załącznik nr 3 lub załącznik nr 3a do SIWZ (stosownie do zakresu przedmiotowego złożonej oferty). Do przedstawionego projektu umowy zostaną wprowadzone wszystkie zobowiązania Wykonawcy wyłonionego w trakcie procedury, wynikające z przedstawionej przez niego oferty.

XX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

1. Wykonawcom, którzy mają lub mieli interes w uzyskaniu zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej przewidziane w Dziale VI ustawy Pzp: odwołanie i skarga.
2. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
3. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
4. Na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.

Załączników 7 na 128 ark.

Załącznik nr 1	-	Opisy Przedmiotów Zamówienia do części 1 i 2 zamówienia
Załącznik nr 2 i 2a	-	Formularze ofertowe do części 1 i 2 zamówienia
Załącznik nr 3 i 3a	-	Projekty umów do części 1 i 2 zamówienia wraz z Instrukcjami Bezpieczeństwa Przemysłowego
Załącznik nr 4	-	Przykładowy wzór zobowiązania do oddania do dyspozycji niezbędnych zasobów na potrzeby wykonania zamówienia

Wzory oświadczeń, które zostaną złożone przez Wykonawcę na wezwanie Zamawiającego (zgodnie z treścią Rozdziału VIII pkt 2 SIWZ)

Załącznik nr 5	-	Wzór oświadczenia o braku orzeczenia wobec Wykonawcy zakazu ubiegania się o zamówienie tytułem środka zapobiegawczego.
Załącznik nr 6	-	Wzór oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne
Załącznik nr 7	-	Wykaz osób, które zostaną skierowane przez Wykonawcę do realizacji zamówienia

Załącznik nr **1** do SIWZ
numer sprawy 14/BF/BŁiI/17
(dotyczy części **1** i **2** zamówienia)

Opis Przedmiotu Zamówienia

„Rozbudowa systemu telekomunikacyjnego Straży Granicznej" –

opis części 1 i części 2 zamówienia

.....

Warszawa – 2017 r.

Spis treści

I. Wstęp

Straż Graniczna działając na podstawie Ustawy o Straży Granicznej wykorzystuje w codziennej służbie systemy teleinformatyczne niezbędne w procesie kontroli ruchu granicznego, ochrony granicy państwowej i części granicy zewnętrznej Unii Europejskiej. Straż Graniczna wykorzystuje sieć teleinformatyczną w całości zbudowaną w oparciu o platformę sprzętową firmy Cisco Systems. Zastosowane urządzenia umożliwiają przenoszenie wszelkiego rodzaju usług typu dane, głos, video w oparciu o protokół IP oraz implementację elementów ochrony. Wszystkie jednostki Straży Granicznej tj. Komenda Główna SG, Oddziały SG oraz inne placówki połączone są hierarchicznie siecią WAN za pomocą dynamicznych tuneli VPN (DMVPN) obsługiwanych przez routery CISCO, opartych na protokołach GRE, NHRP i IPSEC oraz na protokołach routingu EIGRP, OSPF i trasach statycznych. Na bazie wymienionych urządzeń sieciowych oraz protokołów, w tym w szczególności protokołu DMVPN Straż Graniczna wdrożyła i skonfigurowała sieć teleinformatyczną.

Głównym punktem systemu jest Centralny Węzeł Teleinformatyczny w Warszawie przy ul. 17 Stycznia 23, w którym koncentruje się cały ruch z WAN oraz znajdują się punkty styków z innymi sieciami, Centrum Przetwarzania Danych, Centralny Węzeł Głosowy oraz Centrum Zarządzania Siecią Teleinformatyczną. Infrastruktura techniczna Platformy Teleinformatycznej SG obejmuje między innymi: routery Cisco serii 2900, 3900, 7200, ASR1000, przełączniki Catalyst serii 6500, 4500, 3750, 2960 oraz przełączniki Nexus 7706 z kartami F3, system telefonii IP zarządzany serwerami Cisco Unified Communication Manager 10.5 oraz urządzenia bezpieczeństwa sieciowego Cisco ASA5585, ASA5520, ASA5515, ASA5516-FPWR, ASA5510, moduły AIM-SM i AIP-SSM w placówkach, Cisco Firewall oraz zaawansowany system zarządzania urządzeniami bezpieczeństwa Cisco FireSight. Administracja częścią infrastruktury sieciowej odbywa się za pomocą systemów Cisco Prime LMS 4.2.5 i Prime Infrastructure 2.1 zwanych dalej systemami zarządzania. Całość rozwiązania zarządzana jest centralnie z Centrum Zarządzania Siecią w Warszawie przez odpowiednio przeszkolonych inżynierów systemowych Straży Granicznej w oparciu o system kontroli dostępu realizowany przez urządzenia Cisco ACS 5.5 z wykorzystaniem protokołu TACACS+ zapewniającego rozliczalność komend. Uwierzytelnianie stacji końcowych jest realizowane przez Centralny System Uwierzytelniania Stacji Końcowych oparty na oprogramowaniu Cisco ISE 2.1 wdrożonym w modelu dystrybucyjnym.

Ponadto Straż Graniczna wykorzystuje system telefonii IP zbudowany w oparciu o technologie Cisco Systems zainstalowany na serwerach Cisco UCS 5108. Ponad 10 tys. terminali telefonicznych IP (modele Cisco 7971, Cisco 791) zarządzanych jest przez centralny Cisco Unified Communication Manager v 10.5 z sygnalizacją SCCP, który posiada funkcjonujący system rejestracji wewnętrznych połączeń telefonicznych IP. W celu optymalizacji wykorzystania pasma wykorzystywany jest centralnie zarządzany system akceleratorów ruchu opartych na rozwiązaniu Cisco WAAS (WAE512, WAE674, WAE7371 oraz Virtual WAAS na routerach Cisco serii 3900) wykorzystujący protokół WCCP. Łączność urządzeń bezprzewodowych oparta jest na kontrolerach Cisco WLAN 5508. Do konsolidacji sieci LAN i SAN wykorzystywane są moduły UCS-FI-6248UP.

Zamawiający wykorzystuje Centralny System Proxy zapewniający bezpieczny dostęp do zasobów sieci Internet. Składa się on z urządzeń WSA Cisco IronPort zarządzanych przez Centralny System Zarządzający oparty na urządzeniu Cisco M670. Serwery proxy pracują w trybie „forwarding proxy". Licencjonowanie aktualnie wykorzystywanych użytkowników zapewniają licencje typu „Web-Security-Premium". Logowanie ruchu realizowane jest w oparciu Centralny System Zarządzający oraz analizer logów Sawmill for IronPort. Straż Graniczna posiada dedykowane łącze do Internetu o przepustowości 350Mb/s z planowaną rozbudową do 1Gb/s. Aktualnie Straż Graniczna posiada 12000 sztuk licencji typu Web Security Premium ważnych do 24.12.2017

II. Przedmiot zamówienia

Przedmiotowe zamówienie jest podzielone na dwie części, przy czym:

- w ramach realizacji części 1 zamówienia Wykonawca zrealizuje dostawę urządzeń sieciowych wraz z gwarancją producenta, oprogramowaniem i licencjami do jednostek organizacyjnych Straży Granicznej oraz przeprowadzi szkolenia z obsługi dostarczonych urządzeń;

- w ramach realizacji części 2 zamówienia Wykonawca obejmie gwarancją producenta wskazane przez Zamawiającego urządzenia, licencje i oprogramowanie obecnie eksploatowane przez Straż Graniczną i zapewni zaawansowane wsparcie techniczne dla jednostek organizacyjnych Zamawiającego przy rozwiązywaniu problemów i administrowaniu systemem telekomunikacyjnym Straży Granicznej, które będzie realizowane przez inżynierów sieciowych producenta urządzeń, a także przeprowadzi szkolenia z obsługi dostarczonych urządzeń.

Wykonawca może złożyć ofertę na jedną lub dwie części zamówienia.

Poniżej przedstawiono Opis Przedmiotu Zamówienia (OPZ) oddzielnie dla każdej z dwóch części zamówienia.

A. OPIS CZĘŚCI 1 ZAMÓWIENIA

1. Zakres zamówienia

Zamówienie składa się z zamówienia podstawowego i zamówienia objętego prawem opcji.

1) **Zamówienie podstawowe będzie realizowane w dwóch etapach**:

   a) **Etap pierwszy** – zostanie wykonany w terminie do dnia **11.12.2017r**. i będzie obejmował dostawę urządzeń sieciowych (wraz z oprogramowaniem, licencjami i gwarancją producenta) do wskazanych jednostek organizacyjnych Straży Granicznej (w tym wdrożenie niektórych z dostarczonych urządzeń w Bieszczadzkim Oddziale Straży Granicznej) oraz przeprowadzenie szkoleń z obsługi tych urządzeń.

   Wykaz jednostek organizacyjnych objętych Etapem pierwszym zamówienia wraz informacją nt. rodzajów urządzeń, które będą dostarczane do tych jednostek w ramach realizacji tego etapu zamówienia **określono w punkcie 1 Załącznika nr 1 do niniejszego OPZ**.

   b) **Etap drugi** – zostanie wykonany w terminie do dnia **28.09.2018r**.,

   Etap ten będzie obejmował dostawę urządzeń sieciowych (wraz oprogramowaniem, licencjami i gwarancją producenta) do jednostek organizacyjnych Straży Granicznej oraz przeprowadzenie szkoleń z obsługi tych urządzeń.

   Wykaz jednostek organizacyjnych objętych Etapem drugim zamówienia wraz informacją nt. rodzajów urządzeń, które będą dostarczane do tych jednostek w ramach realizacji tego etapu zamówienia określono **w punkcie 2 Załącznika nr 1 do niniejszego OPZ**.

2) **Zamówienie objęte prawem opcji** – w przypadku skorzystania przez Zamawiającego z prawa opcji Wykonawca zrealizuje zamówienie w terminie do dnia **28.09.2018r.** i będzie ono obejmowało dostawę urządzeń sieciowych (wraz oprogramowaniem, licencjami i gwarancją producenta) do wskazanych jednostek organizacyjnych Straży Granicznej oraz przeprowadzenie szkoleń z obsługi tych urządzeń.

   Wykaz jednostek organizacyjnych, do których będą dostarczane urządzenia wraz informacją nt. rodzajów urządzeń, które będą dostarczane do tych jednostek w ramach realizacji zamówienia objętego prawem opcji **określono w punkcie 3 Załącznika nr 1 do niniejszego OPZ**.

   Zamówienie zrealizowane w ramach opcji musi zostać oznakowane zgodnie ze sposobem opisanym w punkcie 9 niniejszego rozdziału.

2. Specyfikacja elementów zamówienia

2.1. Wymagania ogólne

Wymagania ogólne dla urządzeń i oprogramowania sieciowego dostarczanego w ramach zamówienia.

1) Całość dostarczanego sprzętu, oprogramowania i licencji musi pochodzić z autoryzowanego kanału sprzedaży producentów.
2) Całość dostarczanego sprzętu musi być fabrycznie nowa (nieużywana we wcześniejszych projektach) i wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą).
3) W przypadku uszkodzenia modułu pamięci (flash, RAM) lub dysku twardego w okresie obowiązywania serwisu gwarancyjnego zostaną one wymienione na nowe, a uszkodzone pozostają u użytkownika.
4) Urządzenia, oprogramowanie i licencje objęte ofertą Wykonawcy nie mogą być urządzeniami, oprogramowaniem i licencjami dla których ogłoszono koniec życia produktu.

2.2. Wspólne wymagania dla przełączników

1) Przełączniki dla określonej jednostki organizacyjnej muszą posiadać wkładki zgodnie z załącznikiem nr 1 do niniejszego OPZ.
2) Przełącznik musi zapewniać przełączanie w warstwie drugiej.
3) Przełącznik musi obsługiwać co najmniej 100 sieci VLAN
4) System operacyjny (licencja) wspierający SSH.
5) Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 4 plików konfiguracyjnych.
6) Przełącznik musi umożliwiać zestawianie połączeń typu trunk w standardzie IEEE 802.1Q.
7) Przełącznik musi umożliwiać wyczyszczenie tablicy adresów MAC (wpisów nauczonych dynamicznie) z poziomu linii poleceń. Wymagana jest możliwość usunięcia wszystkich adresów nauczonych dynamicznie, konkretnego adresu

nauczonego dynamicznie, adresów nauczonych dynamicznie dla konkretnej sieci VLAN lub por-tu.

8) Urządzenia muszą umożliwiać uwierzytelnianie, autoryzacje oraz rozliczalność komend (AAA) w oparciu o system kontroli dostępu Zamawiającego .
9) Przełącznik musi umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu.
10) Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN.
11) Przełącznik musi umożliwiać skonfigurowanie i określenie sieci VLAN służącej do zarządzania przełącznikiem tzw. VLAN zarządzający (Management VLAN).
12) Przełącznik musi zapewniać na jednym porcie jednoczesny dostęp do sieci typu voice i data z wykorzystaniem telefonów Zamawiającego.
13) Przełącznik musi wspierać funkcjonalność przekazywania znakowania QoS od urządzeń typu telefon pracujących w sieci Straży Granicznej
14) Przełącznik musi wspierać funkcjonalność NetFLOW co najmniej w wersji 5
15) Przełącznik musi wspierać funkcjonalność Link Layer Discovery Protocol
16) Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    - IEEE 802.1w Rapid Spanning Tree,
    - IEEE 802.1s Multi-Instance Spanning Tree,
    - możliwość grupowania do min. 8 portów tego samego typu w jeden kanał logiczny zgodnie ze specyfikacją IEEE 802.3ad (LACP),
    - możliwość grupowania w kanały IEEE 802.3ad (LACP) portów tego samego typu fizycznie znajdujących się na różnych przełącznikach tworzących stos,
17) Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    - wiele poziomów dostępu administracyjnego poprzez konsolę,
    - zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilage-level).
    - dostęp do urządzenia przez SNMPv3 i SSHv2,
    - wyłączenie sieci VLAN nr 1 dla portu typu trunk,
    - funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLAN-u (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym,
    - funkcjonalność dynamicznej inspekcji protokołu ARP, czyli możliwość zablokowania przesyłania przez dołączone stacje pakietów tzw. gratitious ARP (GARP), umożliwiających przejęcie ruchu innych stacji komunikujących się między sobą w obrębie tej samej podsieci IP,
    - funkcjonalność inspekcji adresów źródłowych pakietów IP, czyli możliwość zablokowania przesyłania przez dołączone stacje pakietów IP ze źródłowymi adresami IP do nich nie należących (tzw. IP spoofing),
    - autoryzację użytkowników/portów w oparciu o IEEE 802.1x wraz z obsługą funkcjonalności MAC Authentication Bypass umożliwiającą podłączenia do portów z autentykacją 802.1x urządzeń nie wyposażonych w suplikanta 802.1x (np. drukarki, telefony IP) i autentykację tych urządzeń na bazie adresu MAC,
    - funkcjonalność inspekcji adresów źródłowych pakietów IP (IP Source Guard), czyli możliwość zablokowania przesyłania przez dołączone stacje pakietów IP ze źródłowymi adresami IP do nich nie należących (tzw. IP spoofing),
18) W zakresie SpanningTree przełącznik musi obsługiwać mechanizmy:
    - Spanning-tree PortFast: natychmiastowe przejście portu dostępowego L2 do trybu „forwarding" z pominięciem fazy „listening" oraz „learning",
    - PortFast Guard: zamknięcie / wyłączenie (shutdown) portu w trybie PortFast po otrzymaniu ramki BPDU,

19) Urządzenia muszą współpracować z systemem zarządzania wykorzystywanym w Straży Granicznej, a w szczególności:
   - wgrywania, aktualizacji, ściągania i analizy konfiguracji;
   - inwentaryzacji;
   - zmiany oprogramowania.
20) Urządzenie musi być wyposażone w minimum 1 port konsoli do czynności administratorskich;
21) Dostarczone urządzenia muszą posiadać aktualną dostępną na rynku wersję firmware.
22) Urządzenia muszą posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V.
23) W celu usprawnienia diagnostyki urządzenia oraz połączeń sieciowych wymaga się, aby przełącznik był wyposażony w lampki sygnalizacyjne LED umożliwiające wizualne określenie dla każdego z portów statusu portu tj. wyłączony, aktywny, prędkość, full-duplex.
24) Urządzenie musi posiadać możliwość konfiguracji 802.1x na portach w oparciu o Centralny System Uwierzytelnień (Cisco Identity Service Engine w wersji 2.1)
25) Urządzenie musi posiadać możliwość aplikowania na porty przełącznika dynamicznych list ACL (dACL), przesyłanych z Centralnego Systemu Uwierzytelnień (listy dACL są w pełni przesyłane w komunikatach Radius z serwera, nie muszą być wcześniej wysyłane na przełączniki w osobnym trybie administracyjnym. Nie dopuszcza się rozwiązania w którym lista ACL jest wcześniej skonfigurowana na przełączniku, a komunikat Radius zawiera tylko nazwę statycznej listy ACL.)
26) dynamiczne listy ACL (dACL) powinny być przypisywane na port niezależnie dla każdego urządzenia uwierzytelnionego na porcie (każde urządzenie powinno mieć możliwość "otrzymania" w momencie uwierzytelnienia różnej listy dACL i taka dACL powinna działać tylko dla tego urządzenia rozpoznawanego poprzez jego adres IP)
27) możliwość konfiguracji portów przełączników w co najmniej 3 trybach 802.1x:
   - "tryb otwarty" (konfiguracja 802.1x która jest na porcie pracuje w trybie "monitoringu" - błędne uwierzytelnienie lub jego brak popranego nie wpływa na ruch realizowany przez dany port przełącznika. Zdarzenia z portu są pokazywane przez Centralny System Uwierzytelnień)
   - "tryb otwarty z listą ACL" (tryb monitoringu, z dodatkowym ograniczeniem, że w przypadku braku uwierzytelnienia lub jego błędu ruch na porcie jest ograniczany zgodnie ze statyczną listą ACL skonfigurowaną przez administratora przełącznika na porcie)
   - "tryb zamknięty" (ruch poprzez port przełącznika jest dozwolony tylko w przypadku poprawnego uwierzytelnienia przez Centralny System Uwierzytelnień)
28) możliwość wykorzystania jednej konfiguracji na wszystkich portach przełącznika pozwalającej realizować uwierzytelnienie w oparciu o Centralny System Uwierzytelnień z wykorzystaniem MAB oraz różnych metod EAP (np. PEAP, TLS). Wybór metody powinna określać konfiguracja Centralnego Systemu Uwierzytelnień, nie konfiguracja portu (tzn. różne urządzenia podłączane do tego samego portu powinny mieć możliwość realizacji różnej formy uwierzytelniania)
29) możliwość wykonywania przez Centralny System Uwierzytelnia zmiany stanu uwierzytelniania tzw. CoA (Change of Authorization) umożliwiając co najmniej:
   - zdalne wymuszenie ponownego uwierzytelnienia pojedynczego urządzenia przyłączonego do portu przełącznika
   - zdalne wyłączenie portu przełącznika
   - zmiany stanu uwierzytelnienia związanego z ponownym przypisaniem dynamicznej listy dACL lub zmiany VLAN
30) konfiguracja portu przełącznika w trybie 802.1x powinna mieć możliwość regularnego, automatycznego wymuszania ponownego uwierzytelniania,

niezależnie od konfiguracji Centralnego Systemu Uwierzytelnień lub działań administratorów

31) przełącznik powinien poprawnie pracować w sytuacji której:
   - na wszystkich jego portach są przyłączone komputery poprzez telefon IP
   - na wszystkich portach jest skonfigurowane 802.1x
   - na wszystkich portach są przypisane dACL różne dla każdego urządzenia przyłączonego do danego portu przełącznika
   - na wszystkich portach przełącznika zostały przypisane listy dACL o długości co najmniej 30 linii. Przełącznik w takiej sytuacji powinien pracować z pełną wydajnością przełączania pakietów opisanej w dokumentacji. Nie dopuszcza się degradacji wydajności pracy związanej z przypisanymi dACL

2.3. Przełącznik 48 portowy z uplink 4xSFP

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 48 portów 10/100/1000
2) Przełącznik musi być wyposażony w minimum 4 interfejsy uplink SFP Gigabit Ethernet
3) Porty dostępowe 10/100/1000 muszą zapewniać wsparcie dla zasilania przez sieć LAN zgodnie z IEEE 802.3af oraz IEEE 802.3at na wszystkich portach jednocześnie z maksymalna mocą. Budżet mocy dla PoE musi wynosić co najmniej 740 W.
4) Urządzenie musi posiadać min. 512MB pamięci DRAM i min.128MB pamięci flash.
5) Urządzenie musi być wyposażone w funkcjonalność łączenia w stos z innymi przełącznikami tego samego typu oraz innymi należącymi do tej samej rodziny przełączników (używanie funkcjonalności nie powinno wymagać od Zamawiającego dodatkowych zakupów) .
6) Urządzenia tworzące stos z punktu widzenia zarządzania muszą stanowić jedno logiczne urządzenie.
7) Funkcjonalność łączenia w stos musi umożliwiać pracę min. 8 urządzeń w stosie.
8) Dla funkcjonalności łączenia urządzeń w stos musi być dostępny mechanizm redundancji 1:N polegający na tym, że w przypadku, gdy awarii ulega jednostka główna tj. jednostka sterująca stosem (przełącznik, który logicznie steruje, zarządza pracą stosu) wówczas inny z przełączników tworzących stos może zastąpić jednostkę główną i przejąć jej zadania.
9) Zamawiający wymaga dostarczenia kabla do łączenia urządzeń w stos.
10) Urządzenie musi być przygotowane do montażu w szafie 19"

2.4. Przełącznik 48 portowy z uplink 2xSFP+

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 48 portów 10/100/1000
2) Przełącznik musi być wyposażony w minimum 2 interfejsy TenGigabit Ethernet , które muszą mieć możliwość wyboru trybu pracy zamiennie, miedziany (RJ-45) lub światłowodowy (SFP lub GBIC).
3) Porty dostępowe 10/100/1000 muszą zapewniać wsparcie dla zasilania przez sieć LAN zgodnie z IEEE 802.3af oraz IEEE 802.3at na wszystkich portach jednocześnie z maksymalna mocą. Budżet mocy dla PoE musi wynosić co najmniej 740 W.

4) Urządzenie musi posiadać min. 512MB pamięci DRAM i min. 128MB pamięci flash.
5) Urządzenie musi być wyposażone w funkcjonalność łączenia w stos z innymi przełącznikami tego samego typu oraz innymi należącymi do tej samej rodziny przełączników (używanie funkcjonalności nie powinno wymagać od Zamawiającego dodatkowych zakupów) .
6) Urządzenia tworzące stos z punktu widzenia zarządzania muszą stanowić jedno logiczne urządzenie.
7) Funkcjonalność łączenia w stos musi umożliwiać pracę min. 8 urządzeń w stosie.
8) Dla funkcjonalności łączenia urządzeń w stos musi być dostępny mechanizm redundancji 1:N polegający na tym, że w przypadku, gdy awarii ulega jednostka główna tj. jednostka sterująca stosem (przełącznik, który logicznie steruje, zarządza pracą stosu) wówczas inny z przełączników tworzących stos może zastąpić jednostkę główną i przejąć jej zadania.
9) Zamawiający wymaga dostarczenia kabla do łączenia urządzeń w stos.
10) Urządzenie musi być przygotowane do montażu w szafie 19"

2.5. Przełącznik 24 portowy z uplink 2xSFP+

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 24 porty 10/100/1000.
2) Przełącznik musi być wyposażony w minimum 2 interfejsy TenGigabit Ethernet , które muszą mieć możliwość wyboru trybu pracy zamiennie, miedziany (RJ-45) lub światłowodowy (SFP lub GBIC).
3) Porty dostępowe 10/100/1000 muszą zapewniać wsparcie dla zasilania przez sieć LAN zgodnie z IEEE 802.3af oraz IEEE 802.3at na wszystkich portach jednocześnie z maksymalna mocą. Budżet mocy dla PoE musi wynosić co najmniej 370 W.
4) Urządzenie musi posiadać min. 512MB pamięci DRAM i min. 128MB pamięci flash.
5) Urządzenie musi być wyposażone w funkcjonalność łączenia w stos z innymi przełącznikami tego samego typu oraz innymi należącymi do tej samej rodziny przełączników (używanie funkcjonalności nie powinno wymagać od Zamawiającego dodatkowych zakupów) .
6) Urządzenia tworzące stos z punktu widzenia zarządzania muszą stanowić jedno logiczne urządzenie.
7) Funkcjonalność łączenia w stos musi umożliwiać pracę min. 8 urządzeń w stosie.
8) Dla funkcjonalności łączenia urządzeń w stos musi być dostępny mechanizm redundancji 1:N polegający na tym, że w przypadku, gdy awarii ulega jednostka główna tj. jednostka sterująca stosem (przełącznik, który logicznie steruje, zarządza pracą stosu) wówczas inny z przełączników tworzących stos może zastąpić jednostkę główną i przejąć jej zadania.
9) Zamawiający wymaga dostarczenia kabla do łączenia urządzeń w stos.
10) Urządzenie musi być przygotowane do montażu w szafie 19"

2.6. Przełącznik 24 portowy z uplink 4xSFP

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 24 porty 10/100/1000.
2) Przełącznik musi być wyposażony w minimum 4 interfejsy SFP Gigabit Ethernet
3) Porty dostępowe 10/100/1000 muszą zapewniać wsparcie dla zasilania przez sieć LAN zgodnie z IEEE 802.3af oraz IEEE 802.3at na wszystkich portach jednocześnie z maksymalna mocą. Budżet mocy dla PoE musi wynosić co najmniej 370 W.
4) Urządzenie musi posiadać min. 512MB pamięci DRAM i min. 128MB pamięci flash.
5) Urządzenie musi być wyposażone w funkcjonalność łączenia w stos z innymi przełącznikami tego samego typu oraz innymi należącymi do tej samej rodziny przełączników (używanie funkcjonalności nie powinno wymagać od Zamawiającego dodatkowych zakupów) .
6) Urządzenia tworzące stos z punktu widzenia zarządzania muszą stanowić jedno logiczne urządzenie.
7) Funkcjonalność łączenia w stos musi umożliwiać pracę min. 8 urządzeń w stosie.
8) Dla funkcjonalności łączenia urządzeń w stos musi być dostępny mechanizm redundancji 1:N polegający na tym, że w przypadku, gdy awarii ulega jednostka główna tj. jednostka sterująca stosem (przełącznik, który logicznie steruje, zarządza pracą stosu) wówczas inny z przełączników tworzących stos może zastąpić jednostkę główną i przejąć jej zadania.
9) Zamawiający wymaga dostarczenia kabla do łączenia urządzeń w stos.
10) Urządzenie musi być przygotowane do montażu w szafie 19"

2.7. Przełącznik 12 portowy z uplink 2xSFP

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 12 portów 10/100/1000 (RJ-45).
2) Przełącznik musi być wyposażony w minimum 2 interfejsy SFP Gigabit Ethernet
3) Porty dostępowe 10/100/1000 muszą zapewniać wsparcie dla zasilania przez sieć LAN zgodnie z IEEE 802.3af na wszystkich portach jednocześnie z maksymalna mocą. Budżet mocy dla PoE musi wynosić co najmniej 190 W.
4) Urządzenie musi posiadać min. 512MB pamięci DRAM i min.128MB pamięci flash.
5) Urządzenie musi być wyposażone w pasywne chłodzenie.
6) Urządzenie musi być przygotowane do montażu w szafie 19"

2.8. Przełącznik 8 portowy z uplink 2xSFP

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 8 portów 10/100/1000.
2) Przełącznik musi być wyposażony w minimum 2 interfejsy SFP Gigabit Ethernet które muszą mieć możliwość wyboru trybu pracy zamiennie, miedziany (RJ-45) lub światłowodowy (SFP lub GBIC).
3) Porty dostępowe 10/100/1000 muszą zapewniać wsparcie dla zasilania przez sieć LAN zgodnie z IEEE 802.3af na wszystkich portach jednocześnie z maksymalna mocą. Budżet mocy dla PoE musi wynosić co najmniej 124 W.
4) Urządzenie musi posiadać min. 512MB pamięci DRAM i min. 128MB pamięci flash.
5) Urządzenie musi być wyposażone w pasywne chłodzenie

6) Urządzenie musi być przygotowane do montażu w szafie 19"

2.9. Przełącznik agregacyjny 32 portowy SFP+

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 32 interfejsy TenGigabit Ethernet
2) Przełącznik musi być wyposażony w porty uplink, minimum 2 interfejsy TenGigabit Ethernet
3) Urządzenie musi posiadać min. 4 GB pamięci DRAM i min. 2 GB pamięci flash.
4) Co najmniej 4 porty przełącznika muszą zapewnić wsparcie sprzętowe dla standardu IEEE 802.1ae (MACSec).
5) Przełącznik musi wspierać protokoły routingu wykorzystywane w sieci Zamawiającego.
6) Urządzenie musi wyposażone być w funkcjonalność łączenia w stos fizyczny lub wirtualny z innym przełącznikiem tego samego typu.
7) Urządzenia tworzące stos z punktu widzenia zarządzania muszą stanowić jedno logiczne urządzenie.
8) Urządzenia połączone w stos muszą mieć możliwość geograficznej dyslokacji co najmniej 100 m
9) Funkcjonalność łączenia w stos musi umożliwiać pracę min. 2 urządzeń w stosie.
10) Jeżeli łączenie w stos wymaga specjalnego okablowania wymaga się, aby dostępne były w ofercie producenta urządzeń kable do łączenia urządzeń w stos.
11) Urządzenie musi być przygotowane do montażu w szafie 19"
12) Urządzenie musi mieć redundantne zasilanie.

2.10. Przełącznik agregacyjny 12 portowy SFP

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest przełączników spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 12 portów Gigabit Ethernet
2) Urządzenie musi posiadać min. 4GB pamięci DRAM i min. 2GB pamięci flash.
3) Co najmniej 4 porty przełącznika muszą zapewnić wsparcie sprzętowe dla standardu IEEE 802.1ae (MACSec).
4) Przełącznik musi wspierać protokoły routingu wykorzystywane w sieci Zamawiającego.
5) Urządzenie musi być wyposażone w funkcjonalność łączenia w stos z innymi przełącznikami tego samego typu oraz innymi należącymi do tej samej rodziny przełączników (używanie funkcjonalności nie powinno wymagać od Zamawiającego dodatkowych zakupów).
6) Urządzenia tworzące stos z punktu widzenia zarządzania muszą stanowić jedno logiczne urządzenie.
7) Funkcjonalność łączenia w stos musi umożliwiać pracę min. 3 urządzeń w stosie.
8) Dla funkcjonalności łączenia urządzeń w stos musi być dostępny mechanizm redundancji 1:N polegający na tym, że w przypadku, gdy awarii ulega jednostka główna tj. jednostka sterująca stosem (przełącznik, który logicznie steruje, zarządza pracą stosu) wówczas inny z przełączników tworzących stos może zastąpić jednostkę główną i przejąć jej zadania.
9) Zamawiający wymaga dostarczenia kabla do łączenia urządzeń w stos.
10) Urządzenie musi być przygotowane do montażu w szafie 19"

11) Urządzenie musi mieć redundantne zasilanie.

2.11. Wspólne wymagania dla przełączników modularnych

1) Architektura urządzenia musi umożliwiać zmianę wydajności urządzenia poprzez wymianę modułu jednostki sterująco-przełączającej. Nie dopuszcza się rozwiązania, w którym matryca przełączająca (switch fabric) jest na stałe zintegrowana z chassis urządzenia.
2) Urządzenie musi posiadać min. 2GB pamięci DRAM i min. 1GB pamięci flash.
3) Wydajność jednostki sterująco-przełączającej per moduł musi być na poziomie 48Gbps
4) przełącznik musi realizować przełączanie w warstwie trzeciej oraz definiowanie routingu IPv4 w oparciu o routing statyczny oraz co najmniej protokoły routingu dynamicznego RIP v1, RIP v2.
5) przełącznik musi realizować funkcjonalność Layer 2 Traceroute lub równoważną umożliwiającą identyfikację fizycznej ścieżki, którą został przetransmitowany pakiet z przełącznika źródłowego do docelowego. Funkcjonalność powinna umożliwiać co najmniej określenie ścieżki dla pakietów unicastowych z podaniem źródłowego i docelowego adresu MAC oraz w przypadku gdy przełącznik docelowe oraz źródłowy znajdują się z tej samem podsieci poprzez podanie adresów IP przełącznika docelowego i źródłowego,
6) przełącznik musi umożliwiać tworzenie logicznych interfejsów IP, tj. interfejsów IP odpowiadających sieciom wirtualnym VLAN oraz fizycznych interfejsów IP tj. interfejsów odpowiadające konkretnym portom fizycznym,
7) przełącznik musi zapewniać obsługę ruchu IP Multicast, w tym funkcjonalność IGMP (wersja v1, v2, v3) oraz mechanizmu IGMP Snooping (dla wersji IGMP v1, v2, v3), obsługę filtrowania grup IGMP na portach dostępowych oraz portach TRUNK, a także obsługę protokołów Protocol Independent Multicast [PIM], Source Specific Multicast [SSM], Distance Vector Multicast Routing Protocol [DVMRP],
8) przełącznik musi wspierać następujące standardy sieciowe:
   - Gigabit Ethernet: IEEE 802.3z, 802.3ab,
   - IEEE 802.3af PoE,
   - IEEE 802.1D Spanning Tree Protocol,
   - IEEE 802.1w Rapid Spanning Tree Protocol,
   - IEEE 802.1s – wiele instancji VLAN dla protokołu Spanning Tree,
   - IEEE 802.3ad LACP – możliwość logicznego grupowania portów tego samego typu w jeden kanał logiczny,
   - obsługa priorytetyzacji zgodnie z IEEE 802.1p CoS,
   - obsługa portów typu TRUNK zgodnie z IEEE 802.1Q VLAN,
   - uwierzytelnianie użytkowników zgodnie z IEEE 802.1x,
   - RMON (obsługa 4 grup: history, statistics, alarms, and events),
   - możliwość klasyfikacji pakietów przez urządzenie w oparciu o pola CoS oraz DSCP,
   - klasyfikację i oznaczanie ruchu IP na bazie informacji z nagłówka L3 lub L4 pakietów IP,
   - implementację co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi,
   - możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
   - możliwość definiowania mechanizmów ograniczania transmisji dla określonego ruchu (tzw. policer). Urządzenie powinno umożliwiać tworzenie policerów na wejściu oraz wyjściu, z których każdy może być dedykowany do ograniczania jednej indywidualnej klasy ruchu (na porcie lub VLAN-ie) lub ograniczania zagregowanego ruchu należącego do kilku różnych klas. Policer powinien

umożliwiać odrzucanie nadmiaru ruchu (ponad zdefiniowany profil) oraz wymuszać zmianę parametrów QoS zapisanych w pakiecie,
- możliwość kontroli i ograniczenia na poziomie portu „sztormów" dla ruchu broadcastowego oraz unicastowego. Możliwość skonfigurowania działania podejmowanego w przypadku detekcji „sztormu" na wyłączenie (shutdown) portu lub wygenerowanie komunikatu SNMP trap,

9) realizacja funkcji serwera DHCP dla urządzeń pracujących w sieci LAN,
10) realizacja funkcji DHCP snooping,
11) urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    - wiele poziomów dostępu administracyjnego poprzez konsolę,
    - autoryzację użytkowników/portów w oparciu o IEEE 802.1x wraz z obsługą funkcjonalności MAC Authentication Bypass umożliwiającą podłączenia do portów z autentykacją 802.1x urządzeń nie wyposażonych w suplikanta 802.1x (np. drukarki, telefony IP) i autentykację tych urządzeń na bazie adresu MAC,
    - autoryzację użytkowników w oparciu o 802.1x umożliwiająca przydział sieci VLAN, przydział sieci VLAN dla obsługi głosu,
    - obsługę IEEE 802.1x Multidomain Authentication,
    - obsługę SNMP v1, v2, v3 oraz SSH v1, v2,
    - możliwość uzyskania dostępu do urządzenia poprzez protokół TELNET z możliwością określenia zakresu adresów IP lub podsieci IP, z których taki dostęp jest możliwy,
    - funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLAN-u (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym,
    - w celu zabezpieczenia się przed atakami z wykorzystaniem protokołu DHCP wymaga się, aby przełącznik umożliwiał monitorowanie zapytań i odpowiedzi protokołu DHCP (DHCP Snooping) oraz blokowanie prób przyznawania za pomocą tego protokołu adresów IP przez stacje przyłączone do nie autoryzowanych do tego celu portów przełącznika,
    - możliwość ochrony serwera DHCP poprzez określenie i ograniczenie ilości zapytań DHCP na sekundę otrzymywanych na porcie,
    - w celu ochrony segmentu sieci LAN przed atakami w warstwie 2 z wykorzystaniem protokołu ARP wymaga się, aby przełącznik posiadał zaimplementowaną funkcjonalność dynamicznej inspekcji protokołu ARP,
    - funkcjonalność inspekcji adresów źródłowych pakietów IP (IP Source Guard), czyli możliwość zablokowania przesyłania przez dołączone stacje pakietów IP ze źródłowymi adresami IP do nich nie należących (tzw. IP spoofing),
    - możliwość filtrowania ruchu wejściowego IPv4 na danym porcie L2 w oparciu o dane warstwy trzeciej takie jak: źródłowy i docelowy adres IP z możliwością określenia zakresu adresów za pomocą maski, port TCP, ustawienia QoS pakietu IP,
    - możliwość filtrowania ruchu wejściowego innego niż IPv4 na danym porcie L2 w oparciu o dane warstwy drugiej takie jak: źródłowy i docelowy adres MAC z możliwością określenia zakresu adresów za pomocą maski,
    - możliwość filtrowania ruchu wejściowego i wyjściowego IP na poziomie interfejsów L3 w oparciu o dane warstwy trzeciej takie jak: źródłowy i docelowy adres IP z możliwością określenia zakresu adresów za pomocą maski, port TCP, ustawienia QOS,
12) przełącznik musi umożliwiać wyczyszczenie tablicy adresów MAC (wpisów nauczonych dynamicznie) z poziomu linii poleceń. Wymagana jest możliwość usunięcia wszystkich adresów nauczonych dynamicznie, konkretnego adresu nauczonego dynamicznie, adresów nauczonych dynamicznie dla konkretnej sieci VLAN lub portu,

13) przełącznik musi wspierać funkcjonalność NetFLOW co najmniej w wersji 5
14) przełącznik musi wspierać funkcjonalność Link Layer Discovery Protocol
15) przełącznik musi zapewniać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu,
16) przełącznik musi zapewniać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN,
17) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien być możliwy do edycji w trybie off-line. Wymagana jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian,
18) możliwość konfiguracji 802.1x na portach w oparciu o Centralny System Uwierzytelnień (Cisco Identity Service Engine w wersji 2.1)
19) możliwość aplikowania na porty przełącznika dynamicznych list ACL (dACL), przesyłanych z Centralnego Systemu Uwierzytelnień (listy dACL, są w pełni przesyłane w komunikatach Radius z serwera, nie muszą być wcześniej wysyłane na przełączniki w osobnym trybie administracyjnym. Jako dynamicza lista ACL - dACL, nie dopuszcza się rozwiązania w którym lista ACL jest wcześniej skonfigurowana na przełączniku, a komunikat Radius zawiera tylko nazwę statycznej listy ACL.)
20) dynamiczne listy ACL (dACL) powinny być przypisywane na port niezależnie dla każdego urządzenia uwierzytelnionego na porcie (każde urządzenie powinno mieć możliwość "otrzymania" w momencie uwierzytelnienia różnej listy dACL i taka dACL powinna działać tylko dla tego urządzenia rozpoznawanego poprzez jego adres IP)
21) możliwość konfiguracji portów przełączników w co najmniej 3 trybach 802.1x:
    - "tryb otwarty" (konfiguracja 802.1x która jest na porcie pracuje w trybie "monitoringu" - błędne uwierzytelnienie lub jego brak popranego nie wpływa na ruch realizowany przez dany port przełącznika. Zdarzenia z portu są pokazywane przez Centralny System Uwierzytelnień)
    - "tryb otwarty z listą ACL" (tryb monitoringu, z dodatkowym ograniczeniem, że w przypadku braku uwierzytelnienia lub jego błędu ruch na porcie jest ograniczany zgodnie ze statyczną listą ACL skonfigurowaną przez administratora przełącznika na porcie)
    - "tryb zamknięty" (ruch poprzez port przełącznika jest dozwolony tylko w przypadku poprawnego uwierzytelnienia przez Centralny System Uwierzytelnień)
22) możliwość wykorzystania jednej konfiguracji na wszystkich portach przełącznika pozwalającej realizować uwierzytelnienie w oparciu o Centralny System Uwierzytelnień z wykorzystaniem MAB oraz różnych metod EAP (np. PEAP, TLS). Wybór metody powinna określać konfiguracja Centralnego Systemu Uwierzytelnień, nie konfiguracja portu (tzn. różne urządzenia podłączane do tego samego portu powinny mieć możliwość realizacji różnej formy uwierzytelniania)
23) możliwość wykonywania przez Centralny System Uwierzytelnia zmiany stanu uwierzytelniania tzw, CoA (Change of Authorization) umożliwiając co najmniej:
    - zdalne wymuszenie ponownego uwierzytelnienia pojedynczego urządzenia przyłączonego do portu przełącznik
    - zdalne wyłączenie portu przełącznika
    - zmiany stanu uwierzytelnia związanego z ponownym przypisaniem dynamicznej listy dACL lub zmiany VLAN
24) konfigurację portu przełącznika w trybie 802.1x powinna mieć możliwość regularnego, automatycznego wymuszania ponownego uwierzytelniania, niezależnie od konfiguracji Centralnego Systemu Uwierzytelnień lub działań administratorów
25) przełącznik powinien poprawnie pracować w sytuacji której:

- na wszystkich jego portach są przyłączone komputery poprzez telefon IP
- na wszystkich portach jest skonfigurowane 802.1x
- na wszystkich portach są przypisane dACL różne dla każdego urządzenia przyłączonego do danego portu przełącznika
- na wszystkich portach przełącznika zostały przypisane listy dACL o długości co najmniej 30 linii. Przełącznik w takiej sytuacji powinien pracować z pełną wydajnością przełączania pakietów opisanej w dokumentacji. Nie dopuszcza się degradacji wydajności pracy związanej z przypisanymi dACL

2.12. Wymagania dla karty światłowodowej do przełącznika modularnego

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie kart do przełączników spełniających poniższe wymagania:

1) Karty z możliwością instalacji modułów interfejsowych wymiennych z portami GigabitEthernet typu 1000BASE-SX, 1000BASE-ZX,1000BASE-LX/LH, 1000BASE-BX-D (1490NM), GLC-FE-100BX-D
2) przepustowość karty powinna być minimum 48Gbps dla kart 48 portowych i minimum 24Gbps dla kart 24 portowych

2.13. Wymagania dla karty 48 portowej RJ-45 do przełącznika modularnego

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie kart do przełączników spełniających poniższe wymagania:

1) 48 portów GigabitEthernet 10/100/10000 z PoE IEEE 802.3af i 802.3at PoE+,
2) przepustowość karty powinna być na poziomie minimum 24 Gbps

2.14. Przełącznik modularny 3 slotowy

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników modularnych umożliwiających zainstalowanie 3 modułów (wliczając w to moduł jednostki sterująco-przełączającej).

2.15. Przełącznik modularny 6 slotowy

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej w placówkach Zamawiającego niezbędne jest dostarczenie przełączników modularnych umożliwiających zainstalowanie 6 modułów (wliczając w to moduł jednostki sterująco-przełączającej).

2.16. Zasilacze do przełączników modularnych

Urządzenia muszą być wyposażone w redundantne zasilacze zapewniające obsługę PoE dla wszystkich portów kart miedzianych w zależności od przełącznika modularnego (3, 6 modularnego).

2.17. Router do PSTN

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci PSTN niezbędne jest dostarczenie ruterów spełniających poniższe wymagania:

1. System operacyjny (licencja) wspierający IPsec, SSH.
2. System operacyjny (licencja) wspierający Voice gateway.
3. Urządzenie musi być routerem modularnym (możliwości rozbudowy, wymiany) z minimum 4 interfejsów Gigabit Ethernet 10/100/1000. Interfejsy muszą mieć możliwość obsadzenia wkładkami typu SFP.

1.1. Urządzenie musi posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupie-nie licencji na użytkowanie pozostałych portów.

4. Urządzenie musi posiadać minimum 3 sloty z zainstalowanymi minimum 2 kartami E1 dla zapewnienia łączności głosowej do sieci PSTN/ISDN. Zamawiający wymaga łącznie 4 porty E1 w routerze. Wszystkie sloty muszą umożliwiać zainstalowanie kart.
5. Urządzenie musi mieć możliwość działania jako brama IP do IP albo inaczej SBC (Session Border Controller) dla połączeń głosowych i wideo realizowanych w sieci IP.
6. Urządzenie wraz z licencją musi obsługiwać co najmniej 100 jednoczesnych połączeń typu CUBE w trybie redundantnym (łącznie realizowanym przez dwa routery).
7. Urządzenie musi mieć możliwość pracy jako mostek do połączeń VoIP wielopunktowych
8. Urządzenie musi obsługiwać funkcje współpracy miedzy systemami telefonicznej w zakresie:
   a. obsługi połączeń na bazie protokołów H.323 oraz SIP (SIP-SIP, SIP-H.323, H.323-H.323)
   b. możliwości dopasowania (normalizacji) protokołów H.323 oraz SIP
   c. obsługi połączeń głosowych na bazie protokołów G.711, G.729, G.722, iLBC
   d. obsługi połączeń wideo na bazie protokołów H.263 oraz H.264 AVC
   e. możliwości dopasowania kodeków (transcoding oraz transrating) dla protokołów G.711, G.729, G.722, iLBC z wykorzystaniem zasobów procesorów sygnałowych DSP posiadanych przez bramę
   f. obsługi połączeń T.38
9. Urządzenie musi być wyposażone w wewnętrzny układ DSP:
   a. o gęstości nie mniejszej niż 128 kanałów,
   b. pozwalającymi na dynamiczne alokowanie DSP do obsługi interfejsów głosowych, transkodowania faksów analogowych i konferencji w systemie telefonii Zamawiającego z granulacją do 1 DSP,
10. Urządzenie musi posiadać minimum 4 GB pamięci RAM wspierająca ECC. Zewnętrzna Pamięć typu Flash minimum 16 GB.
11. Minimum 1 port konsoli USB typu B lub szeregowy port konsoli.

12. Dostarczone urządzenia muszą posiadać aktualną dostępną na rynku wersję firmware oraz obsługę funkcjonalności voice.
13. Urządzenie musi współpracować z systemem zarządzania wykorzystywanym w Straży Granicznej, a w szczególności:
    a. wgrywania, aktualizacji, ściągania i analizy konfiguracji;
    b. inwentaryzacji;
    c. zmiany oprogramowania.
14. Urządzenie musi umożliwiać uwierzytelnianie, autoryzacje oraz rozliczalność (AAA) w oparciu o system kontroli dostępu Zamawiającego.
15. Urządzenie musi posiadać wiele poziomów dostępu administracyjnego przez konsolę. Musi ono umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilage-level).
16. Oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji.
17. Urządzenie musi posiadać obsługę protokołów routingu IP wykorzystywanych w sieci Zamawiającego.
18. Urządzenie musi posiadać obsługę dynamicznego tunelowania wykorzystywanego przez Zamawiającego,
19. Urządzenie musi posiadać wsparcie dla funkcjonalności Policy Based Routing.
20. Urządzenie musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2.
21. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF).
22. Urządzenie musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.
23. Urządzenie musi obsługiwać IPv6 w tym ICMP dla IPv6.
24. Urządzenie musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL.
25. Urządzenie musi umożliwiać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast.
26. Mechanizm NAT musi zapewniać wsparcie dla H.224/H.245.
27. Urządzenie musi posiadać obsługę mechanizmu DiffServ.
28. Urządzenie musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
29. Urządzenie musi zapewniać obsługę mechanizmów kolejkowania ruchu:
    a. z obsługą kolejki absolutnego priorytetu,
    b. ze statyczną alokacją pasma dla typu ruchu,
    c. WFQ.
30. Urządzenie musi obsługiwać mechanizm WRED.
31. Urządzenie musi obsługiwać protokół RSVP.
32. Urządzenie musi obsługiwać mechanizm Generic Traffic Shaping.
33. Urządzenie musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu.
34. Urządzenie musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.
35. Urządzenie musi obsługiwać protokół NTP.
36. Urządzenie musi obsługiwać DHCP w zakresie Client , Server.
37. Urządzenie musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy, który:
    a. musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych

b. musi pozwalać na generowanie akcji:
   - Wykonanie komendy z poziomu linii poleceń urządzenia
   - Wykonanie skryptu
   - Wygenerowanie SNMP trap
   - Ustawienie lub modyfikacja określonego licznika systemowego
c. funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa;
d. możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym przesyłu, który jest:
   - poddawany inspekcji,
   - odrzucany,
   - przenoszony bez inspekcji;

38. Urządzenie musi być zarządzalne za pomocą SNMPv2, SNMPv3,
39. Urządzenie musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI)
40. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo.
41. Urządzenie musi być przygotowane do montażu w szafie 19"
42. Urządzenie musi być wykonane z metalu. Ze względu na różne warunki, w których pracować będą urządzenia. Nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
43. Urządzenie musi posiadać dwa wbudowane zasilacze umożliwiające zasilanie prądem przemiennym 230V.

2.18. Przełącznik agregacyjny 48 SFP+ 6xQSFP+

W celu realizacji zadania w zakresie zapewnienia właściwego podłączenia serwerów Straży Granicznej niezbędne jest dostarczenie urządzeń spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 48 portów 1/10/25 Gbps
2) Przełącznik musi być wyposażony w minimum 6 interfejsów 40 Gbps.
3) Urządzenie musi posiadać min. 24 GB pamięci systemowej oraz dysk wewnętrzny min. 64 GB
4) Architektura przełącznika musi umożliwiać przepustowość co najmniej 1.5 Tbps.
5) Urządzenie musi mieć możliwość dołączenia co najmniej 4 zewnętrznych, wyniesionych modułów liniowych lub przełączników zapewniających każdy co najmniej 2 x porty 40GE oraz 48 x portów 1/10 Gbps i zarządzania tymi modułami lub przełącznikami wyłącznie z centralnego punktu sterowania na urządzeniu. Dołączenie modułów/przełączników nie może być zrealizowane z wykorzystaniem mechanizmów L2 Bridging/Spanning Tree, musi zapewniać bez pętlową topologię.
6) Urządzenie musi umożliwiać połączenie parami w jeden wirtualny przełącznik (widoczny jako jedno urządzenie) zapewniający topologię wolna od pętli w warstwie 2 i uproszczenie routingu.
7) Urządzenie musi obsługiwać co najmniej 4 sesje span.
8) Urządzenie musi obsługiwać następujące standardy Ethernet DCB (Data Center Bridging):
   a) IEEE 802.1Qbb PFC (Priority Based Flow Control),
   b) IEEE 802.1Qaz Enhanced Transmission Selection,

c) IEEE 802.1AB DCBX Protocol,

9) Przełącznik musi wspierać protokoły działające w sieci Zamawiającego, a także wszystkie podstawowe protokoły i funkcjonalności niezbędne dla budowy warstwy 2 i 3, a w szczególności:
   a) trunking IEEE 802.1Q VLAN,
   b) wsparcie dla 500 VLAN,
   c) wsparcie dla 64,000 adresów MAC,
   d) wsparcie dla Spanning Tree,
   e) grupowanie EtherChannel (co najmniej 16 portów per wiązka EtherChannel),
   f) Link Aggregation Control Protocol (LACP): IEEE 802.3ad,
   g) grupowanie typu MCEC/MLAG/virtual PortChannel polegające na terminowaniu pojedynczej wiązki EtherChannel (LACP) na 2 niezależnych urządzeniach,
   h) ramki Jumbo dla wszystkich portów (min. 9216 bajtów),
   i) prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast,
   j) Implementacja Private VLAN,
   k) 64,000 prefiksów IPv4 lub 32,000 prefiksów IPv6,
   l) 1 000 wpisów na potrzeby ACL/QoS,
   m) Protokoły routingu dla IPv4: OSPFv2, and BGP,
   n) Protokoły routingu dla IPv6: OSPFv3, BGPv6,
   o) Policy Based Routing dla IPv4 oraz IPv6,
   p) co najmniej 50 instancji VRF,
10) urządzenie musi współpracować z systemem zarządzania wykorzystywanym w Straży Granicznej, a w szczególności:
   a) wgrywania, aktualizacji , ściągania i analizy konfiguracji;
   b) inwentaryzacji;
   c) zmiany oprogramowania.
11) urządzenie musi umożliwiać uwierzytelnianie, autoryzacje oraz rozliczalność (AAA) w oparciu o system kontroli dostępu Zamawiającego.
12) urządzenie musi posiadać co najmniej 2 zasilacze o mocy co najmniej 1 KW każdy.
13) musi być wykonany z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
14) urządzenie musi posiadać wiele poziomów dostępu administracyjnego przez konsolę. Musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilage-level).
15) urządzenie musi obsługiwać protokół NTP.
16) urządzenie musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI)
17) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo. Nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
18) urządzenie musi być przygotowane do montażu w szafie 19"
19) Zamawiający wymaga dostarczenia wkładek do przełącznika GLC-T oraz wkładek SFP+10G-SR zgodnie z załącznikiem nr 1 do niniejszego OPZ.

2.19. Przełącznik agregacyjny 48 RJ-45 6xQSFP+

W celu realizacji zadania w zakresie zapewnienia właściwego podłączenia serwerów Straży Granicznej niezbędne jest dostarczenie urządzeń spełniających poniższe wymagania:

1) Przełącznik musi być wyposażony w minimum 48 portów RJ-45 1/10 Gbps
2) Przełącznik musi być wyposażony w minimum 6 interfejsów 40 Gbps.
3) Urządzenie musi posiadać min. 24 GB pamięci systemowej oraz dysk wewnętrzny min. 64 GB
4) Architektura przełącznika musi umożliwiać przepustowość co najmniej 1,5 Tbps.
5) Urządzenie musi mieć możliwość dołączenia co najmniej 4 zewnętrznych, wyniesionych modułów liniowych lub przełączników zapewniających każdy co najmniej 2 x porty 40GE oraz 48 x portów 1/10 Gbps i zarządzania tymi modułami lub przełącznikami wyłącznie z centralnego punktu sterowania na urządzeniu. Dołączenie modułów/przełączników nie może być zrealizowane z wykorzystaniem mechanizmów L2 Bridging/Spanning Tree, musi zapewniać bez pętlową topologię.
6) Przełącznik musi umożliwiać połączenie parami w jeden wirtualny przełącznik (widoczny jako jedno urządzenie) zapewniający topologię wolna od pętli w warstwie 2 i uproszczenie routingu.
7) Urządzenie musi obsługiwać co najmniej 4 sesje span.
8) Urządzenie musi obsługiwać następujące standardy Ethernet DCB (Data Center Bridging):
   a) IEEE 802.1Qbb PFC (Priority Based Flow Control),
   b) IEEE 802.1Qaz Enhanced Transmission Selection,
   c) IEEE 802.1AB DCBX Protocol,
9) Przełącznik musi wspierać protokoły działające w sieci Zamawiającego, a także wszystkie podstawowe protokoły i funkcjonalności niezbędne dla budowy warstwy 2 i 3, a w szczególności:
   a) trunking IEEE 802.1Q VLAN,
   b) wsparcie dla 500 VLAN,
   c) wsparcie dla 64,000 adresów MAC,
   d) wsparcie dla Spanning Tree,
   e) grupowanie EtherChannel (co najmniej 16 portów per wiązka EtherChannel),
   f) Link Aggregation Control Protocol (LACP): IEEE 802.3ad,
   g) grupowanie typu MCEC/MLAG/virtual PortChannel polegające na terminowaniu pojedynczej wiązki EtherChannel (LACP) na 2 niezależnych urządzeniach,
   h) ramki Jumbo dla wszystkich portów (min. 9216 bajtów),
   i) prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast,
   j) Implementacja Private VLAN,
   k) 64,000 prefiksów IPv4 lub 32,000 prefiksów IPv6,
   l) 1 000 wpisów na potrzeby ACL/QoS,
   m) Protokoły routingu dla IPv4: OSPFv2, and BGP,
   n) Protokoły routingu dla IPv6: OSPFv3, BGPv6,
   o) Policy Based Routing dla IPv4 oraz IPv6,
   p) co najmniej 50 instancji VRF,
10) urządzenie musi współpracować z systemem zarządzania wykorzystywanym w Straży Granicznej, a w szczególności :
   a) wgrywania, aktualizacji , ściągania i analizy konfiguracji;
   b) inwentaryzacji;
   c) zmiany oprogramowania.
11) urządzenie musi umożliwiać uwierzytelnianie, autoryzacje oraz rozliczalność (AAA) w oparciu o system kontroli dostępu Zamawiającego.
12) przełącznik musi posiadać co najmniej 2 zasilacze o mocy co najmniej 0,6 KW każdy.
13) musi być wykonany z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.

14) urządzenie musi posiadać wiele poziomów dostępu administracyjnego przez konsolę. Musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilage-level).
15) musi obsługiwać protokół NTP.
16) musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI)
17) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo. Nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
18) Urządzenie musi być przygotowane do montażu w szafie 19"

2.20. Firewall dla dostępu zdalnego

W celu realizacji zadania w dostępu zdalnego dla administratorów do sieci Straży Granicznej niezbędne jest dostarczenie urządzeń bezpieczeństwa spełniających poniższe wymagania:

1) Urządzenie musi posiadać możliwość zarzadzania poprzez centralny system zarządzania urządzeniami bezpieczeństwa Zamawiającego (wymagane jest dostarczenie niezbędnych licencji)
2) możliwość wykonywania przez Centralny System Uwierzytelnia zmiany stanu uwierzytelniania tzw, CoA (Change of Authorization)
3) Urządzenie musi pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.
4) Urządzenie nie musi posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
5) Urządzenie musi pozwalać na definiowanie firewalli w trybie warstwy 3 OSI (routed) i warstwy drugiej OSI (transparentnej).
6) Wymagane jest dostarczenie funkcjonalności dla co najmniej 5 firewalli wirtualnych/kontekstów.
7) Urządzenie musi posiadać co najmniej 8GB pamięci RAM i 8GB pamięci Flash.
8) Urządzenie musi posiadać co najmniej :
   a) 6 portów 10/100/1000Base-T GigabitEthernet z możliwością tworzenia grup redundantnych (minimum trzy),
   b) 1 port 10/100Base-T FastEthernet. – port z dostępem do kontekstu administracyjnego,
   c) 1 port konsoli USB typu B lub szeregowy port konsoli (Urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie konsoli).
   d) Wbudowany dysk w RAID po minimum 100 GB
9) urządzenie musi posiadać pełną funkcjonalność systemu IPS (Intrusion Prevention System) przy pomocy wbudowanego modułu funkcjonalnego, moduł ten musi posiadać następujące funkcje:
   a) umożliwiać pracę w trybie IPS (In-line);
   b) umożliwiać wysyłanie próbek oprogramowania do analizy środowisku sandbox;
   c) musi wykrywać ataki w oparciu o sygnatury oraz o wykrywanie anomalii;
   d) blokowania, śledzenia , analizowania i naprawiania skutków (retrospekcja) ukierunkowanych i uporczywych ataków szkodliwego oprogramowania typu malware.

e) Wizualizację oraz geolokalizację zestawionych połączeń
f) Umożliwiać blokowanie połączeń w oparciu o geolokalizacje
g) Wizualizacje zagrożeń i zdarzeń w sieci
h) Wizualizacje i kontrola wykorzystywanych aplikacji
i) Inwentaryzacja sieci w czasie rzeczywistym (jakie systemy operacyjne, aplikacje) są używane
j) Możliwość integracji z AD i tworzenia polityk dostępu per grupy użytkowników
k) Filtracje url
l) Możliwość centralnego zarzadzania

10) urządzenie musi być dostarczone z aktualizacjami sygnatur na okres gwarancji.
11) urządzenie musi umożliwiać terminowanie co najmniej 250 jednoczesnych tuneli IPSec.
12) Urządzenie musi terminować co najmniej 250 jednoczesnych sesji VPN opartych o protokół HTTP/SSL. Zamawiający wymaga dostarczenie niezbędnych licencji.
13) przepustowość urządzenia przy jednoczesnym włączeniu usług zapory ogniowej oraz IPS musi być nie mniejsza niż 250 Mbps.
14) urządzenie musi zapewnić mechanizmy inspekcji aplikacyjnej i kontroli następujących protokołów:
    a) Hypertext Transfer Protocol (HTTP),
    b) File Transfer Protocol (FTP),
    c) Simple Mail Transfer Protocol (SMTP),
    d) Domain Name System (DNS),
    e) H.323
    f) Session Initiation Protocol (SIP)
    g) Lightweight Directory Access Protocol (LDAP)
    h) Internet Control Message Protocol (ICMP)
    i) Network File System (NFS)
15) urządzenie musi posiadać możliwość wyeksportowania konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline
16) urządzenie musi zapewniać co najmniej 250 Mbps dla szyfrowania VPN algorytmami AES (programowa funkcjonalność szyfrowania nie jest wymagana ale musi być dostępna w oparciu o zakup dodatkowych licencji lub wymiany oprogramowania)
17) rozwiązanie musi umożliwiać zestawienie sesji IPSec VPN, Site-to-site VPN i SSLVPN
18) urządzenie musi obsługiwać IKE i IKEv2
19) urządzenie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPSec z IKEv2 dla dostępu zdalnego w oparciu o Klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat)
20) urządzenie musi obsługiwać współpracę z serwerami certyfikatów (CA)
21) urządzenie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS w szczególności z Centralny System Uwierzytelniania Zamawiającego.
22) urządzenie musi umożliwiać obsługę co najmniej 100 VLAN.
23) urządzenie musi umożliwiać implementację w celu redundancji funkcji failover typu Active/Standy, Active-Active
24) urządzenie musi umożliwiać translację adresów sieciowych NAT – zarówno dla ruchu wchodzącego, jak i wychodzącego, obsługę protokołów routingu dynamicznego wykorzystywanego przez Zamawiającego.
25) urządzenie musi mieć możliwość montażu w szafie 19"
26) urządzenie musi posiadać dwa wbudowane, redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V. Zasilacze muszą być wymienne.

2.21. Firewall dla PSG Okęcie, KGSG (ul. Niepodległości), KGSG (ul. Podchorążych), MGMT dla CPSI, Extranetu i APN

W celu realizacji zadania dostępu zdalnego dla administratorów do sieci Straży Granicznej niezbędne jest dostarczenie urządzeń bezpieczeństwa spełniających poniższe wymagania:

1) Urządzenie musi posiadać możliwość zarzadzania poprzez centralny system zarządzania urządzeniami bezpieczeństwa Zamawiającego (wymagane dostarczenie niezbędnych licencji)
2) możliwość wykonywania przez Centralny System Uwierzytelnia zmiany stanu uwierzytelniania tzw, CoA (Change of Authorization)
3) urządzenie musi pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.
4) urządzenie musi pozwalać na definiowanie firewalli w trybie warstwy 3 OSI (routed) i warstwy drugiej OSI (transparentnej).
5) urządzenie musi posiadać co najmniej:
   a) 12 portów 10/100/1000Base-T GigabitEthernet z możliwością tworzenia grup redundantnych (minimum trzy),
   b) 4 interfejsy 1Gigabit Ethernet SFP
   c) 1 port 10/100Base-T FastEthernet. – port z dostępem do kontekstu administracyjnego,
   d) 1 port konsoli USB lub szeregowy port konsoli (Urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie konsoli).
   e) Wbudowany dysk SSD min. 100 GB
6) urządzenie musi posiadać pełną funkcjonalność systemu IPS (Intrusion Prevention System) przy pomocy wbudowanego modułu funkcjonalnego, moduł ten musi posiadać następujące funkcje:
   a) umożliwiać pracę w trybie IPS (In-line);
   b) umożliwiać wysyłanie próbek oprogramowania do analizy środowisku sandbox;
   c) musi wykrywać ataki w oparciu o sygnatury oraz o wykrywanie anomalii;
   d) blokowania, śledzenia , analizowania i naprawiania skutków (retrospekcja) ukierunkowanych i uporczywych ataków szkodliwego oprogramowania typu malware.
   e) Wizualizację oraz geolokalizację zestawionych połączeń
   f) umożliwiać blokowanie połączeń w oparciu o geolokalizacje
   g) Wizualizację zagrożeń i zdarzeń w sieci
   h) Wizualizację i kontrolę wykorzystywanych aplikacji
   i) Inwentaryzacja sieci w czasie rzeczywistym (jakie systemy operacyjne, aplikacje) są używane
   j) Możliwość integracji z AD i tworzenia polityk dostępu per grupy użytkowników
   k) Filtracja url
   l) Możliwość centralnego zarzadzania
7) musi być dostarczone z aktualizacjami sygnatur na okres gwarancji.
8) przepustowość urządzenia przy jednoczesnym włączeniu usług zapory ogniowej oraz IPS musi być wyższa niż 1,5 Gbps.
9) rozwiązanie musi zapewnić mechanizmy inspekcji aplikacyjnej i kontroli następujących protokołów:
   a) Hypertext Transfer Protocol (HTTP),
   b) File Transfer Protocol (FTP),
   c) Simple Mail Transfer Protocol (SMTP),
   d) Domain Name System (DNS),
   e) H.323
   f) Session Initiation Protocol (SIP)
   g) Lightweight Directory Access Protocol (LDAP)
   h) Internet Control Message Protocol (ICMP)

i) Network File System (NFS)

10) urządzenie musi umożliwiać terminowanie co najmniej 2000 jednoczesnych tuneli IPSec.
11) na urządzeniu musi istnieć możliwość terminowania sesji SSLVPN nie mniej niż 2000.
12) urządzenie musi umożliwiać zestawienie sesji IPSec VPN, Site-to-site VPN i SSLVPN
13) urządzenie musi obsługiwać IKE i IKEv2
14) urządzenie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPSec z IKEv2 dla dostępu zdalnego w oparciu o Klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat)
15) urządzenie musi obsługiwać współpracę z serwerami certyfikatów (CA)
16) urządzenie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS w szczególności z Centralny System Uwierzytelniania Zamawiającego.
17) urządzenie musi umożliwiać obsługę co najmniej 100 VLAN.
18) urządzenie musi umożliwiać implementację w celu redundancji funkcji failover typu Active/Standy, Active-Active
19) urządzenie musi umożliwiać translację adresów sieciowych NAT – zarówno dla ruchu wchodzącego, jak i wychodzącego, obsługę protokołów routingu dynamicznego wykorzystywanego przez Zamawiającego.
20) urządzenie musi mieć możliwość montażu w szafie 19"
21) urządzenie musi posiadać dwa wbudowane, redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V. Zasilacze muszą być wymienne.

2.22. Firewall do Internetu

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci Internet niezbędne jest dostarczenie urządzeń bezpieczeństwa - firewall spełniających poniższe wymagania:

1) urządzenie musi posiadać możliwość zarzadzania poprzez centralny system zarządzania urządzeniami bezpieczeństwa Zamawiającego (wymagane dostarczenie niezbędnych licencji);
2) urządzenie musi pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji;
3) urządzenie musi pozwalać na definiowanie firewalli w trybie warstwy 3 OSI (routed) i warstwy drugiej OSI (transparentnej);
4) wymagane jest dostarczenie funkcjonalności dla co najmniej 5 firewalli wirtualnych/kontekstów.
5) urządzenie musi posiadać co najmniej 1 slot na kartę rozszerzeń.
6) urządzenie musi posiadać co najmniej:
   a) 8 interfejsy 10Gigabit Ethernet SFP+(lub inny standard np. XFP),
   b) 1 port 1 Gigabit Ethernet. – port z dostępem do kontekstu administracyjnego,
   c) 1 port konsoli USB lub szeregowy port konsoli (Urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie konsoli).
7) urządzenie musi posiadać pełną funkcjonalność systemu IPS (Intrusion Prevention System) przy pomocy wbudowanego modułu funkcjonalnego, moduł ten musi posiadać następujące funkcje:
   a) umożliwiać pracę w trybie IPS (In-line);
   b) umożliwiać wysyłanie próbek oprogramowania do analizy środowisku sandbox;
   c) musi wykrywać ataki w oparciu o sygnatury oraz o wykrywanie anomalii;
   d) blokowania, śledzenia , analizowania i naprawiania skutków (retrospekcja) ukierunkowanych i uporczywych ataków szkodliwego oprogramowania typu malware.

e) Wizualizacja oraz geolokalizacja zestawionych połączeń
f) Możliwość blokowania połączeń w oparciu o geolokalizacje
g) Wizualizacja zagrożeń i zdarzeń w sieci
h) Wizualizacja i kontrola wykorzystywanych aplikacji
i) Inwentaryzacja sieci w czasie rzeczywistym (jakie systemy operacyjne, aplikacje) są używane
j) Możliwość integracji z AD i tworzenia polityk dostępu per grupy użytkowników
k) Filtracja url
l) Możliwość centralnego zarzadzania
m) musi być dostarczone z aktualizacjami sygnatur na okres gwarancji.

8) urządzenie musi mieć możliwość obsługi min. 2 000 000 jednoczesnych sesji połączeń (concurrent session)
9) przepustowość urządzenia przy jednoczesnym włączeniu usług zapory ogniowej oraz IPS musi być wyższa niż 10 Gbps.
10) urządzenie musi zapewnić mechanizmy inspekcji aplikacyjnej i kontroli następujących protokołów:
    a) Hypertext Transfer Protocol (HTTP), a
    b) File Transfer Protocol (FTP),
    c) Simple Mail Transfer Protocol (SMTP),
    d) Domain Name System (DNS),
    e) H.323
    f) Session Initiation Protocol (SIP)
    g) Lightweight Directory Access Protocol (LDAP)
    h) Internet Control Message Protocol (ICMP)
    i) Network File System (NFS)
11) urządzenie musi umożliwiać zestawienie sesji IPSec VPN, Site-to-site VPN i SSLVPN
12) urządzenie musi obsługiwać IKE i IKEv2
13) urządzenie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPSec z IKEv2 dla dostępu zdalnego w oparciu o Klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat)
14) urządzenie musi obsługiwać współpracę z serwerami certyfikatów (CA)
15) urządzenie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS w szczególności z Centralny System Uwierzytelniania Zamawiającego.
16) urządzenie musi umożliwiać obsługę co najmniej 100 VLAN.
17) urządzenie musi umożliwiać implementację w celu redundancji funkcji failover typu Active/Standy, Active-Active oraz Cluster (wymagane dostarczenie licencji umożliwiające uruchomienie Cluster dla co najmniej 2 urządzeń)..
18) urządzenie musi umożliwiać translację adresów sieciowych NAT – zarówno dla ruchu wchodzącego, jak i wychodzącego, obsługę protokołów routingu dynamicznego wykorzystywanego przez Zamawiającego.
19) urządzenie musi mieć możliwość montażu w szafie 19"
20) urządzenie musi posiadać dwa wbudowane, redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V. Zasilacze muszą być wymienne.

2.23. Firewall dla bloku CPSI

W celu realizacji zadania w dostępu zdalnego dla użytkowników sieci Straży Granicznej niezbędne jest dostarczenie 10 licencji na wirtualne urządzenia bezpieczeństwa spełniających poniższe wymagania:

1) Urządzenie wirtualne musi mieć możliwość zarzadzania poprzez centralny system zarządzania urządzeniami bezpieczeństwa Zamawiającego (wymagane dostarczenie niezbędnych licencji)
2) Urządzenie wirtualne musi pełnić rolę statefull firewall w trybach transparentnym oraz L3.
3) Urządzenia wirtualne muszą umożliwiać uwierzytelnianie, autoryzacje oraz rozliczalność (AAA) w oparciu o system kontroli dostępu Zamawiającego.
4) Urządzenie wirtualne musi mieć możliwość instalacji w środowisku VMware ESX/ESXi 5.x,
5) Urządzenie wirtualne musi terminować co najmniej 250 jednoczesnych sesji VPN opartych o protokół HTTP/SSL. Zamawiający wymaga dostarczenie niezbędnych licencji.
6) Maksymalna przepustowość obsługiwana przez urządzenie wirtualne nie może być mniejsza niż 500 Mbps w trybie Stateful inspection
7) Urządzenie wirtualne musi umożliwiać obsługę co najmniej 50 VLAN.
8) Urządzenie wirtualne musi umożliwiać implementację w celu redundancji funkcji failover typu Active/Standby.
9) Urządzenie wirtualne musi umożliwiać translację adresów sieciowych NAT – zarówno dla ruchu wchodzącego, jak i wychodzącego, obsługę protokołu routingu wykorzystywanego przez Zamawiającego.
10) Urządzenie wirtualne muszą współpracować z systemem zarządzania urządzeniami bezpieczeństwa wykorzystywanym w Straży Granicznej, a w szczególności:
    a) wgrywania, aktualizacji , ściągania i analizy konfiguracji,
    b) zmiany oprogramowania.

2.24. Centralny system zarzadzania IPS

Zamawiający wymaga dostarczenia 20 licencji dla posiadanego systemu zarządzania urządzeniami bezpieczeństwa dla dostarczonych urządzeń IPS.

2.25. Router do Internetu

W celu realizacji zadania w zakresie zapewnienia właściwego dostępu do sieci Internet niezbędne jest dostarczenie ruterów spełniających poniższe wymagania:

1) system operacyjny (licencja) wspierający IPsec, Firewall
2) urządzenie musi posiadać obsługę protokołów routingu IP wykorzystywanych w sieci Zamawiającego.
3) urządzenie musi posiadać obsługę protokołu BGP i pomieścić minimum 2 kopie całej tablicy internetowej BGP IPv4
4) urządzenie musi posiadać obsługę dynamicznego tunelowania wykorzystywanego przez Zamawiającego,
5) urządzenie musi być routerem umożliwiającym jednoczesne wykorzystanie minimum 6 interfejsów Gigabit Ethernet SFP i 4 interfejsami SFP+ 10 Gbit/s.
6) urządzenie musi obsłużyć ruch internetowy :
   - od dwóch niezależnych ISP (dwie pełne tablice BGP IPv4 i IPv6)
   - dwóch łączy symetrycznych o przepustowości min. 2 Gb/s każde
7) urządzenie musi posiadać minimum 16 GB pamięci RAM wspierająca ECC.
8) musi by wyposażone w pamięć bootflash o pojemności co najmniej 16 GB do przechowywania obrazów systemu operacyjnego, konfiguracji i logów systemowych.
9) urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie konsoli.
10) minimum 1 port konsoli USB typu B lub szeregowy port konsoli.
11) dostarczone urządzenia muszą posiadać aktualną dostępną na rynku wersję firmware
12) urządzenie musi współpracować z systemem zarządzania wykorzystywanym w Straży Granicznej, a w szczególności:

a) wgrywania, aktualizacji , ściągania i analizy konfiguracji;
b) inwentaryzacji;
c) zmiany oprogramowania

13) urządzenie musi umożliwiać uwierzytelnianie, autoryzacje oraz rozliczalność (AAA) w oparciu o system kontroli dostępu Zamawiającego (w szczególności autoryzację pojedynczych komend administracyjnych).
14) urządzenie musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
15) oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji.
16) urządzenie musi posiadać obsługę protokołów routingu IP wykorzystywanych w sieci Zamawiającego.
17) urządzenie musi posiadać wsparcie dla funkcjonalności Policy Based Routing.
18) urządzenie musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2.
19) urządzenie musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF).
20) urządzenie musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.
21) urządzenie musi obsługiwać IPv6 w tym ICMP dla IPv6.
22) urządzenie musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL.
23) urządzenie musi umożliwiać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast.
24) urządzenie musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 50 instancji VRF.
25) urządzenie musi być w stanie obsłużyć 1000 wpisów w tablicach VRF (sumaryczna wartość dla wszystkich VRF).
26) urządzenie musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
27) urządzenie musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu.
28) musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.
29) urządzenie musi obsługiwać protokół NTP.
30) urządzenie musi zapewniać obsługę mechanizmów kolejkowania ruchu:
    a) z obsługą kolejki absolutnego priorytetu,
    b) ze statyczną alokacją pasma dla typu ruchu,
    c) WFQ.
31) urządzenie musi obsługiwać mechanizm WRED.
32) urządzenie musi obsługiwać protokół RSVP.
33) urządzenie musi obsługiwać mechanizm Generic Traffic Shaping.
34) urządzenie musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy, który:
    a) musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych
    b) musi pozwalać na generowanie akcji:
        - wykonanie komendy z poziomu linii poleceń urządzenia
        - wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej
        - wykonanie skryptu
        - wygenerowanie SNMP trap

- ustawienie lub modyfikacja określonego licznika systemowego

35) urządzenie musi posiadać wsparcie dla następujących funkcjonalności:
   a) funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów AES - 256.
   b) możliwość konfiguracji tuneli IPv4 IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2) dla rozwiązań dynamicznego tunelowania wykorzystywanego przez Zamawiającego,
   c) funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall);
   d) funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa ;
   e) możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym przesyłu, który jest:
      - poddawany inspekcji,
      - odrzucany,
      - przenoszony bez inspekcji;
36) urządzenie musi posiadać możliwość rozbudowania o funkcjonalności w oparciu o zakup dodatkowych licencji lub opcji sprzętowe realizujące optymalizacje ruchu sieciowego poprzez współpracę z wykorzystywanymi przez Zamawiającego akceleratorami ruchu.
37) urządzenie musi być zarządzane za pomocą SNMPv2, SNMPv3.
38) urządzenie musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI).
39) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo. Nie opuszcza się częściowych restartów urządzenia po dokonaniu zmian.
40) Urządzenie musi być przygotowane do montażu w szafie 19"
41) urządzenie musi posiadać dwa wbudowane redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V.
42) urządzenie musi posiadać wiele poziomów dostępu administracyjnego przez konsolę. Musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilage-level).

2.26. Router do OST112

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci OST112 niezbędne jest dostarczenie ruterów spełniających poniższe wymagania:

1) system operacyjny (licencja) wspierający IPsec, Firewall
2) urządzenie musi posiadać obsługę protokołów routingu IP wykorzystywanych w sieci Zamawiającego.
3) urządzenie musi posiadać obsługę dynamicznego tunelowania wykorzystywanego przez Zamawiającego,
4) urządzenie musi być routerem modularnym (możliwości rozbudowy, wymiany) z możliwością zainstalowania w nim minimum 4 interfejsów Gigabit Ethernet 10/100/1000 i 4 interfejsów TenGigabit Ethernet dla realizacji połączenia do sieci LAN, WAN i łączy awaryjnych. Interfejsy muszą mieć możliwość obsadzenia wkładkami typu SFP lub SFP+
5) Dedykowany sprzętowy akcelerator kryptograficzny wspierający NSA Cryptography SUITE-B zapewniający obsługę ruchu szyfrowanego minimum 20 Gb/s.
   a) musi umożliwiać wymianę modułów w trakcie pracy (ang. hot swap).
   b) musi posiadać wbudowany sprzętowy moduł akceleracji szyfrowania

6) urządzenie musi obsługiwać co najmniej 4 000 tuneli GRE.
7) urządzenie musi posiadać minimum 16 GB pamięci RAM wspierająca ECC.
8) urządzenie musi by wyposażone w wewnętrzna pamięć bootflash o pojemności co najmniej 1 GB do przechowywania obrazów systemu operacyjnego, konfiguracji i logów systemowych.
9) urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie konsoli
10) urządzenie musi być wyposażone w minimum 1 port konsoli USB typu B lub szeregowy port konsoli.
11) urządzenie musi posiadać aktualną dostępną na rynku wersję firmware oraz obsługę security.
12) urządzenie musi współpracować z systemem zarządzania wykorzystywanym w Straży Granicznej, a w szczególności :
    a) wgrywania, aktualizacji , ściągania i analizy konfiguracji;
    b) inwentaryzacji;
    c) zmiany oprogramowania.
13) urządzenie musi umożliwiać uwierzytelnianie, autoryzacje oraz rozliczalność komend (AAA) w oparciu o system kontroli dostępu Zamawiającego.
14) Urządzenie musi być wykonane z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
15) oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji.
16) urządzenie musi być musi posiadać obsługę protokołów routingu IP wykorzystywanych w sieci Zamawiającego.
17) urządzenie musi posiadać obsługę ruchu VPN wykorzystywanego w sieci WAN Zamawiającego
18) urządzenie musi posiadać wsparcie dla funkcjonalności Policy Based Routing.
19) urządzenie musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF).
20) urządzenie musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.
21) urządzenie musi obsługiwać IPv6 w tym ICMP dla IPv6.
22) urządzenie musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL.
23) urządzenie musi umożliwiać obsługę NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast.
24) urządzenie musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 50 instancji VRF.
25) urządzenie musi być w stanie obsłużyć 1000 wpisów w tablicach VRF (sumaryczna wartość dla wszystkich VRF).
    urządzenie musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
26) urządzenie musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu.
27) urządzenie musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.
28) urządzenie musi obsługiwać protokół NTP.
29) urządzenie musi obsługiwać DHCP w zakresie Client , Server.
30) urządzenie musi zapewniać obsługę mechanizmów kolejkowania ruchu:
    a) z obsługą kolejki absolutnego priorytetu,
    b) ze statyczną alokacją pasma dla typu ruchu,
    c) WFQ.
31) urządzenie musi obsługiwać mechanizm WRED.
32) urządzenie musi obsługiwać protokół RSVP.
33) urządzenie musi obsługiwać mechanizm Generic Traffic Shaping.

34) urządzenie musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy, który:
    a) musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych
    b) musi pozwalać na generowanie akcji:
        - wykonanie komendy z poziomu linii poleceń urządzenia
        - wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej
        - wykonanie skryptu
        - wygenerowanie SNMP trap
        - ustawienie lub modyfikacja określonego licznika systemowego
35) urządzenie musi posiadać wsparcie dla następujących funkcjonalności:
    a) funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów AES - 256.
    b) możliwość konfiguracji tuneli IPv4 IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2) dla rozwiązań dynamicznego tunelowania wykorzystywanego przez Zamawiającego,
    c) funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall);
    d) funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa ;
    e) możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym przesyłu, który jest:
        - poddawany inspekcji,
        - odrzucany,
        - przenoszony bez inspekcji;
36) urządzenie musi być zarządzalne za pomocą SNMPv2, SNMPv3.
37) musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI).
38) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo. Nie opuszcza się częściowych restartów urządzenia po dokonaniu zmian.
39) urządzenie musi być przygotowane do montażu w szafie 19"
40) urządzenie musi posiadać dwa wbudowane redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V.
41) urządzenie musi posiadać wiele poziomów dostępu administracyjnego przez konsolę. Musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilage-level).

2.27. Router do sieci MetroEthernet

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci MAN niezbędne jest dostarczenie ruterów spełniających poniższe wymagania:

1) urządzenie musi posiadać obsługę protokołów routingu IP wykorzystywanych w sieci Zamawiającego oraz IS-IS i BGP.
2) urządzenie musi posiadać architekturę umożliwiającą przełączanie w warstwie 2 ethernet oraz obsługiwać routing ipv4, ipv6 i MPLS oraz technologie MetroEthernet
3) urządzenie musi być wyposażone w poniższe porty:

a) co najmniej 8 portów dostępowych Ethernet 1000BASE-T IEEE 802.3ab (RJ45). Wszystkie porty muszą być aktywne i pracować z maksymalną prędkością
b) co najmniej 12 portów 1GE SFP IEEE 802.3z wyposażone w 8 modułów SFP 1000BASE-T (RJ45). Wszystkie porty muszą być aktywne i pracować z maksymalną prędkością
c) co najmniej 2 porty 10 Gigabit Ethernet SFP+ obsługujących co najmniej moduły, zgodne ze standardem IEEE 802.3ae: SFP+ 10GBASE-LR i 10GBASE-SR. Jeden port musi być wyposażony w moduł 10GBASE-LR 10km w pełni kompatybilne z modułami oferowanymi przez producenta urządzenia. Drugi port musi być wyposażony w moduł 10GBASE-SR w pełni kompatybilne z modułami oferowanymi przez producenta urządzenia. Wszystkie porty muszą być aktywne i pracować z maksymalną prędkością

4) urządzenie musi posiadać minimum 4 GB pamięci RAM wspierająca ECC.
5) urządzenie musi by wyposażone w wewnętrzna pamięć bootflash o pojemności co najmniej 2 GB do przechowywania obrazów systemu operacyjnego, konfiguracji i logów systemowych.
6) urządzenie musi mieć wydajność co najmniej 64Gb/s
7) urządzenie powinno być wyposażone w dwa w redundantne zasilacze AC, przystosowane do zasilania z sieci 230V/50Hz.
8) urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie konsoli.
9) Urządzenie musi posiadać minimum 1 port konsoli USB typu B lub szeregowy port konsoli.
10) urządzenie musi posiadać aktualną dostępną na rynku wersję firmware
11) urządzenie musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
12) urządzenie powinno być wyposażone w dwa w redundantne zasilacze AC, przystosowane do zasilania z sieci 230V/50Hz.
13) urządzenie obsługuje co najmniej 16000 adresów MAC, w tym co najmniej 1000 adresów MAC opisanych statycznie w konfiguracji.
14) urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1Q w ilości nie mniejszej niż 4000 z zakresu 1-4090 VLAN ID. Musi istnieć możliwość konfigurowania subinterfejasów L3 z lokalnym znaczeniem vlanu dla danego interfejsu.
15) Urządzenie musi obsługiwać agregowanie połączeń zgodnie z IEEE 802.3ADUrządzenie musi obsługiwać MultiChassis LACP.
16) urządzenie musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL. Urządzenie realizuje sprzętowo nie mniej niż 2000 reguł filtrowania ruchu dla pakietów ipv4 lub ipv6. Jest dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu oraz możliwość zliczania pakietów spełniających wybrane parametry.
17) urządzenie jest wyposażone dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
18) urządzenie umożliwia ustawienie co najmniej 4000 limitów pakietów (policers) akceptowanych na wskazanych portach w jednostce czasu (tzw. rate-limit). Urządzenie odrzuca pakiety przekraczające limit. Istnieje możliwość ustawiania limitów pakietów indywidualnie dla każdego interfejsu.
19) urządzenie obsługuje Private VLANs (across switches).
20) urządzenie posiada funkcjonalność netFlow lub funkcjonalnie odpowiednią (np. RFC3176 sFlow) umożliwiającą monitorowanie ruchu w warstwach 3 do 4 modelu OSI dla pakietów IPv4.
21) urządzenie obsługuje protokół Spanning Tree i Rapid Spannig Tree, a także Multiple Spanning Tree (nie mniej niż 16 instancji MSTP) oraz VLAN Spanning Tree Protocol (lub równoważny) dla co najmniej 128 vlan-ów.
22) urządzenie obsługuje protokół MVR (Multicast VLAN Registration).
23) urządzenie obsługuje sprzętowo takie mechanizmy bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, IP Source Guard, DHCP Snooping dla protokołu

ipv4 i ich odpowiedniki w protokole ipv6, tzn. Negihbor Discover Inspection oraz filtruje Router Advertisements na niezaufanych portach.

24) urządzenie potrafi pracować w trybie proxy ARP oraz wykonywać DHCP relay (ipv4 i ipv6) na zadanych interfejsach
25) urządzenie posiada możliwość wyłączenia Spanning Tree oraz filtrowania (ignorowania) ramek BPDU na wskazanych portach.
26) urządzenie musi obsługiwać sprzętowo co najmniej 20000 tras routingu unicast ipv4, 5000 tras ipv6; 16000 pozycji ARP, 100 tras multicast ipv4 (lub IGMP groups) równocześnie.
27) urządzanie musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 30 instancji VRF
28) urządzenie musi posiadać wsparcie dla funkcjonalności Policy Based Routing.
29) Urządzenie obsługuje protokół GRE, umożliwiając tunelowanie pakietów ipv4 oraz ipv6.
30) urządzenie musi obsługiwać protokół MPLS w oparciu o LDP i RSVP, również FRR;
31) minimum 128 instancji L2VPN, L3VPN oraz VPLS (co najmniej 32 PE (neighbours) dla każdej instancji), z sygnalizacją LDP oraz BGP;
    a) inter-AS VPN;
    b) MPLS OAM (ping);
    c) Multicast VPN (BGP mVPN)
32) urządzenie Musi istnieć możliwość pisania prostych skryptów na urządzeniu (Embedded Event Manager), realizujących zadane operacje po zajściu wyspecyfikowanego zdarzenia.
33) urządzenie umożliwia zdefiniowanie osobnego filtra do ochrony procesora CPU (Control Plane Policy) lub inny mechanizm umożliwiający limitowanie (rate-limit) poszczególnych rodzajów pakietów wymagających obsługi przez CPU.
34) musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
35) urządzenie musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu.
36) urządzenie musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.
37) urządzenie musi obsługiwać protokół NTP.
38) urządzenie musi obsługiwać DHCP w zakresie Client , Server.
39) urządzenie musi zapewniać obsługę mechanizmów kolejkowania ruchu:
    a) z obsługą kolejki absolutnego priorytetu,
    b) ze statyczną alokacją pasma dla typu ruchu,
    c) WFQ.
40) urządzenie musi obsługiwać mechanizm WRED.
41) urządzenie musi obsługiwać protokół RSVP.
42) urządzenie musi obsługiwać mechanizm Generic Traffic Shaping.
43) urządzenie musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy, który:
    a) musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych
    b) musi pozwalać na generowanie akcji:
        a) wykonanie komendy z poziomu linii poleceń urządzenia
        b) wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej
        c) wykonanie skryptu
        d) wygenerowanie SNMP trap
        e) ustawienie lub modyfikacja określonego licznika systemowego
44) urządzenie musi być zarządzalne za pomocą SNMPv2, SNMPv3.
45) urządzenie musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI).
46) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian

konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo. Nie opuszcza się częściowych restartów urządzenia po dokonaniu zmian.

47) urządzenie musi mieć możliwość montażu w szafie 19".
48) urządzenie musi posiadać dwa wbudowane redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V.
49) urządzenie musi posiadać wiele poziomów dostępu administracyjnego przez konsolę. Musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilage-level).

2.28. Karty do NEXUS 24 portowa 40Gbps

W celu realizacji zadania w zakresie zapewnienia właściwego działania szkieletu sieci Straży Granicznej niezbędne jest dostarczenie kart do posiadanych przez Zamawiającego przełączników Nexus N77-C7706-B23S2E wyposażonych w karty N77-F348XP-23. Karty muszą spełniać następujące wymagania:

1) Moduł musi być wyposażony w porty 40 GigabitEthernet o gęstości 24 portów umożliwiający instalację wkładek QSFP. Zamawiający wymaga dostarczenia do kart łącznie :
   - 20 wkładek światłowodowych typu QSFP-40G-SR4-S
   - 20 połączeń typu 40GE Twinax 2 metrowych,
   - 20 połączeń typu 40GE Twinax 10 metrowych,
   - 10 patchord'ów światłowodowych 25 m do połączenia pomiędzy wkładkami typu QSFP-40G-SR4-S
2) Pełna współpraca z wykorzystywanym przez Zamawiającego przełącznikiem Cisco Nexus 7706.
3) Moduł musi mieć możliwość podzielenia na co najmniej 12 grup portów przypisywanych do oddzielnych przełączników wirtualnych.
4) moduł musi mieć przepustowość 960 Gbps
5) moduł musi mieć możliwość dołączenia, wyniesionych modułów liniowych lub przełączników z przepustowością 10Gbps – 40Gbps. Dołączenie modułów/przełączników nie może być zrealizowane z wykorzystaniem mechanizmów L2 Bridging/Spanning Tree, musi zapewniać bez pętlową topologię.
6) Moduł musi wspierać funkcjonalność vPC stosowaną przez Zamawiającego zapewniającą topologię wolna od pętli w warstwie 2 i uproszczająca routing.
7) Moduł musi wspierać protokoły działające w sieci Zamawiającego, a także wszystkie podstawowe protokoły niezbędne dla budowy warstwy 2 i 3.

2.29. Oprogramowanie do balansowania ruchu

W celu realizacji zadania w zakresie równoważnego obciążenia ruchu sieciowego w CWT niezbędne jest dostarczenie aplikacji spełniających poniższe wymagania:

1) System musi umożliwiać realizację rozdziału ruchu w oparciu o informację z warstw 4-7 modelu ISO/OSI.
2) Obsługa inteligentnego równoważenia ruchu dla farm serwerów przy wsparciu dla protokołów:
   - TCP

- UDP
- FTP
- http
- HTTPS
- DNS
- RADIUS
- SQL
- RDP

3) System ma umożliwiać balansowanie ruchu w oparciu o algorytmy:
   a) Round Robin
   b) obciążenie serwerów
   c) ilość połączeń
   d) dostępne pasmo
   e) czas odpowiedzi
   f) hashing (URL, Domain, source IP, Destination IP)
4) System ma umożliwiać mechanizm dowiązania sesji (session persistant) w oparciu o:
   a) source IP
   b) Cookie
   c) Server
   d) Sesję SSL
5) System ma umożliwiać monitorowanie stanów serwerów i na tej podstawie dokonywania decyzji o przełączaniu w oparciu o :
   a) Ping
   b) TCP
   c) URL
   d) Skrypty
   e) Dynamic Server Response Time
6) System ma wspierać content switching w oparciu o:
   a) polityki:
      - URL
      - URL query
      - URL wildcard
      - Domain
      - Source IP
      - Destination IP
      - Nagłówek http
      - Dane HTTP i TCP
      - UDP
   b) protokoły w przychodzących pakietach
7) System ma zapewnić Database load balancing w zakresie:
   a) wsparcie dla Microsoft SQL Server 2012
   b) algorytmy przełączania w oparciu o zapytania SQL takie jak użytkownik, nazwy i parametry komend
   c) możliwość klastrowania kilku balancerów aby były widoczne jako jeden system
   d) możliwość skonfigurowania głównego węzła w celu synchronizacji i zarządzania
   e) wsparcie dla kluster link aggregation groups zgodnie z IEEE 802.3ad
   f) wsparcie dla replikacji z systemami redundantnymi
8) System ma zapewniać mechanizmy ograniczenia ruchu dla poszczególnych serwerów w oparciu o:
   a) Połączenia na sekundę
   b) Pakiety na sekundę
   c) Użycie pasma
   d) Source IP
   e) Destination IP
9) System ma wspierać Globar Server load balancing (GSLB):

a) w oparciu o algorytmy:
   - Stanu węzła
   - Geograficznej lokalizacji
   - Sąsiedztwa sieciowego
   - Połączeń
   - Przepustowości
b) stan węzła sprawdzany na podstawie:
   - Statusu
   - Stanu połączeń
   - Ilości pakietów
   - SNMP

10) System ma zapewnić kontrolę:
    a) nad ilością połączeń TCP i zapytań HTTP
    b) nad priorytetyzacją ruchu dla krytycznych aplikacji
11) System musi umożliwiać :
    a) obsługę list kontroli dostępu dla 3 i 4 warstwy ISO/OSI
    b) zabezpieczenie przed atakami http Dos
    c) zabezpieczenie przed atakami SYN flood
    d) zabezpieczenie przed atakami Ping of Death
    e) kontrola nad ICMP i UDP
    f) NAT
    g) dla funkcji firewall minimalną przepustowość 500 Mbps
12) System musi umożliwiać obsługę sieci co najmniej w zakresie:
    a) Routingu statycznego
    b) OSPF, RIP1/2,BGP
    c) LACP
    d) VLAN 802.1q
13) System musi wspierać wysoką dostępność:
    a) Active/passive
    b) Active/active
    c) VRPP
    d) ECMP
    e) Connection Mirroring
14) System musi umożliwiać zarządzanie za pomocą interfejsu graficznego przez:
    a) przeglądarkę internetową, w tym co najmniej przy pomocy Google Chrome, Microsoft IE , Mozilla Firefox
    b) CLI, Telnet,SSH
15) System musi umożliwiać autentykacje w oparciu o:
    a) LDAP
    b) RADIUS
    c) protokołu AAA wykorzystywanego przez Zamawiającego
    d) Certyfikaty
16) Przepustowość HTTP i HTTPS musi wynosić minimum 1Gbps.
17) Urządzenie musi mieć możliwość obsługi min. 500 jednoczesnych nowych sesji połączeń SSL.
18) Urządzenie musi mieć możliwość obsługi min. 200 000 jednoczesnych sesji połączeń (concurrent session)
19) System musi posiadać wsparcie techniczne na czas określony w Umowie z możliwością m.in.: podnoszenie wersji oprogramowania, zgłaszanie problemów związanych z funkcjonowaniem systemy, wykrycia tzw. bug'ów.
20) System musi być dostarczony z odpowiednimi do wymagań licencjami.
21) System musi być dostarczony w najnowszej, dostępnej w chwili realizacji zamówienia wersji.

2.30. Urządzenie do balansowania ruchu

W celu realizacji zadania w zakresie równoważnego obciążenia ruchu sieciowego w CWT niezbędne jest dostarczenie urządzeń spełniających poniższe wymagania:

1) Obudowa – z możliwością montażu w szafie 19", max wysokość 2RU.
2) Minimum 6 portów 10/100/1000BaseT oraz minimum 2 porty 10 Gigabit Ethernet SFP+ wyposażone we wkładki 10GBASE-SR ,
3) Wymagane min. 32 GB pamięci DRAM
4) System musi umożliwiać realizację rozdziału ruchu w oparciu o informację z warstw 4-7 modelu ISO/OSI.
5) Obsługa inteligentnego równoważenia ruchu dla farm serwerów przy wsparciu dla protokołów:
   - TCP
   - UDP
   - FTP
   - http
   - HTTPS
   - DNS
   - RADIUS
   - SQL
   - RDP
6) System ma umożliwiać balansowanie ruchu w oparciu o algorytmy:
   a) Round Robin
   b) obciążenie serwerów
   c) ilość połączeń
   d) dostępne pasmo
   e) czas odpowiedzi
   f) hashing (URL, Domain, source IP, Destination IP)
7) System ma umożliwiać mechanizm dowiązania sesji (session persistant) w oparciu o:
   a) source IP
   b) Cookie
   c) Server
   d) Sesję SSL
8) System ma umożliwiać monitorowanie stanów serwerów i na tej podstawie dokonywania decyzji o przełączaniu w oparciu o :
   a) Ping
   b) TCP
   c) URL
   d) Skrypty
   e) Dynamic Server Response Time
9) System ma wspierać content switching w oparciu o:
   a) polityki:
- URL
- URL query
- URL wildcard
- Domain
- Source IP
- Destination IP
- Nagłówek http
- Dane HTTP i TCP
- UDP
   b) protokoły w przychodzących pakietach
10) System ma zapewnić Database load balancing w zakresie:
   a) wsparcie dla Microsoft SQL Server 2012

b) algorytmy przełączania w oparciu o zapytania SQL takie jak użytkownik, nazwy i parametry komend
c) możliwość klastrowania kilku balancerów aby były widoczne jako jeden system
d) możliwość skonfigurowania głównego węzła w celu synchronizacji i zarządzania
e) wsparcie dla kluster link aggregation groups zgodnie z IEEE 802.3ad
f) wsparcie dla replikacji z systemami redundantnymi

11) System ma zapewniać mechanizmy ograniczenia ruchu dla poszczególnych serwerów w oparciu o:
a) Połączenia na sekundę
b) Pakiety na sekundę
c) Użycie pasma
d) Source IP
e) Destination IP

12) System ma wspierać Globar Server load balancing (GSLB):
a) w oparciu o algorytmy:
- Stanu węzła
- Geograficznej lokalizacji
- Sąsiedztwa sieciowego
- Połączeń
- Przepustowości

b) stan węzła sprawdzany na podstawie:
- Statusu
- Stanu połączeń
- Ilości pakietów
- SNMP

13) System ma zapewnić kontrolę:
a) nad ilością połączeń TCP i zapytań HTTP
b) nad priorytetyzacją ruchu dla krytycznych aplikacji

14) System musi umożliwiać :
a) obsługę list kontroli dostępu dla 3 i 4 warstwy ISO/OSI
b) zabezpieczenie przed atakami http Dos
c) zabezpieczenie przed atakami SYN flood
d) zabezpieczenie przed atakami Ping of Death
e) kontrola nad ICMP i UDP
f) NAT
g) dla funkcji firewall minimalną przepustowość 500 Mbps

15) System musi umożliwiać obsługę sieci co najmniej w zakresie:
a) Routingu statycznego
b) OSPF, RIP1/2,BGP
c) LACP
d) VLAN 802.1q

16) System musi wspierać wysoką dostępność:
a) Active/passive
b) Active/active
c) VRPP
d) ECMP
e) Connection Mirroring

17) System musi umożliwiać zarządzanie za pomocą interfejsu graficznego przez:
a) przeglądarkę internetową, w tym co najmniej przy pomocy Google Chrome, Microsoft IE, Mozilla Firefox
b) CLI, Telnet,SSH

18) System musi umożliwiać autentykacje w oparciu o:
a) LDAP
b) RADIUS
c) protokołu AAA wykorzystywanego przez Zamawiającego

d) Certyfikaty

19) Przepustowość HTTP i HTTPS musi wynosić minimum 4 Gbps.
20) Urządzenie musi mieć możliwość obsługi min. 4000 jednoczesnych sesji połączeń SSL.
21) Urządzenie musi mieć możliwość obsługi min. 200 000 jednoczesnych sesji połączeń (concurrent session)
22) System musi posiadać wsparcie techniczne na czas określony w Umowie z możliwością m.in.: podnoszenie wersji oprogramowania, zgłaszanie problemów związanych z funkcjonowaniem systemy, wykrycia tzw. bug'ów.
23) System musi być dostarczony z odpowiednimi do wymagań licencjami.
24) System musi być dostarczony w najnowszej, dostępnej w chwili realizacji zamówienia wersji.

2.31. Serwer PROXY

Zamawiający wymaga dostarczenia fizycznych serwerów do Centralnego Systemu Proxy spełniający wymagania:

1) obsługa ruchu Internetowego 1Gbps przy założeniu:
   - uruchomione 2 skanery Anti-Malware w ramach licencji IronPort: webroot oraz sophos
   - wykorzystywanie: AUC (Cisco WUC with AVC), WREP (Web Reputation Filters)
   - uruchomiony offload SSL dla całego ruchu HTTPS (Web reputation Score nie jest wykorzysytwane do wyłączenia offload SSL dla stron z bardzo dobrą reputacją)
   - uwierzytelnienie użytkowników oparte o NTLMSSP
   - włączony cache dyskowy
2) urządzenie posiada wbudowaną macierz dyskową z min. 8 dysków10k SAS z możliwością wymiany dysków "na gorąco"
3) urządzenie posiada min 6 interfejsów sieciowych 10/100/1000 RJ45 oraz min. 6 interfejsy sieciowe światłowodowe 10G Base-SR
4) urządzenie posiada redundantne zasilacze (min. 2 sztuki)
5) urządzanie powinno mieć możliwość instalacji w 19" szafie rack
6) urządzenie powinno posiadać min 64 GB pamięci RAM
7) urządzenie powinno posiadać min. 2 fizyczne procesory, każdy z min. 24 niezależnymi rdzeniami
8) współpraca z centralnym systemem zarządzania opartym o urządzenie Cisco M670 (realizujący funkcję kolektora logów oraz dystrybucji konfiguracji na urządzenia proxy)

2.32. Licencje do Centralnego Systemu Uwierzytelniania Stacji Końcowych

Zamawiający wymaga dostarczenia licencji TACACS L-ISE-TACACS lub równoważnych implementujących w Centralnym Systemie Uwierzytelnienia Stacji Końcowych Zamawiającego funkcjonalność rozliczalności komend na urządzeniach sieciowych Zamawiającego.

3. Gwarancja i serwis

Wykonawca jest zobowiązany objąć gwarancją producenta dostarczone urządzenia, oprogramowanie i licencje przez okres co najmniej 48 miesięcy, przy czym:

a) gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach realizacji Etapu pierwszego zamówienia rozpocznie swój bieg od dnia podpisania przez Strony Protokołu Odbioru ilościowego urządzeń (oprogramowania i licencji) dostarczonych do tej jednostki organizacyjnej;

b) gwarancja na urządzenia, oprogramowanie i licencje dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach realizacji Etapu drugiego zamówienia rozpocznie swój bieg od dnia podpisania przez Strony Protokołu Odbioru Ilościowego urządzeń, oprogramowania i licencji dostarczonych do tej jednostki organizacyjnej;

c) gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach zamówienia objętego prawem opcji rozpocznie swój bieg od dnia podpisania przez Strony Protokołu Odbioru Ilościowego urządzeń, oprogramowania i licencji dostarczonych do tej jednostki organizacyjnej w ramach zamówienia objętego prawem opcji.

d) gwarancja będzie obejmować:
   - wymianę uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii, jeżeli zgłoszenie awarii wpłynęło w dniu roboczym do godziny 12:00; wymianę uszkodzonego sprzętu najpóźniej w ciągu dwóch dni roboczych licząc od dnia zgłoszenia awarii, jeżeli zgłoszenie wpłynęło w dniu roboczym po godzinie 12:00
   - możliwość pobierania poprawek i aktualizacji oprogramowania (zarówno update jak i upgrade) oraz sygnatur dla systemów IPS przez 7 dni w tygodniu i 24 godziny na dobę, przez wszystkie dni w roku.

e) przez pojęcie dnia roboczego należy rozumieć dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy.

f) dla umożliwienia Zamawiającemu dokonywania zgłoszeń o awarii, Wykonawca przekaże adres poczty elektronicznej oraz numer telefonu dostępny dla Zamawiającego całodobowo. O każdej zmianie adresu poczty elektronicznej Wykonawca zobowiązany jest niezwłocznie powiadomić Zamawiającego w formie pisemnej. Powiadomienie o powyższych zmianach nie stanowi zmiany umowy wymagającej sporządzenia aneksu;

g) Wykonawca zobowiązuje się do przyjmowania od Zamawiającego zgłoszeń awarii serwisowych przez 7 dni w tygodniu i 24 godziny na dobę, przez wszystkie dni w roku. Reakcja na zgłoszenie i rozpoczęcie naprawy nie może być dłuższa niż 2 godziny od momentu zgłoszenia przez Zamawiającego. W ramach czasu reakcji Zamawiający wymaga potwierdzenia (telefonicznie lub pocztą elektroniczną) otrzymanego zgłoszenia na adres poczty elektronicznej z podaniem w potwierdzeniu daty i godziny przystąpienia do naprawy.

h) Gwarancja musi być świadczona w miejscu użytkowania systemu i sprzętu.

i) Gwarancja nie może ograniczać praw Zamawiającego do zmiany miejsca instalacji sprzętu w obrębie siedziby Zamawiającego, instalowania i wymiany w dostarczonym sprzęcie standardowych podzespołów i urządzeń, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego lub przez autoryzowanego przez producenta sprzętu inżyniera innego Wykonawcy.

j) Wykonawca zobowiązuje się do usunięcia powstałych awarii. Wykonawca będzie pośredniczył w zgłaszaniu wszelkich problemów do Centrum Serwisowego Producenta dostarczonego sprzętu.

k) Zamawiający wymaga, aby świadczenie usługi serwisowej było objęte jednym centrum obsługi zgłoszeń serwisowych. Wymagane formy zgłaszania awarii to telefon, e-mail.

l) Wykonawca zobowiązuje się przenieść na Zamawiającego wszelkie uprawnienia z tytułu gwarancji udzielonych przez producentów urządzeń będących przedmiotem umowy.

m) W przypadku, gdy wadą objęte będą urządzenia, sprzęt teleinformatyczny posiadający nośnik pamięci (np. dysk twardy), nośnik ten zostanie wymontowany przed przekazaniem wadliwego urządzenia, sprzętu teleinformatycznego Wykonawcy do naprawy. Uszkodzone nośniki danych, w tym dyski twarde pozostają własnością Zamawiającego.

4. Wdrożenie w Bieszczadzkim Oddziale Straży Granicznej

Wykonawca wykona następujące prace wdrożeniowe w siedzibie komendy Bieszczadzkiego Oddziału Straży Granicznej oraz wskazanych placówkach Bieszczadzkiego Oddziału Straży Granicznej:

- instalację 94 urządzeń spośród wszystkich urządzeń, które będą dostarczone do Bieszczadzkiego Oddziału Straży Granicznej
- rekonfiguracja ww. urządzeń,
- sprawdzenie działania ww. urządzeń poprzez testy akceptacyjne określone przez Zamawiającego na etapie wdrożenia.

5. Lokalizacja dostaw

Wykaz adresów jednostek organizacyjnych, do których będą realizowane dostawy zawarto w załączniku nr 2 do niniejszego OPZ.

6. Szkolenia

W ramach realizacji przedmiotu zamówienia Wykonawca zapewni szkolenia z zakresów opisanych poniżej:

L.p.	Typ szkolenia	Ilość osób		
		Etap 1	Etap 2	Opcja
1.	Zaawansowane szkolenie z konfigurowania przełączników	6	8	6
2.	Zaawansowane szkolenie z konfigurowania routerów	X	10	X
3.	Zaawansowane szkolenie z konfigurowania firewall	X	10	X
4.	Szkolenie z konfigurowania balanser'a ruchu	X	10	X

1) **Zaawansowane szkolenie z konfigurowania urządzeń przełączników** musi swoim zakresem obejmować co najmniej nw. zagadnienia:
   a) Koncepcja przełączania na poziomie warstwy drugiej, trzeciej i czwartej modelu ISO/OSI,
   b) Projektowanie sieci kampusowych i wirtualizacji przełączników sieciowych,
   c) Implementacja PoE,
   d) Implementacja VLANs, łączy typu trunk, usług DHCP, agregacji portów,
   e) Implementacja rodziny protokołów STP,
   f) Routing pomiędzy VLANami,
   g) Konfiguracja sieci wysokiej niezawodności, konfiguracji protokołów redundancji warstwy trzeciej,
   h) Wykorzystanie mirroringu portów do monitorowania ruchu w sieci,
   i) Bezpieczeństwo sieci kampusowych
2) **Zaawansowane szkolenie z konfigurowania routerów** musi swoim zakresem obejmować co najmniej nw. zagadnienia:
   a) Koncepcja protokołów routingu dynamicznego,
   b) Konfiguracja protokołów routingu w środowisku sieci IPv4 i IPv6,
   c) Implementacja technik redystrybucji adresów sieciowych wraz z opcjami ich filtrowania,
   d) Implementacja narzędzi kontroli ścieżki i metod korporacyjnego dostępu do Internetu,
   e) Dobre praktyki w zabezpieczeniu routerów i metod autentykacji w protokołach routingu dynamicznego.
3) **Zaawansowane szkolenie z konfigurowania firewall** musi swoim zakresem obejmować co najmniej nw. zagadnienia:
   a) Koncepcje bezpieczeństwa
   b) Zabezpieczanie urządzeń sieciowych
   c) Bezpieczeństwo 2 warstwy
   d) Firewall
   e) VPN
4) **Szkolenie z konfigurowania balanser'a ruchu** musi swoim zakresem obejmować co najmniej nw. zagadnienia:
   a) Obsługa inteligentnego równoważenia ruchu dla farm serwerów przy wsparciu różnych protokołów (TCP,UDP itp.)
   b) balansowanie ruchu w oparciu o algorytmy:
   - Round Robin
   - obciążenie serwerów
   - ilość połączeń

- dostępne pasmo
- czas odpowiedzi
- hashing (URL, Domain, source IP, Destination IP)

c) mechanizm dowiązania sesji (session persistant)
d) monitorowanie stanów serwerów
e) content switching
f) Database load balancing
g) mechanizmy ograniczenia ruchu dla poszczególnych serwerów
h) Globar Server load balancing (GSLB):
i) System ma zapewnić kontrola ilości połaczeń , zapytań i priorytetyzacją ruchu dla krytycznych aplikacji
j) Funkcja firewall
k) wysoka dostępność

Szkolenia muszą odbyć się w Warszawie. Szkolenia muszą być przeprowadzone w języku polskim. Wykonawca zapewni materiały szkoleniowe, zakwaterowanie oraz całodobowe wyżywienie w czasie trwania szkolenia. Typ szkoleń: 4-5 dniowe, otwarte, grupa szkoleniowa nie może jednak liczyć więcej niż 8 osób. Szkolenia będą zrealizowane w autoryzowanych centrach szkoleniowych producenta sprzętu.

Terminy szkoleń muszą zostać uzgodnione z przedstawicielem Zamawiającego. Realizacja szkoleń dla danej jednostki organizacyjnej Straży Granicznej musi się zakończyć najpóźniej na 15 dni przed podpisaniem Protokołu odbioru danej jednostki.

7. Procedury odbioru

7.1. Ogólne zasady odbioru prac

1. Prace związane z realizacją przedmiotu zamówienia będą odbierane według procedur opisanych poniżej.
2. Osobami odpowiedzialnymi za podpisywanie protokołów odbioru prac są osoby upoważnione przez Zamawiającego oraz przez Wykonawcę

7.2. Procedury odbioru - część 1 zamówienia - etap 1

1) Dostawa oznacza dostarczenie sprzętu/oprogramowania/licencji do wskazanej jednostki organizacyjnej Zamawiającego w terminach uzgodnionych z Zamawiającym.
2) Odbiór ilościowy sprzętu/oprogramowania/licencji w danej jednostce organizacyjnej będzie polegał na sprawdzeniu zgodności ilości dostarczonego sprzętu/ oprogramowania/licencji z listem przewozowym i stwierdzeniu braku zewnętrznych uszkodzeń dostarczonych urządzeń oraz na dostarczeniu przez Wykonawcę oświadczenia producenta:
   a) o wykupieniu przez Wykonawcę wymaganych przez Zamawiającego gwarancji na dostarczone urządzenia, oprogramowanie i licencje.
   b) o dacie produkcji urządzeń.
   c) informacje, potwierdzające, że całość dostarczonych urządzeń , oprogramowania i licencji pochodzi z autoryzowanego kanału sprzedaży producenta.
3) Odbiór ilościowy zostanie zakończony podpisaniem przez strony Protokołu Odbioru Ilościowego potwierdzającego dostarczenie urządzeń, oprogramowania i licencji w wymaganym zakresie do danej jednostki organizacyjnej.
4) W przypadku stwierdzenia rozbieżności w dostawie Produktów Wykonawca sporządzi protokół rozbieżności i uzgodni z Zamawiającym termin uzupełnienia dostawy.
5) Odbiór prac wdrożeniowych w Bieszczadzkim Oddziale Straży Granicznej (BOSG)
   a. Prace wdrożeniowe wykonane przez Wykonawcę na rzecz Zamawiającego będą odbierane lub akceptowane na podstawie zdefiniowanych Testów Akceptacyjnych. Prace, kończące się Testami Akceptacyjnymi, zostają uznane za zakończone po pomyślnym zakończeniu Testów Akceptacyjnych.
   b. Przed przystąpieniem do Testów Akceptacyjnych Wykonawca zgłosi Zamawiającemu, gotowość do przystąpienia do Testów Akceptacyjnych. Zamawiający jest zobowiązany do wyznaczenia daty rozpoczęcia Testów Akceptacyjnych, nie późniejszej jednak niż 2 dni od daty zgłoszenia gotowości przez Wykonawcę do testów.
   c. O negatywnych wynikach testów akceptacyjnych Zamawiający zostanie powiadomiony natychmiast przez zespół testujący. W ciągu 2 dni od zakończenia testów zostanie przekazana do Wykonawcy lista błędów i uwag dotycząca testów akceptacyjnych. Po weryfikacji uwag przez

Wykonawcę i wprowadzeniu poprawek nastąpi ponowne zgłoszenie gotowości do testów jak powyżej.

d. Zakres i sposób przeprowadzania Testów Akceptacyjnych (Scenariusze Testów Akceptacyjnych) dla poszczególnych prac zostaną przekazane przez Zamawiającego w terminie 14 dni od daty podpisania umowy
e. Po pozytywnym przeprowadzeniu Testów Akceptacyjnych Zamawiający i Wykonawca podpiszą Protokół Testów Akceptacyjnych.

6) Wykonawca powiadomi pisemnie Zamawiającego o gotowości do rozpoczęcia odbioru.
7) Zamawiający ustali datę i godzinę rozpoczęcia odbioru (od poniedziałku do piątku w godzinach 8:30 – 14:30), nie później niż w terminie pięciu dni roboczych od uzyskania informacji od Wykonawcy o gotowości do odbioru.
8) Odbiór przedmiotu Umowy zostanie dokonany komisyjnie z udziałem upoważnionego przedstawiciela Wykonawcy i Zamawiającego.
9) Po pozytywnym zakończeniu procedur odbioru wszystkich prac (w tym szkoleń) w danej jednostce organizacyjnej Zamawiający i Wykonawca podpiszą Protokół Odbioru Końcowego potwierdzający zakończenie realizacji zamówienia w danej jednostce organizacyjnej w ramach realizacji etapu 1 zamówienia części 1
10) Rezultatem wykonania zamówienia w danej jednostce organizacyjnej będą:
    a) dostarczony sprzęt/oprogramowanie/licencje,
    b) podpisany Protokołu Odbioru Ilościowego dostawy urządzeń, oprogramowania, i licencji,
    c) W przypadku Bieszczadzkiego Oddziału Straży Granicznej podpisany Protokół Testów Akceptacyjnych,
    d) zrealizowane szkolenia potwierdzone podpisaniem przez strony Protokołu Odbioru Szkoleń w danej jednostce organizacyjnej
    e) podpisany przez Strony Protokół Odbioru Końcowego dotyczący zakończenia realizacji zamówienia w danej jednostce organizacyjnej w ramach etapu 1 części 1 zamówienia będzie podstawą do wystawienia przez Wykonawcę faktury VAT za wykonanie zamówienia w tej jednostce organizacyjnej. W przypadku Bieszczadzkiego Oddziału Straży Granicznej wymagany jest również podpisany Protokół Testów Akceptacyjnych.

7.3. Procedury odbioru - część 1 zamówienia - etap 2

1) Dostawa oznacza dostarczenie sprzętu/oprogramowania/licencji do wskazanej jednostki organizacyjnej Zamawiającego w terminach uzgodnionych z Zamawiającym.
2) Odbiór ilościowy sprzętu/oprogramowania/licencji w danej jednostce organizacyjnej będzie polegał na sprawdzeniu zgodności ilości dostarczonego sprzętu/ oprogramowania/licencji z listem przewozowym i stwierdzeniu braku zewnętrznych uszkodzeń dostarczonych urządzeń oraz na dostarczeniu przez Wykonawcę oświadczenia producenta:
    a) wykupieniu przez Wykonawcę wymaganych przez Zamawiającego gwarancji na dostarczone urządzenia, oprogramowanie i licencje.
    b) o dacie produkcji urządzeń.
    c) informacje, potwierdzające, że całość dostarczonych urządzeń , oprogramowania i licencji pochodzi z autoryzowanego kanału sprzedaży producenta.
3) Odbiór ilościowy zostanie zakończony podpisaniem Protokołu Odbioru Ilościowego potwierdzającego dostarczenie urządzeń, oprogramowania i licencji w wymaganym zakresie do danej jednostki organizacyjnej

4) W przypadku stwierdzenia rozbieżności w dostawie Produktów Wykonawca sporządzi protokół rozbieżności i uzgodni z Zamawiającym termin uzupełnienia dostawy.
5) Wykonawca powiadomi pisemnie Zamawiającego o gotowości do rozpoczęcia odbioru.
6) Zamawiający ustali datę i godzinę rozpoczęcia odbioru (od poniedziałku do piątku w godzinach 8:30 – 14:30), nie później niż w terminie pięciu dni roboczych od uzyskania informacji od Wykonawcy o gotowości do odbioru.
7) Odbiór przedmiotu Umowy zostanie dokonany komisyjnie z udziałem upoważnionego przedstawiciela Wykonawcy i Zamawiającego.
8) Po pozytywnym zakończeniu procedur odbioru wszystkich prac (w tym szkoleń) w danej jednostce organizacyjnej Zamawiający i Wykonawca podpiszą Protokół Odbioru Końcowego potwierdzający zakończenie realizacji zamówienia w danej jednostce organizacyjnej w ramach realizacji etapu 2 części 1 zamówienia
9) Rezultatem wykonania Zamówienia w danej jednostce organizacyjnej będą:
   a) dostarczenie sprzęt/oprogramowanie/licencje
   b) podpisanie Protokołu Odbioru Ilościowego dostawy urządzeń, oprogramowania, licencji
   c) zrealizowanie szkolenia potwierdzone podpisaniem przez strony Protokołu Odbioru Szkoleń w danej jednostce organizacyjnej
   d) podpisany przez Strony Protokół Odbioru Końcowego dotyczący zakończenia realizacji zamówienia w danej jednostce organizacyjnej w ramach etapu 2 zamówienia części 1 będzie podstawą do wystawienia przez Wykonawcę faktury VAT za wykonanie zamówienia w tej jednostce organizacyjnej.

8. Wzory formularzy

PROTOKÓŁ ODBIORU ILOŚCIOWEGO

.....

(część i etap)

.....

(jednostka organizacyjna Straży Granicznej)

na podstawie umowy nr zawartej w dniu ...

pomiędzy Komendantem Głównym Straży Granicznej
a firmą

Miejsce:	
Data przekazania:	
Miejsce i data wystawienia	

(Nazwa firmy) oświadcza, iż Umowa dla .....została zrealizowana.

(jednostka organizacyjna Straży Granicznej)

Wykaz dostarczonych urządzeń:

Lp.	Symbol urządzenia/oprogramowania	Nr seryjny	Ilość	Nazwa gwarancji	Termin ważności [od-do]
1.					
2.					

W czasie odbioru dokonano sprawdzenia stanu ilościowego oraz zgodności z umową.

Zamawiający nie wnosi żadnych zastrzeżeń.

Uwagi Zamawiającego:

Podpis osoba upoważniona Zamawiającego	Podpis osoba upoważniona Wykonawcy

PROTOKÓŁ ODBIORU SZKOLENIA

na podstawie umowy nr ..... zawartej w dniu .....

pomiędzy Komendą Główną Straży Granicznej

a firmą .....

Lp.	Szkolenie	Ilość
1.		

1. ..... oświadcza, iż wymienione powyżej szkolenie zostało zrealizowane w terminie:..... W związku z powyższym przedstawiamy do akceptacji niniejszy Protokół Odbioru Szkolenia.

2. Do niniejszego protokołu załączono:

- lista obecności osób ze strony Zamawiającego: szt. ....., stron .....

- skany certyfikatów osób ze strony Zamawiającego: szt..... stron .....

Uwagi Zamawiającego:

.....

.....

.....

.....

Podpis osoba upoważniona Zamawiającego (data, pieczęć, czytelny podpis)	Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)

PROTOKÓŁ TESTÓW AKCEPTACYJNYCH

.....

(część i etap)

.....

(jednostka organizacyjna Straży Granicznej)

na podstawie umowy nr zawartej w dniu ...

pomiędzy Komendantem Głównym Straży Granicznej
a firmą

Miejsce:	
Data przekazania:	
Miejsce i data wystawienia	

(Nazwa firmy) oświadcza, iż testy akceptacyjne dla ..... zostały zakończone

(jednostka organizacyjna Straży Granicznej)

pozytywnie.

W związku z powyższym przedstawiamy do akceptacji niniejszy Protokół Testów Akceptacyjnych.

Wykaz dostarczonych urządzeń:

Lp.	Nazwa testu	Test zakończony pozytywnie / negatywnie	Uwagi
1.			
2.			
3.			

Zamawiający nie wnosi żadnych zastrzeżeń.

Uwagi Zamawiającego:

Do Protokołu załączono scenariusze testów akceptacyjnych

Podpis osoba upoważniona Zamawiającego	Podpis osoba upoważniona Wykonawcy

PROTOKÓŁ ODBIORU KOŃCOWEGO

.....

(część i etap)

.....

(jednostka organizacyjna Straży Granicznej)

na podstawie umowy nr zawartej w dniu ...

pomiędzy Komendantem Głównym Straży Granicznej
a firmą

Miejsce i data wystawienia protokołu:	

(Nazwa firmy .....) oświadcza, iż Umowa została zrealizowana. W związku z powyższym przedstawiamy do akceptacji niniejszy Protokół Odbioru Końcowego.

Do niniejszego protokołu załączono:

Protokoły Odbioru Ilościowego; stron .....

Protokół z Testów Akceptacyjnych; stron .....

Protokół Szkoleń; stron .....

Uwagi Zamawiającego:

.....
.....

Podpis osoba upoważniona Zamawiającego (data, pieczęć, czytelny podpis)	Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)

PROTOKÓŁ NAPRAWY URZĄDZENIA NR.....

na podstawie umowy nr ..... zawartej w .....

pomiędzy Komendantem Głównym Straży Granicznej

a firmą .....

Miejsce i czasookres naprawy urządzenia:		Od	Do
Typ urządzenia, Nr seryjny, Nr Ewidencyjny Straży Granicznej			

Rodzaj gwarancji

Sporządził:

(czytelny podpis inżyniera serwisu)

Opis Awarii:

.....

.....

Podjęte czynności:

.....

.....

Opis stanu urządzenia po usunięciu awarii:

.....

.....

Przedłużenie okresu gwarancji zgodnie z umową:

Naliczone dodatkowe dni gwarancji	(wyliczenia zgodnie z umową)
Sprawdził:	(czytelny podpis osoby upoważnionej SG)

Dodatkowe uwagi:

.....

.....

.....

Na tym raport zakończono.

Podpis osoba upoważniona Zamawiającego (data, pieczęć, czytelny podpis)	Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)

9. Oznaczenie projektu *(dotyczy wyłącznie zamówienia objętego prawem opcji)*

Na sprzęcie dostarczonym w ramach realizacji zamówienia objętego prawem opcji należy umieścić informację dotyczącą źródła finansowania projektu w sposób zgodny z poniższymi zasadami.

Projekt w części objętej prawem opcji jest współfinansowany z funduszy europejskich. W związku z powyższym Zamawiający wymaga od Wykonawcy oznaczenia dostarczonych produktów poprzez Umieszczenie na dostarczonym sprzęcie informacji dotyczącej źródła finansowania projektu.

Wykonawca zobowiązany jest do umieszczenia na dostarczonym w ramach realizacji umowy sprzęcie informacji dotyczącej źródła finansowania projektu. Informacja ta musi być umieszczona w widocznym miejscu. Dlatego też fakt współfinansowania powyższego sprzętu ze środków Funduszu Bezpieczeństwa Wewnętrznego musi być podany w jasny i widoczny sposób (wraz z logo UE).

WYTYCZNE DOTYCZĄCE GODŁA I DEFINICJA STANDARDOWEJ KOLORYSTYKI

OPIS SYMBOLICZNY

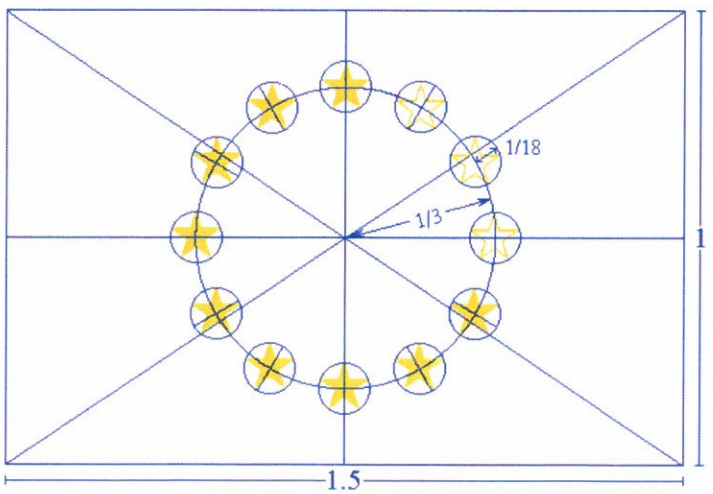
Na błękitnym tle dwanaście złotych gwiazd tworzy okrąg, reprezentujący unię narodów Europy.

Liczba gwiazd jest stała (12) i symbolizuje doskonałość i jedność.

OPIS HERALDYCZNY

Na błękitnym polu okręg z dwunastu złotych gwiazd, niedotykających się ramionami.

OPIS GEOMETRYCZNY



Godło ma kształt niebieskiej prostokątnej flagi, której długość jest równa 1,5 szerokości. Dwanaście złotych gwiazd, umieszczonych w równych odstępach, tworzy niewidoczny okrąg

ze środkiem w miejscu przecięcia przekątnych prostokąta. Promień okręgu jest równy jednej trzeciej szerokości flagi. Każda z gwiazd ma pięć ramion, kończących się na obwodzie niewidocznego okręgu o promieniu równym 1/18 szerokości flagi. Wszystkie gwiazdy są ustawione w pozycji pionowej, tzn. jedno ramię znajduje się w pionie, a dwa ramiona na linii prostej prostopadłej do osi szerokości. Okrąg ustawiony jest tak, że gwiazdy są w miejscu godzin na tarczy zegara. Ich liczba jest niezmienna.

PRZEPISOWE KOLORY

Kolory godła są następujące:

Powierzchnia prostokąta: NIEBIESKI PANTONE REFLEX (PANTONE REFLEX BLUE);

Gwiazdy: ŻÓŁTY PANTONE (PANTONE YELLOW).

Druk czterobarwny

Przy stosowaniu druku czterobarwnego dwa standardowe kolory powstają przez użycie czterech kolorów w procesie czterobarwnym.

ŻÓŁTY PANTONE uzyskuje się stosując 100 % „process yellow".

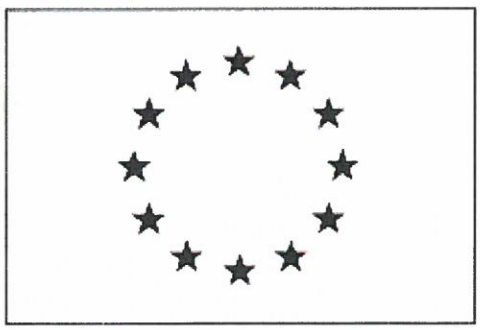
NIEBIESKI PANTONE REFLEX uzyskuje się poprzez wymieszanie 100 % „process cyan" z 80 % „process magenta".

INTERNET

Na stronach internetowych NIEBIESKI PANTONE REFLEX odpowiada kolorowi RGB:0/0/153 (w systemie szesnastkowym: 000099), a ŻÓŁTY PANTONE - kolorowi RGB:255/204/0 (w systemie szesnastkowym: FFCC00).

REPRODUKCJE JEDNOBARWNE

Jeśli używany jest czarny kolor, prostokąt powinien posiadać czarną obwódkę a gwiazdy powinny być czarne na białym tle.



Przy użyciu koloru niebieskiego (Reflex Blue) należy używać 100 %-owy niebieski z białym negatywem do reprodukcji gwiazd.

REPRODUKCJE NA KOLOROWYM TLE

Jeżeli tło musi być kolorowe, wokół prostokąta należy wykonać białą obwódkę o szerokości 1/25 wysokości prostokąta.

Przykładowe formy wizualizacji:

Naklejka na urządzenia

UNIA EUROPEJSKA

Projekt współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego – Bezgraniczne Bezpieczeństwo

UNIA EUROPEJSKA

FUNDUSZ BEZPIECZEŃSTWA

WEWNĘTRZNEGO

Projekt współfinansowany przez

UNIĘ EUROPEJSKĄ

Fundusz Bezpieczeństwa Wewnętrznego