SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO NA:

Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych

Przetarg nieograniczony

Znak: BDG.741.016.2020

1. DEFINICJE I SKRÓTY

Wyrażenia i skróty używane w specyfikacji istotnych warunków zamówienia oznaczają:

IPU	-	istotne postanowienia umowy
OPZ	-	opis przedmiotu zamówienia
SIWZ	-	specyfikacja istotnych warunków zamówienia
ustawa	-	ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843)
Zamawiający	-	Ministerstwo Spraw Zagranicznych

2. ZAMAWIAJĄCY

Ministerstwo Spraw Zagranicznych

Adres do korespondencji:
Ministerstwo Spraw Zagranicznych
al. J. Ch. Szucha 23, 00-580 Warszawa
e-mail: bzp@msz.gov.pl, tel. +48 22 523 9910
https://www.gov.pl/web/dyplomacja/zamowienia-publiczne-do-ktorych-stosuje-sie-przepisy-ustawy-pzp
Godziny pracy Zamawiającego: 8.15 – 16.15

3. POSTANOWIENIA OGÓLNE

3.1 Tryb udzielenia zamówienia

Postępowania prowadzone jest w trybie przetargu nieograniczonego.

3.2 Oznaczenie postępowania

Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych; znak: BDG.741.016.2020 .

Wykonawcy winni we wszystkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie – zarówno tytuł jak i znak.

Zamawiający nie bierze odpowiedzialności za skutki niedochowania przez Wykonawcę powyższych wymogów.

3.3 Wartość zamówienia

Szacunkowa wartość zamówienia przekracza wyrażoną w złotych równowartość kwoty określonej w przepisach wydanych na podstawie art. 11 ust. 8 ustawy.

4. PRZEDMIOT ZAMÓWIENIA

4.1 Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia jest modernizacja i rozbudowa infrastruktury sieciowej Zamawiającego poprzez:

1. Dostawę urządzeń infrastruktury sieciowej wraz z oprogramowaniem oraz usługami subskrypcyjnymi, fabrycznie nowych (wyprodukowanych nie wcześniej niż 6 miesięcy

przed dostawą), z możliwością objęcia wsparciem producenta przez minimum 36 miesięcy od daty zakupu, nieużywanych we wcześniejszych projektach, pochodzących z legalnego kanału sprzedaży producentów na rynek europejski. Przedmiotem zamówienia nie jest objęta instalacja i konfiguracja urządzeń;

2. Objęcie usługami serwisowymi oprogramowania i sprzętu dostarczanego w ramach zamówienia.

Szczegółowy opis przedmiotu zamówienia stanowi Załącznik nr 1 do SIWZ.

4.2 Kod CPV

32424000-1 – Infrastruktura sieciowa

4.3 Oferty częściowe

Zamawiający nie dopuszcza składania ofert częściowych w rozumieniu przepisów ustawy.

4.4 Oferty wariantowe

Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu przepisów ustawy. Zamówienie musi być zrealizowane zgodnie z wymaganiami określonymi w niniejszej SIWZ.

4.5 Informacja o zamówieniach podobnych lub dodatkowych.

Zamawiający nie przewiduje możliwości udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 6 ustawy.

4.6 Podwykonawstwo

4.6.1 Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.

4.6.2 Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców.

5. MIEJSCE I TERMIN WYKONANIA ZAMÓWIENIA

5.1 Miejsce wykonania zamówienia

Obiekty Ministerstwa Spraw Zagranicznych znajdujące się na terenie Warszawy.

5.2 Termin realizacji zamówienia

Dostawa urządzeń – 60 dni od zawarcia umowy.

Wsparcie serwisowe – minimum 1 rok, w zależności od oferty Wykonawcy.

6. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI – NIE DOTYCZY SKŁADANIA OFERT I WNIOSKÓW.

6.1 Porozumiewanie się Zamawiającego z Wykonawcami odbywa się wyłącznie drogą elektroniczną, z tytułem wiadomości: **Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych, znak sprawy: BDG.741.016.2020.**

6.2 Ofertę składa się zgodnie z wymaganiami określonymi w pkt 10.

6.3 Oświadczenia, wnioski, zawiadomienia oraz informacje należy przekazywać na adres poczty elektronicznej wskazany w pkt 2 SIWZ. Każda ze stron na żądanie drugiej niezwłocznie potwierdzi fakt ich otrzymania.

6.4 Dokumenty o których mowa w pkt 6.3, Wykonawca składa w postaci elektronicznej, a w określonych przepisami przypadkach opatrzonej kwalifikowanym podpisem elektronicznym.

6.5 Osobami upoważnionymi do porozumiewania się z Wykonawcami są: Paweł Gola, Radosław Wojda, e-mail: bzp@msz.gov.pl.

6.6 Wykonawca może pobrać SIWZ ze strony internetowej Zamawiającego: https://www.gov.pl/web/dyplomacja/zamowienia-publiczne-do-ktorych-stosuje-sie-przepisy-ustawy-pzp

6.7 Wyjaśnienia treści SIWZ:

1) Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ. Zastosowanie mają przepisy art. 38 ustawy.
2) Zapytania należy przesyłać na adres e-mail podany w pkt 2 SIWZ.
3) Zamawiający niezwłocznie udzieli wyjaśnień, jednak nie później niż na **6 dni** przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później, niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
4) Treść zapytań wraz z wyjaśnieniami Zamawiający zamieści na stronie internetowej Zamawiającego, o której mowa w pkt 2 SIWZ, bez ujawniania źródła zapytania.
5) Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w pkt 3).

7. WARUNKI UDZIAŁU W POSTĘPOWANIU

7.1 O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

1) nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12-23 ustawy;
2) spełniają warunki udziału w postępowaniu, dotyczące:
   a) zdolności technicznej lub zawodowej

b) sytuacji ekonomicznej lub finansowej

7.2 Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się niezbędnym doświadczeniem, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał, a w przypadku świadczeń okresowych lub ciągłych również wykonuje należycie, nie mniej niż **dwie dostawy** odpowiadające swoim rodzajem i wartością przedmiotowi zamówienia, z których każda:

- polega na dostarczeniu sprzętu służącego do budowy sieci LAN/WAN;

- posiada wartość minimalną 1 750 000 zł (słownie: jeden milion siedemset pięćdziesiąt tysięcy zł).

Poprzez dostawę wykonywaną Zamawiający rozumie dostawę będącą w trakcie realizacji, przy czym wartość zrealizowanej części dostaw w ramach zawartej umowy na dzień składania ofert nie może być niższa niż 1 750 000,00 zł brutto.

W przypadku, gdy wartości dostaw będą wyrażone w walucie innej niż PLN, Zamawiający przeliczy te wartości na PLN po kursie ogłaszanym przez Narodowy Bank Polski wg kursu średniego podanego w dniu, w którym zostało przekazane przez Zamawiającego ogłoszenie o zamówieniu do publikacji w Dzienniku Urzędowym Unii Europejskiej.

7.3 Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego sytuacji ekonomicznej lub finansowej, Zamawiający wymaga aby Wykonawcy posiadali środki finansowe lub zdolność kredytową na poziomie minimum 3 000 000,00 zł.

W przypadku posiadania środków finansowych w walucie innej niż złotówki, Zamawiający oceni zdolność finansową Wykonawcy przeliczając daną walutę na zł po kursie ogłaszanym przez Narodowy Bank Polski wg kursu średniego podanego w dniu, w którym zostało przekazane przez Zamawiającego ogłoszenie o zamówieniu do publikacji w Dzienniku Urzędowym Unii Europejskiej.

7.4 Wykonawca, który nie wykaże spełniania warunków udziału w postępowaniu, określonych w pkt 7.2 - 7.3 SIWZ lub braku podstaw do wykluczenia określonych w art. 24 ust. 1 pkt 12-23 ustawy zostanie wykluczony z postępowania.

7.5 Zamawiający może, na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych lub sytuacja finansowa Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia.

7.6 Wykonawca, który podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 13 i 14, 16-20 ustawy, 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.

Powyższego nie stosuje się, jeżeli wobec Wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.

7.7 Wykonawca nie zostanie wykluczony z postępowania, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające dowody wskazane w pkt 7.6 SIWZ.

7.8 Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, o których mowa w pkt 7.2 - 7.3 SIWZ, polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

7.8.1 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.

7.8.2 Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–22 ustawy.

7.8.3 Wykonawca, który polega na sytuacji finansowej innych podmiotów, odpowiada solidarnie z podmiotem, który zobowiązał się do udostępnienia zasobów, za szkodę poniesioną przez Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.

7.8.4 W odniesieniu do warunków dotyczących kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi, do realizacji których te zdolności są wymagane.

7.9 Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia na zasadach określonych w art. 23 ustawy. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo w postaci dokumentu elektronicznego, podpisane kwalifikowanym podpisem elektronicznym należy dołączyć do oferty.

7.10 W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, warunki określone w pkt 7.2 - 7.3 SIWZ musi spełniać co najmniej jeden Wykonawca samodzielnie. Powyższe zasady stosuje się również w sytuacji, gdy Wykonawca polega na zdolnościach technicznych lub zawodowych innych podmiotów. Każdy z Wykonawców musi samodzielnie wykazać, że nie zachodzą wobec niego przesłanki wykluczenia z postępowania określone w art. 24 ust 1. pkt 13-23 ustawy.

7.11 Zamawiający może, zgodnie z art. 24aa ust. 1 ustawy, najpierw dokonać oceny ofert, a następnie zbadać, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

8. WYKAZ OŚWIADCZEŃ I DOKUMENTÓW, POTWIERDZAJĄCYCH BRAK PODSTAW DO WYKLUCZENIA

8.1 W celu wstępnego potwierdzenia spełniania warunków udziału w postępowaniu, określonych w pkt 7.2 - 7.3 SIWZ oraz wykazania braku podstaw do wykluczenia, Wykonawcy zobowiązani są złożyć wraz z ofertą:

8.1.1 Aktualne na dzień składania ofert oświadczenie w zakresie wskazanym przez Zamawiającego w SIWZ, w formie jednolitego dokumentu (JEDZ).

a) Wykonawca sporządza JEDZ zgodnie z wzorem standardowego formularza określonym w rozporządzeniu wykonawczym Komisji (UE) 2016/7 z dnia 5 stycznia 2016 r., w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym i przesyła zgodnie z zasadami określonymi w pkt 10 SIWZ.

b) Informacje zawarte w JEDZ będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu z postępowania oraz spełnia warunki udziału w postępowaniu.

c) Wykonawca wypełnia cześć II, III, IV oraz VI formularza. W części IV Wykonawca może ograniczyć się do wypełnienia sekcji α formularza. Wykonawca nie musi wypełniać pozostałych sekcji części IV formularza, dotyczącej kryteriów kwalifikacji, zaś właściwej (dowodowej) weryfikacji spełniania konkretnych, określonych przez zamawiającego warunków udziału w postępowaniu zamawiający dokona w oparciu o stosowne dokumenty Wykonawcy, którego oferta zostanie najwyżej oceniona, składane na wezwanie Zamawiającego, w trybie art. 26 ust. 1 ustawy.

d) W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, JEDZ składa każdy z Wykonawców. JEDZ ma potwierdzać spełnianie warunków udziału w postepowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

e) Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu, składa także JEDZ dotyczący tych podmiotów.

f) Zamawiający dopuszcza następujące formaty przesyłanych danych: .pdf lub .xml, .doc, .docx.

g) Wykonawca wypełnia JEDZ, tworząc dokument elektroniczny. Może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu elektronicznego, w jednym

z ww. formatów.

Zamawiający na swojej stronie internetowej https://www.gov.pl/web/dyplomacja/zamowienia-publiczne-do-ktorych-stosuje-sie-przepisy-ustawy-pzp - załącznik nr 6) udostępnia Wykonawcom formularz JEDZ dostosowany do niniejszego postępowania w formacie .xml, do zapisania na dysku lokalnym i wykorzystania w serwisie eESPD. Po zaznaczeniu pola „Jestem wykonawcą" Wykonawca ma możliwość zaimportowania zapisanego formularza JEDZ/ESPD w celu jego wypełnienia lub połączenia dwóch formularzy JEDZ/ESPD, tj. formularza przygotowanego przez zamawiającego dla danego postępowania oraz formularza wykorzystanego przez Wykonawcę we wcześniejszym postępowaniu. Po wypełnieniu formularz należy ponownie zapisać na dysku lokalnym.

h) Po stworzeniu lub wygenerowaniu przez wykonawcę dokumentu elektronicznego JEDZ, wykonawca podpisuje ww. dokument kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniające wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2019 r. poz. 162).

8.1.2 Pisemne zobowiązanie innych podmiotów do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia (lub inny dowód) – jeżeli Wykonawca w celu potwierdzenia spełniania warunków udziału w postępowaniu, o których mowa w pkt 7.2 - 7.3 SIWZ, polega na zasobach innych podmiotów na zasadach określonych w art. 22a ustawy, złożone w oryginale w postaci dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym.

8.1.3 W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia – pełnomocnictwo do reprezentowania wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia, złożone w oryginale w postaci dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym.

8.2 Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej Zamawiającego informacji, o której mowa w art. 86 ust. 5 ustawy (informacje z otwarcia ofert), jest zobowiązany do przekazania Zamawiającemu oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy, z Wykonawcami, którzy złożyli odrębne oferty w przedmiotowym postępowaniu.

a) Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dokumenty bądź informacje potwierdzające, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu.
b) W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia – oświadczenie składa każdy z Wykonawców.
c) Wzór oświadczenia stanowi Załącznik nr 4 do SIWZ.
d) Oświadczenie składane jest w oryginale, w postaci dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym lub w elektronicznej kopii oświadczenia poświadczonej za zgodność z oryginałem przy użyciu

kwalifikowanego podpisu elektronicznego.

8.3 **Dokumenty składane na wezwanie Zamawiającego.**

Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 10 dni, terminie, aktualnych na dzień złożenia następujących oświadczeń lub dokumentów:

8.3.1 wykaz dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane, oraz załączeniem dowodów określających czy te usługi zostały wykonane lub są wykonywane należycie. Wzór wykazu stanowi Załącznik nr 7 do SIWZ.

Dowodami, o których mowa w niniejszym punkcie są:

- referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane.

  W przypadku świadczeń okresowych lub ciągłych nadal wykonywanych, referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

- oświadczenie Wykonawcy, jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o których mowa powyżej.

8.3.2 informacja banku lub spółdzielczej kasy oszczędnościowo – kredytowej potwierdzająca wysokość posiadanych środków kredytowych lub zdolność kredytową wykonawcy, w okresie nie wcześniejszym niż 1 miesiąc przed upływem terminu składania ofert.

- inny dokument, który w wystarczający sposób potwierdza spełnianie opisanego przez zamawiającego warunku udziału w postępowaniu (o których mowa w art. 26 ust. 2c ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych), jeżeli z uzasadnionej przyczyny wykonawca nie może złożyć wymaganych przez zamawiającego dokumentów, o których mowa powyżej.

8.3.3 informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy, wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

Powyższe informacje należy złożyć w zakresie: wykonawcy będącego osobą fizyczną lub podmiotem zbiorowym oraz urzędujących członków organu zarządzającego lub nadzorczego, wspólników spółki w spółce jawnej lub partnerskiej albo komplementariuszy w spółce komandytowej lub komandytowo-akcyjnej lub prokurentów.

8.3.4 oświadczenie wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub

składek na ubezpieczenia społeczne lub zdrowotne, albo - w przypadku wydania takiego wyroku lub decyzji - dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności. Wzór oświadczenia stanowi Załącznik nr 8 do SIWZ.

8.3.5 oświadczenie wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne. Wzór oświadczenia stanowi Załącznik nr 8 do SIWZ.

8.4 W celu oceny, czy wykonawca polegając na zdolnościach innych podmiotów będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia oraz oceny, czy stosunek łączący wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, zamawiający może żądać złożenia dokumentów, które określają w szczególności:

a) zakres dostępnych wykonawcy zasobów innego podmiotu,
b) sposób wykorzystania zasobów innego podmiotu, przez wykonawcę, przy wykonywaniu zamówienia;
c) zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego;
chyba że informacje te wynikają z dokumentu, o którym mowa w pkt 8.1.2.

8.5 Dokumenty i oświadczenia wymienione w pkt 8.3 SIWZ składane są w oryginale, w postaci dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem. **Poświadczenie za zgodność z oryginałem elektronicznej kopii dokumentu elektronicznego lub oświadczenia następuje przy użyciu kwalifikowanego podpisu elektronicznego.**

8.6 W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia i dokumenty wymienione w pkt 8.3.1– 8.3.5 składa każdy z tych Wykonawców.

8.7 W przypadku polegania przez Wykonawcę na zasobach lub sytuacji innych podmiotów, Wykonawca składa oświadczenia i dokumenty wymienione w pkt 8.3.1– 8.3.5 dotyczące tego Wykonawcy oraz każdego z tych podmiotów.

8.8 Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów, o których mowa w pkt 8.3 SIWZ, jeżeli Zamawiający posiada oświadczenia lub dokumenty dotyczące tego Wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2019 r. poz. 700. t.j. ze zm.). W tej sytuacji Wykonawca zobowiązany jest podać nazwę i znak postępowania, w którym te dokumenty zostały przez niego złożone lub wskazać bezpłatną i ogólnodostępną bazę danych, o której mowa powyżej. Zamawiający korzysta z tych oświadczeń lub dokumentów w celu potwierdzenia okoliczności, o których mowa w pkt 7.1 SIWZ, o ile są one aktualne.

8.9 Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w pkt 8.3.3 Wykonawca 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.

8.10 Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, lub miejsce zamieszkania ma osoba, której dotyczy dokument, nie wydaje się dokumentu, o którym mowa w pkt 8.9, zastępuje go się dokumentem zawierającym oświadczenie Wykonawcy, ze wskazaniem osoby lub 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.

8.11 Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w pkt 8.3.3, składa dokument, o którym mowa w pkt 8.9 w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 ustawy. 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.

8.12 Dokumenty, o których mowa w pkt 8.9 – 8.11 powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

8.13 Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

8.14 Dokumenty powinny być podpisane przez osoby upoważnione do reprezentacji Wykonawcy, w przypadku gdy dokumenty podpisują osoby, których upoważnienie do reprezentacji nie wynika z dokumentów rejestrowych, wymaga się aby Wykonawca dołączył do oferty pełnomocnictwo w postaci dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym (do ewentualnego wykorzystania wzór w Załączniku nr 5 do SIWZ).

8.15 Pozostałe wymagania dotyczące składanych przez Wykonawców oświadczeń i dokumentów określa Rozporządzenie Ministra Przedsiębiorczości i Technologii z dnia 16 października 2018 r. zmieniające rozporządzenie w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. poz. 1993).

9. WYMAGANIA DOTYCZĄCE WADIUM

9.1 Zamawiający wymaga wniesienia wadium w kwocie **100 000,00 PLN** (słownie: sto tysięcy złotych $^{00}/_{100}$).

9.2 Wadium może być wnoszone w jednej lub kilku z następujących form:

a) pieniądzu,

b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym,

c) gwarancjach bankowych,

d) gwarancjach ubezpieczeniowych,

e) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2019 r., poz. 310 ze zm.).

9.3 W przypadku wniesienia wadium w formie pieniężnej należy dokonać przelewu na rachunek bankowy Narodowego Banku Polskiego nr **39 1010 1010 0007 3613 9120 0000**.

9.4 W przypadku wnoszenia wadium w innych formach niż w pieniądzu (gwarancje/poręczenie), należy wraz z ofertą przedłożyć dokument elektroniczny, podpisany kwalifikowanym podpisem elektronicznym przez podmiot wystawiający gwarancję/poręczenie (przez osoby upoważnione do wystawienia dokumentu). Dokument wadialny należy złożyć w oryginale w postaci elektronicznej. Zamawiający nie dopuszcza możliwości złożenia skanu dokumentu wadialnego opatrzonego kwalifikowanym podpisem elektronicznym.

9.5 Zamawiający zwróci wadium wszystkim Wykonawcom niezwłocznie po wyborze oferty najkorzystniejszej lub unieważnieniu postępowania, z wyjątkiem Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, z zastrzeżeniem pkt 9.9 lit. d).

9.6 Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, Zamawiający zwraca wadium niezwłocznie po zawarciu umowy w sprawie zamówienia publicznego.

9.7 Zamawiający zwróci niezwłocznie wadium na wniosek Wykonawcy, który wycofał ofertę przed upływem terminu składania ofert.

9.8 Zamawiający zażąda ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium na podstawie pkt 9.5, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca wniesie wadium w terminie określonym przez Zamawiającego.

9.9 Zamawiający zatrzyma wadium wraz z odsetkami, jeżeli:

a) Wykonawca, którego oferta zostanie wybrana odmówi podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie;

b) Wykonawca nie wniósł wymaganego zabezpieczenia należytego wykonania umowy;

c) zawarcie umowy w sprawie zamówienia publicznego stanie się niemożliwe z przyczyn leżących po stronie Wykonawcy, którego oferta zostanie wybrana;

d) Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 i 3a ustawy, z przyczyn leżących po jego stronie, nie złożył oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy, 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 ustawy, co spowodowało brak możliwości wybrania oferty złożonej przez Wykonawcę jako najkorzystniejszej.

10. SPOSÓB PRZYGOTOWANIA OFERTY

10.1 Wymagania ogólne:

a) Każdy Wykonawca może złożyć tylko jedną ofertę;
b) Składanie oferty odbywa się przy użyciu miniPortalu https://miniportal.uzp.gov.pl/, ePUAPu https://epuap.gov.pl/wps/portal;
c) Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku;
d) Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminie ePUAP;
e) Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty lub wniosku wynosi 150 MB;
f) Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP;
g) Identyfikator postępowania i klucz publiczny dla danego postępowania o udzielenie zamówienia dostępne są na Liście wszystkich postępowań na miniPortalu oraz na stronie internetowej Zamawiającego.
h) Ofertę należy sporządzić w języku polskim;
i) Wymagane specyfikacją dokumenty sporządzone w języku obcym powinny być złożone wraz z tłumaczeniem na język polski;
j) Formularz oferty wraz z załącznikami i dokumentami sporządzanymi przez Wykonawcę powinien być podpisany przez osoby upoważnione do reprezentacji Wykonawcy; w przypadku, gdy ofertę podpisują osoby, których upoważnienie do reprezentacji nie wynika z dokumentów rejestrowych, wymaga się aby Wykonawca dołączył do oferty pełnomocnictwo w postaci dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym (do ewentualnego wykorzystania wzór w Załączniku nr 5 do SIWZ);
k) Wskazane jest, aby wszystkie strony oferty były ponumerowane, a także żeby oferta zawierała spis zawartości wraz z numerami stron do których się ona odnosi;
l) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

10.2 Oferta powinna zawierać:

a) Formularz oferty zawierający wszelkie informacje zawarte we wzorze stanowiącym Załącznik nr 3 do SIWZ,
b) Formularz rzeczowo – cenowy zgodnie ze wzorem stanowiącym Załącznik nr 3a do SIWZ, przy czym Wykonawca załączy do oferty Formularz rzeczowo - cenowy również w wersji edytowalnej;
c) Pełnomocnictwo do reprezentowania Wykonawcy, w tym podpisania oferty, o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą. Treść pełnomocnictwa musi jednoznacznie określać czynności, co do wykonywania których pełnomocnik jest upoważniony;

d) Pełnomocnictwo do reprezentowania Wykonawców w postępowaniu albo reprezentowania Wykonawców w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego, w przypadku gdy Wykonawcy wspólnie ubiegają się o udzielenie zamówienia zgodnie z art. 23 ustawy;
e) Dokument wadialny – sposób złożenia dokumentu wadialnego został określony w pkt 9.4;
f) Oświadczenia i dokumenty, o których mowa w pkt 8.1;
g) Wyjaśnienia uzasadniające zastrzeżenie tajemnicy przedsiębiorstwa (jeżeli dotyczy).

10.3 Złożenie oferty

a) Wykonawca składa ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionego również na miniPortalu. Klucz publiczny niezbędny do zaszyfrowania oferty przez Wykonawcę jest dostępny dla wykonawców na miniPortalu.
b) Oferta powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej w formacie danych .pdf, .doc, .docx. i podpisana kwalifikowanym podpisem elektronicznym. Sposób złożenia oferty, w tym zaszyfrowania oferty opisany został w Regulaminie korzystania z miniPortal. Ofertę należy złożyć w oryginale.
c) Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wraz z plikami stanowiącymi jawną część oferty skompresowane do jednego pliku archiwum (ZIP).
d) Do oferty należy dołączyć Jednolity Europejski Dokument Zamówienia w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
e) Oświadczenia podmiotów składających ofertę wspólnie oraz podmiotów udostępniających potencjał składane na formularzu JEDZ muszą mieć formę dokumentu elektronicznego, podpisanego kwalifikowanym podpisem elektronicznym przez każdego z nich w zakresie w jakim potwierdzają okoliczności, o których mowa w treści art. 22 ust. 1 ustawy.
f) JEDZ musi być podpisany przez osoby uprawnione do reprezentowania odpowiednio Wykonawcy / każdego Wykonawcy występującego wspólnie / innego podmiotu.
g) Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionych również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu.
h) Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

11. OPIS SPOSOBU OBLICZENIA CENY

11.1 Obliczenie ceny oferty

a) Podstawą do określenia ceny jest pełen zakres zamówienia określony w Załączniku nr 1 (OPZ) oraz Załączniku nr 2 (IPU) do SIWZ, wskazany przez wykonawcę w Formularzu Oferty, a także w Formularzu rzeczowo – cenowym (Załącznik nr 3a do SIWZ) i wyliczony

zgodnie z tym formularzem. Cena oferty winna obejmować wszystkie koszty, jakie poniesie Wykonawca z tytułu należytej realizacji przedmiotu zamówienia, zgodnie z warunkami wynikającymi z ww. dokumentów.

b) Cena oferty jest stała – wysokość wynagrodzenia Wykonawcy podlega waloryzacji wyłącznie na warunkach wskazanych w Załączniku nr 2 (IPU).

11.2 Jeżeli 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 prowadzić 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.

11.3 Zamawiający nie przewiduje dokonywania rozliczeń z Wykonawcą w walutach obcych.

12. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

12.1 Przy wyborze oferty zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	60
2.	Okres objęcia dostarczanego sprzętu i oprogramowania wsparciem	40
	SUMA:	**100**

12.2 Przy ocenie ofert w kryterium „Cena” (PC) punkty zostaną przyznane w poniższy sposób:

1) Cena – znaczenie 60% (maksymalnie do 60 pkt)
2) Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
3) Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

$$C = \frac{C_{min}}{C_N} \times 60$$

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena”

C_{min} – najniższa cena brutto spośród badanych ofert

C_N – cena brutto badanej ofert

4) Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 3 do SIWZ.

12.3 Przy ocenie ofert w kryterium „Okres objęcia dostarczanego sprzętu i oprogramowania wsparciem” (G) punkty zostaną przyznane w poniższy sposób:

1) Okres objęcia dostarczanego sprzętu i oprogramowania wsparciem – znaczenie 40 % (maksymalnie 40 pkt)

2) Punkty w kryterium „Okres objęcia dostarczanego sprzętu i oprogramowania wsparciem" zostaną przyznane na podstawie informacji umieszczonych przez Wykonawcę w rzeczowo-cenowym (Załącznik nr 3a do SIWZ) oraz formularzu ofertowym (Załącznik nr 3 do SIWZ).

- za zaoferowanie minimum 1 roku wsparcia (wymagane) – oferta otrzyma 0 pkt;
- za zaoferowanie minimum 2 lat wsparcia – oferta otrzyma 20 pkt;
- za zaoferowanie 3 lat wsparcia lub więcej – oferta otrzyma 40 pkt.

12.4 Sumaryczna liczba punktów zostanie obliczona według wzoru:

W = C + G
gdzie:
W – łączna liczba punktów przyznanych w poszczególnych kryteriach,
C – liczba punktów przyznanych w kryterium „Cena",
G - liczba punktów przyznanych w kryterium „Okres objęcia dostarczanego sprzętu i oprogramowania wsparciem",

12.5 Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

12.6 Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.

12.7 W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.

13. TERMIN SKŁADANIA OFERT I OTWARCIA OFERT

13.1 Termin składania ofert upływa dnia **20 maja 2020 r**., o godz. **9:00**.

13.2 Otwarcie ofert nastąpi w dniu **20 maja 2020 r.,** o godzinie **14:00**, w siedzibie Ministerstwa Spraw Zagranicznych, 00-580 Warszawa, al. J. Ch. Szucha 23 – wejście „C".

13.3 Otwarcie ofert następuje poprzez użycie aplikacji do szyfrowania ofert dostępnej na miniPortalu i dokonywane jest poprzez odszyfrowanie i otwarcie ofert za pomocą klucza prywatnego.

13.4 Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

13.5 Otwarcie ofert jest jawne.

13.6 Podczas otwarcia ofert podane zostaną: nazwy (firmy) oraz adresy Wykonawców, a także informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

13.7 Niezwłocznie po otwarciu ofert Zamawiający zamieści na swojej stronie internetowej informacje dotyczące:

a) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia,

b) firm oraz adresów wykonawców, którzy złożyli oferty w terminie,

c) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

14. TERMIN ZWIĄZANIA OFERTĄ

14.1 Wykonawca pozostaje związany złożoną ofertą przez okres 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

14.2 Wniesienie odwołania po upływie terminu składania ofert zawiesza bieg terminu związania ofertą do czasu ogłoszenia orzeczenia przez Krajową Izbę Odwoławczą (art. 182 ust. 6 ustawy).

15. ISTOTNE POSTANOWIENIA UMOWY

Istotne Postanowienia Umowy stanowią Załącznik nr 2 do SIWZ.

16. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

16.1 Zamawiający będzie żądał od Wykonawcy wniesienia zabezpieczenia należytego wykonania umowy w wysokości 10 % całkowitej ceny oferty brutto. Zabezpieczenie musi być wniesione w pełnej wysokości, niezależnie od formy jego wniesienia, najpóźniej w dniu zawarcia umowy, ale przed jej podpisaniem.

16.2 Zabezpieczenie może być wnoszone w jednej lub kilku następujących formach:

a) pieniądzu;

b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym;

c) gwarancjach bankowych;

d) gwarancjach ubezpieczeniowych;

e) poręczeniach udzielanych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2019 r., poz. 310 ze zm.).

16.3 Zabezpieczenie może być wniesione również za uprzednią pisemną zgodą Zamawiającego:

a) w wekslach z poręczeniem wekslowym banku lub spółdzielczej kasy oszczędnościowo-kredytowej;

b) przez ustanowienie zastawu na papierach wartościowych emitowanych przez Skarb Państwa lub jednostkę samorządu terytorialnego;

c) przez ustanowienie zastawu rejestrowego na zasadach określonych w przepisach o zastawie rejestrowym i rejestrze zastawów.

16.4 W przypadku wniesienia zabezpieczenia w formie pieniężnej należy dokonać przelewu na rachunek bankowy Narodowego Banku Polskiego nr **39 1010 1010 0007 3613 9120 0000**.

16.5 W przypadku zabezpieczenia wnoszonego w pieniądzu należy przedłożyć oryginał lub kopię (poświadczoną za zgodność z oryginałem) polecenia przelewu bankowego lub dowód wpłaty. W przypadku wnoszenia zabezpieczenia w innych formach: oryginał dokumentu zabezpieczenia.

16.6 Zamawiający dokona zwrotu zabezpieczenia należytego wykonania umowy w terminie 30 dni od dnia wykonania przedmiotu umowy i uznania umowy za należycie wykonaną.

16.7 W przypadku wniesienia wadium w pieniądzu Wykonawca może wyrazić zgodę na zaliczenie kwoty wadium na poczet zabezpieczenia.

17. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCOM W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO

W toku postępowania o udzielenie zamówienia Wykonawcom przysługują środki ochrony prawnej przewidziane w Dziale VI ustawy.

18. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

18.1 Zamawiający, o ile nie wpłynie odwołanie, zawrze umowę w sprawie przedmiotowego zamówienia w terminie nie krótszym niż 10 dni od dnia przekazania zawiadomienia o wyborze najkorzystniejszej oferty drogą elektroniczną. Zawarcie umowy nastąpi w miejscu i terminie wskazanym przez Zamawiającego.

18.2 Zamawiający może zawrzeć umowę w sprawie przedmiotowego zamówienia publicznego przed upływem terminu, o którym mowa w pkt 18.1, jeżeli w przedmiotowym postępowaniu zostanie złożona tylko jedna oferta.

18.3 Wykonawca wniesie zabezpieczenie należytego wykonania umowy w wysokości, o której mowa w pkt 16.1 Zabezpieczenie musi być wniesione w pełnej wysokości, niezależnie od formy jego wniesienia, najpóźniej w dniu zawarcia umowy, ale przed jej podpisaniem.

19. INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

19.1 W związku z wejściem w życie z dniem 25 maja 2018 r. przepisów o ochronie danych osobowych Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", Zamawiający wymaga, aby Wykonawca złożył oświadczenie w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 i/lub art. 14 RODO względem osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał na potrzeby niniejszego postępowania (zgodnie ze wzorem określonym w pkt 9 Formularza oferty).

19.2 Ponadto, w związku z przetwarzaniem przez Zamawiającego danych osobowych w ramach przedmiotowego postępowania Zamawiający w pkt 19.3 (poniżej) zamieszcza klauzulę informacyjną przewidzianą w art. 13 RODO.

19.3 Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych, informuję, że:

a) Administratorem, w rozumieniu art. 4 pkt 7 RODO, Pani/Pana danych osobowych jest: Minister Spraw Zagranicznych, z siedzibą w Warszawie, Al. J. Ch. Szucha 23, tel. +48 225230000;

b) Minister Spraw Zagranicznych powołał inspektora ochrony danych (IOD), który realizuje swoje obowiązki w odniesieniu do danych przetwarzanych w Ministerstwie Spraw Zagranicznych i placówkach zagranicznych.
   Dane kontaktowe IOD:
   adres siedziby: Al. J. Ch. Szucha 23, 00-580 Warszawa
   adres e-mail: iod@msz.gov.pl
c) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pt. Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych; znak sprawy BDG.741.016.2020, prowadzonym w trybie przetargu nieograniczonego,
d) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 ze zm.), dalej „ustawa Pzp”;
e) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
f) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
g) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
h) posiada Pani/Pan:
   - na podstawie art. 15 RODO, prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO, prawo do sprostowania Pani/Pana danych osobowych*;
   - na podstawie art. 18 RODO, prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
i) nie przysługuje Pani/Panu:
   - w związku z art. 17 ust. 3 lit. b, d lub e RODO, prawo do usunięcia danych osobowych;
   - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   - na podstawie art. 21 RODO, prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

20. POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w niniejszej SIWZ, zastosowanie mają przepisy ustawy Prawo zamówień publicznych.

21. ZAŁĄCZNIKI

Załącznik nr 1	–	Opis przedmiotu zamówienia
Załącznik nr 2	–	Istotne postanowienia umowy
Załącznik nr 3	–	Wzór Formularza oferty
Załącznik nr 3a	-	Wzór Formularza rzeczowo - cenowego
Załącznik nr 4	–	Wzór oświadczenia o przynależności lub braku przynależności do grupy kapitałowej
Załącznik nr 5	–	Wzór pełnomocnictwa
Załącznik nr 6	–	Wzór JEDZ
Załącznik nr 7	–	Wzór wykazu dostaw
Załącznik nr 8	–	Wzór oświadczenia o braku wyroku lub orzeczenia sądu

Znak: BDG.741.016.2020

Załącznik nr 1 do SIWZ

Opis przedmiotu zamówienia

I. Przedmiot zamówienia

Przedmiotem zamówienia jest modernizacja i rozbudowa infrastruktury sieciowej Zamawiającego poprzez:

1. Dostawę urządzeń infrastruktury sieciowej wraz z oprogramowaniem oraz usługami subskrypcyjnymi, fabrycznie nowych (wyprodukowanych nie wcześniej niż 6 miesięcy przed dostawą), z możliwością objęcia wsparciem producenta przez minimum 36 miesięcy od daty zakupu, nieużywanych we wcześniejszych projektach, pochodzących z legalnego kanału sprzedaży producentów na rynek europejski. Przedmiotem zamówienia nie jest objęta instalacja i konfiguracja urządzeń;
2. Objęcie usługami serwisowymi oprogramowania i sprzętu dostarczanego w ramach zamówienia.

II. Dostawa urządzeń infrastruktury sieciowej wraz z oprogramowaniem

1. Urządzenia odpowiedzialne za dołączanie urządzeń końcowych zapewniające jednocześnie bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
1.0	**N9K-C93240YC-FX2**	Nexus 9300 with 48p 10/25G SFP+ and 12p 100G QSFP28	-	4
1.1	CON-SNT-N93YCFX2	SNTC-8X5XNBD Nexus 9300 with 48p 10/25G SFP+ and 12p	12	4
1.2	NXOS-9.3.3	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 9.3.3	-	4
1.3	N3K-C3064-ACC-KIT	Nexus 3K/9K Fixed Accessory Kit	-	4
1.4	NXK-MEM-8GB	Additional memory of 8GB for Nexus Switches	-	4
1.5	NXA-FAN-35CFM-PE	Nexus 2K/3K/9K Single Fan, 35CFM, port side exhast airflow	-	20
1.6	NXA-PAC-1100W-PE2	Nexus AC 1100W PSU - Port Side Exhaust	-	8
1.7	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	-	8
1.8	C1A1TN9300XF-3Y	DCN Advantage Term N9300 XF, 3Y	36	4
1.9	SVS-B-N9K-ADV-XF	EMBEDDED SOLN SUPPORT SWSS FOR ACI NEXUS 9K	-	4

2. Urządzenia odpowiedzialne za dołączanie urządzeń końcowych zapewniające jednocześnie bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość

2.0	**N9K-C9332C**	Nexus 9K ACI & NX-OS Spine, 32p 40/100G & 2p 10G	-	4
2.1	CON-SNT-N9KC9332	SNTC-8X5XNBD Nexus 9K ACI NX-OS Spine, 32p 40/100G	12	4
2.2	MODE-NXOS	Dummy PID for mode selection	-	4
2.3	NXOS-9.3.3	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 9.3.3	-	4
2.4	N3K-C3064-ACC-KIT	Nexus 3K/9K Fixed Accessory Kit	-	4
2.5	NXA-FAN-35CFM-PE	Nexus 2K/3K/9K Single Fan, 35CFM, port side exhast airflow	-	20
2.6	NXA-PAC-1100W-PE2	Nexus AC 1100W PSU - Port Side Exhaust	-	8
2.7	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	-	8
2.8	C1A1TN9300XF-3Y	DCN Advantage Term N9300 XF, 3Y	36	4
2.9	SVS-B-N9K-ADV-XF	EMBEDDED SOLN SUPPORT SWSS FOR ACI NEXUS 9K	-	4

3. Urządzenia odpowiedzialne za dołączanie urządzeń końcowych zapewniające jednocześnie bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
3.0	C9500-32QC-A	Catalyst 9500 32-port 40/100G only, Advantage	-	4
3.1	CON-SNT-C9532ACQ	SNTC-8X5XNBD Catalyst 9500 32-port 40/100G only, Adva	12	4
3.2	C9500-NW-A	C9500 Network Stack, Advantage	-	4
3.3	SC9500HUK9-1612	Cisco Catalyst 9500H XE.16.12 UNIVERSAL	-	4
3.4	C9K-PWR-650WAC-R	650W AC Config 4 Power Supply front to back cooling	-	4
3.5	C9K-PWR-650WAC-R/2	650W AC Config 4 Power Supply front to back cooling	-	4
3.6	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	-	8
3.7	C9K-F1-SSD-BLANK	Cisco pluggable SSD storage	-	4
3.8	C9500-DNA-32QC-A	C9500 DNA Advantage, Term License	-	4
3.9	C9500-DNA-A-3Y	Cisco Catalyst 9500 DNA Advantage 3 Year License	36	4
3.10	PI-LFAS-T	Prime Infrastructure Lifecycle & Assurance Term - Smart Lic	-	12
3.11	PI-LFAS-AP-T-3Y	PI Dev Lic for Lifecycle & Assurance Term 3Y	36	12
3.12	NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment	-	4
3.13	C9500-NM-8X=	Cisco Catalyst 9500 8 x 10GE Network Module	-	4

4. Urządzenia odpowiedzialne za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
4.0	ISR4461/K9	Cisco ISR 4461 (2x10GE+4x1GE,3NIM,3SM,8G FLASH,4G DRAM)	-	2
4.1	CON-SNT-ISR44619	SNTC-8X5XNBD Cisco ISR 4461 (4GE,3NIM,3SM,8G FLASH,4G	12	2
4.2	SL-44-IPB-K9	IP Base License for Cisco ISR 4400 Series	-	2
4.3	FL-4460-BOOST-K9	Booster Performance License for 4460 Series	-	2
4.4	MEM-4460-16G	16G DRAM (1 DIMM) for Cisco ISR 4461	-	2
4.5	MEM-FLSH-8GU16G	8G to 16G Flash Memory Upgrade for Cisco ISR 4400	-	2
4.6	PWR-4460-650-AC	650W AC Power Supply for Cisco ISR 4461	-	2
4.7	PWR-4460-650-AC2	Redundant 650W AC Power Supply for Cisco ISR 4461	-	2
4.8	CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	-	4
4.9	POE-COVER-4450	Cover for empty POE slot on Cisco ISR 4450	-	4
4.10	ACS-4460-FANASSY	Cisco ISR 4460 Fan Assembly	-	2
4.11	MEM-4460-DP-4G	4G DRAM for Cisco ISR 4460 Data Plane	-	2
4.12	SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	-	4
4.13	SM-F-BLANK	Fixed faceplate for SM slot on Cisco 4461 ISR	-	2
4.14	NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	-	6
4.15	SISR4400V2UK9-169	Cisco ISR 4400 Series IOS XE Universal	-	2
4.16	SL-44-SEC-K9	Security License for Cisco ISR 4400 Series	-	2
4.17	FL-44-HSEC-K9	U.S. Export Restriction Compliance license for 4400 series	-	2

5. Urządzenia odpowiedzialne za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
5.0	FPR4110-ASA-K9	Cisco Firepower 4110 ASA Appliance, 1U, 2 x NetMod Bays	-	4
5.1	CON-SSSNT-FPR41GHP	SOLN SUPP 8X5XNBD Cisco Firepower 4110 ASA Appliance, 1U,	12	4
5.2	FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	-	4
5.3	CAB-AC-EUR	Power Cord - Europe, 16/10A,250V, 2500mm, -40C to +85C	-	8

5.4	SF-FXOS4K-2.2-K9	Cisco Firepower Extensible Operating System v2.2 for FPR4000	-	4
5.5	SF-F4K-ASA9.8.2-K9	Cisco ASA 9.8.2 Software for Firepower 4100 appliance series	-	4
5.6	FPR4K-ASASC-10	Cisco Firepower 4100 - Add 10 Security Context Licenses	-	4
5.7	FPR4K-ENC-K9	Cisco Firepower 4100 Strong Encryption (3DES/AES)	-	4
5.8	FPR4100-ASA	Cisco Firepower 4100 Standard ASA License	-	4
5.9	GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	-	4
5.10	FPR4K-SSD200	Firepower 4000 Series SSD for FPR-4110/4120	-	4
5.11	FPR4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	-	4
5.12	FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	-	4
5.13	FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit	-	4
5.14	FPR4K-FAN	Firepower 4000 Series Fan	-	24
5.15	FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	-	4
5.16	GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	-	4
5.17	FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	-	4
5.18	FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	-	4

6. Urządzenia odpowiedzialne za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
6.0	ISR4321/K9	Cisco ISR 4321 (2GE,2NIM,4G FLASH,4G DRAM,IPB)	-	2
6.1	CON-SNT-ISR4321K	SNTC-8X5XNBD Cisco ISR 4321 (2GE,2NIM,4G FLASH,4G DRAM,IPB)	12	2
6.2	SL-4320-IPB-K9	IP Base License for Cisco ISR 4320 Series	-	2
6.3	SL-4320-SEC-K9	Security License for Cisco ISR 4320 Series	-	2
6.4	MEM-4320-4GU8G	4G to 8G DRAM Upgrade (Fixed 4G + additional 4G) for ISR4320	-	2
6.5	MEM-FLSH-4U8G	4G to 8G eUSB Flash Memory Upgrade for Cisco ISR 4300	-	2
6.6	NIM-2T	2-Port Serial WAN Interface card	-	2
6.7	NIM-ES2-8-P	8-port POE/POE+ Layer 2 GE Switch Network Interface Module	-	2
6.8	PWR-4320-POE-AC	AC Power Supply with POE for Cisco ISR 4320	-	2

6.9	CAB-C15-ACE	AC Power Cord (Europe), C15, CEE 7, 2.5m	-	2
6.10	SISR4300UK9-1612	Cisco ISR 4300 Series IOS XE Universal	-	2

7. Urządzenia odpowiedzialne za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
7.0	FPR1010-NGFW-K9	Cisco Firepower 1010 NGFW Appliance, Desktop	-	2
7.1	CON-SNT-FPR1010N	SNTC-8X5XNBD Cisco Firepower 1010 NGFW Appliance, Des	12	2
7.2	FPR1K-EXCLUDE-SUBS	Cisco Firepower 1000 Series - Exclude Subscriptions	-	2
7.3	FPR1K-DT-PWR-AC	Cisco Firepower 1K Series 150W Power Adapter for FPR-1010	-	2
7.4	CAB-AC-C5-EUR	AC Power Cord, Type C5, Europe	-	2
7.5	SF-F1K-TD6.4-K9	Cisco Firepower Threat Defense software v6.4 for FPR1100	-	2
7.6	FPR1K-DT-ACY-KIT	Cisco Firepower 1K Series Accessory Kit for FPR-1010	-	2
7.7	FPR1000-ASA	Cisco Firepower 1000 Standard ASA License	-	2

8. Rozbudowa posiadanej infrastruktury Cisco ISE w tym subskrypcje:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
8.0	R-ISE-VMS-K9=	Cisco ISE Virtual Machine Small	-	1
8.1	CON-ECMU-RISEV9SM	SWSS UPGRADES Cisco ISE Virtual Machine Small	12	1

9. Rozbudowa posiadanej infrastruktury Cisco ISE:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
9.0	L-ISE-BSE-PLIC	Cisco ISE Base License	-	1
9.1	L-ISE-BSE-P4	Cisco ISE Base License - Sessions 1000 to 2499	-	1

10. Subskrypcje w ramach posiadanej infrastruktury Cisco ISE:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
10.0	L-ISE-PLS-LIC=	Cisco ISE Plus License	-	1

10.1	L-ISE-PLS-3Y-S2	Cisco ISE Plus License, 3Y, 250 - 499 Sessions	36	1

11. Subskrypcje w ramach posiadanej infrastruktury Cisco ISE:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
11.0	L-ISE-APX-LIC=	Cisco ISE Apex License	-	1
11.1	L-ISE-APX-3Y-S1	Cisco ISE Apex License, 3Y, 100 - 249 Sessions	36	1

12. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
12.0	L-ASA5545-TA=	Cisco ASA5545 FirePOWER IPS License	-	8
12.1	L-ASA5545-TA-3Y	Cisco ASA5545 FirePOWER IPS 3YR Subscription	36	8

13. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
13.0	L-ASA5506-TA=	Cisco ASA5506 FirePOWER IPS License	-	4
13.1	L-ASA5506-TA-3Y	Cisco ASA5506 FirePOWER IPS 3YR Subscription	36	4

14. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
14.0	L-ASA5508-TA=	Cisco ASA5508 FirePOWER IPS License	-	4
14.1	L-ASA5508-TA-3Y	Cisco ASA5508 FirePOWER IPS 3YR Subscription	36	4

15. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
15.0	L-FPR2130T-TC=	Cisco FPR2130 Threat Defense Threat and URL License	-	4
15.1	L-FPR2130T-TC-3Y	Cisco FPR2130 Threat Defense Threat and URL 3Y Subs	36	4

16. Rozbudowa posiadanych urządzeń:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
16.0	QSFP-40G-SR-BD=	QSFP40G BiDi Short-reach Transceiver	-	52

17. Rozbudowa posiadanych urządzeń:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
17.0	SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	-	160

18. Rozbudowa posiadanych urządzeń:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
18.0	SFP-10G-LR-S=	10GBASE-LR SFP Module, Enterprise-Class	-	4

19. Rozbudowa posiadanych urządzeń:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
19.0	SFP-10G-ER-S=	10GBASE-ER SFP Module, Enterprise-Class	-	14

20. Rozbudowa posiadanych urządzeń:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
20.0	GLC-SX-MMD=	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	-	40

21. Rozbudowa posiadanych urządzeń:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
21.0	CVR-QSFP-SFP10G=	QSFP to SFP10G adapter	-	40

22. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość

22.0	C9200-48P-E	Catalyst 9200 48-port PoE+, Network Essentials	-	102
22.1	CON-SNT-C92048PE	SNTC-8X5XNBD Catalyst 9200 48-port PoE+, Network Esse	12	102
22.2	C9200-NW-E-48	C9200 Network Essentials, 48-port license	-	102
22.3	C9200-NM-NONE	No Network Module Selected	-	102
22.4	CAB-TA-EU	Europe AC Type A Power Cable	-	102
22.5	PWR-C5-BLANK	Config 5 Power Supply Blank	-	102
22.6	C9200-DNA-E-48	C9200 Cisco DNA Essentials, 48-Port Term Licenses	-	102
22.7	C9200-DNA-E-48-3Y	C9200 Cisco DNA Essentials, 48-port - 3 Year Term License	36	102
22.8	C9200-STACK-KIT	Cisco Catalyst 9200 Stack Module	-	102
22.9	C9200-STACK	Catalyst 9200 Stack Module	-	204
22.10	STACK-T4-50CM	50CM Type 4 Stacking Cable	-	102
22.11	NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment	-	102

23. Rozbudowa posiadanych urządzeń z punktu 22:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
23.0	C9200-NM-4X=	Catalyst 9200 4 x 10G Network Module	-	40

24. Rozbudowa posiadanych urządzeń z punktu 22:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
24.0	PWR-C5-1KWAC=	1KW AC Config 5 Power Supply	-	10
24.1	CAB-TA-EU	Europe AC Type A Power Cable	-	10

25. Rozbudowa posiadanych urządzeń z punktu 22:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
25.0	STACK-T4-1M	1M Type 4 Stacking Cable	-	16

26. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
26.0	WS-C3560CX-8PT-S	Cisco Catalyst 3560-CX PD PSE 8 Port PoE, 1G Uplinks IP Base	-	4
26.1	CON-SNT-WSC356CT	SNTC-8X5XNBD Cisco Catalyst 3560-CX 8 Port PoE, 1G Up	12	4
26.2	PWR-ADPT	Power adaptor for compact switches	-	4
26.3	CAB-AC2E	AC Power cord Europe	-	4

27. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych (bramki głosowe):

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
27.0	VG310	Modular 24 FXS Port VoIP Gateway with PVDM3-64	-	2
27.1	CON-SNT-VG310ICV	SNTC-8X5XNBD Cisco VG310 - Modular 24 FXS Port Voice	12	2
27.2	SVG3XUK9-15603M	Cisco VG3X0 UNIVERSAL	-	2
27.3	MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR	-	2
27.4	CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	-	2
27.5	PVDM3-64	64-channel high-density voice DSP module	-	2
27.6	HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR	-	2
27.7	SL-VG3X0-IPB-K9	Cisco VG3X0 IP Base License	-	2
27.8	SL-VG3X0-UC-K9	Cisco VG3X0 Unified Communications License	-	2

28. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych (bramki głosowe):

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
28.0	VG204XM	Cisco VG204XM Analog Voice Gateway	-	5
28.1	CON-SNT-VG204XM	SNTC-8X5XNBD Cisco VG204 Analog V	12	5
28.2	SVG2XAISK9-15703M	Cisco VG20X Series IOS ADVANCED IP SERVICES	-	5
28.3	CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	-	5
28.4	PS-SWITCH-AC-3P	3 Prong C13/C14 On-Off AC Power Supply Switch	-	5
28.5	CAB-ETH-S-RJ45	Yellow Cable for Ethernet, Straight-through, RJ-45, 6 feet	-	5
28.6	PWR-30W-AC	Power Supply 30 Watt AC	-	5

29. Platforma serwerowa z przeznaczeniem dla Unified Communication (Mostek wideokonferencyjny)

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
29.0	CTI-CMS1KM5-BUN-K9	Cisco Meeting Server 1000 M5 Bundle	-	1
29.1	R-CMS-K9	Virtual Edition Cisco Meeting Server (CMS)	-	1
29.2	CON-ECMU-RCMSK9	SWSS UPGRADES Virtual Edition Cisc	12	1
29.3	LIC-CMS-K9	Cisco Meeting Server Release key (encryption enabled)	-	1
29.4	CON-ECMU-LICCMSLG	SWSS UPGRADES Cisco Meeting Server	12	1
29.5	LIC-CMS-PAK	Cisco Meeting Server (CMS) PAK	-	1
29.6	SW-CMS-2X-K9	Cisco Meeting Server (CMS) 2.x Software image	-	1
29.7	CON-ECMU-SWCM2XK9	SWSS UPGRADES Cisco Meeting Serve	12	1
29.8	CTI-CMS-1000-M5-K9	CMS 1000 M5 Server	-	1
29.9	CON-SNT-CTICMSM5	SNTC-8X5XNBD CMS 1000 M5 Server	12	1
29.10	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	-	2
29.11	VMW-VS6-CVSTD-K9	Embedded License, Cisco Collab Virt. Standard 6.x (2-socket)	-	1
29.12	CON-ECMU-VMWVS6CV	SWSS UPGRADES Embedded License, Cisco Collab Virt. Sta	12	1
29.13	CMS1K-SW-2X	Cisco Meeting server 1000 sw preload	-	1
29.14	CIT3-CPU-6140	2.3 GHz 6140/140W 18C/24.75MB Cache/DDR4 2666MHz	-	2
29.15	CIT3-HD300G10K12N	300GB 12G SAS 10K RPM SFF HDD	-	2
29.16	CIT3-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	-	2
29.17	CIT3-MR-X16G1RS-H	16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v	-	8
29.18	CIT3-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	-	1
29.19	R2XX-RAID1	Enable RAID 1 Setting	-	1

30. Rozbudowa posiadanych urządzeń oraz pozycji 29.

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
30.0	R-CMS-K9	Virtual Edition Cisco Meeting Server (CMS)	-	1

30.1	CON-ECMU-RCMSK9	SWSS UPGRADES Virtual Edition Cisc	-	1
30.2	LIC-CMS-PAK	Cisco Meeting Server (CMS) PAK	-	1
30.3	SW-CMS-2X-K9	Cisco Meeting Server (CMS) 2.x Software image	-	1
30.4	CON-ECMU-SWCM2XK9	SWSS UPGRADES Cisco Meeting Serve	-	1
30.5	LIC-CMS-K9	Cisco Meeting Server Release key (encryption enabled)	-	1
30.6	CON-ECMU-LICCMSLG	SWSS UPGRADES Cisco Meeting Server	-	1

31. System rejestracji połączeń głosowych.

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
31.0	ZOOM-REC	SolutionsPlus: ZOOM SolutionsPlus Package	36	1
31.1	ZI-CR-UCM-CON	SolutionsPlus:Zoom CallREC - Concurrent for CUCM	36	30
31.2	ZI-CR-UCM-CON-S	SolutionsPlus:M&S for ZOOM CallREC - Concurrent for CUCM	36	90
31.3	ZI-HA-CR	SolutionsPlus:ZOOM High Availability for CallREC	36	30
31.4	ZI-HA-CR-S	SolutionsPlus:M&S for HA for CallRec	36	90
31.5	ZI-ZQM-AS	SolutionsPlus:ZOOM Advanced Security for Encrypted Calls	36	30
31.6	ZI-ZQM-AS-S	SolutionsPlus:M&S for Adv Security	36	90
31.7	L-SP-PRODUCT-TERMS	SolutionsPlus vendor terms available at http://cs.co/spla	36	1

32. Zestaw rozszerzony systemu wideokonferencji:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
32.0	CS-ROOM55-K9	Room 55 with Touch10 and Mount	-	2
32.1	CON-SSSNT-CSROOMK9	SOLN SUPP 8X5XNBD Cisco Spark Room 55 with Touch10 and Mou	12	2
32.2	PWR-CORD-EUR-F	Power Cord for Europe 5m 10A	-	2
32.3	CS-ROOM55-FSK	Webex Room 55, Floor Stand Kit	-	2
32.4	CAB-PRES-2HDMI-GR-	Presentation cable 8m GREY HDMI 1.4b (W/ REPEATER)	-	2
32.5	CS-TOUCH10+	Cisco Touch10 controller for collaboration endpoints	-	2

32.6	CAB-DV10-8M-	8 meter flat grey Ethernet cable for Touch 10	-	2
32.7	CAB-ETH-5M-GR-	CAB (16,4 feet / 5m) GREY ETHERNET	-	2
32.8	CS-MIC-TABLE-J+	Cisco Table Microphone with Jack plug	-	4
32.9	CS-R55-UNI2-K9+	Cisco Webex Room 55 Main Unit	-	2
32.10	SW-S53200-CE9	SW Image for Cisco Spark Room	-	2

33. Zestaw podstawowy systemu wideokonferencji:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
33.0	CS-KIT-K9	Room Kit with integrated microphone, speakers and Touch 10	-	3
33.1	CON-SNT-CSKITK9	SNTC-8X5XNBD Room Kit with integrated microphone, spe	12	3
33.2	PWR-CORD-EUR-B	Power Cord for Europe 2m 10A	-	6
33.3	CS-MIC-TABLE-J	Cisco Table Microphone with Jack plug	-	6
33.4	CON-SNT-CSMICTMP	SNTC-8X5XNBD Cisco Table Microphone with Jack plug	12	6
33.5	CAB-2HDMI-1.5M-GR-	1.5m GREY HDMI 2.0	-	3
33.6	CAB-ETH-5M-GR-	CAB (16,4 feet / 5m) GREY ETHERNET	-	6
33.7	PSU-12VDC-70W-GR-	Powersupply - AC/DC, 12V, 6.25A, grey	-	3
33.8	CS-KIT-WMK-	Wall Mount for Cisco Spark Kit	-	3
33.9	CS-TOUCH10+	Cisco Touch10 controller for collaboration endpoints	-	3
33.10	CS-KIT-SMK-	Screen Mount for Cisco Spark Kit	-	3
33.11	CAB-DV10-8M-	8 meter flat grey Ethernet cable for Touch 10	-	3
33.12	CS-POE-INJ+	Touch PoE power injector	-	3

34. Urządzenia odpowiedzialne za bezpieczeństwo sieci:

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
34.0	CPAP-SG5600-NGTP-SSD	5600 Next Generation Threat Prevention Appliance with SSD	-	1
34.1	CPAP-SG5600-NGTP-SSD-HA	5600 Next Generation Threat Prevention Appliance for High Availability with SSD	-	1
34.2	CPSB-NGTP-5600-3Y	Next Generation Threat Prevention Package subscription for 3 year for 5600 Appliance	-	1

34.3	CPSB-NGTP-5600-3Y-HA	Next Generation Threat Prevention Package subscription for 3 year for 5600 Appliance HA	-	1
34.4	CPAC-4-10F-B-INSTALL	4 Port 10GBase-F SFP+ interface card compatible with 5600, 5800, 5900, 15000 and 23000 Security Gateways only	-	2
34.5	CPAC-TR-10SR-B	SFP+ transceiver for 10G fiber Ports - short range (10GBase-SR) compatible with CPAC-4-10F-B, CPAC-2-10F-B, CPAC-2-10FSR-BP-B, CPAC-2-10F-SM only	-	8
34.6	CPAC-RAM8GB-5000-INSTALL	Memory Upgrade Kit from 8GB to 16GB for 5000 series appliances	-	2
34.7	CPAC-LOM-B-INSTALL	Light Out Management module appliances	-	2
34.8	CPAC-Rails-5000	Slide Rails for 5000 series, Smart-1 405, Smart-1 410 and SandBlast, TE100X (22inch-32inch)	-	2
34.9	CPAC-PSU-5600/5800	Additional/Replacement AC Power Supply for 5600 and 5800 appliances	-	2
34.10	CPCES-CO-PREMIUM-ADD	Premium Collaborative Enterprise Support For XXXXX Days. Start date: February 10, 2020. Renewal Date: December 31, 2023	-	1

35. Rozbudowa posiadanych urządzeń.

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
35.0	AFM735	AFM735 Interfejs SFP 100BASE-FX	-	40

36. Rozbudowa posiadanych urządzeń.

L.p.	Nazwa elementu	Opis	Czas trwania usługi	Ilość
36.0	AGM731F	ProSafe AGM731F 1000BASE-SX SFP GBIC	-	4

III. Zakup usług serwisowych dla oprogramowania i sprzętu, dla dostarczanych w ramach zamówienia urządzeń infrastruktury sieciowej

Usługi serwisowe i gwarancyjne oprogramowania i sprzętu świadczone przez certyfikowanych inżynierów producenta, będą realizowane przez Wykonawcę w dwóch aktualnie dostępnych lokalizacjach Zamawiającego, w których funkcjonuje produkcyjnie infrastruktura zaawansowanych systemów sieciowych (al. J. Ch. Szucha 21/23 oraz ul. Karmazynowa 1A), na warunkach określonych przez producenta oprogramowania i sprzętu.

Wykonawca zobowiązany jest dostarczyć pakiety serwisowe dla sprzętu i oprogramowania będącego przedmiotem niniejszego zamówienia oraz dokonać ich aktywacji, gwarantujące:

1. Wymianę uszkodzonego sprzętu w terminie do następnego dnia roboczego po zgłoszeniu

awarii w okresie obowiązywania umowy, z zastrzeżeniem, że dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucji;

2. Świadczenie usług subskrypcji sprzętu i oprogramowania, w tym możliwość pobierania poprawek i aktualizacji posiadanego oprogramowania w tym telefonii IP (zarówno update jak i upgrade - przed i po kropce) oraz sygnatur w okresie obowiązywania umowy, dostęp do poprawek i aktualizacji musi posiadać Wykonawca i Zamawiający;
3. Zgłaszanie zapytań i problemów technicznych oraz awarii sprzętu i oprogramowania do Centrum zgłoszeń producenta wraz z priorytetem zgłoszenia serwisowego, zgodnie z procedurą przyjętą przez producenta sprzętu, bezpośrednio przez Zamawiającego jak i Wykonawcę.
4. Bieżące zarządzanie zgłoszeniami serwisowymi składanymi w Centrum zgłoszeń serwisowych producenta oraz eskalacjami (otwieranie zgłoszeń serwisowych, monitorowanie zgłoszonych problemów bezpośrednio przez Zamawiającego jak i Wykonawcę).

IV. Harmonogram dostaw:

1. Harmonogram dostaw:

Dostawa w roku 2020, w ciągu 60 dni od podpisania umowy.

2. Objęcie dostarczonych przez Wykonawcę urządzeń i oprogramowania usługami serwisowymi (gwarancyjnymi) nastąpi w ciągu 1 dnia od dostawy urządzenia.

V. Kryteria równoważności:

W odniesieniu do wszystkich wymienionych elementów, Zamawiający wymaga pełnego współdziałania z posiadanymi urządzeniami przy jednoczesnym zagwarantowaniu funkcjonalności wyszczególnionego / przedstawionego elementu. Jednocześnie Zamawiający wymaga zapewnienia, że oferowane, jako zamienniki (niebędące elementami, które wymienia Zamawiający w OPZ) elementy nie spowodują utraty świadczeń gwarancyjnych zarówno urządzeń, do których są dedykowane jak również całości rozwiązań technicznych autoryzowanych przez producenta urządzenia.

Wymagania ogólne dla urządzeń aktywnych

- dostarczane urządzenia muszą być nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem, nie refabrykowane) oraz nie używane – wyjątkiem są elementy rozbudowujące posiadaną infrastrukturę, o ile ich produkcja została zakończona
- dostarczane rozwiązania muszą odpowiadać wymaganiom Polskich Norm przenoszących normy europejskie lub norm innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy
- urządzenia wraz z zainstalowanym na nich oprogramowaniem muszą pochodzić z legalnego źródła i być przeznaczone do użytkowania na terenie Unii Europejskiej

- całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie co najmniej 24 miesięcy od daty dostawy (chyba że wymagania szczegółowe określają inny czas) – wymagane jest zapewnienie możliwości bezpośredniego kontaktu z centrum wsparcia technicznego producentów
- korzystanie przez użytkownika z dostarczonych produktów nie może stanowić naruszenia majątkowych praw autorskich osób trzecich
- każdego dostarczanego urządzenia/materiału należy dostarczyć Certyfikat Pochodzenia lub inny dokument wystawiony przez producenta lub jego lokalnego przedstawiciela (zawierającego m.in. dane identyfikacyjne produktu pozwalające na jego identyfikację np. kod produktu, nr seryjny itp.) potwierdzający, że dany dostarczony produkt jest fabrycznie nowy, jest oznakowany symbolem CE, pochodzi z autoryzowanej sieci sprzedaży – oficjalnego kanału sprzedaży na rynek europejski.
- dostarczone oprogramowanie musi być oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy albo ostatniej opublikowanej)
- jeżeli wymagania szczegółowe nie stanowią inaczej, wszystkie wymagane funkcjonalności muszą być dostępne w oferowanych rozwiązaniach w dniu dostawy
- poszczególne funkcjonalności i protokoły wymagane przełączników muszą być kompatybilne
- wymagane jest zapewnienie możliwości aktualizacji oprogramowania w okresie gwarancyjnym
- Zamawiający zastrzega sobie prawo do zwrócenia się do oferenta lub producentów oferowanych rozwiązań o potwierdzenie spełniania wybranych wymagań i wskazanie potwierdzenia ich spełnienia w publicznie dostępnej dokumentacji produktów (dopuszczalny język polski lub angielski)
- całość sprzętu i oprogramowania musi być objęta serwisem gwarancyjnym bazującym na pakietach serwisowych producenta rozwiązania, umożliwiających aktualizację oprogramowania systemowego i bezpośredni dostęp do centrum wsparcia technicznego producenta na okres co najmniej 12 miesięcy
- w przypadku oprogramowania z licencjami ograniczonymi czasowo lub licencjami subskrypcyjnymi wymagane jest ich dostarczenie na okres co najmniej 36 miesięcy.

Przełączniki CPD (Centra Przetwarzania Danych)

<u>Wymagania ogólne</u>

- Funkcjonalności warstwy L2:
  - Trunking IEEE 802.1Q VLAN;
  - Wsparcie sprzętowe dla co najmniej 3.000 sieci VLAN;
  - Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
  - Wsparcie sprzętowe dla minimum 50.000 adresów MAC
  - IEEE 802.1w Rapid Spanning Tree (RST)
  - IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje
  - Wsparcie sprzętowe dla tunelowania QinQ
  - Zabezpieczenie przeciwko incydentom w topologii Spanning Tree
  - Internet Group Management Protocol (IGMP) Versions 2, 3;
  - Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach

- Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce
- Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów);

- Funkcjonalności warstwy L3
  - Sprzętowe przełączanie pakietów w warstwie L3
  - Routing w oparciu o trasy statyczne
  - Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
  - Policy Based Routing (PBR) dla IPv4
  - VRRP v3
  - Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol)
  - Wsparcie sprzętowe dla minimum 250.000 prefixów / wpisów hosta w tablicy routingu IP
  - Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast)
  - Wsparcie dla IGMPv3 oraz MSDP
  - Wsparcie sprzętowe dla minimum 5.000 tras multicastowych
  - Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking)
  - Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP)
  - Minimum 2.000 wejściowych oraz 2.000 wyjściowych wpisów dla ACL - access control list
- Przełącznik posiada możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów lub przełączników nie jest realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3 a jedynie w ramach domeny fizycznej bądź stosu urządzeń. Porty modułu wyniesionego są udostępniane do zarządzania i monitorowania z poziomu przełącznika macierzystego.
- Mechanizmy związane z z funkcjonalnością VXLAN:
  - obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint)
  - sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway)
  - obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP
  - obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
  - implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol)
  - obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).
- Mechanizmy związane z zapewnieniem jakości usług w sieci:
  - layer 2 IEEE 802.1p (CoS);
  - klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4;
  - kolejkowanie na wyjściu w oparciu o CoS 802.1p;
  - bezwzględne (strict-priority) kolejkowanie na wyjściu;
  - kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny
  - ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych
  - kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych

- protokół PFC (Priority Flow Control) IEEE 802.1Qbb
- Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
- wejściowe ACL (standardowe oraz rozszerzone);
- standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
- standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
- ACL oparte o VLAN-y (VACL)
- ACL oparte o porty (PACL)
- DHCP Snooping
- ARP Inspection
- IP Source Guard
- prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
- Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
- RMON (przynajmniej grupy Events, Alarms)
- Openflow 1.3
- sFlow lub netFlow
- IEEE 802.1ab LLDP
- możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
- ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
- kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror)
- network Time Protocol (NTP);
- ping, traceroute
- Narzędzia programowania i zarzadzania przełącznikiem:
- interfejs programistyczny REST API wraz z upublicznionym SDK
- wsparcie dla NETCONF i zarządzania poprzez XML
- wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32- i 64-bitowych w oparciu o narzędzie typu yum i paczki rpm niezależnie od systemu operacyjnego przełącznika. Kontener musi mieć możliwość wykorzystywania portów fizycznych przełącznika.
- klient Chef
- agent Puppet
- interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
- wsparcie dla OpenStack Neutron plugin
- przełącznik musi mieć możliwość zarządzania przez komercyjnie dostępny kontroler SDN (Software Defined Networking), umożliwiający:
  - automatyzację konfiguracji zarządzanej sieci w oparciu o model sieciowych polityk grupowych powiązanych z aplikacjami
  - polityka definiowana na kontrolerze musi opisywać model działania aplikacji w oparciu o relacje pomiędzy punktami styku elementów aplikacji z siecią

- zintegrowanie usług zewnętrznych poprzez zapewnienie konfiguracji mechanizmu przekierowania ruchu (redirection) dla warstw 4-7
- możliwość wydzielania izolowanych wirtualnych środowisk sieciowych SDN wraz z dedykowanymi zespołami administratorów i prawami dostępu dla co najmniej 3 takich środowisk (multitenant).
- możliwość tworzenia wirtualnych instancji sieciowych umożliwiających nakładanie się adresacji IP w wielu zaimplementowanych równocześnie instancjach (VRF)
- możliwość implementacji funkcjonalności dedykowanej bramy wyjściowej L2/L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7 dla wirtualnych środowisk sieciowych SDN i wielu zaimplementowanych równocześnie instancji (VRF)
- możliwość tworzenia segmentów sieci L2 w oparciu o technologię VXLAN

konwersja przełącznika do formy zarządzanej przez kontroler musi być bezkosztowa w okresie co najmniej 3 lat – należy przewidzieć wszystkie niezbędne licencje i akcesoria

- zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej
- obudowa przeznaczona do montażu w szafie rackowej 19”

1. Urządzenia odpowiedzialne za dołączanie urządzeń końcowych zapewniające jednocześnie bezpieczeństwo sieci (N9K-C93240YC-FX2).

Wymagania szczegółowe – przełączniki dostępowe CPD **(np. Cisco Nexus 93240YC-FX2)**

- Przełącznik posiada:
  - minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej
  - minimum 12 portów 40/100GE definiowanych za pomocą wkładek QSFP
  - sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit na wszystkich portach
- Parametry wydajnościowe:
  - prędkość przełączania „wirespeed” dla każdego portu przełącznika
  - urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
  - obsługiwana łączna przepływność (pasmo) min. 4,8Tbps
  - obsługiwana łączna przepustowość pakietowa przełącznika min. 1.600 Mpps
  - średnie opóźnienie przełączania pakietów nie większe niż 2 µs

2. Urządzenia odpowiedzialne za dołączanie urządzeń końcowych zapewniające jednocześnie bezpieczeństwo sieci (N9K-C9332C).

Wymagania szczegółowe – przełączniki agregacyjne CPD **(np. Cisco Nexus 9332C)**

- Przełącznik posiada:
  - minimum 32 porty 10/40/100GE definiowanych za pomocą wkładek QSFP
  - sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit na co najmniej 8miu portach

- Parametry wydajnościowe:
  - prędkość przełączania „wirespeed" dla każdego portu przełącznika
  - urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
  - obsługiwana łączna przepływność (pasmo) min. 6,4Tbps
  - obsługiwana łączna przepustowość pakietowa przełącznika min. 2.000 Mpps
  - średnie opóźnienie przełączania pakietów nie większe niż 2 µs

Przełączniki dostępowe LAN

Wymagania ogólne

- wszystkie porty Ethernet muszą być dostępne od przodu urządzenia
- wyposażony w:
  - redundantne i wymienne moduły wentylatorów
  - wymienne zasilacze prądu zmiennego AC
  - redundantny wewnętrzny zasilacz
- skalowalność:
  - min. 1.000 sieci VLAN, interfejsów SVI,
  - min. 30.000 adresów MAC
  - sprzętowa dla QoS i ACL - minimum 1.000 wpisów sprzętowych
- urządzenia muszą zapewniać łączenie w stos
  - obsługa co najmniej 8 urządzeń w stosie
  - przepustowość w stosie min. 160 Gbps
  - stos widoczny jako jedno urządzenie z perspektywy protokołów sieciowych, routingu i zarządzania
  - połączenie urządzeń w stos nie może zmniejszać dostępnej ilości portów Ethernet
  - dołączone okablowanie umożliwiające łączenie w stos
- przełączanie w warstwie 2 i 3
  - obsługa VLAN 802.1Q i trunk na wszystkich portach
  - obsługa routingu statycznego i dynamicznego (RIPv2, RIPng, OSPF v2/v3 dla IPv4 i IPv6 – co najmniej 200 tras)
  - możliwość rozbudowy funkcjonalności o:
    - obsługa pełnego routingu dynamicznego (OSPF v2/v3, IS-IS, BGP dla IPv4 i IPv6), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM)
    - obsługę co najmniej 4ech wirtualnych tablic routingu (VRF) dla IPv4/IPv6 (w ramach VRF wymagana obsługa routingu statycznego i dynamicznego)
    - obsługę VXLAN
    - obsługę Policy-Based Routing dla IPv4 i IPv6
    - obsługę protokołu BFD (Bidirectional Forwarding Detection) dla IPv4 i IPv6 dla routingu statycznego oraz dynamicznego – minimum dla protokołów OSPF, IS-IS i BGP
  - obsługa protokołu redundancji bramy VRRP/HSRP lub innego równoważnego
  - tablica routingu (FIB) musi umożliwiać obsługę minimum:
    - 3.000 wpisów dla IPv4
    - 1.500 wpisów dla IPv6

- 1.000 wpisów dla ruchu multicast (IPv4/IPv6)
- przełącznik musi obsługiwać ramki Jumbo (do min. 9100 bajtów)
- mechanizm związane z zapewnieniem ciągłości pracy sieci:
- 802.1w Rapid Spanning Tree
- 802.1s Multi-Instance Spanning Tree
- 802.3ad Link Aggregation Control Protocol
- mechanizmy związane z zapewnieniem jakości usług w sieci:
- obsługa 8 kolejek sprzętowych dla różnego rodzaju ruchu
- obsługa co najmniej jednej kolejki ze statusem strict priority
- klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- możliwość "re-kolorowania" pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP.
- obsługa kolejkowania, ograniczania (rate-limiting), kształtowania (shaping), zarządzania pasmem
- obsługa zaawansowanych mechanizmów aktywnego zarządzania długością kolejki (typu WTD lub podobny) oraz unikania zatorów (typu WRED lub podobny),
- kontrola sztormów dla ruchu boradcast i multicast
- możliwość określenia ograniczeń ruchu (rate limiting) per użytkownik dla przełączników
- mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
- min. 5 poziomów dostępu administracyjnego poprzez konsolę
- autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
- obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- obsługa funkcji Voice VLAN umożliwiającej segmentację ruchu głosowego od ruchu użytkowników
- możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
- możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
- możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2
- możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec-128) line-rate dla wszystkich portów 1/10GE przełącznika (dla połączeń przełącznik-przełącznik)
- obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6 (na poziomie portu, VLANu, interfejsu L3)
- obsługa mechanizmu uRPF
- obsługa mechanizmów bezpieczeństwa Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
- obsługa mechanizmów bezpieczeństwa dla ruchu IPv6 na brzegu sieci – DHCPv6 Guard, IPv6 Snooping, IPv6 Router Advertisement (RA) Guard, IPv6 Source Guard
- możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1X) do serwerów RADIUS lub TACACS+

- funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym
- mechanizmy związane z zarządzaniem urządzeniem:
- możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 10.000 (wymagane wsparcie sprzętowe)
- przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN i RSPAN) – wymagana jest obsługa min. 8 sesji SPAN/RSPAN na przełączniku (bi-directional)
- funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
- obsługa protokołu LLDP i LLD-MED
- 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 10 plików konfiguracyjnych i 2 wersji oprogramowania
- możliwość cofnięcia ostatnich zmian konfiguracyjnych (config rollback)
- funkcjonalność umożliwiająca tworzenie makr konfiguracyjnych aplikowanych do portu przy wykryciu dołączenie urządzenia określonego typu
- urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
- urządzenie musi posiadać wbudowany analizator pakietów
- obsługa standardowego interfejsu programistycznego NetCONF i modeli YANG
- obsługa telemetrii strumieniowej opartej o modele YANG
- dedykowany port Ethernet do zarządzania urządzeniem
- obudowa przystosowana do montażu w szafie 19”, wysokość 1U
- możliwość rozbudowy o zarządzanie za pomocą znajdującego się w ofercie komercyjnej kontrolera SDN, umożliwiającego budowę na bazie przełączników fabryki sieciowej (network fabric) zapewniającej:
- jednolitą, zautomatyzowaną i pełną obsługę (uruchomienie, konfigurację, utrzymanie) sieci przewodowej i bezprzewodowej
- zarządzanie za pomocą polityk opartych o tożsamość użytkownika, nie jego adres czy przynależność do VLAN
- mikrosegmentację opartą o mechanizmy L3
- analitykę umożliwiającą wgląd w zachowanie użytkowników i aplikacji, monitorowanie anomalii i wykrywanie zagrożeń
- mobilność użytkowników w ramach fabryki bez zmiany adresu
- umożliwienie zarządzania za pomocą kontrolera nie może wymagać modyfikacji sprzętowej przełączników czy zmiany topologii sieci
- zestaw udokumentowanych narzędzi pozwalających na kontrolę pochodzenia przełączników i działającego na nich oprogramowania oraz wykluczenie możliwości ich modyfikacji podczas procesów produkcyjnych lub logistycznych (zgodnie z ideą Trustworthy Systems), obejmujący co najmniej:

- podpisywanie cyfrowe i weryfikacja podpisu wszystkich komponentów programowych przełącznika (BIOS, firmware itp.)
- bezpieczne uruchamianie (secure boot), zapewniające sprzętową weryfikację sekwencji startowej i uniemożliwiając uruchomienie nielegalnie zmodyfikowanego oprogramowania
- wyposażenie przełączników w bezpieczne, odporne na manipulacje układy kryptograficzne, gwarantujące uwierzytelnienie oryginalności sprzętu

3. Urządzenia odpowiedzialne za dołączanie urządzeń końcowych zapewniające jednocześnie bezpieczeństwo sieci (C9500-32QC-A).

Przełącznik agregacyjny LAN (np. Cisco Catalyst 9500-32QC-A)

- wszystkie porty Ethernet muszą być dostępne od przodu urządzenia
- wyposażony w:
  - minimum 32 porty 40GBase-X QSFP+ i co najmniej 16 portów 100GBase-X QSFP+ (dopuszczalne zamienne wykorzystanie portów)
  - redundantne i wymienne moduły wentylatorów
  - redundantne, wymienne zasilacze prądu zmiennego AC
- skalowalność:
  - min. 1.000 sieci VLAN, interfejsów SVI,
  - min. 60.000 adresów MAC
  - sprzętowa dla QoS i ACL - minimum 10.000 wpisów sprzętowych
- wydajność:
  - przepustowość nie mniejsza niż 3,2Tb/s
  - szybkość przełączania/routingu minimum 900Mp/s
- urządzenia muszą zapewniać łączenie co najmniej dwóch urządzeń w klaster widoczny jako jedno urządzenie z perspektywy protokołów sieciowych, routingu z obsługą ISSU
- przełączanie w warstwie 2 i 3
  - obsługa VLAN 802.1Q i trunk na wszystkich portach
  - obsługa routingu statycznego i dynamicznego (RIPv2, RIPng, OSPF v2/v3, IS-IS, BGP dla IPv4 i IPv6), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM)
  - obsługę co najmniej 20tu wirtualnych tablic routingu (VRF) dla IPv4/IPv6 (w ramach VRF wymagana obsługa routingu statycznego i dynamicznego)
  - obsługa Policy-Based Routing dla IPv4 i IPv6
  - obsługa protokołu BFD (Bidirectional Forwarding Detection) dla IPv4 i IPv6 dla routingu statycznego oraz dynamicznego – minimum dla protokołów OSPF, IS-IS i BGP
  - obsługa protokołu redundancji bramy VRRP/HSRP lub innego równoważnego
  - tablica routingu (FIB) musi umożliwiać obsługę minimum:
    - 200.000 wpisów dla IPv4
    - 100.000 wpisów dla IPv6
    - 20.000 wpisów dla ruchu multicast (IPv4/IPv6)
  - przełącznik musi obsługiwać ramki Jumbo (do min. 9100 bajtów)
- obsługa MPLS:

- 6PE, 6VPE
- EoMPLS, VPLS, L3VPN, mVPN
- VXLAN

- mechanizm związane z zapewnieniem ciągłości pracy sieci:
  - 802.1w Rapid Spanning Tree
  - 802.1s Multi-Instance Spanning Tree
  - 802.3ad Link Aggregation Control Protocol
- mechanizmy związane z zapewnieniem jakości usług w sieci:
  - obsługa 8 kolejek sprzętowych dla różnego rodzaju ruchu
  - obsługa co najmniej jednej kolejki ze statusem strict priority
  - klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
  - możliwość "re-kolorowania" pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP.
  - obsługa kolejkowania, ograniczania (rate-limiting), kształtowania (shaping), zarządzania pasmem
  - obsługa zaawansowanych mechanizmów aktywnego zarządzania długością kolejki (typu WTD lub podobny) oraz unikania zatorów (typu WRED lub podobny),
  - kontrola sztormów dla ruchu boradcast i multicast
- mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
  - min. 5 poziomów dostępu administracyjnego poprzez konsolę
  - możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2
  - możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec-256) line-rate dla wszystkich portów przełącznika (dla połączeń przełącznik-przełącznik)
  - obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6 (na poziomie portu, VLANu, interfejsu L3)
  - obsługa mechanizmu uRPF
  - obsługa mechanizmów bezpieczeństwa Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
  - obsługa mechanizmów bezpieczeństwa dla ruchu IPv6 na brzegu sieci – DHCPv6 Guard, IPv6 Snooping, IPv6 Router Advertisement (RA) Guard, IPv6 Source Guard
  - możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1X) do serwerów RADIUS lub TACACS+
  - funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym
- mechanizmy związane z zarządzaniem urządzeniem:
  - możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 40.000 (wymagane wsparcie sprzętowe)
  - przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN i RSPAN) – wymagana jest obsługa min. 8 sesji SPAN/RSPAN na przełączniku (bi-directional)

- funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
- obsługa protokołu LLDP i LLD-MED
- 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 10 plików konfiguracyjnych i 2 wersji oprogramowania
- możliwość cofnięcia ostatnich zmian konfiguracyjnych (config rollback)
- funkcjonalność umożliwiająca tworzenie makr konfiguracyjnych aplikowanych do portu przy wykryciu dołączenie urządzenia określonego typu
- urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
- urządzenie musi posiadać wbudowany analizator pakietów
- obsługa standardowego interfejsu programistycznego NetCONF i modeli YANG
- obsługa telemetrii strumieniowej opartej o modele YANG
- dedykowany port Ethernet do zarządzania urządzeniem

- obudowa przystosowana do montażu w szafie 19”
- możliwość rozbudowy o zarządzanie za pomocą znajdującego się w ofercie komercyjnej kontrolera SDN, umożliwiającego budowę na bazie przełączników fabryki sieciowej (network fabric) zapewniającej:
  - jednolitą, zautomatyzowaną i pełną obsługę (uruchomienie, konfigurację, utrzymanie) sieci przewodowej i bezprzewodowej
  - zarządzanie za pomocą polityk opartych o tożsamość użytkownika, nie jego adres czy przynależność do VLAN
  - mikrosegmentację opartą o mechanizmy L3
  - analitykę umożliwiającą wgląd w zachowanie użytkowników i aplikacji, monitorowanie anomalii i wykrywanie zagrożeń
  - mobilność użytkowników w ramach fabryki bez zmiany adresu
  - umożliwienie zarządzania za pomocą kontrolera nie może wymagać modyfikacji sprzętowej przełączników czy zmiany topologii sieci
- możliwość osadzenia na przełącznikach aplikacji działających jako maszyna wirtualna lub w kontenerze – wymagana separacja zasobów od zasobów systemu operacyjnego urządzenia oraz możliwość alokacji zasobów dla aplikacji
- zestaw udokumentowanych narzędzi pozwalających na kontrolę pochodzenia przełączników i działającego na nich oprogramowania oraz wykluczenie możliwości ich modyfikacji podczas procesów produkcyjnych lub logistycznych (zgodnie z ideą Trustworthy Systems), obejmujący co najmniej:
  - podpisywanie cyfrowe i weryfikacja podpisu wszystkich komponentów programowych przełącznika (BIOS, firmware itp.)
  - bezpieczne uruchamianie (secure boot), zapewniające sprzętową weryfikację sekwencji startowej i uniemożliwiając uruchomienie nielegalnie zmodyfikowanego oprogramowania
  - wyposażenie przełączników w bezpieczne, odporne na manipulacje układy kryptograficzne, gwarantujące uwierzytelnienie oryginalności sprzętu

22. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych (C9200-48P-E); 23. Rozbudowa posiadanych urządzeń z punktu 22:; 24. Rozbudowa posiadanych urządzeń z punktu 22; 25. Rozbudowa posiadanych urządzeń z punktu 22:

Wymagania szczegółowe – **(np. Cisco Catalyst 9200-48P-E)**

- minimum 48 portów 100/1000GBase-T z obsługą IEEE 802.3at PoE+ (dostępne co najmniej 1440W mocy dla PoE+ przy pracujących obu zasilaczach)
- slot umożliwiający instalację modułu z portami uplink obsługującego co najmniej:
  - 4 interfejsów 1/10GE SFP+
  - 2 interfejsów 25GE SFP28
  - 2 interfejsów 40GE QSFP
- wydajność:
  - przepustowość nie mniejsza niż 336Gb/s
  - szybkość przełączania/routingu minimum 120Mp/s

26. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych:

Przełączniki dostępowe LAN Cisco Catalyst 3560-CX-8PT-S

- minimum 8 portów 100/1000GBase-T z obsługą IEEE 802.3at PoE+ (dostępne co najmniej 123,2W mocy dla PoE)
- minimum 2 porty 1GBase-T – przełącznik musi posiadać możliwość zasilania z urządzenia agregacyjnego za pośrednictwem PoE+ na tych portach
- wydajność:
  - przepustowość nie mniejsza niż 20Gb/s
  - szybkość przełączania/routingu minimum 12Mp/s
- wszystkie porty Ethernet muszą być dostępne od przodu urządzenia
- skalowalność:
  - min. 1.000 sieci VLAN
  - min. 15.000 adresów MAC
  - sprzętowa dla QoS i ACL - minimum 500 wpisów sprzętowych
- przełączanie w warstwie 2 i 3
  - obsługa VLAN 802.1Q i trunk na wszystkich portach
  - obsługa routingu statycznego (dla IPv4/IPv6 – co najmniej 10 tras) i dynamicznego (OSPF v2 dla IPv4 – co najmniej 10 tras)
  - możliwość rozbudowy funkcjonalności o:
    - obsługa pełnego routingu dynamicznego (OSPF v2/v3, IS-IS, BGP dla IPv4 i IPv6), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM)
    - obsługę Policy-Based Routing dla IPv4 i IPv6

- przełącznik musi obsługiwać ramki Jumbo (do min. 9100 bajtów)

- mechanizm związane z zapewnieniem ciągłości pracy sieci:
- 802.1w Rapid Spanning Tree
- 802.1s Multi-Instance Spanning Tree
- 802.3ad Link Aggregation Control Protocol

- mechanizmy związane z zapewnieniem jakości usług w sieci:
- obsługa 8 kolejek sprzętowych dla różnego rodzaju ruchu
- obsługa co najmniej jednej kolejki ze statusem strict priority
- klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- możliwość "re-kolorowania" pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP.
- obsługa kolejkowania, ograniczania (rate-limiting), zarządzania pasmem
- obsługa zaawansowanych mechanizmów aktywnego zarządzania długością kolejki (typu WTD lub podobny),
- kontrola sztormów dla ruchu boradcast i multicast

- mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
- min. 5 poziomów dostępu administracyjnego poprzez konsolę
- autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
- obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- obsługa funkcji Voice VLAN umożliwiającej segmentację ruchu głosowego od ruchu użytkowników
- możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
- możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
- możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2
- obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6 (na poziomie portu)
- obsługa mechanizmów bezpieczeństwa Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
- obsługa mechanizmów bezpieczeństwa dla ruchu IPv6 na brzegu sieci – DHCPv6 Guard, IPv6 MLD Snooping, IPv6 Router Advertisement (RA) Guard
- możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1X) do serwerów RADIUS lub TACACS+
- funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym

- mechanizmy związane z zarządzaniem urządzeniem:

- możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 10.000 (wymagane wsparcie sprzętowe)
- przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN/RSPAN) – wymagana jest obsługa min. 4 sesji SPAN/RSPAN na przełączniku (bi-directional)
- obsługa protokołu LLDP i LLD-MED
- 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 10 plików konfiguracyjnych i 2 wersji oprogramowania
- funkcjonalność umożliwiająca tworzenie makr konfiguracyjnych aplikowanych do portu przy wykryciu dołączenie urządzenia określonego typu

Routery dostępowe

Wymagania ogólne

- Musi być urządzeniem pełniącym rolę wielousługowego routera modularnego.
- Architektura
  - Musi posiadać zainstalowany wewnętrzny sprzętowy moduł akceleracji szyfrowania.
  - Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora.
  - 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.
  - Sloty urządzenia dla kart sieciowych (o ile dany typ ma je posiadać) muszą mieć możliwość obsadzenia kartami:
    - z przełączanymi portami GE (10/100/1000) z obsługą PoE+ (IEEE 802.3at)
    - z modemem 4G (LTE Advanced)
    - z portami szeregowymi o gęstości co najmniej 4 porty na moduł,
    - z interfejsem ISDN PRI o gęstości 1 portu per moduł, 2 portów per moduł, 4 portów per moduł oraz 8 portów per moduł,
    - umożliwiającymi instalację dysków SSD
  - Sloty urządzenia dla interfejsów głosowych (o ile dany typ ma je posiadać) muszą mieć możliwość obsadzenia kartami:
    - z portami analogowymi FXO, FXS (co najmniej 4 porty na kartę)
    - z portami cyfrowymi E1
  - Slot urządzenia przewidziany pod rozbudowę o moduł z układami DSP (o ile dany typ ma je posiadać) musi mieć możliwość obsadzenia modułem:
    - o gęstości nie mniejszej niż 256 kanałów,
    - pozwalającym na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing),
    - posiadającym wsparcie dla usług wideo.

- Oprogramowanie/funkcjonalności

○ Oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji.

○ Musi posiadać obsługę protokołów routingu IPv4 takich, jak RIPv2, OSPF, BGPv4, OSPF, ISIS, EIGRP, a także routingu statycznego.

○ Musi posiadać obsługę protokołów routingu IPv6 takich, jak RIPng, OSPFv3, BGPv4, ISIS, EIGRP, a także routingu statycznego.

○ Musi posiadać obsługę protokołów routingu multicastowego PIM Sparse oraz PIM SSM, a także oraz routingu statycznego.

○ Protokół BGP musi posiadać obsługę 4 bajtowych ASN.

○ Musi posiadać wsparcie dla funkcjonalności Policy Based Routing.

○ Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF).

○ Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.

○ Musi obsługiwać IPv6 w tym ICMP dla IPv6 oraz protokoły routingu IPv6 takie jak EIGRP, RIP, OSPFv3, IS-IS,

○ 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.

○ Musi posiadać wsparcie dla protokołów WCCP i WCCPv2.

○ Musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 4000 instancji VRF.

○ Musi posiadać obsługę mechanizmu DiffServ.

○ Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.

○ Musi zapewniać obsługę mechanizmów kolejkowania ruchu:

- z obsługą kolejki absolutnego priorytetu,
- ze statyczną alokacją pasma dla typu ruchu,
- WFQ.

○ Musi obsługiwać mechanizm WRED.

○ Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.

○ Musi obsługiwać protokół NTP.

○ Musi obsługiwać DHCP w zakresie Client , Server.

○ Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika).

○ Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+.

○ Musi posiadać obsługę MPLS oraz MPLS TE.

○ Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD) lub odpowiednika.

○ Funkcjonalność BFD (lub odpowiednik) musi posiadać wsparcie dla protokołów BGP, OSPF, IS-IS, EIGRP, routingu statycznego oraz HSRP lub odpowiednika.

○ Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy:

- funkcjonalność 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.

- funkcjonalność musi pozwalać na generowanie akcji takich jak:
- 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.

o Musi posiadać funkcjonalność automatycznej optymalizacji routingu dla połączeń typu multihomed:

- optymalizacji ruchu przychodzącego z wykorzystaniem rozgłaszania informacji BGP do zewnętrznych routerów (BGP external peers),
- optymalizacji ruchu głosowego,
- optymalizacji w oparciu o informację z protokołów warstw wyższych (protokoły i porty UDP/TCP),
- optymalizacji ruchu dla tuneli VPN IPSec/GRE,
- optymalizacji ruchu w oparciu o automatyczne wykrywanie ruchu aplikacyjnego.

o Musi posiadać wsparcie dla Layer-2 Tunneling Protocol Version 3.

o Opcjonalnie funkcjonalności optymalizacji i akceleracji

- funkcję optymalizatora ruchu sieciowego realizującego następujące funkcje:
- kompresja ruchu z wykorzystaniem algorytmu kompresji danych (Lempel-Ziv lub analogicznego),
- zmniejszenie rozmiaru przesyłanych danych poprzez wysyłanie krótkich indeksów numerycznych zamiast powtarzających się bloków danych (Data Redundancy Elimination lub odpowiednik),
- optymalizacja algorytmu TCP (optymalizacja pracy algorytmu okien TCP),
- dopuszcza się, aby funkcja optymalizatora sieciowego realizowana była wydzielonych rdzeniach procesora obsługującego system operacyjny.

o funkcjonalności bezpieczeństwa sieciowego:

- obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast.
- funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES/AES
- algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:
- Elliptic Curve Diffie-Hellman (ECDH),
- Galois Counter Mode Advanced Encryption Standard (GCM-AES) 128/256 bitów,
- Galois Message Authentication Code (GMAC-AES) 128/256 bitów,
- Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2,
- możliwość konfiguracji tuneli IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2). Wsparcie dla IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych, dla ruchu IPv4 oraz IPv6,
- funkcjonalność VPN musi wspierać tworzenie niezależnych VPN (w tym różnego typu: site-2-site, dynamicznych) per VRF,
- technologia umożliwiająca szyfrowanie IPSec ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem z użyciem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547, w tym:
- mechanizm pasywnego IPSec SA, w którym urządzenie akceptuje zaszyfrowany i niezaszyfrowany ruch przychodzący, ale wysyła zawsze ruch zaszyfrowany,

- mechanizm fail-close, w którym urządzenie nie wysyła ruchu, w sytuacji kiedy miałby on pozostać niezaszyfrowany w przypadku kiedy urządzenie jest niezarejestrowane w sieci VPN,
- mechanizm współdzielenia kluczy przez redundantne serwery kluczy,
- mechanizm zmiany podstawowego serwera kluczy (Key Server) w scenariuszu z wysoką dostępnością serwerów kluczy,
- funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall),
- funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall),
- możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym:
  - przesyłu, który jest poddawany inspekcji,
  - przesyłu, który jest odrzucany,
  - przesyłu, który jest przenoszony bez inspekcji,
- ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU,
- możliwość logowania pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU,
- możliwość wymuszenia reguł złożoności haseł tworzonych na urządzeniu,
- w przypadku modułu przełącznika, działającego jako urządzenie dostępowe RADIUS (NAD - Network Access Devices), wsparcie funkcjonalności 802.1x.

- Opcjonalnie funkcjonalności głosowe:
  - funkcjonalność procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia),
  - funkcje pozwalające na automatyzację konfiguracji ustawień QoS (w szczególności dla usług VoIP) w postaci automatycznego tworzenia wzorców konfiguracyjnych na potrzeby implementacji QoS,
  - funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia "tam i z powrotem" (roundtrip, jitter i utraty pakietów),
  - możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych, przy czym brama taka musi mieć możliwość pracy w sposób niezależny lub być sterowana przez system centralny procesowania połączeń.

- Zarządzanie i konfiguracja
  - Musi być zarządzalne za pomocą SNMPv1, SNMPv2, SNMPv3, Telnet, SSH.
  - Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Neftflow/JFlow lub odpowiednika.
  - Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI).
  - 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 powinno 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 dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

- Obudowa

○ Musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.

○ Musi mieć możliwość montażu w szafie 19”.

- Zasilanie

○ Urządzenie musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacz AC).

○ Urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia (w przypadku typów wyposażonych w takie moduły, funkcjonalność musi być uwzględniona).

6. Urządzenia odpowiedzialne za bezpieczeństwo sieci (ISR4321/K9)

Wymagania szczegółowe – router Typ I (np. ISR4321-VSEC/K9)

- Architektura

○ Musi pozwalać na instalację co najmniej:

▪ 2 kart sieciowych z interfejsami

▪ modułu DSP

○ Wydajność na poziomie co najmniej 50 Mbps z możliwością podwojenia (dla kombinacji usług routingu, firewall, IPSEC VPN i QoS)

- Oprogramowanie/funkcjonalności

○ Obsługa grup funkcjonalności podstawowych i bezpieczeństwa sieciowego:

▪ obsługa co najmniej 300 tuneli VPN

○ Możliwość rozbudowy o grupy funkcjonalności optymalizacji i akceleracji oraz głosowe

- Wyposażenie

○ Urządzenie musi być wyposażone w minimum 2 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN. Co najmniej jeden interfejs musi mieć możliwość pracy z gigabitowym portem światłowodowym definiowanym przez wkładkę SFP lub równoważną

○ Zainstalowane karty sieciowe z co najmniej:

▪ 2 portami szeregowymi

▪ 8 portami GE LAN z obsługą PoE+

○ Urządzenie musi być wyposażone w minimum 8GB pamięci Flash

○ Urządzenie musi być wyposażone w minimum 8GB pamięci RAM.

○ Urządzenie musi być wyposażone w port USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.

4. Urządzenia odpowiedzialne za bezpieczeństwo sieci (ISR4461/K9)

Wymagania szczegółowe – router Typ II (np. ISR4461-SEC/K9)

- Architektura
  - Musi pozwalać na instalację co najmniej:
    - 6 kart sieciowych z interfejsami
    - modułu DSP
  - Wydajność na poziomie co najmniej 4 Gbps z możliwością podwojenia (dla kombinacji usług routingu, firewall, IPSEC VPN i QoS)
- Oprogramowanie/funkcjonalności
  - Obsługa grup funkcjonalności podstawowych i bezpieczeństwa sieciowego:
    - obsługa co najmniej 4.000 tuneli VPN
  - Możliwość rozbudowy o grupy funkcjonalności optymalizacji i akceleracji oraz głosowe
- Wyposażenie
  - Urządzenie musi być wyposażone w minimum 2 interfejsy 10 Gigabit Ethernet definiowane przez SFP+ lub równoważne
  - Urządzenie musi być wyposażone w minimum 4 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN. Interfejsy muszą mieć możliwość pracy z gigabitowym portem światłowodowym definiowanym przez wkładki SFP lub równoważne
  - Urządzenie musi być wyposażone w minimum 16GB pamięci Flash
  - Urządzenie musi być wyposażone w minimum 16GB pamięci RAM.
  - Urządzenie musi być wyposażone w port USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.

5. Urządzenia odpowiedzialne za bezpieczeństwo sieci (FPR4110-ASA-K9)

Urządzenia bezpieczeństwa brzegowego FW (np. Cisco FPR4110-ASA)

- architektura urządzenia
  - urządzenie o konstrukcji modularnej pełniące funkcje ściany ogniowej (firewall) typu Statefull inspection i Application Inspection
  - urządzenie musi być dedykowaną platformą sprzętową, nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia
  - urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia
- urządzenie wyposażone w co najmniej:
  - 8 interfejsów 1/10Gigabit Ethernet definiowanych przez moduły SFP+
  - możliwość rozbudowy o co najmniej 8 interfejsów 1/10Gbase-X definiowanych przez moduły SFP+ lub co najmniej 2 interfejsy 40GBase-X definiowane przez moduły QSFP+
  - dedykowany interfejs Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania

- obsługa znakowania VLAN 802.1q na interfejsach fizycznych, nie mniej niż 1.000 podsieci sumarycznie
- wyposażone w pamięć Flash oraz pamięć RAM dostosowaną do wymagań wydajnościowych
- redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V (niedopuszczalne rozwiązania zewnętrzne)

- obudowa
  - metalowa obudowa
  - możliwość instalacji w szafie typu rack 19".
  - dostarczone z elementami montażowymi dla szafy rack 19"
  - przystosowane do pracy w zakresie temperatur 0-40 stopni Celsjusza
- wydajność urządzenia
  - przepustowość firewall dla ruchu wieloprotokołowego nie mniej niż 15 Gbps
  - obsługa dla funkcjonalności firewall co najmniej 8.000.000 jednoczesnych sesji/połączeń z prędkością zestawiania co najmniej 100.000 połączeń na sekundę
  - sprzętowy układ odciążający procesor urządzenia przy wykonywaniu operacji szyfrowania algorytmami DES/3DES/AES i oferować wydajność szyfrowania nie mniejszą niż 5 Gbps
  - jednoczesna obsługa co najmniej 1.000 tuneli VPN wykorzystujących IPsec i SSL
  - funkcja ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji

  - możliwość konfiguracji wirtualnych firewalli. Wymagana jest docelowa obsługa co najmniej 100 wirtualnych firewalli, w ofercie należy przewidzieć obsługę 10 wirtualnych firewalli
  - możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z oferowanym modułem autoryzacji użytkowników
  - możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos
  - urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
  - możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI
  - możliwość grupowanie VLANów w transparentnym trybie pracy firewalla. Wymagana jest możliwość zdefiniowania co najmniej 8 takich grup po 4 VLANy. Każda tak zdefiniowana grupa musi umożliwiać realizację odrębnych list kontroli dostępu
  - zbieranie informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL)
  - możliwość konfiguracji globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie
  - możliwość konfiguracją reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu
- listy kontroli dostępu muszą umożliwiać definiowanie reguł w oparciu co najmniej o następujące podstawowe parametry:
- źródłowy i docelowy adres IPv4
- źródłowy i docelowy adres IPv6
- źródłowy i docelowy numer portu UD
- źródłowy i docelowy numer portu TC
- nazwy domenowej hosta źródłowego lub doceloweg
- nazwa użytkownika w module autoryzacji użytkownikó

- nazwa grupy w module autoryzacji użytkowników
- czas

o urządzenie nie może posiadać żadnych programowych ograniczeń na liczbę reguł dostępu jakie mogą być równocześnie wykorzystywane

o obsługa funkcjonalności Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego

- translacja adresów (NAT) dla ruchu multicastowego
- translacja adresów sieciowych NAT i translowania adresów i portów PAT w co najmniej następujących wariantach: z IPv6 na IPv6, z IPv4 na IPv4, z IPv4 na IPv6
- więcej niż 65535 dynamicznych translacji PAT do pojedynczego zewnętrznego adresu IP
- możliwość konfiguracji czasu ważności translacji PAT
- urządzenie wykonując dynamiczne translacje PAT do puli zewnętrznych adresów IP, musi równomiernie korzystać ze wszystkich zdefiniowanych w puli adresów

o mechanizmy inspekcji aplikacyjnej i kontroli co najmniej następujących usług:

- Hypertext Transfer Protocol (HTTP),
- File Transfer Protocol (FTP),
- Extended Simple Mail Transfer Protocol (ESMTP),
- Domain Name System (DNS),
- Simple Network Management Protocol v1/2/3 (SNMP),
- Internet Control Message Protocol (ICMP),
- inspekcji protokołów dla ruchu głos/wideo – H.323 (włącznie z H.239), SIP, RTSP

o zaawansowana normalizacja ruchu TCP w zakresie kontroli co najmniej:

- poprawności pola TCP ACK (invalid-ack)
- poprawności sekwencjonowania segmentów TCP (seq-past-window)
- poprawności ustanawiania sesji TCP z danymi (synack-data)
- limitowania czasu oczekiwania na segmenty nie w kolejności
- poprawności pola MSS (exceed-mss).
- poprawności pola długości TCP
- poprawności skali okna segmentów TCP non-SYN
- poprawności wielkości okna TCP

o zaawansowane badanie stanu każdej sesji TCP w zakresie co najmniej:

- sprawdzania opcji TCP, usuwania opcji TCP i odrzucania segmentów z opcjami TCP
- poprawności pola TCP ACK
- poprawności sekwencjonowania segmentów TCP (seq-past-window) ze wsparciem mechanizmów akceleracji sieci WAN wprowadzających przesunięcie numerów sekwencyjnych TCP
- weryfikacji sumy kontrolnej segmentu TCP
- weryfikacji pola TCP SACK ALLOW
- weryfikacji wielkości okna TCP
- usuwania flagi URG
- usuwania segmentów przekraczających maksymalny rozmiar (MSS)
- usuwania segmentów z flagą SYN i z flagami SYN/ACK, jeśli zawierają one dane

o możliwość ograniczenia maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów

o możliwość ograniczenia maksymalnej liczby równoczesnych półotwartych połączeń TCP zestawionych do hosta lub do grupy hostów

- możliwość zresetowania otwartego połączenia TCP, jeśli przez określony okres czasu przez połączenie nie przesyłano żadnych danych
- możliwość inspekcji ruchu IPv4 z wykorzystaniem co najmniej nagłówków: End of Options List, No Operation, Router Alarm.
- możliwość inspekcji ruchu IPv6 z wykorzystaniem co najmniej nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload.
- jeśli pakiet IPv4/IPv6 został pofragmentowany, urządzenie musi odtworzyć oryginalny pakiet kontrolując przy tym kolejność fragmentów i ich integralność

- możliwość skonfigurowania maksymalnej dopuszczalnej liczby równocześnie odtwarzanych z fragmentów pakietów IPv4/IPv6 per każdy interfejs urządzenia realizujący usługę firewalla
- możliwość równoczesnego odtwarzania co najmniej 10.000 pofragmentowanych pakietów
- możliwość skonfigurowania maksymalnej dopuszczalnej liczby fragmentów w ramach jednego odtwarzanego pakietu
- możliwość skonfigurowania maksymalnego dopuszczalnego okresu czasu, w którym musi otrzymać wszystkie fragmenty niezbędne do odtworzenia pakietu

- możliwość inspekcji ruchu HTTP w zakresie:

- zgodności z formalną definicją protokołu
- ukrywania nagłówka Server w odpowiedzi http
- filtrowania dopuszczalnych metod http
- filtrowania dopuszczalnych typów MIME
- filtrowania dopuszczalnych adresów URL

- możliwość inspekcji ruchu SMTP w zakresie:

- zgodności z formalną definicją protokołu ESMTP
- ukrywania wiadomości powitalnej serwera
- filtrowania długości wydawanych komend
- filtrowania listy odbiorców dłuższej niż określona liczba
- filtrowania długości adresu nadawcy
- filtrowania długości pola MIME
- filtrowania dopuszczalnych typów MIME

- możliwość inspekcji ruchu DNS w zakresie:

- zgodności z formalną definicją protokołu DNS
- filtrowania długości wiadomości
- filtrowania po typie zapytania
- randomizowania numeru identyfikacyjnego wiadomości
- weryfikacji zgodności numeru indentyfikacyjnego zapytania i odpowiedzi
- blokowania innych odpowiedzi niż pierwsza (ochrona przed atakiem dns spoofing i dns poisoning)

- wsparcie stosu protokołów IPv6 w tym co najmniej:

- list kontroli dostępu dla IPv6
- możliwości filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload
- inspekcji protokołu IPv6, pracując w trybie transparentnym
- adresacji IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover)

- realizacji połączeń VPN typu site-to-site opartych o co najmniej IKEv1 z użyciem protokołu IPv6
- możliwość współpracy z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik

- funkcja koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i Client VPN)
  - obsługa protokołów IKEv1 i IKEv2
  - obsługa IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode
  - obsługa funkcji skrótu SHA-2 o długości 256, 384 i 512 bitów.
  - obsługa szyfrowania protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM) i Galois Message Authentication Code (GMAC).
  - obsługa protokołu Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19,20 i 21.
  - obsługa protokołu DSA w przestrzeni krzywych eliptycznych (ECDSA)
  - obsługa RADIUS CoA (RFC3576 i późniejsze)
  - obsługa proxy dla protokołu SCEP i możliwość zautomatyzowanego procesu pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN
  - wsparcie użytkowników korzystających z trybu klienta VPN (IPSec oraz SSL) w zakresie obsługi haseł w module autoryzacji użytkowników, bezpośrednio lub poprzez oprogramowanie pośredniczące, co najmniej dla obsługi sytuacji wygaśnięcia terminu ważności hasła w module autoryzacji użytkowników, umożliwiając zmianę przeterminowanego hasła
  - Zamawiający posiada licencje VPN Cisco Anyconnect. W przypadku oferowania rozwiązania nie obsługującego tych licencji wymagane jest dostarczenie licencji umożliwiających terminowanie co najmniej 1.000 jednoczesnych sesji VPN (IPSec/SSL) oraz zapewnienie komercyjnego klienta VPN co najmniej dla systemów Windows, MacOS, Linux, Android i iOS
- mechanizmy redundancji w tym co najmniej
  - możliwość konfiguracji urządzeń w układ zapasowy (failover / klaster) działający w trybie wysokiej dostępności (HA) active/standby i active/active
  - synchronizacja tablicy połączeń pomiędzy węzłami pracującymi w trybie wysokiej dostępności HA
  - możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia
  - funkcjonalność stateful failover dla ruchu VPN
- obsługa routingu L3:
  - obsługa routingu statycznego i dynamicznego (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).
  - obsługa ruchu multicast w zakresie wsparcia protokołu PIM, IGMP i definiowania list kontroli dostępu dla ruchu multicast
  - możliwość pominięcia kontroli stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu
- obsługa serwera DHCP i przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay) dla IPv4 i IPv6
- obsługa ramek Ethernet typu Jumbo (o rozmiarze co najmniej 9100 bajtów)
- obsługa protokołu WCCPv2
- możliwość rozbudowy o funkcjonalność IPS

- możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. Wymagane jest by moduł tworzył kontekst z wykorzystaniem co najmniej poniższych parametrów
  - wiedza o użytkownikach – uwierzytelenienie
  - wiedza o urządzeniach – pasywne skanowanie ruchu
  - wiedza o urządzeniach mobilnych
  - wiedza o aplikacjach wykorzystywanych po stronie klienta
  - wiedza o podatnościach
  - wiedza o bieżących zagrożeniach
  - baza danych URL
- możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez urządzenie)
- możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu)
- możliwość wykrywania i uniemożliwiać szeroką gamę zagrożeń w tym co najmniej
  - złośliwe oprogramowanie,
  - skanowanie sieci,
  - ataki na usługę VoIP,
  - próby przepełnienia bufora,
  - ataki na aplikacje P2P,
  - zagrożenia dnia zerowego, itp.)
- możliwość wykrywania modyfikacji znanych ataków (sygnatury) jak i te nowo powstałe, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)
- co najmniej poniższe sposoby wykrywania zagrożeń
  - sygnatury ataków opartych na exploitach,
  - reguły oparte na zagrożeniach,
  - mechanizm wykrywania anomalii w protokołach
  - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
- możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
- mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives).
- możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
- wiele możliwości reakcji na zdarzenia, co najmniej:
  - tylko monitorowanie,
  - blokowanie ruchu zawierającego zagrożenia,
  - zastąpienie zawartości pakietów
  - zapisywanie pakietów
- możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
- możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności – co najmniej zbierana
  - informacja o systemach operacyjnych,

- informacja o serwisach,
- informacja o otwartych portach, aplikacjach
- informacja o zagrożeniach

○ możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych

○ możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.

○ możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji

○ możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego

○ mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne

○ możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie

○ zarządzany tylko poprzez moduł zarzadzania bezpieczeństwem brzegowym za pomocą szyfrowanego połączenia

○ obsługa reguł Snort

○ możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS

○ mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. indication of compromise)

○ mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa

○ możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewalla dla uzyskania pełnej widoczności ruchu – w szczególności musi posiadać możliwość pracy w trybie failover firewalla oraz w trybie klastrowania

- zarządzanie i konfiguracja

○ zarządzanie przez linię poleceń (ang. Command Line Interface), dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2

○ zarządzanie przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji

○ zarządzanie programowo przez interfejs API dostępny przy pomocy protokołu https

○ zarządzanie przez protokół SNMPv1/2/3 ze wsparciem dla integralności i poufności komunikacji

○ zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.

○ obsługa protokołu NTP

○ współpraca z serwerami CA

○ urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.

○ urządzenie musi umożliwiać konfigurację maksymalnej równoczesnej liczby sesji zdalnego zarządzania.

○ urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.

- urządzenie musi umożliwiać wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.
- urządzenie musi mieć możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG. Wymagane jest wsparcie szyfrowanej transmisji wiadomości SYSLOG przy pomocy SSL/TLS.
- urządzenie musi wspierać eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow v9 (RFC 3954)
- urządzenie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu RADIUS
- urządzenie musi umożliwiać zrzucenie obecnego stanu programu (coredump) dla potrzeb diagnostycznych
- wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łącznością w sieciach IP
- uwierzytelnienie i konfigurację poziomu dostępu administratora w oparciu o role (ang. Role Based Access Control) z wykorzystaniem bazy danych użytkowników zdefiniowanej lokalnie na urządzeniu lub na zewnętrznych serwerach dostępnych przy pomocy protokołu RADIUS

7. Urządzenia odpowiedzialne za bezpieczeństwo sieci (FPR1010-NGFW-K9)

Urządzenia bezpieczeństwa brzegowego NGFW (np. Cisco FPR1010-NGFW)

- Ściana ogniowa (firewall) typu NGFW
  - wydajność na poziomie co najmniej 600 Mbps
  - co najmniej 8 interfejsów GE 100/1000 (RJ45)
  - obsługa co najmniej 100.000 jednoczesnych połączeń zestawianych z szybkością co najmniej 5.000 na sekundę
  - wydajność szyfrowania IPSec na poziomie co najmniej 200 Mbps
  - obsługa deszyfracji SSL/TLS z wydajnością co najmniej 100Mbps
- Realizowany jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania)
- Funkcja ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji (NGFW):
  - możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (tzw. Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory
  - możliwość uwierzytelnienia użytkowników z wykorzystaniem LDAP, NTLM oraz Kerberos
  - bez ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
  - możliwość pracy jako transparentna ściana ogniowa warstwy drugiej modelu ISO OSI
  - obsługa protokołu NTP
  - współpraca z serwerami CA
  - obsługa funkcjonalności Network Address Translation (NAT oraz PAT) - zarówno dla ruchu wchodzącego, jak i wychodzącego
  - obsługa translacji adresów (NAT) dla ruchu multicast

- możliwość konfiguracji reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu
- mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
  - Hypertext Transfer Protocol (HTTP),
  - File Transfer Protocol (FTP),
  - Simple Mail Transfer Protocol (SMTP),
  - Domain Name System (DNS),
  - Simple Network Management Protocol v 1/2/3 (SNMP),
  - Internet Control Message Protocol (ICMP),
  - SQL*Net,
- współpraca z serwerami autoryzacji w zakresie przypisania polityk dostępowych z granulacją per użytkownik
- obsługa routingu statycznego i dynamicznego (min. dla protokołów RIP, OSPF i BGP)
- możliwość zbierania informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL)
- możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System musi tworzyć konteksty z wykorzystaniem poniższych parametrów:
  - wiedza o użytkownikach - uwierzytelnienie
  - wiedza o urządzeniach - pasywne skanowanie ruchu
  - wiedza o aplikacjach wykorzystywanych po stronie klienta
  - wiedza o podatnościach
  - wiedza o bieżących zagrożeniach
- funkcjonalności automatycznego wykrywania i klasyfikacji aplikacji:
  - możliwość klasyfikacji ruchu i wykrywania 3.000 aplikacji sieciowych
  - możliwość tworzenia profili użytkowników korzystających ze wskazanych aplikacji z dokładnością do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług
  - możliwość wykorzystania informacji geolokacyjnych dotyczących użytkownika lub aplikacji
  - współpraca z otwartym (udokumentowanym i dostępnym dla użytkowników) systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach
- Zarządzanie
  - obsługa eksportu zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub równoważnego
  - możliwość eksportu aktualnego stanu (tzw. coredump) dla potrzeb diagnostycznych
  - kontrola dostępu administracyjnego za pomocą protokołu TACACS+
  - narzędzia umożliwiające śledzenie ścieżki pakietu przez urządzenie
- Możliwość rozbudowy o moduł NGIPS:
  - Możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
  - Możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu)

- Możliwość wykrywania i eliminowania szerokiej gamy zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługę VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, itp.)
- Możliwość wykrywania modyfikacji znanych ataków, jak i tych nowo powstałych, które nie zostały jeszcze dogłębnie opisane
- Zapewnienie co najmniej następujących sposobów wykrywania zagrożeń:
  - sygnatury ataków opartych na exploitach,
  - reguły oparte na zagrożeniach,
  - mechanizm wykrywania anomalii w protokołach
  - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
- Możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego, włącznie z możliwością sprawdzania zawartości pakietu
- Mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives)
- Możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
- Zróżnicowane możliwości reakcji na zdarzenia, takich jak monitorowanie, blokowanie ruchu zawierającego zagrożenia, zastępowanie zawartość pakietów
- możliwość pasywnego zbierania informacji o:
  - urządzeniach sieciowych oraz ich aktywności (systemy operacyjne, serwisy, otwarte porty, aplikacje oraz zagrożenia) w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności
  - przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych
  - detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
- Możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS - w tym celu stosuje odpowiedni mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
- Mechanizm bezpiecznej aktualizacji sygnatur - zestawy sygnatur/reguł pobierane są z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
- Możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
- Obsługa reguł Snort
- Możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
- Mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (tzw. Indication of Compromise)
- Mechanizmy automatyzacji w zakresie dostrojenia polityk bezpieczeństwa
- Narzędzia umożliwiające śledzenie ścieżki pakietu przez urządzenie
- Realizowany jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania)
- Rozwiązanie musi być dojrzałym, uznanym na rynku – jako potwierdzenie tej pozycji uznane będzie jego uwzględnienie w zestawieniach Gartner Magic Quadrant for Intrusion Detection and Prevention Systems w ostatnich 3 latach

- Możliwość rozbudowy o moduł ochrony przed malware

- sprawdzanie reputacji plików w systemie globalnym
- sprawdzanie plików w sandbox (realizowanym lokalnie lub w chmurze)
- zapewnia wykrywanie ataków typu Zero-Day
- narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych później jako oprogramowanie złośliwe (analiza retrospektywna ze śledzeniem trajektorii plików)

- Możliwość rozbudowy o moduł filtracji URL
  - obsługa co najmniej 70 kategorii stron
  - moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
  - Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 250 milionów rekordów URL
  - mechanizmy filtrowania w oparciu o reputację domeny
  - obsługa białych i czarnych list URL

Bramki głosowe

Wymagania ogólne

- Urządzenie musi pełnić rolę adaptera przeznaczonego do dostosowania analogowych aparatów telefonicznych oraz transmisji faksowej do pracy w sieciach IP.
- Każdy z portów FXS musi mieć przyporządkowaną linię abonencką (numer telefoniczny).
- Urządzenie musi posiadać co najmniej jeden port Ethernet 10/100 BASE-T do dołączenia do sieci LAN.
- Urządzenie musi wspierać kodeki audio co najmniej określone przez standardy G.711u, G.711a, G.729a, G.729ab, G.726. Musi obsługiwać przekazywanie DTMF zgodnie z RFC 2833.
- Urządzenie musi wspierać mechanizmy transmisji faksowej w sieciach IP typu T38 fax relay oraz Fax pass-through.
- Urządzenie musi wspierać faksy grupy 3 dla obu trybów T38 fax relay oraz Fax pass-through.
- Urządzenie musi realizować funkcje likwidacji echa (echo cancellation).
- Urządzenie musi wspierać sygnalizację SIP.
- Urządzenie musi wspierać szyfrowanie sRTP oraz TLS. Musi wspierać TLS w wersji 1.1 oraz 1.2.
- Urządzenie musi zapewniać wsparcie dla protokołów sieciowych TFTP, DHCP, SSH. Musi wspierać zaszyfrowane pliki konfiguracyjne pobierane z TFTP.
- Urządzenie musi wspierać funkcjonalność wykrywania ciszy (Voice Activity Detection) i niewysyłaniu pakietów głosowych IP w czasie jej trwania.
- Urządzenie musi wspierać funkcjonalność generowania szumu (Comfort Noise Generation) podczas rozmowy w czasie trwania ciszy.
- Urządzenie musi wspierać konfigurację VLAN zgodnie z IEEE 802.1Q.
- Urządzenie musi być zarządzane centralnie poprzez posiadany system komunikacyjny Zamawiającego (Cisco Communications Manager 11.5 oraz wersje wyższe) w zakresie co najmniej:
  - Pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego
  - Obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne Zamawiającego

- Możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki)
- Możliwości zdalnego restartu urządzenia lub grupy urządzeń
- Możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego
- Centralnego wyłączenia funkcji w zakresie interfejsu WWW przeznaczonego do podglądu parametrów pracy oraz trwających połączeń.

27. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych (VG310)

Wymagania szczegółowe – bramka głosowa Typ I **(np. Cisco VG310)**

- Co najmniej 24 porty FXS
- Moduły DSP o gęstości co najmniej 64 kanały
- Obudowa przystosowana do montażu w szafie rack 19”
- Zasilacz 230V AC

28. Urządzenia odpowiedzialne za dołączenie urządzeń końcowych (VG204XM):

Wymagania szczegółowe – bramka głosowa Typ II **(np. Cisco VG204XM)**

- Co najmniej 4 porty FXS
- Moduły DSP o gęstości co najmniej 4 kanały
- Obudowa typu desktop
- Zasilacz 230V AC

29. Platforma serwerowa z przeznaczeniem dla Unified Communication (Mostek wideokonferencyjny); 30. Rozbudowa posiadanych urządzeń oraz pozycji 29.

Mostek wideo (np. Cisco CMS 1000 M5)

- Rozbudowa posiadanego systemu komunikacji zintegrowanej opartego o rozwiązanie Cisco Unified Communications Manager – dostarczane rozwiązanie musi zapewniać udokumentowaną kompatybilność z posiadanym rozwiązaniem
- Wymagana jest dostawa platformy sprzętowej umożliwiającej uzyskanie opisanej funkcjonalności na bazie posiadanych licencji typu Personal Multiparty i Shared Multiparty lub dostarczenie rozwiązania zapewniającego uzyskanie opisanych funkcjonalności we współpracy z posiadanym systemem dla co najmniej 96 portów wideo HD (720p30)

- Mostek musi umożliwiać realizację wirtualnych spotkań z wykorzystaniem kanałów audio, wideo i web.
- Możliwość podłączenia do wirtualnego spotkania za pomocą:
  - dedykowanej aplikacji
  - przeglądarki implementującej WebRTC
  - terminali wideo
  - klienta programowego do standardowych połączeń audio i wideo na bazie SIP,
  - klienta programowego Microsoft Skype for Business
  - połączenia telefonicznego
- System konferencji musi być wspierany na platformach typu PC, laptop, tablet, smartfon (Windows, OS X, iOS oraz przeglądarki WebRTC).
- Dostarczona platforma musi pozwalać na obsługę co najmniej (alternatywnie):
  - 48 połączeń FHD (1080p30)
  - 24 połączeń HD (720p30)
  - 2000 połączeń audio
- Dostarczona platforma musi pozwalać na wykorzystanie zasobów dla jednej lub wielu konferencji.
- Mechanizmy optymalizacji przepustowości dla lokalizacji z niską przepustowością łącza.
- System konferencji musi wspierać poniższe standardy:
  - Wideo:
    - H.263, H.263+, H.263++
    - H.264 AVC (Baseline, High Profile)
    - H.264 SVC
    - WebM, VP8
    - Microsoft RTV
    - HTML5/WebRTC
    - SIP,
    - H.323,
    - TIP
  - Audio:
    - AAC-LD
    - Speex
    - Opus
    - G.722, G.722.1, G.722.1c,
    - G.728,
    - G.729a,
    - G.711a/u
- Musi obsługiwać rozdzielczość transmisji strumienia wideo co najmniej 1080p dla 60 klatek na sekundę. Musi wspierać przepustowość 6Mbit/s dla połączenia wideo.
- Musi obsługiwać rozdzielczość transmisji prezentacji co najmniej 1080p dla 30 klatek na sekundę.
- Musi obsługiwać układy wideokonferencji dla uczestników konferencji ze strony standardowych terminali SIP:

- układ wyświetlania tylko osoby mówiącej,
- układ wyświetlania osoby mówiącej oraz pozostałych min. 3 stron w dolnym pasku ekranu,
- układ matrycowy typu NxN dla co najmniej 25 stron,
- układ matrycowy z wyróżnieniem osoby mówiącej typu OneplusN dla co najmniej 9 stron.

- Musi zapewniać współpracę z systemem Microsoft Lync oraz Microsoft Skype for Business w zakresie:
  - dołączenia użytkowników Skype for Business do konferencji z obsługą kanałów audio, wideo i wymiany prezentacji,
  - wykonania automatycznej kaskady z serwerem konferencji Skype for Business, w celu zapewnienia układu ekranu typu „Gallery View" dla uczestników Skype oraz klasycznych układów wideokonferencji dla uczestników konferencji ze strony standardowych terminali SIP.
  - konwersji i dopasowania protokołów dla potrzeb dwukierunkowej wymiany prezentacji standardowego protokołu BFCP oraz RDP Microsoft stosowanego w Skype for Business,
  - planowania spotkań w środowisku Skype for Business.
- Musi posiadać funkcje w zakresie zarządzania:
  - Język skryptowy na potrzeby konfiguracji,
  - REST API w celu monitorowania i diagnostyki,
  - Strumieniowanie rekordów CDR na potrzeby audytu,
  - Syslog na potrzeby diagnostyki,
  - SNMP,
  - Funkcje archiwizacji i odtwarzania konfiguracji systemu,
- Musi wspierać mechanizmy w zakresie bezpieczeństwa:
  - Szyfrowanie połączeń Secure Real-Time Transport Protocol z wykorzystaniem AES,
  - Szyfrowanie połączeń sygnalizacyjnych z wykorzystaniem TLS/SSL,
  - Wsparcie dla rozszerzeń DNSSEC,
  - Obsługa kodów bezpieczeństwa/PIN dla połączeń do spotkań,
  - Informacje o połączeniu i szyfrowaniu na ekranie połączenia,
  - Informacja o udziale uczestników audio w konferencji wideo na ekranie połączenia.
- Musi umożliwiać obsługę wielu równoczesnych konferencji współdzielonych, tzn. bez przypisanego gospodarza spotkania.
- Musi współpracować z pozostałymi elementami systemu komunikacyjnego zapewniając kierowanie połączeń audio oraz wideo w oparciu o zdefiniowany plan numeracyjny oraz schemat SIP URI.
- Musi pozwalać na dopasowanie widoku ekranu powitalnego konferencji, np. dodanie graficznego logo organizacji, a także zapowiedzi głosowych i komunikatów podczas prowadzenia spotkań do wymagań Zamawiającego.
- Musi umożliwiać klastrowanie z posiadanym mostkiem Cisco CMS 1000 – wymagane jest dostarczenie wszelkich licencji i akcesoriów niezbędnych do utworzenia klastra.
- Musi posiadać możliwość rozbudowy w przyszłości o funkcjonalność nagrywania spotkań wideo wg poniższych wskazań:
  - Nagrywanie na żądanie oraz nagrywanie zaplanowane, jako opcja zaznaczona w systemie planowania spotkań wideo.
  - Musi umożliwiać nagrywanie co najmniej 10 jednoczesnych spotkań wideo.
  - Nagrywanie spotkań musi być realizowane w jakości co najmniej 1080p30.

- Musi umożliwiać nagrywanie głównego strumienia wideo oraz skomponowanej w strumieniu wideo prezentacji współdzielonej w ramach spotkania wideo. Nagrywane spotkanie oznacza 1 sesję HD złożoną ze strumienia wideo 1080p30 zgodnie z kodekiem H.264 AVC.
- Musi współpracować z opcjonalnym systemem dystrybucji mediów w zakresie udostępniania nagrywanych spotkań wideo do dalszej dystrybucji.
- System musi udostępniać otwarte API do integracji z systemami zewnętrznymi. Należy dostarczyć interfejs API.
- Z uwagi na wymaganą stabilność, niezawodność i zgodność rozwiązania system musi posiadać udokumentowaną współpracę z całym systemem komunikacyjnym, z komponentami z którymi współpracuje, w tym co najmniej z systemem przetwarzania połączeń oraz z systemem planowania spotkań wideo.
- Musi współpracować z zewnętrznymi zasobami dyskowymi w celu zapisywania oraz przechowywania nagrań ze spotkań wideo.
- Musi zapisywać nagrania ze spotkań wideo w formacie umożliwiającym dalsze przetwarzanie nagranego materiału.
- Wymagany format zapisywanych nagrań co najmniej format MP4.

31. System rejestracji połączeń głosowych.

Moduł rejestracji połączeń (np. Zoom Int.)

Wykonawca dostarczy system nagrywania rozmów telefonicznych współpracujący z systemem telefonii VoIP opartym na urządzeniach firmy Cisco (Cisco Unified Call Manager w wersji 11.5 oraz wyższe, bramy głosowe Cisco).

<u>Wymagania dla systemu nagrywania rozmów:</u>

- Oferowane rozwiązanie będzie rozwiązaniem instalowanym w środowisku wirtualnym VMware (wsparcie dla wersji Vmware 5.5 i wyższych).
- Rozwiązanie musi umożliwiać instalację na serwerach będących w posiadaniu Zamawiającego (UCS C220-M3), jako aplikacja UC kolokowana wraz z posiadanym systemem Cisco Communications Manager.
- Rozwiązanie zapewni nagrywanie minimum 30 kanałów głosowych równoległych.
- System zapewni obserwowanie minimum 1.500 terminali (telefonów).
- Rozwiązanie umożliwi integrację z dowolnym serwerem SMTP.
- System zapewni przechowywanie nagrań co najmniej przez okres 12 miesięcy.
- Interfejs użytkownika musi być oparty o przeglądarkę stron WWW oraz wspierać protokół HTTPS.
- Rozwiązanie GUI musi wspierać przynajmniej wymienione przeglądarki: Internet Explorer i Google Chrome.
- Rozwiązanie musi składać się z określonej liczby odrębnych komponentów, które można rozmieścić na różnych serwerach w celu umożliwienia skalowania rozwiązania.

- Rozwiązanie nie powinno wymagać jakichkolwiek dodatkowych licencji na oprogramowanie bazy danych oraz systemu operacyjnego.
- Dostawca rozwiązania do nagrywania powinien zapewnić dostęp do bazy danych oraz schematu bazy danych bez dodatkowych dopłat.
- System ma zawierać aplikacje administracyjne oparte o przeglądarkę WWW dla potrzeb zarządzania użytkownikami.
- Rozwiązanie ma mieć możliwość obsłużenia nieograniczonej licencyjnie liczby stanowisk pracy użytkownika/stacji roboczych do odtwarzania nagrań.
- System musi umożliwiać monitorowanie przy użyciu SNMP. SNMP musi dostarczać szczegółowych informacji na temat stanów wszystkich komponentów, jak również informację o nagraniach.
- Zaproponowane rozwiązanie musi zapewniać API do pauzowania/wznawiania nagrywania.
- Zaproponowane rozwiązanie musi zapewniać API do oznaczania połączeń.
- System ma posiadać moduł zarządzania użytkownikami, który musi zawierać wielopoziomowe uprawnienia umożliwiające precyzyjną kontrolę widoczności użytkowników.
- Administrator systemu musi mieć możliwość ograniczenia dostępu grupy użytkowników lub określonych użytkowników do nagranych połączeń w oparciu o jeden lub większą liczbę filtrów. Filtry muszą mieć możliwość dopasowania do określonych prefiksów, sufiksów, rodzajów połączeń oraz zakresu dat.
- System musi zabierać moduł (aplikację) wspierającą autoryzację użytkowników względem protokołu LDAP.
- System musi zawierać Funkcję Administracji Użytkownika, która będzie zawierać wielopoziomowe uprawnienia umożliwiające precyzyjną kontrolę praw użytkowników (tzn. tego, co użytkownicy mogą robić).
- Rozwiązanie musi zawierać obszerny zbiór mechanizmów kontroli dostępu obejmujący selektywnie ograniczający dostęp do aplikacji i funkcji aplikacji (odtwarzanie, pobieranie, przeglądanie, itp.).
- Rozwiązanie musi zapewnić możliwości odtwarzania nagrania za pomocą interfejsu użytkownika bez konieczności instalowania aplikacji firm trzecich lub wtyczek do przeglądarek WWW innych, niż standardowa przeglądarka internetowa.
- Rozwiązanie musi wspierać kodowanie AES dla nagranych połączeń. Rozwiązanie musi wspierać rotację kluczy szyfrujących, których ważność można konfigurować.
- Zasady dotyczące haseł muszą wspierać poniższe:
  - Minimalna liczba znaków,
  - Minimalna liczba małych liter,
  - Minimalna liczba dużych liter,
  - Minimalna liczba cyfr,
  - Minimalna liczba znaków nie będących znakami alfanumerycznymi,
  - Żywotność hasła liczona w dniach,
  - Liczba logowań zakończona niepowodzeniem przed zablokowaniem.
- System musi zapewnić szczegółowy dziennik kontroli, który dostarczy przynajmniej informacje określone poniżej:
  - Jaka czynność została wykonana,
  - Czy czynność została wykonana z powodzeniem, czy nie,

- Który użytkownik wykonał czynność,
- Data i godzina, w której czynność miała miejsce,
- Informacja o wykonanej czynności.

- System zapewni możliwość archiwizacji nagrań na zdefiniowanym zewnętrznym zasobie.
- Rozwiązanie ma zawierać funkcję automatycznego archiwizowania/tworzenia kopii zapasowej, która wspiera archiwizowanie do jakichkolwiek nośników/urządzeń.
- Rozwiązanie musi obsługiwać centralizację wielu zdalnych lokalizacji. Rozwiązanie musi obsługiwać mechanizm synchronizacji połączeń z wielu serwerów nagrywających połączenia.
- Planowanie i reguły nagrywania (definicja tego, które połączenia powinny być nagrane) muszą być konfigurowalne za pośrednictwem interfejsu opartego o przeglądarkę WWW.
- Ważność każdej reguły nagrywania może zostać ograniczona co do dnia tygodnia oraz godziny.
- Interfejs użytkownika musi zapewniać dostosowanie kolumn do potrzeb klienta w widoku użytkownika.
- Interfejs użytkownika ma zapewnieniać możliwości wyszukiwania w oparciu o liczbę segmentów, rodzaju połączenia oraz czasu.
- Rozwiązanie musi zapewniać wszystkie funkcje wymagane do zagwarantowania zgodności z GDPR (RODO).
- Rozwiązanie musi posiadać możliwość automatycznego usuwania połączeń w oparciu o wymagane kryteria.
- Rozwiązanie musi umożliwiać funkcję nagrywania na żądanie uwzględniające fakt, iż wszystkie połączenia są nagrywane w trybie prerecordingu, a użytkownik może oznaczyć chęć zachowania danego nagrania za pomocą aplikacji telefonicznej XML na telefonie IP Cisco. Wszystkie segmenty połączenia są nagrywane, wliczając czas przed zgłoszeniem żądania zachowania nagrania przez użytkownika.
- System musi umożliwiać różne tryby nagrywania:
  - Pasywne – w oparciu o przechwytywanie SIP i komunikatów sygnalizacyjnych,
  - Pasywne zaawansowane – tam, gdzie sygnalizacja jest przechwytywana za pośrednictwem interfejsu CTI z Systemu Zarządzania Komunikacją Głosową, a strumienie RTP są przechwytywane w porcie SPAN,
  - CUBE Sip Dial Peer forking tam, gdzie sesja nagrywania jest zarządzana przez CUBE, a strumienie RTP są replikowane przez CUBE,
  - Aktywne - tam, gdzie sygnalizacja jest przechwytywana za pośrednictwem interfejsu CTI z Systemu Zarządzania Komunikacją Głosową, a strumienie RTP są wysyłane bezpośrednio z aparatu monitorowanego.
- System musi obsługiwać wiele metod nagrywania na pojedynczym serwerze (np. nagrywanie Passive i Active).
- System musi umożliwiać nagrywanie rozmów kodowanych przez standardy: G.711, G.729, G722.
- System musi obsługiwać opcję active/hot standby dla Active Recording. Strumienie RTP mogą być przesyłane wyłącznie i zawsze na jeden serwer. Rozwiązanie musi wspierać przetwarzanie strumieni na serwerze HA, jeżeli jakikolwiek inny komponent serwera głównego przestanie działać
- System musi zapewniać mechanizm do synchronizacji połączeń, który będzie w stanie rozpoznać różne kopie tego samego połączenia w celu zaoszczędzania miejsca składowania.

- Aplikacja odtwarzania nie może nakładać ograniczeń względem liczby użytkowników, którzy mogą uzyskać jednoczesny dostęp do pojedynczego nagrania połączenia.
- Rozwiązanie powinno obsługiwać eksport nagranych połączeń wraz z metadanymi przez upoważniony personel. Metadane muszą być dostarczane w formacie CSV.
- System musi wspierać możliwość przechowywania nagranych połączeń w skompresowanym formacie MP3 z konfigurowalną przepływnością.
- System musi posiadać możliwość przechowywania nagranych połączeń w nieskompresowanym formacie WAV.
- System ma zapewnić przechowywanie wraz z nagraniem informacji o tym, kto rozłączył się pierwszy (osoba wykonująca połączenie, czy osoba odbierająca połączenie).
- Rozwiązanie ma zapewnić możliwość porównywania nagranych połączeń z zestawionymi połączeniami w oparciu CDR-y (Call Details Records).
- System musi obsługiwać nagrywanie szyfrowanych połączeń z wykorzystaniem aktywnego nagrywania. Rozwiązanie musi mieć zdolność nie tylko do przetwarzania sRTP (zakodowanych danych głosowych), lecz także zabezpieczania połączeń z Systemem Zarządzania Komunikacją Głosową SIP TLS.
- System musi umożliwiać kompresję do formatu mp3 lub podobnego dla połączeń importowanych z innych systemów nagrywania.
- System ma obsługiwać identyfikację "warm transfer" połączenia. Gdy klient jest przełączony przez agenta A agentowi B, wszystkie trzy segmenty rozmowy (Klient z agentem A, Agent A z Agentem B, Klient z Agentem B) są identyfikowane jako jedna rozmowa.
- System musi mieć możliwość łączenia rozmowy rozdzielonej na segmenty poprzez wstrzymania "hold" i przełączenia "transfers" oraz eksportowania ich, jako pojedynczego nagrania.
- Aplikacja odtwarzania multimediów musi być funkcjonalnie podobna do odtwarzacza multimedialnego Microsoft i wspierać standardowe funkcje odtwarzania obejmujące: regulację głośności, przewijanie do przodu, przewijanie do tyłu, bezpośredni dostęp (pasek przewijania) do fragmentów nagrania oraz wizualizację połączenia.
- Rozwiązanie musi zapewniać widok całego połączenia obejmując hold i transfer itp. włączając w to połączenia przekazywane z jednego centrum do drugiego. Musi być wspierane odtwarzanie całości nagrania (wszystkie segmenty) za jednym kliknięciem.
- Wymagane są certyfikaty potwierdzające prawidłowe współdziałanie z systemami firmy Cisco lub referencje z wdrożenia systemu nagrywania rozmów w środowisku Cisco Unified Communications.

8. Rozbudowa posiadanej infrastruktury Cisco ISE w tym subskrypcje R-ISE-VMS-K9=); 9. Rozbudowa posiadanej infrastruktury Cisco ISE; 10. Subskrypcje w ramach posiadanej infrastruktury Cisco ISE; 11. Subskrypcje w ramach posiadanej infrastruktury Cisco ISE:

Oprogramowanie zarządzania tożsamością (np. Cisco ISE)

Podstawowe cechy systemu

- System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) wirtualnych (wymagane dostarczenie licencji dla co najmniej 5ciu maszyn).

- System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
- System musi umożliwiać instalację na maszynie wirtualnej (VM) lub maszynie fizycznej
- System musi umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:
  - Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie
  - Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
    - przełączników dostępowych
    - sesji uwierzytelniania 802.1X
    - zdarzeń kontroli dostępu (autoryzacji)
    - zdarzeń związanych z błędami
    - zdarzeń związanych z alarmami systemowymi
  - Wydzielenie serwerów usługowych realizujących funkcje:
    - serwera RADIUS/TACACS+ dla infrastruktury sieciowej
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
    - serwera profilowania stacji końcowych
- System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, w tym:
  - zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
  - zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
- System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS
- System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
- System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
- System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
- System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni
- System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
  - dostęp do interfejsu konfiguracji usług tożsamości 802.1X
  - dostęp do interfejsu konfiguracji urządzeń sieciowych
  - dostęp do interfejsu konfiguracji polityk
  - dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
  - dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania

- System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.

Mechanizmy uwierzytelniania

- System musi wspierać następujące protokoły uwierzytelniania i standardy:
  - RADIUS, zgodnie z dokumentami:
    - RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
    - RFC 2139 — RADIUS Accounting
    - RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
    - RFC 2866 — RADIUS Accounting
    - RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
    - RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
    - RFC 2869 — RADIUS Extensions
  - RADIUS Proxy dla zewnętrznego serwera RADIUS
  - TACACS+
- System musi wspierać protokół Windows Active Directory, w tym co najmniej następujące repozytoria AD:
  - Microsoft Windows Active Directory 2003 32bit
  - Microsoft Windows Active Directory 2003 R2 32bit i 64bit
  - Microsoft Windows Active Directory 2008 32bit i 64bit
  - Microsoft Windows Active Directory 2008 R2 64bit
  - Microsoft Windows Active Directory 2012
  - Microsoft Windows Active Directory 2012 R2
- System musi wspierać protokół Lightweight Directory Access Protocol (LDAP)
- System musi wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865
- System musi wspierać następujące protokoły uwierzytelniania:
  - PAP/ASCII
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - EAP-MD5
  - LEAP
  - EAP-TLS
  - Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
    - EAP-MS-CHAPv2
    - EAP-GTC
    - EAP-TLS
  - System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect
- System musi wspierać implementację 802.1X z przynajmniej następującymi suplikantami:
  - wbudowanym klientem 802.1X dla Windows XP
  - wbudowanym klientem 802.1X dla Windows Vista
  - wbudowanym klientem 802.1X dla Windows 7

- wbudowanym klientem 802.1X dla Windows 8 i 8.1
- Apple Mac OS X Supplicant
- Apple iOS Supplicant
- Google Android Supplicant

- System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).
- System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
- System musi umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych złożone o reguły.
- System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)
- System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC.
- System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC
- System musi wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
  - tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
  - tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
  - tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden w host w domenie danych (Data VLAN) na jednym porcie fizycznym
  - tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym
  - mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny
  - mechanizm umożliwiający poprawną obsługę sytuacji w której nowy host podłącza się do portu na którym uprzednio było uwierzytelnione urządzenie, w tym w VLANie głosowym
  - mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA.
  - mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X
  - mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X
  - obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki
  - mechanizm 802.1x umożliwiajacy realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla uzytkowników gościnnych
  - mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny
  - przypisanie przez serwer AAA dla uzytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
  - uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego sie w VLANie głosowym

- współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
- możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web
- możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika

- System musi wspierać uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)

Realizacja dostępu gościnnego

- System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, co najmniej dla :
  - Microsoft Windows 8.1, Windows 8, Windows 7, Microsoft Windows Vista, Microsoft Windows XP
  - Apple Mac OS X 10.x
  - Apple iOS 8.0, 7.x, 6.1, 6, 5.1, 5.0.1
  - Google Android dla 2.2 i nowszych
  - Linux
- System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsor).
- System musi zapewniać uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o:
  - wewnętrzną bazę użytkowników
  - zewnętrzne repozytorium użytkowników
- System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do:
  - logowania się do systemu
  - tworzenia pojedynczego konta gościnnego
  - tworzenia wielu kont gościnnych
  - importowania kont gościnnych z pliku CSV
  - wysyłania wiadomości email po utworzeniu konta gościnnego
  - wysyłania wiadomości SMS po utworzeniu konta gościnnego
  - wyświetlenia hasła konta gościnnego
  - wydrukowania danych konta gościnnego
  - wyświetlenia danych stworzonych kont gościnnych
  - zawieszenia (suspend) i reinicjacji kont gościnnych
- System musi umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:
  - zmianę logo strony logowania
  - zmianę obrazu tła strony logowania
  - zmianę logo bannera
  - zmianę obrazu tła bannera
  - zmianę koloru tła strony z treścią
- System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS
- System musi umożliwiać zmianę adresu URL i FQDN strony sponsora.

- System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System musi umozliwiać wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych
- System musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim
- System musi umożliwiać stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.
- System musi umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
  - Imienia
  - Nazwiska
  - Firmy
  - adresu e-mail
  - numeru telefonu
  - danych opcjonalnych (nie mniej niż 5 dodatkowych pól)
- System musi umożliwiać konfigurację dla użytkowników gościnnych:
  - wyświetlenia im informacji polityce akceptowalnego użycia sieci (AUP)
  - zezwolenia gościom na zmianę hasła
  - samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
- System musi umożliwiać honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
- System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.
- System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługiwać co najmniej 20 urządzeń per konto gościnne.
- System musi umożliwiać konfigurację czasu ważności hasła w dniach w przedziale zadanym przedziale w dniach.
- System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny
- System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych:
- System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika
- System musi umożliwiać tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.
- System musi umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.
- System musi umożliwiać udostepnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,
- System musi wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

<u>Profilowanie urządzeń</u>

- System musi umożliwiać rozbudowę o możliwość dokonania profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
- System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.
- System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:
  - DHCP
  - DHCP SPAN
  - HTTP
  - RADIUS
  - DNS
  - SNMP
  - Network Scan (NMAP lub inne narzędzie profilowania aktywnego)
- System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.
- System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
- System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:
  - Stacji roboczych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,
  - Urządzeń mobilnych: Android, Apple, Blackberry
  - Telefonów IP
  - Drukarek sieciowych
  - Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych
  - Routerów
  - Punktów dostępu bezprzedowowego
  - Konsoli gier
- System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:
  - reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci
  - reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt
- System musi umożliwiać włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.
- System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

<u>Obsługa klientów mobilnych.</u>

- Możliwość (we współpracy z agentem na stacji końcowej) inspekcji stanu stacji klienta sprawdzająca co najmniej:

- poprawność pracy aplikacji (antywirus, firewall, backup)
- stan określonych procesów
- obecność określonych poprawek systemu operacyjnego
- możliwość określenia reakcji na wynik inspekcji – zestawienie sesji, blokada sesji, powiadomienie użytkownika, przeniesienie do kwarantanny, wymuszenie korekty stanu.

- Możliwość integracji z systemami klasy MDM (Mobile Device Management)

Obsługa serwerów certyfikatów CA.

- System musi posiada funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.
- Funkcja CA musi umożliwiać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.
- System musi wspierać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów.
- Funkcja CA musi zapewniać przynajmniej następujące funkcjonalności:
  - Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS
  - Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym
  - Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji
  - Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA

Raportowanie

System musi umożliwiać generowanie przynajmniej następujących raportów:

- raportów dla protokołów AAA:
  - diagnostyki protokołów AAA
  - trendów uwierzytelnienia 802.1X
  - accountingu RADIUS
  - uwierzytelniania RADIUS
- raportów dozwolonych protokołów
  - sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
    - uwierzytelnień pomyślnych
    - uwierzytelnień nieudanych
  - „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
    - uwierzytelnień pomyślnych
    - uwierzytelnień nieudanych
- raportów dla poszczególnych instancji serwerów systemu, w tym:
  - uwierzytelnień RADIUS per serwer
  - Top „N"uwierzytelnień per serwer

- monitorowania Online Certificate Status Protocol (OCSP)
- administratorów systemu i ich uprawnień
- logowania administratorów do systemu
- zmian konfiguracji serwera dokonanych przez administratorów
- stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
- zmian operacyjnych serwera dokonanych przez administratorów
- zmian haseł przez użytkowników

- raportów dla stacji końcowych, w tym:
  - uwierzytelnień typu MAC Authentication
  - Top „N"uwierzytelnień per adres MAC stacji
  - Top „N" uwierzytelnień per maszyna
  - Top „N"uwierzytelnień per RADIUS Calling Station ID
  - działań podsystemu profilera per adres MAC
  - czasu wymaganego na sprofilowanie stacji per adres MAC
- raportów dla błędów, w tym:
  - błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
  - sumarycznych przyczyn nieudanych uwierzytelnień
  - Top „N" uwierzytelnień per rodzaj błędu
- raportów dla urządzeń sieciowych:
  - sumarycznych uwierzytelnień dla urządzeń sieciowych
  - Top „N" uwierzytelnień per urządzenie sieciowe
  - niedostępności serwera AAA dla urządzenia sieciowego
  - wiadomości logowanych przez urządzenia sieciowe
  - stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
- raportów użytkowników:
  - sumarycznych uwierzytelnień użytkowników
  - Top „N"uwierzytelnień per użytkownik
  - sesji użytkowników gościnnych
  - aktywności użytkowników gościnnych
  - sumarycznych uwierzytelnień sponsorów dostępu gościnnego
  - uwierzytelnień per unikalny użytkownik
- raportów katalogu sesji
  - aktywnych sesji RADIUS
  - historii sesji RADIUS
  - zaterminowanych sesji RADIUS

<u>Alarmy</u>

- System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą
  - wiadomości e-mail
  - syslog
- Alarmy muszą być generowane w następujących sytuacjach:
  - ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
  - opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego

- status krytycznych procesów będzie niepożądany, w tym status:
  - procesu wewnętrznej bazy danych systemu
  - serwera aplikacyjnego systemu
  - bazy danych sesji
  - kolektora i procesora wiadomości log
  - błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
  - stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
- obciążenie systemu (load)
- zajętość pamięci
- System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
  - badanie łączności IP za pomocą ping, nslookup, traceroute
  - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
    - nazwy użytkownika
    - adresu MAC
    - statusu uwierzytelnienia (udana lub nieudana)
    - powodu, jeżeli uwierzytelnienie nieudane
    - zakresu czasowego, co do dnia, godziny i minuty
  - wykonanie zdalnego polecenia na urządzeniu sieciowym
  - ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
    - definicji serwerów AAA
    - protokołu RADIUS
    - odkrywania urządzeń
    - logowania
    - uwierzytelniania Web
    - konfiguracji trybu 802.1X
  - wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

<u>Licencje systemu</u>

System musi być dostarczony z licencjami umożliwiającymi:

- instalację co najmniej 1 maszyny wirtualnej umożliwiających obsługę co najmniej 5.000 użytkowników
- obsługę co najmniej 1000 użytkowników na poziomie bazowym (obsługa autoryzacji 802.1x, MAB, web, obsługa MACSec, obsługa SSO, portalu gościnnego)
- obsługę co najmniej 250 użytkowników na poziomie rozszerzonym (obsługa profilowania, BYOD)
- obsługę co najmniej 100 użytkowników na poziomie zaawansowanym (obsługa inspekcji stanu stacji, integracji z systemami MDM)
- jeśli funkcjonalność jest licencjonowana czasowo, to wymaga się dostarczenia odpowiedniej subskrypcji na okres co najmniej trzech lat

16. Rozbudowa posiadanych urządzeń; 17. Rozbudowa posiadanych urządzeń; 18. Rozbudowa posiadanych urządzeń; 19. Rozbudowa posiadanych urządzeń; 20. Rozbudowa posiadanych urządzeń; 21. Rozbudowa posiadanych urządzeń:

Elementy rozbudowujące posiadaną infrastrukturę

Dostarczane elementy muszą posiadać udokumentowaną kompatybilność z rozbudowywanymi elementami oraz nie mogą powodować jakichkolwiek ograniczeń w świadczeniach gwarancyjnych lub procedurach serwisowych producentów rozbudowywanej infrastruktury.

Moduły światłowodowe

- Moduły QSFP 40G, BiDir, SR, umożliwiające osiągnięcie zasięgu 100m na standardowej parze włókien wielomodowych OM3, kompatybilne z przełącznikami Cisco Nexus 9300, złącza LC
- Moduły SFP+ 10GbaseSR, umożliwiające osiągnięcie zasięgu 300m na standardowej parze włókien wielomodowych OM3, kompatybilne z przełącznikami Cisco Nexus 9300, złącza LC
- Moduły SFP+ 10GbaseLR, umożliwiające osiągnięcie zasięgu 10km na standardowej parze włókien jednomodowych G.652, kompatybilne z przełącznikami Cisco Nexus 9300, złącza LC
- Moduły SFP+ 10GbaseER, umożliwiające osiągnięcie zasięgu 40km na standardowej parze włókien jednomodowych G.652, kompatybilne z przełącznikami Cisco Nexus 9300, złącza LC

35. Rozbudowa posiadanych urządzeń; 36. Rozbudowa posiadanych urządzeń.

- Moduły AFM735 Interfejs SFP 100BASE-FX, umożliwiające osiągnięcie zasięgu 100m na standardowej parze włókien wielomodowych OM3, kompatybilne z przełącznikami Netgear GSM7328FS-200NES,
- Moduły ProSafe AGM731F 1000BASE-SX SFP GBIC, umożliwiające osiągnięcie zasięgu 100m na standardowej parze włókien wielomodowych OM3, kompatybilne z przełącznikami Netgear GSM7328FS-200NES,

12. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci:; 13. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci; 14. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci; 15. Subskrypcje w ramach posiadanej infrastruktury odpowiedzialnej za bezpieczeństwo sieci;

Subskrypcje systemów bezpieczeństwa

- subskrypcja IPS i filtracji URL na okres 3 lat dla posiadanych urządzeń Cisco Firepower 2130
- subskrypcja IPS na okres 3 lat dla posiadanych urządzeń Cisco ASA 5545 with Firepower Services
- subskrypcja IPS na okres 3 lat dla posiadanych urządzeń Cisco ASA 5508 with Firepower Services
- subskrypcja IPS na okres 3 lat dla posiadanych urządzeń Cisco ASA 5506 with Firepower Services

32. Zestaw rozszerzony systemu wideokonferencji:

Terminal wideo rozszerzony zintegrowany do pracy grupowej (np. Cisco Webex Room 55)

- Urządzenie musi pełnić funkcję grupowego terminala wideo, przeznaczonego do pracy w sali konferencyjnej.
- Zintegrowany w jednej obudowie monitor LCD, system nagłośnienia, mikrofon, kamera, kodek wideokonferencyjny, moduł bezprzewodowego współdzielenia prezentacji oraz podstawa umożliwiająca łatwą instalację i ustawienie terminala w sali. Wszystkie komponenty muszą być wzajemnie kompatybilne i pochodzić od jednego producenta.
- Musi posiadać do sterowania dotykowy, kolorowy panel sterujący LCD:
  - do nawiązywania, zawieszania i rozłączania połączeń
  - do włączenia statusu „nie przeszkadzać" dla terminala
  - rozpoczynanie i zatrzymywanie współdzielenia treści z dołączonego komputera PC
  - kontekstowe menu zależne od statusu połączenia
  - dający możliwość uproszczonego dodzwonienia się do zaplanowanej wideokonferencji przez pojedyncze naciśnięcie przycisku na panelu
  - możliwość dodania graficznego menu do realizacji funkcji sterowania z urządzenia innymi systemami peryferyjnymi w sali konferencyjnej: oświetlenie, zasłanianie rolet, matryce wideo
  - dołączony do terminala przez port LAN/Ethernet (RJ-45) 10/100 z PoE
  - wyświetlacz dotykowy pojemnościowy LCD
  - przekątna min. 10 cali
  - rozdzielczość wyświetlacza, co najmniej 1280x800 pikseli
- Musi obsługiwać połączenia wideo w protokołach:
  - H.323 oraz SIP
  - H.264
  - H.265
  - H.460.18, H.460.19
  - H.239 oraz BFCP
  - połączenia SIP poprzez zapory sieciowe z wykorzystaniem protokołu realizującego funkcje Firewall Traversal
  - udostępnianie prezentacji z komputera PC bezprzewodowo, poprzez aplikację na PC. Aplikacja musi komunikować się z terminalem poprzez protokół IP oraz posiadać mechanizm sprawdzający obecność komputera PC prezentera w sąsiedztwie terminala, np. poprzez ultradźwięki.
- Musi obsługiwać połączenia wideo w przepustowości 6Mb/s
- Musi zapewniać wysyłanie i odbieranie (encoding i decoding) obrazu w rozdzielczościach:
  - 720p30 oraz 1080p30
  - 720p60 oraz 1080p60
  - musi realizować efektywne kodowanie wideo dla kodeka H.264 zapewniające możliwość przesłania wideo HD 720p30 w paśmie nie większym niż 800 kb/s oraz FullHD 1080p30 w paśmie nie większym niż 1500 kb/s
- Musi obsługiwać szyfrowanie połączeń:
  - w protokole H.323 oraz w protokole SIP

- połączeń z wykorzystaniem protokołów H.239 i BFCP
- standardem H.235
- standardem AES
- z automatyczną wymianą klucza

▪ Musi obsługiwać dźwięk w połączeniach wideo w protokołach:

- G.711, G.722, G.722.1, G.729 AB
- MPEG4 AAC-LD
- Opus

▪ Współdzielenie prezentacji jako drugi strumień wideo w protokołach H.239 i BFCP z minimalną rozdzielczością:

- 3840 x 2160p5 dla sygnału z wejścia HDMI
- 1080p5 dla sygnału z modułu bezprzewodowego współdzielenia prezentacji, wbudowanego w urządzenie.

▪ Wbudowany moduł rozpoznawania osoby mówiącej, w celu realizacji funkcji automatycznego kadrowania osób w sali podczas trwającego spotkania wideo

- wykorzystanie dedykowanej, wbudowanej w urządzenie matrycy mikrofonów do triangulacji źródła dźwięku
- wykorzystanie wbudowanych algorytmów rozpoznawania twarzy
- liczenie osób w pomieszczeniu
- zasięg co najmniej 5m

▪ Musi obsługiwać dwa ekrany: wbudowany oraz dodatkowy, dołączany poprzez port wyjściowy HDMI urządzenia:

- Wyświetlanie wideo na jednym ekranie oraz prezentacji na drugim ekranie podczas trwania połączenia wideo
- Wyświetlanie lokalne dwóch prezentacji, tzn. prezentacji z wejścia HDMI na jednym ekranie oraz drugiej prezentacji z modułu bezprzewodowego współdzielenia prezentacji na drugim ekranie, w sytuacji bez trwającego połączenia wideo

▪ Musi posiadać system audio o następujących cechach:

- System audio stanowi integralną część terminala
- Minimum cztery głośniki stanowiące integralną część terminala
- Wbudowany mikrofon oraz dołączone dwa dodatkowe zewnętrzne nabiurkowe mikrofony dookólne
- Automatyczna kasacja echa
- Automatyczna redukcja szumów
- Praca w trybie stereo
- Pasmo przenoszenia, co najmniej od 75Hz do 20kHz
- Moc wzmacniacza, co najmniej 75W
- Zestaw mikrofonów w formie, co najmniej 6-punktowej matrycy do realizacji funkcji śledzenia osoby mówiącej

▪ Musi posiadać wsparcie dla funkcjonalności i protokołów z rodziny IP:

- Protokoły DNS, DiffServ, TCP/IP, DHCP
- Dzwonienie URI
- Automatyczne odnajdowanie gatekeepera H.323
- Pobieranie czasu i daty z serwera NTP
- HTTPS, SOAP, XML, SSH, HTTP

- Zabezpieczenie hasłem dostępu poprzez interfejs IP
- Możliwość wyłączenia usług IP: HTTP, HTTPS, SSH
- Zabezpieczenie hasłem dostępu do ustawień interfejsu IP z poziomu interfejsu użytkownika
- Obsługa DTMF poprzez RFC 4733 oraz H.245

- Musi mieć następujące funkcje książki adresowej:
  - Lokalna książka adresowa przechowywane w pamięci terminala dla minimum 200 wpisów
  - Obsługa dostępu do centralnej książki adresowej z nieograniczoną ilością wpisów
  - Obsługa serwerów LDAP i możliwość współpracy z systemami obsługującymi H.350
  - Historia połączeń przychodzących, wychodzących i nieodebranych wraz datą i godziną
- Monitor LCD musi mieć minimalne parametry:
  - Przekątna 55 cali
  - Rozdzielczość Ultra HD 3840 x 2160
  - Ekran monitora musi być dedykowany do długotrwałego użytku i musi pochodzić z profesjonalnej klasy rozwiązań w odróżnieniu od rozwiązań konsumenckich o ograniczonej gwarancji
  - Kontrast 1000
  - Kąt wyświetlania 178 stopni
  - Czas reakcji 8 ms
  - Jasność 500 cd/metr kw.
- Zintegrowana kamera wideo musi mieć następujące cechy:
  - Sensor kamery 15MP
  - Praca w trybie 5K UltraHD przy 60 fps i 30 fps
  - Zoom cyfrowy min. 3x
  - Kąt widoczności horyzontalny min. +/-80°
  - Kąt widoczności wertykalny min. +/-50°
  - Automatyczna regulacja ostrości, jasności oraz balansu bieli
  - Współpraca z wbudowanym w urządzenie modułem rozpoznawania osoby mówiącej w celu realizacji funkcji automatycznego kadrowania osób w sali podczas spotkania wideo.
  - Obiektyw kamery ze światłem nie gorszym niż f 1.7
- Musi posiadać wbudowany zasilacz przystosowany do zasilenia prądem przemiennym 230V
- Musi posiadać, co najmniej dwa wejścia HDMI o parametrach:
  - Rozdzielczość 4Kp30 oraz 1080p60
  - Funkcja CEC (Consumer Electronics Control) w wersji 2.0
  - Protokół HDCP dla lokalnej prezentacji na co najmniej jednym z wejść HDMI.
- Musi posiadać, co najmniej jedno wyjście HDMI umożliwiające dołączenie drugiego zewnętrznego wyświetlacza. Parametry wyjścia HDMI:
  - Rozdzielczość 4Kp60
  - Wyświetlanie obrazu strony zdalnej z połączania wideo w jakości 1080p30 oraz 1080p60
  - Funkcja CEC (Consumer Electronics Control) w wersji 2.0
- Musi posiadać, co najmniej jeden porty LAN/Ethernet (RJ-45) 10/100/1000 oraz jeden port LAN/Ethernet (RJ-45) 10/100 oferujący zasilanie PoE do dołączenia dotykowego panelu sterującego
- Musi posiadać wbudowany interfejs bezprzewodowy WLAN w standardzie IEEE 802.11a/b/g/n/ac w paśmie 2.4 GHz oraz 5 GHz, co najmniej tryb 2x2 MIMO
- Musi posiadać dedykowany port serwisowy w formie złącza USB.
- Musi posiadać w komplecie poniższe okablowanie peryferyjne:

- przewód połączeniowy do sieci Ethernet o długości, co najmniej 5m do dołączenia urządzenia do sieci LAN
- przewód HDMI do prezentacji o długości, co najmniej 6m
- Urządzenie powinno być zarządzane centralnie poprzez posiadany system komunikacyjny (Cisco Communications Manager) w zakresie, co najmniej:
  - Pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego
  - Obsługa przesyłania plików konfiguracyjnych zaszyfrowanych przez serwery komunikacyjne Zamawiającego
  - Możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU)
  - Możliwości zdalnego restartu urządzenia lub grupy urządzeń
  - Możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego.
  - Kontrola pasma w sieci IP przeznaczona do transmisji wideo dla urządzenia.
  - Rejestracja oraz praca w trybie zdalnym tj. spoza własnej sieci IP, realizowana poprzez bramę wideo z obsługą funkcji Firewall Traversal dla SIP oraz H.323.
- Opcja uruchomienia w przyszłości wbudowanego mostka wideokonferencyjnego oferującego następujące cechy:
  - Dwa tryby pracy: 4 porty konferencyjne obsługujące rozdzielczość 720p30 lub 3 porty konferencyjne obsługujące rozdzielczość 1080p30.
  - Obsługa drugiego strumienia (H.239/BFCP) z min. rozdzielczością 4K 3840 x 2160p5
  - Szyfrowanie połączeń wielopunktowych
  - Możliwość ustawienia dedykowanego układu ekranu dla każdego uczestnika spotkania - bez zmiany układu obrazu dla pozostałych uczestników.
  - Indywidualne transkodowanie audio i wideo dla każdego uczestnika spotkania
  - Możliwość połączenia w jednej konferencji terminali SIP, H.323 oraz VoIP`
  - Możliwość wdzwonienia się na spotkanie wielopunktowe
  - Możliwość dołączenia uczestnika do spotkania z poziomu terminala
  - Uruchomienie wbudowanego mostka nie może wymagać rozbudowy sprzętowej (dopuszczalne dodanie licencji).

33. Zestaw podstawowy systemu wideokonferencji:

Terminal wideo podstawowy do pracy grupowej (np. Cisco Webex Room Kit)

- Urządzenie musi pełnić funkcję grupowego terminala wideo, przeznaczonego do pracy w sali konferencyjnej.
- Zintegrowane w jednej obudowie kamera, kodek wideokonferencyjny, mikrofon, system audio, moduł bezprzewodowego współdzielenia prezentacji. Wszystkie komponenty muszą być wzajemnie kompatybilne i pochodzić od jednego producenta.
- Musi posiadać do sterowania dotykowy, kolorowy panel sterujący LCD:
  - do nawiązywania, zawieszania i rozłączania połączeń

- do włączenia statusu „nie przeszkadzać" dla terminala
- rozpoczynanie i zatrzymywanie współdzielenia treści z dołączonego komputera PC
- kontekstowe menu zależne od statusu połączenia
- dający możliwość uproszczonego dodzwonienia się do zaplanowanej wideokonferencji przez pojedyncze naciśnięcie przycisku na panelu
- możliwość dodania graficznego menu do realizacji funkcji sterowania z urządzenia innymi systemami peryferyjnymi w sali konferencyjnej: oświetlenie, zasłanianie rolet, matryce wideo
- dołączony do terminala przez port LAN/Ethernet (RJ-45) 10/100 z PoE
- wyświetlacz dotykowy pojemnościowy LCD
- przekątna min. 10 cali
- rozdzielczość wyświetlacza, co najmniej 1280x800 pikseli

- Musi obsługiwać połączenia wideo w protokołach:
  - H.323 oraz SIP
  - H.264
  - H.265
  - H.460.18, H.460.19
  - H.239 oraz BFCP
  - połączenia SIP poprzez zapory sieciowe z wykorzystaniem protokołu realizującego funkcje Firewall Traversal
  - udostępnianie prezentacji z komputera PC bezprzewodowo, poprzez aplikację na PC. Aplikacja musi komunikować się z terminalem poprzez protokół IP oraz posiadać mechanizm sprawdzający obecność komputera PC prezentera w sąsiedztwie terminala, np. poprzez ultradźwięki.
- Musi obsługiwać połączenia wideo w przepustowości 6Mb/s
- Musi zapewniać wysyłanie i odbieranie (encoding i decoding) obrazu w rozdzielczościach:
  - 720p30 oraz 1080p30
  - 720p60 oraz 1080p60
  - musi realizować efektywne kodowanie wideo dla kodeka H.264 zapewniające możliwość przesłania wideo HD 720p30 w paśmie nie większym niż 800 kb/s oraz FullHD 1080p30 w paśmie nie większym niż 1500 kb/s
- Musi obsługiwać szyfrowanie połączeń:
  - w protokole H.323 oraz w protokole SIP
  - połączeń z wykorzystaniem protokołów H.239 i BFCP
  - standardem H.235
  - standardem AES
  - z automatyczną wymianą klucza
- Musi obsługiwać dźwięk w połączeniach wideo w protokołach:
  - G.711, G.722, G.722.1, G.729 AB
  - MPEG4 AAC-LD
  - Opus
- Współdzielenie prezentacji jako drugi strumień wideo w protokołach H.239 i BFCP z minimalną rozdzielczością:
  - 3840 x 2160p5 dla sygnału z wejścia HDMI
  - 1080p5 dla sygnału z modułu bezprzewodowego współdzielenia prezentacji, wbudowanego w urządzenie.

- Wbudowany moduł rozpoznawania osoby mówiącej, w celu realizacji funkcji automatycznego kadrowania osób w sali podczas trwającego spotkania wideo
  - wykorzystanie dedykowanej, wbudowanej w urządzenie matrycy mikrofonów do triangulacji źródła dźwięku
  - wykorzystanie wbudowanych algorytmów rozpoznawania twarzy
  - liczenie osób w pomieszczeniu
  - zasięg co najmniej 5m
- Musi obsługiwać dwa ekrany dołączane poprzez porty wyjściowe HDMI urządzenia:
  - Wyświetlanie wideo na jednym ekranie oraz prezentacji na drugim ekranie podczas trwania połączenia wideo
  - Wyświetlanie lokalne dwóch prezentacji, tzn. prezentacji z wejścia HDMI na jednym ekranie oraz drugiej prezentacji z modułu bezprzewodowego współdzielenia prezentacji na drugim ekranie, w sytuacji bez trwającego połączenia wideo
- Musi posiadać system audio o następujących cechach:
  - System audio stanowi integralną część terminala
  - Minimum cztery głośniki stanowiące integralną część terminala
  - Wbudowany mikrofon oraz dołączone dwa dodatkowe zewnętrzne nabiurkowe mikrofony dookólne
  - Automatyczna kasacja echa
  - Automatyczna redukcja szumów
  - Praca w trybie stereo
  - Pasmo przenoszenia, co najmniej od 75Hz do 20kHz
  - Moc wzmacniacza, co najmniej 20W
  - Zestaw mikrofonów w formie, co najmniej 6-punktowej matrycy do realizacji funkcji śledzenia osoby mówiącej
- Musi posiadać wsparcie dla funkcjonalności i protokołów z rodziny IP:
  - Protokoły DNS, DiffServ, TCP/IP, DHCP
  - Dzwonienie URI
  - Automatyczne odnajdowanie gatekeepera H.323
  - Pobieranie czasu i daty z serwera NTP
  - HTTPS, SOAP, XML, SSH, HTTP
  - Zabezpieczenie hasłem dostępu poprzez interfejs IP
  - Możliwość wyłączenia usług IP: HTTP, HTTPS, SSH
  - Zabezpieczenie hasłem dostępu do ustawień interfejsu IP z poziomu interfejsu użytkownika
  - Obsługa DTMF poprzez RFC 4733 oraz H.245
- Musi mieć następujące funkcje książki adresowej:
  - Lokalna książka adresowa przechowywane w pamięci terminala dla minimum 200 wpisów
  - Obsługa dostępu do centralnej książki adresowej z nieograniczoną ilością wpisów
  - Obsługa serwerów LDAP i możliwość współpracy z systemami obsługującymi H.350
  - Historia połączeń przychodzących, wychodzących i nieodebranych wraz datą i godziną
- Zintegrowana kamera wideo musi mieć następujące cechy:
  - Sensor kamery 15MP
  - Praca w trybie 5K UltraHD przy 60 fps i 30 fps
  - Zoom cyfrowy min. 3x
  - Kąt widoczności horyzontalny min. +/-80°

- Kąt widoczności wertykalny min. +/-50°
- Automatyczna regulacja ostrości, jasności oraz balansu bieli
- Współpraca z wbudowanym w urządzenie modułem rozpoznawania osoby mówiącej w celu realizacji funkcji automatycznego kadrowania osób w sali podczas spotkania wideo.
- Obiektyw kamery ze światłem nie gorszym niż f 1.7

- Musi posiadać wbudowany zasilacz przystosowany do zasilenia prądem przemiennym 230V
- Musi posiadać wejście HDMI o parametrach:
  - Rozdzielczość 4Kp30 oraz 1080p60
  - Funkcja CEC (Consumer Electronics Control) w wersji 2.0
  - Protokół HDCP dla lokalnej prezentacji na co najmniej jednym z wejść HDMI.
- Musi posiadać, co najmniej dwa wyjścia HDMI umożliwiające dołączenie monitorów. Parametry wyjść HDMI:
  - Rozdzielczość 4Kp60
  - Wyświetlanie obrazu strony zdalnej z połączania wideo w jakości 1080p30 oraz 1080p60
  - Funkcja CEC (Consumer Electronics Control) w wersji 2.0
- Musi posiadać, co najmniej jeden porty LAN/Ethernet (RJ-45) 10/100/1000 oraz jeden port LAN/Ethernet (RJ-45) 10/100 oferujący zasilanie PoE do dołączenia dotykowego panelu sterującego
- Musi posiadać wbudowany interfejs bezprzewodowy WLAN w standardzie IEEE 802.11a/b/g/n/ac w paśmie 2.4 GHz oraz 5 GHz, co najmniej tryb 2x2 MIMO
- Musi posiadać dedykowany port serwisowy w formie złącza USB.
- Musi posiadać w komplecie poniższe okablowanie peryferyjne:
  - przewód połączeniowy do sieci Ethernet o długości, co najmniej 5m do dołączenia urządzenia do sieci LAN
  - przewód HDMI do prezentacji o długości, co najmniej 1.5m
- Urządzenie powinno być zarządzane centralnie poprzez posiadany system komunikacyjny (Cisco Communications Manager) w zakresie, co najmniej:
  - Pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego
  - Obsługa przesyłania plików konfiguracyjnych zaszyfrowanych przez serwery komunikacyjne Zamawiającego
  - Możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU)
  - Możliwości zdalnego restartu urządzenia lub grupy urządzeń
  - Możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego.
  - Kontrola pasma w sieci IP przeznaczona do transmisji wideo dla urządzenia.
  - Rejestracja oraz praca w trybie zdalnym tj. spoza własnej sieci IP, realizowana poprzez bramę wideo z obsługą funkcji Firewall Traversal dla SIP oraz H.323.
- Opcja uruchomienia w przyszłości wbudowanego mostka wideokonferencyjnego oferującego następujące cechy:
  - Dwa tryby pracy: 4 porty konferencyjne obsługujące rozdzielczość 720p30 lub 3 porty konferencyjne obsługujące rozdzielczość 1080p30.
  - Obsługa drugiego strumienia (H.239/BFCP) z min. rozdzielczością 4K 3840 x 2160p5
  - Szyfrowanie połączeń wielopunktowych

- Możliwość ustawienia dedykowanego układu ekranu dla każdego uczestnika spotkania - bez zmiany układu obrazu dla pozostałych uczestników.
- Indywidualne transkodowanie audio i wideo dla każdego uczestnika spotkania
- Możliwość połączenia w jednej konferencji terminali SIP, H.323 oraz VoIP`
- Możliwość wdzwonienia się na spotkanie wielopunktowe
- Możliwość dołączenia uczestnika do spotkania z poziomu terminala
- Uruchomienie wbudowanego mostka nie może wymagać rozbudowy sprzętowej (dopuszczalne dodanie licencji).

34. Urządzenia odpowiedzialne za bezpieczeństwo sieci:

Dostarczone urządzenie powinny pracować w klastrze Active-Active, wymagana jest dostawa licencji HA.

Urządzenie powinno posiadać możliwość uruchomienia następujących funkcjonalności, dostarczonych przez jednego producenta:

1. Firewall
2. IPS
3. Zarządzanie identyfikacją użytkownika
4. System automatycznego wykrywania i klasyfikacji aplikacji wraz z filtrowaniem URL
5. Wykrywanie malware oraz komunikacji z serwerami C&C (wykrywanie działających botnetów)
6. Sandbox
7. Wykrywanie wiadomości spam
8. Bramka IPsec VPN
9. Ochrona przed wyciekiem informacji (DLO)
10. Centralne zarządzanie i konfiguracja

Zmawiający wraz z urządzeniami wymaga dostarczenia niezbędnych licencji w celu pełnego uruchomienia niżej wymienionych funkcjonalności:

1. Firewall
2. IPS
3. Zarządzanie identyfikacją użytkownika
4. Centralne zarządzanie i konfiguracja

System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci. System zabezpieczeń firewall musi zapewniać integrację z Active Directory.

Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet, gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym

Dostarczone urządzenia firewall muszą pracować w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów programowych systemu zabezpieczeń oraz łączy sieciowych.

Lp.	Nazwa	Wymagania minimalne
1.	Obudowa	Obudowa typu RACK o wysokości maksymalnie 2U
2.	Interfejsy	Minimum 2x 10GbE SFP+ wraz z wkładkami Minimum 8 x 1GbE 1x 1GbE Management 1x Console
3.	Zarządzanie	Minimum CLI, SSH, GUI Urządzenie muszą być administrowane z poziomu jednej wspólnej konsoli administracyjnej. Jeśli funkcjonalność ta wymaga dodatkowych licencji, licencje te muszą zostać dostarczone wraz z urządzeniami.
4.	Firewall inspection throughput	Minimum: 3.3 Gbps
5.	Full DPI throughput	Minimum: 450 Mbps
6.	Application inspection throughput	Minimum: 1.0 Gbps
7.	IPS throughput	Minimum: 1.0 Gbps
8.	Anti-malware inspection throughput	Minimum: 500 Mbps
9.	TLS/SSL Inspection	Minimum: 250 Mbps
10.	VPN throughput	Minimum: 1.5 Gbps
11.	Connections per second	Minimum: 19 000
12.	VLAN interfaces	Minimum 256
13.	Routing protocols	Minimum: OSPF, BGP, RIP v1/2, static routes

14.	Authentication	Minimum: LDAP, RADIUS, TACACS+, Internal database
15.	NAT mode	Minimum: 1:1, many:1, 1:many, transparent mode, flexible NAT
16.	Zasilanie	Minimum dwa redundantne zasilacze
17.	Subskrypcje	60 miesięcy dla wszystkich wymaganych funkcjonalności
18.	Gwarancja	Minimum pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do 4 godzin od przyjęcia zgłoszenia oraz czasem usunięcia błędu w trybie Next Business Day. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta/wykonawcy lub dedykowaną stronę www.producenta/wykonawcy. Pomoc techniczna musi być świadczona w języku polskim poprzez centrum kompetencyjne zlokalizowane w Polsce. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta/wykonawcy podając unikatowy numer urządzenia, Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń firewall – dokumenty potwierdzające należy załączyć do oferty. Oświadczenie producenta urządzeń firewall, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Uszkodzone dyski pozostają u Zamawiającego.

Załącznik nr 2 do SIWZ

Istotne postanowienia umowy

§ 1. Przedmiot umowy

1. Przedmiotem umowy jest:
   1) dostawa fabrycznie nowych (tzn. wyprodukowanych nie wcześniej niż 6 miesięcy przed dniem dostawy), nieużywanych we wcześniejszych projektach, pochodzących z legalnego kanału sprzedaży producentów na rynek europejski urządzeń infrastruktury sieciowej wraz z odpowiednim oprogramowaniem oraz usług subskrypcyjnych, a także udzielenie stosownych licencji; przedmiotem umowy nie jest objęta instalacja i konfiguracja dostarczanych urządzeń;
   2) dostawa usług serwisowych oprogramowania i sprzętu (Cisco SMARTnet 8x5xNBD) do dostarczanych w ramach zamówienia urządzeń infrastruktury sieciowej, w tym aktywacja tych usług na koncie Zamawiającego „……..”(www.cisco.com); przez usługi serwisowe oprogramowania i sprzętu (Cisco SMARTnet 8x5xNBD) należy rozumieć świadczone przez certyfikowanych inżynierów producenta Cisco, realizowane przez Wykonawcę w dwóch aktualnie dostępnych lokalizacjach Zamawiającego, w których funkcjonuje produkcyjnie infrastruktura zaawansowanych systemów sieciowych (al. J. Ch. Szucha 21/23 oraz ul. Karmazynowa 1A), na warunkach określonych przez producenta oprogramowania i sprzętu, usługi szczegółowo opisane w OPZ (podpunkty od II.1 do II.33)
   3) dostawa usług serwisowych, oprogramowania i sprzętu dla elementów realizowanych przez Wykonawcę w dwóch aktualnie dostępnych lokalizacjach Zamawiającego, w których funkcjonuje produkcyjnie infrastruktura teleinformatyczna Resortu SZ (al. J. Ch. Szucha 21/23 oraz ul. Karmazynowa 1A), na warunkach określonych przez producenta oprogramowania i sprzętu, z przypisaniem do konta Zamawiającego na stronie www.checkpoint.com o nr ID ……., usługi szczegółowo opisane w OPZ (podpunkt II.34).
   4) dostawa usług gwarancyjnych dla pozostałych elementów realizowanych przez Wykonawcę w dwóch aktualnie dostępnych lokalizacjach Zamawiającego, w których funkcjonuje produkcyjnie infrastruktura teleinformatyczna Resortu SZ (al. J. Ch. Szucha 21/23 oraz ul. Karmazynowa 1A), na warunkach określonych przez producenta oprogramowania i sprzętu, usługi szczegółowo opisane w OPZ (podpunkty od II.35 do II.36).
2. Szczegółowo przedmiot umowy określa opis przedmiotu zamówienia, który stanowi załącznik nr 1 do umowy (dalej jako „OPZ”).
3. Przedmiot umowy będzie realizowany na zasadach określonych w niniejszej umowie, w OPZ oraz w ofercie Wykonawcy, stanowiącej załącznik nr 2 do umowy (dalej jako „oferta Wykonawcy”).

§ 2. Miejsce i termin realizacji umowy

1. Wykonawca dostarczać będzie sukcesywnie, zgodnie z harmonogramem dostaw, o którym mowa w punkcie IV OPZ (dalej, jako „harmonogram dostaw”) oraz wykazem ujętym w punkcie II OPZ i zgodnie z ofertą Wykonawcy, na własny koszt i ryzyko, urządzenia infrastruktury sieciowej

wraz z oprogramowaniem, licencjami i/lub kluczami aktywacyjnymi do siedziby Zamawiającego przy ul. Karmazynowej 1A, 02-887 Warszawa. Dokładne terminy i godziny poszczególnych dostaw zostaną uzgodnione między Stronami z odpowiednim wyprzedzeniem.

2. Wykonawca dostarczy wykaz kluczy aktywacyjnych w formie papierowej, wskazując oprogramowanie, do którego licencję aktywuje dany klucz.
3. W ramach dostawy Wykonawca dostarczy również odpowiednie dokumenty licencyjne oraz wykaz zawierający wskazanie:
   1) dostarczonych urządzeń infrastruktury sieciowej;
   2) dostarczonego wraz z tymi urządzeniami oprogramowania;
   3) w odpowiednich przypadkach, oprogramowania niedostarczonego przez Wykonawcę, a objętego zakresem określonym w punkcie II OPZ, które Zamawiający będzie miał możliwość pobrania ze strony producenta, a do którego klucze aktywacyjne Wykonawca dostarczył;
   4) udzielonych licencji, wraz z informacją o okresie ich ważności, w tym o okresie ważności licencji, które Zamawiający będzie aktywował we własnym zakresie za pomocą dostarczonych przez Wykonawcę kluczy aktywacyjnych.
4. Wykaz, o którym mowa w ust. 3 powyżej, Wykonawca dostarczy w formie papierowej oraz w formie elektronicznej na nośniku (płyta CD/DVD).
5. Dostawa usług serwisowych Cisco SMARTnet 8x5xNBD zostanie dokonana zgodnie z harmonogramem dostaw oraz zgodnie z ofertą Wykonawcy, poprzez aktywowanie przez Wykonawcę na koncie Zamawiającego „……” (www.cisco.com) pakietów serwisowych dla dostarczonych urządzeń infrastruktury sieciowej (w tym dostarczonego oprogramowania, przez co rozumie się również oprogramowanie aktywowane za pomocą dostarczonych kluczy aktywacyjnych) oraz poprzez potwierdzenie przez Wykonawcę na piśmie dokonanej aktywacji z wyszczególnieniem aktywowanych w ramach danej dostawy usług serwisowych. Objęcie dostarczonych przez Wykonawcę urządzeń i oprogramowania usługami serwisowymi (Cisco SMARTnet) nastąpi w terminach wskazanych w punkcie 6 OPZ.
6. Usługi serwisowe Cisco SMARTnet 8x5xNBD będą świadczone zgodnie z warunkami określonymi w punkcie III OPZ oraz zgodnie z zakresem tych usług i warunkami ich świadczenia określonymi przez producenta i dostępnymi na stronie internetowej www.cisco.com.
7. Okres, w którym Zamawiający będzie uprawniony do korzystania z danej dostarczonej przez Wykonawcę usługi serwisowej Cisco SMARTnet 8x5xNBD *będzie zgodny z ofertą Wykonawcy, przy czym nie może on być krótszy niż 12 miesięcy*[1].
8. Dostawa usług serwisowych, gwarancyjnych do elementów zawartych w punkcie II.34 zostanie dokonana zgodnie z harmonogramem dostaw oraz zgodnie z ofertą Wykonawcy, na warunkach określonych przez producenta oprogramowania i sprzętu z jednoczesną aktywacją usług na koncie Zamawiającego Account ID …… (www.checkpoint.com).
8. Dostaw usług serwisowych, gwarancyjnych do systemów wideokonferencji zostanie dokona zgodnie z harmonogramem dostaw oraz zgodnie z ofertą Wykonawcy, na warunkach określonych przez producenta oprogramowania i sprzętu.

[1] Postanowienie zostanie dostosowane do oferty Wykonawcy, z którym zawarta zostanie umowa. Dostosowanie nastąpi poprzez wpisanie okresu objęcia usługą serwisowej, zgodnie ze złożoną przez tego Wykonawcę ofertą.

9. Usługi serwisowe, gwarancyjne systemów wideokonferencyjnych będą świadczone zgodnie z warunkami określonymi w punkcie III – OPZ oraz zgodnie z zakresem tych usług i warunkami świadczenia określonymi przez producenta.
10. Okres, w którym Zamawiający będzie uprawniony do korzystania z danej dostarczonej przez Wykonawcę usługi serwisowej, gwarancyjnej *będzie zgodny z ofertą Wykonawcy, przy czym nie może on być krótszy niż 12 miesięcy*[2].

§ 3. Licencje

1. Wykonawca oświadcza, że posiada zgodę producenta oprogramowania będącego przedmiotem umowy, na dostarczanie końcowym użytkownikom licencji na to oprogramowanie oraz zapewnia, że oprogramowanie takie nie jest obciążone prawami, ani roszczeniami osób trzecich, a w szczególności, że zawarcie i wykonanie przez Wykonawcę umowy nie wymaga żadnych zezwoleń osób trzecich.
2. Licencje na oprogramowanie udzielane są na czas i na warunkach określonych przez producenta oprogramowania.
3. Licencja, o której mowa w ust. 2 powyżej, uprawnia do korzystania z oprogramowania na polach eksploatacji określonych w licencji producenta dostarczonej wraz z oprogramowaniem.

§ 4. Zasady i sposób realizacji umowy oraz obowiązki Wykonawcy

1. Wykonawca oświadcza, że jest uprawniony do dostarczenia pakietów serwisowych dla urządzeń sieciowych Cisco, CheckPoint oraz urządzeń pochodzących od innych producentów wchodzących w skład przedmiotu umowy, zgodnie z OPZ i ofertą Wykonawcy.
2. Wykonawca oświadcza, że posiada niezbędne umiejętności, wiedzę i doświadczenie do wykonania przedmiotu umowy i zobowiązuje się wykonać go w sposób i w terminach określonych w umowie, z uwzględnieniem światowych standardów profesjonalnego świadczenia tego typu usług.
3. Wykonawca oświadcza, że dysponuje odpowiednim potencjałem osobowym, materiałowym oraz technicznym pozwalającym na prawidłowe zrealizowanie całości przedmiotu umowy.
4. Wykonawca zobowiązuje się wykonać umowę przy zachowaniu najwyższej staranności wynikającej z zawodowego charakteru prowadzonej działalności, zgodnie z zasadami współczesnej wiedzy technicznej, obowiązującymi przepisami oraz normami, rzetelnie i terminowo, mając na względzie ochronę interesów Zamawiającego.
5. Wykonawca zobowiązuje się do informowania Zamawiającego o wszelkich zagrożeniach związanych z wykonywaniem umowy, w tym także o okolicznościach leżących po stronie Zamawiającego, które mogą mieć wpływ, na jakość, termin bądź zakres wykonywania przedmiotu umowy. Nieprzekazanie takich informacji w wypadku, gdy Wykonawca o takich zagrożeniach wie lub, przy uwzględnieniu wymaganej umową staranności, powinien wiedzieć, powoduje, że wszelkie koszty i dodatkowe czynności związane z konsekwencją danego zdarzenia obciążają Wykonawcę. Ponadto Wykonawca zobowiązuje się do nieodpłatnego informowania w

[2] Postanowienie zostanie dostosowane do oferty Wykonawcy, z którym zawarta zostanie umowa. Dostosowanie nastąpi poprzez wpisanie okresu objęcia usługą serwisowej, zgodnie ze złożoną przez tego Wykonawcę ofertą.

formie pisemnej Zamawiającego o przebiegu realizacji umowy na każde pisemne żądanie Zamawiającego.

§ 5. Odbiory. Współdziałanie Zamawiającego.

1. Zamawiający dokona protokolarnego odbioru poszczególnych dostaw w terminie 5 (pięciu) dni roboczych licząc od daty ich wykonania. Odbiór zostanie potwierdzony przygotowanym przez Wykonawcę i przedstawionym Zamawiającemu przy poszczególnych dostawach protokołem odbioru. Wzór protokołu odbioru stanowi załącznik nr 3 do umowy. Podpisany przez Zamawiającego protokół odbioru będzie podstawą wystawienia faktury VAT.
2. W wypadku stwierdzenia przez Zamawiającego błędów w protokole, o którym mowa w ust. 1, lub istnienia wad w przedstawionym do odbioru przedmiocie umowy, Wykonawca dostarczy, w ciągu 2 (słownie: dwóch) dni roboczych od dnia zgłoszenia tego faktu przez Zamawiającego, nowy egzemplarz protokołu wolny od wad lub wolny od wad przedmiot umowy wraz z nowym protokołem odbioru.

§ 6. Przedstawiciele Stron

1. Strony wyznaczają następujące osoby do kontaktu, nadzoru nad realizacją umowy w tym podpisania protokołów odbioru:
   1) ze strony Zamawiającego: (imię, nazwisko, nr tel., nr faksu, adres mailowy):
      .....;

   2) ze strony Wykonawcy: (imię, nazwisko, nr tel., nr faksu, adres mailowy):

      .....
2. Do współpracy przy realizacji umowy (wsparcie techniczne i serwis oraz subskrypcja) Strony wyznaczają następujące osoby:
   1) ze strony Zamawiającego:
      .....;
   2) ze strony Wykonawcy:
      .....
3. Każda ze Stron uprawniona jest do zmiany osoby upoważnionej. Zmiana wymaga pisemnego powiadomienia drugiej ze Stron i staje się skuteczna z chwilą otrzymania przez adresata pisma z danymi nowej osoby upoważnionej (aneks do umowy nie jest wymagany).
4. Wykonawca odpowiedzialny jest w pełni za działania lub zaniechania wszelkich osób, w tym podwykonawców, realizujących umowę w jego imieniu lub na jego rzecz jak za działania lub zaniechania własne.

§ 7. Wynagrodzenie i warunki płatności

1. Za wykonanie przedmiotu niniejszej umowy przez Wykonawcę, Zamawiający zobowiązuje się zapłacić Wykonawcy, zgodnie z ofertą Wykonawcy, łączne wynagrodzenie w wysokości ..... (słownie: ....., /100) zł netto, powiększone o podatek VAT w wysokości ..... (słownie: ..... /100) zł, co daje kwotę ..... (słownie: …….) zł brutto, dalej również jako „łączne wynagrodzenie brutto”.

2. Wynagrodzenie, o którym mowa w ust. 1 powyżej, będzie wypłacane/wypłacone Wykonawcy w 12 (dwunastu) kwartalnych ratach w wysokości ……. (słownie…) brutto każda.
3. Wynagrodzenie o którym mowa w ust. 2 płatne będzie na rachunek Wykonawcy wskazany na fakturze w następujących terminach:

1) I rata płatna do 21 (słownie: dwudziestu jeden) dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT. Podstawą wystawienia faktury będzie protokół odbioru całości przedmiotu zamówienia;
2) II-XII rata płatne będą kwartalnie w terminie 21 (słownie: dwudziestu jeden) dni od daty zakończenia każdego kwartału kalendarzowego po dokonaniu przez Zamawiającego odbioru usług świadczonych przez Wykonawcę w danym kwartale.

4. Wynagrodzenie uważa się za zapłacone w dniu obciążenia rachunku bankowego Zamawiającego.

5. Kwota wynagrodzenia zawiera wszystkie koszty Wykonawcy związane z realizacją przedmiotu Umowy, a w tym podatki, należności, cła, opłaty oraz inne obciążenia, jakie mogą zostać nałożone, zgodnie z obowiązującymi przepisami. Wynagrodzenie obejmuje również koszty wszystkich czynności niezbędnych do przygotowania i prawidłowej realizacji przedmiotu umowy, nawet jeśli czynności te nie zostały wprost wyszczególnione.
6. Faktura VAT może zostać wystawiona po zatwierdzeniu, przez osobę upoważnioną przez Zamawiającego, protokołu, o którym mowa w § 5 ust. 1 umowy.
7. Wynagrodzenie będzie płatne na podstawie prawidłowo wystawionej przez Wykonawcę faktury VAT przelewem, na konto bankowe wskazane na fakturze, w terminie 21 dni od dnia dostarczenia Zamawiającemu faktury.
8. Za dzień zapłaty uważa się dzień przekazania polecenia przelewu na konto Wykonawcy.
9. W wypadku zwłoki w zapłacie wynagrodzenia Zamawiający zapłaci Wykonawcy odsetki ustawowe od należnej kwoty za każdy dzień zwłoki.
10. Wykonawca nie może bez zgody Zamawiającego dokonać cesji wierzytelności ani przenieść praw i obowiązków wynikających z niniejszej umowy na rzecz osób lub podmiotów trzecich.
11. Wykonawcy nie przysługuje żadne roszczenie o dodatkowe wynagrodzenie, nieprzewidziane w umowie, ani roszczenie o zwrot kosztów poniesionych w związku z wykonaniem umowy.

§ 8. Podwykonawstwo[3]

1. Wykonawcy, który w toku postępowania o udzielenie zamówienia publicznego, powoływał się na zasadach określonych w art. 22a ust. 1 ustawy na zasoby podwykonawcy lub podwykonawców, przysługuje prawo do zmiany albo rezygnacji z podwykonawcy lub podwykonawców w trakcie realizacji umowy po spełnieniu warunków określonych w ustępach poniższych i pod warunkiem przedstawienia, na żądanie Zamawiającego, oświadczenia, o którym mowa w art. 25a ust. 1 ustawy – Prawo zamówień publicznych lub oświadczenia bądź dokumentów potwierdzających brak podstaw wykluczenia wobec tego podwykonawcy.

[3] Paragraf o podwykonawstwie zostanie wprowadzony do umowy i będzie miał odpowiednie zastosowanie w sytuacji, gdy wykonawca, którego oferta zostanie wybrana, w toku postępowania o udzielenie zamówienia publicznego, powoływał się na zasadach określonych w art. 22a ust. 1 ustawy - Prawo zamówień publicznych na zasoby podwykonawcy lub podwykonawców.

2. W przypadku zmiany albo rezygnacji, o których mowa w ust. 1 powyżej, w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy - Prawo zamówień publicznych, Wykonawca jest obowiązany wykazać, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia te warunki w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia.

3. W celu spełnienia powyższego obowiązku Wykonawca, nie później niż 14 (czternaście) dni przed planowanym dokonaniem zmiany albo rezygnacji z podwykonawcy, o którym mowa w ustępie poprzedzającym, przedłoży Zamawiającemu dokumenty wykazujące spełnianie warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy, określonych przez Zamawiającego w SIWZ, z zachowaniem formy dokumentów tam określonych.

4. Zamawiający jest zobowiązany ocenić dokumenty wykazujące spełnianie przez podwykonawcę lub Wykonawcę samodzielnie warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy w terminie 14 (czternastu) dni od dnia doręczenia Zamawiającemu tych dokumentów przez Wykonawcę. Jeżeli w wyniku oceny przedłożonych dokumentów, Zamawiający stwierdzi, że zaproponowany podwykonawca nie spełnia warunków, lub Wykonawca samodzielnie nie spełnia ich w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia, Wykonawca:

    a) uprawniony będzie do realizacji umowy na dotychczasowych warunkach; albo

    b) zobowiązany będzie do zaproponowania innych podwykonawców, którzy w ocenie Zamawiającego spełnią warunki udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy albo, jeżeli w ocenie Zamawiającego, sam spełnia te warunki w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia, do osobistego wykonania umowy.

5. W przypadku niewywiązania się przez Wykonawcę z obowiązku określonego w ust. 2 - 4 powyżej i dokonania zmiany albo rezygnacji z podwykonawcy bez zachowania procedury określonej powyżej w niniejszym paragrafie, Zamawiającemu przysługuje prawo odstąpienia od umowy w terminie 30 (trzydziestu) dni od daty powzięcia wiadomości o tej okoliczności. Odstąpienie w takiej sytuacji traktowane jest jako odstąpienie od umowy z powodu okoliczności, za które odpowiada Wykonawca.

§ 9. Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne wynikłe z niewykonania lub nienależytego wykonania umowy w następujących przypadkach:
    1) w przypadku opóźnienia w wykonaniu poszczególnych świadczeń składających się na przedmiot umowy, w tym opóźnieniu w wykonaniu poszczególnych etapów dostawy, z zastrzeżeniem punktu 2 poniżej - w wysokości ……. zł (……., 00/100 złotych), za każdy rozpoczęty dzień opóźnienia;
    2) za niedochowanie obowiązku poufności - w wysokości 10 % łącznego wynagrodzenia brutto, za każdy przypadek naruszenia obowiązku poufności;
    3) w pozostałych przypadkach nie wykonania lub nienależytego wykonania przedmiotu umowy przez Wykonawcę, w szczególności w zakresie sposobu realizacji umowy oraz

zasad współpracy z Zamawiającym - w wysokości ……. zł (słownie: pięć tysięcy, 00/100 złotych), za każdy stwierdzony przypadek.

2. W przypadku odstąpienia od umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % łącznego wynagrodzenia brutto.
3. Kary umowne są niezależne od siebie i należą się w pełnej wysokości, nawet w przypadku, gdy w wyniku jednego zdarzenia naliczana jest więcej niż jedna kara (np. kara za opóźnienie i kara za odstąpienie).
4. Zapłata kar umownych nie zwalnia Wykonawcy od obowiązku wykonania umowy.
5. Wykonawca wyraża zgodę na potrącanie kar umownych z należnego mu wynagrodzenia lub zabezpieczenia należytego wykonania umowy, wedle wyboru Zamawiającego.
6. Jeżeli całkowite potrącenie nie będzie możliwe, Wykonawca zobowiązuje się do zapłacenia kar umownych w terminie 14 (słownie: czternastu) dni od otrzymania wezwania do zapłaty na rachunek wskazany w wezwaniu.
7. Jeżeli wysokość szkody przekracza wysokość kar umownych lub jeżeli szkoda powstała z przyczyn, dla których Strony nie zastrzegły kar umownych, Zamawiający może dochodzić odszkodowania uzupełniającego na zasadach ogólnych.

§ 10. Odstąpienie od umowy

1. Zamawiający może odstąpić od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy. Oświadczenie o odstąpieniu Zamawiający może złożyć w terminie 30 (słownie: trzydziestu) dni od powzięcia przez Zamawiającego wiadomości o tych okolicznościach.
2. W przypadku, o którym mowa w ustępie 1, Wykonawcy przysługuje wyłącznie wynagrodzenie należne z tytułu wykonania części umowy.
3. Niezależnie od możliwości odstąpienia od umowy na podstawie obowiązujących przepisów, Zamawiający zastrzega sobie prawo odstąpienia od umowy w następujących przypadkach:
    1) w przypadku nieprzystąpienia przez Wykonawcę do dokonania dostaw w terminach określonych w harmonogramie dostaw, po uprzednim wezwaniu przez Zamawiającego do dokonania dostawy w zakreślonym w wezwaniu terminie;
    2) w przypadku opóźnienia Wykonawcy w wykonywaniu obowiązków wynikających z umowy o łączny okres, co najmniej 20 (słownie: dwudziestu) dni;
    3) w innych przypadkach niewykonania lub nienależytego wykonania umowy pomimo bezskutecznego wezwania do naprawienia uchybień i ewentualnego wskazania terminu.

Odstąpienie od umowy z przyczyn wskazanych w punktach 1-3 powyżej będzie traktowane jako odstąpienie z przyczyn leżących po stronie Wykonawcy. Nie oznacza to braku możliwości uznania odstąpienia z innych przyczyn również za odstąpienie z przyczyn leżących po stronie Wykonawcy.

4. Prawo do odstąpienia od umowy przysługuje Zamawiającemu w terminie 30 (słownie: trzydziestu) dni liczonych od dnia powzięcia przez Zamawiającego informacji o wystąpieniu danej okoliczności uzasadniającej rozwiązanie umowy.
5. Odstąpienie od umowy, niezależnie od jej przyczyny, powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia.

6. W przypadku odstąpienia, Strony dokonają odbioru i odpowiedniego rozliczenia przedmiotu umowy do dnia jej rozwiązania. Wykonawca może jedynie żądać wynagrodzenia należnego z tytułu wykonania części umowy odebranej przez Zamawiającego bez uwag, zgodnie z warunkami określonymi w umowie.
7. Odstąpienie od umowy, niezależnie od przyczyn, nie pozbawia Zamawiającego prawa do dochodzenia kar umownych.

§ 11. Zmiany umowy

1. Zmiana umowy w stosunku do treści oferty złożonej przez Wykonawcę w trakcie postępowania o udzielenia zamówienia publicznego obejmującego przedmiot umowy dopuszczalna jest w szczególności w następujących przypadkach i zakresie:
    1) w przypadku zmiany stawki VAT dopuszcza się możliwość zmiany umowy w zakresie kwoty VAT i kwoty wynagrodzenia brutto;
    2) w przypadku innej zmiany powszechnie obowiązujących przepisów prawa dopuszcza się możliwość zmiany tych postanowień umowy, na które zmiana powszechnie obowiązujących przepisów prawa ma wpływ;
    3) w przypadku zaistnienia siły wyższej (§ 14 umowy) uniemożliwiającej wykonanie przedmiotu umowy zgodnie z terminami określonymi w umowie - dopuszcza się możliwość zmiany terminu realizacji umowy, nie dłużej jednak niż o czas trwania tych okoliczności;
    4) w przypadku wystąpienia niezależnych od Wykonawcy okoliczności, innych niż siła wyższa, uniemożliwiających wykonanie przedmiotu umowy zgodnie z terminami określonymi w umowie - dopuszcza się możliwość zmiany tych terminów, nie dłużej jednak niż o czas trwania tych okoliczności; postanowienia tego nie stosuje się w odniesieniu do terminów realizacji etapu I harmonogramu dostaw;
    5) w przypadku opóźnienia w innych projektach Zamawiającego, uniemożliwiającego realizację umowy zgodnie z określonym pierwotnie terminem lub powodującego, że realizowanie umowy zgodnie z określonym terminem jest nieracjonalne technicznie, organizacyjnie lub finansowo, dopuszcza się zmianę terminu realizacji przedmiotu umowy;
    6) w wypadku zaprzestania produkcji zaoferowanych przez Wykonawcę urządzeń infrastruktury sieciowej lub oprogramowania, bądź ich nieosiągalności z przyczyn, za które Wykonawca nie ponosi odpowiedzialności (w szczególności działania siły wyższej), dopuszcza się zastąpienie ich innymi równoważnymi urządzeniami lub oprogramowaniem, spełniającymi wymogi określone w OPZ, pod warunkiem, że nie spowoduje to zwiększenia ceny danego urządzenia lub oprogramowania.
2. Zmiany umowy, w rozumieniu art. 144 ustawy – Prawo zamówień publicznych, nie stanowią:
    1) zmiana wskazanych w umowie osób nadzorujących realizację przedmiotu umowy;
    2) zmiana danych teleadresowych Stron;
    3) zmiana danych rejestrowych Stron;
    4) zmiana miejsca dostawy, o którym mowa w § 2 ust. 1 umowy.
3. W przypadkach określonych w ust. 2 powyżej, dla skuteczności zmiany wystarczające jest niezwłoczne poinformowanie drugiej Strony na piśmie o zaistniałej zmianie.

§ 12. Zachowanie tajemnicy

1. Wykonawca zobowiązuje się do nieujawniania osobom trzecim, bez pisemnej zgody Zamawiającego, żadnych informacji, do których dostęp uzyskał w związku z realizacją umowy, pod rygorem zapłacenia kary umownej, o której mowa w § 9 ust. 1 pkt 2 umowy.
2. Obowiązek dochowania tajemnicy nie dotyczy informacji dostępnych publicznie oraz informacji żądanych zgodnie z obowiązującym prawem przez uprawnione organy.
3. Obowiązek nieujawniania informacji związanych z przedmiotem niniejszej umowy wiąże Strony także po wygaśnięciu lub rozwiązaniu umowy.
4. W ramach obowiązku zachowania tajemnicy Wykonawca zobowiązuje się w szczególności do zachowania w poufności, na zasadach określonych powyżej, wszelkich danych i informacji otrzymanych od Zamawiającego podczas udzielania Wykonawcy wytycznych przy realizacji świadczeń wynikających z przedmiotu umowy.
5. Obowiązek określony w ustępach 1-4 powyżej nie uchybia obowiązkom Stron wynikającym z przepisów prawa powszechnie obowiązującego w zakresie ochrony danych osobowych, w szczególności przepisom ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014.1182- t.j.).
6. Publiczne wykorzystanie informacji o realizowaniu umowy przez Wykonawcę, w tym w celach promocyjnych i marketingowych, wymaga wyraźnej, pisemnej zgody Zamawiającego i uzgodnienia z Zamawiającym treści takiej informacji.
7. Wykonawca zobowiązuje się powiadomić każdego swojego pracownika oraz ewentualnego podwykonawcę o obowiązku zachowania tajemnicy.

§ 13. Zabezpieczenie należytego wykonania umowy

1. Wykonawca wniósł na dzień zawarcia umowy zabezpieczenie należytego wykonania przedmiotu umowy w wysokości 5 % łącznego wynagrodzenia brutto, o którym mowa w § 7 ust. 1 umowy. Wymieniona kwota została wniesiona w postaci …….
2. Zabezpieczeniem, o którym mowa w ust. 1, objęty jest cały zakres realizacji przedmiotu umowy.
3. Zabezpieczenie, o którym mowa w ust. 1, służy pokryciu wszelkich roszczeń z tytułu niewykonania lub nienależytego wykonania umowy, w tym kar umownych oraz roszczeń odszkodowawczych z tytułu szkody jaką Zamawiający poniósł w związku z realizacją przedmiotu umowy.
4. Zamawiający dokona zwrotu zabezpieczenia zgodnie z zasadami i w terminach określonych w art. 151 ustawy – Prawo zamówień publicznych, przy czym kwota pozostawiona na zabezpieczenie roszczeń z tytuły rękojmi za wady wynosi 30% wysokości zabezpieczenia.

§ 14. Siła wyższa

1. Żadna ze Stron niniejszej umowy nie będzie ponosiła odpowiedzialności za niewykonanie lub nienależyte wykonanie swoich obowiązków umownych w przypadku wystąpienia siły wyższej i przez okres jej trwania.
2. Siła wyższa oznacza nadzwyczajny przypadek pozostający poza kontrolą Stron, działaniami lub powstrzymaniem się od działań przez Stronę, którego nie sposób było przewidzieć ani uniknąć, a który zaistniał po dniu podpisania niniejszej umowy i w okresie jej obowiązywania.
3. Obowiązkiem każdej ze Stron jest pisemne, bezzwłoczne, najpóźniej w ciągu 24 (słownie: dwudziestu czterech) godzin od momentu, w którym stanie się to możliwe, zawiadomienie

drugiej Strony o przypadku siły wyższej. Brak takiego zawiadomienia oznaczać będzie, że siła wyższa nie wystąpiła.

§ 15. Sposób porozumiewania się Stron

1. Wszystkie informacje przekazywane pomiędzy Wykonawcą a Zamawiającym w ramach realizacji umowy będą przesyłane, o ile umowa nie stanowi inaczej, pisemnie za pośrednictwem poczty lub kuriera lub drogą elektroniczną. Strony potwierdzą fakt ich otrzymania na żądanie drugiej Strony.
2. Informacje, o których mowa w ust. 1, należy przekazywać:
    1) Zamawiającemu na adres: Ministerstwo Spraw Zagranicznych 00-582 J.Ch. Szucha 23, tel. ……., mail: ……;
    2) Wykonawcy na adres: ..... .
3. W przypadku zmiany adresu do doręczeń, każda ze Stron umowy powiadomi o tym drugą Stronę na piśmie, z odpowiednim wyprzedzeniem. W przypadku niedopełnienia tego obowiązku doręczenia dokonane na poprzedni adres uznaje się za skuteczne.

§ 16. Postanowienia końcowe

1. W granicach wyznaczonych przez bezwzględnie obowiązujące przepisy prawa, nieważność jakiejkolwiek części niniejszej umowy, pozostaje bez wpływu na ważność jej pozostałej części. W przypadku zaistnienia takiej sytuacji Strony zastąpią takie postanowienia, ważnymi postanowieniami wywołującymi taki sam skutek gospodarczy.
2. Wykonawca odpowiada za działania lub zaniechania wszystkich osób i podmiotów, w tym podwykonawców, wykonujących umowę w jego imieniu lub na jego rzecz, jak za działania lub zaniechania własne.
3. Wszelkie spory mogące wynikać w związku z realizacją niniejszej Umowy będą rozstrzygane polubownie, a jeśli to nie będzie możliwe w terminie 45 (słownie: czterdziestu pięciu) dni od daty wszczęcia sporu, to poddane zostaną rozstrzygnięciu właściwemu dla siedziby Zamawiającego sądowi powszechnemu.
4. W sprawach nieuregulowanych niniejszą umową będą miały zastosowanie odpowiednie przepisy prawa, w szczególności ustawy Prawo zamówień publicznych oraz ustawy Kodeks cywilny.
5. Każda ze Stron umowy oświadcza, iż jest prawidłowo umocowana do jej zawarcia.
6. W przypadku rozbieżności lub sprzeczności pomiędzy treścią niniejszej umowy, a treścią załączników do umowy, pierwszeństwo ma treść umowy.
7. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
8. Umowa wchodzi w życie z dniem podpisania przez należycie upoważnionych do tego przedstawicieli obu Stron.
9. Następujące załączniki stanowią integralną część umowy:
    1) załącznik nr 1 – opis przedmiotu zamówienia;
    2) załącznik nr 2 – formularz rzeczowo-cenowy z oferty Wykonawcy;
    3) załącznik nr 3 – wzór protokołu odbioru.

Za Zamawiającego Za Wykonawcę

_____ _____

Data, podpis osoby upoważnionej Data, podpis osoby upoważnionej

Znak: BDG.741.016.2020

Załącznik nr 3 do umowy

nr ……

z dnia ……

Zatwierdza

……

Podpis i data

WZÓR PROTOKOŁU ODBIORU (CZĘŚCI) PRZEDMIOTU UMOWY

Strony niniejszym potwierdzają, że w dniu ……. dokonano odbioru:

1) ……;
2) ……;
3) …….;
4) ……. .

Zamawiający potwierdza, że dostawy wykonane przez Wykonawcę są zgodne z warunkami umowy nr …… z dnia……..

Uwagi:

……

……

……

Ze strony Zamawiającego: **Ze strony Wykonawcy**

……. **……**

(imię i nazwisko) (data) **(imię i nazwisko) (data)**

Wykonano w 1 egzemplarzu – dla Zamawiającego (kopia dla Wykonawcy).

Znak: BDG.741.016.2020
Załącznik nr 3 do SIWZ

Wykonawca:

……..
(pełna nazwa/firma, adres)

nr NIP/KRS ……..
reprezentowany przez:

……..
(imię, nazwisko osoby uprawnionej do reprezentacji Wykonawcy)

....., dnia ..... 2020 r.

FORMULARZ OFERTY

Odpowiadając na ogłoszenie o przetargu nieograniczonym pt. **Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych, znak sprawy BDG.741.016.2020**, zgodnie z wymaganiami określonymi w Specyfikacji Istotnych Warunków Zamówienia dla tego przetargu, składamy niniejszą ofertę.

1. Oferujemy wykonanie przedmiotu zamówienia **za cenę łączną** …….. **złotych brutto** (słownie:
   .....
   zł brutto),
   (należy wstawić kwotę zgodną z formularzem rzeczowo-cenowym)

   Oferujemy wsparcie dla dostarczanego sprzętu i oprogramowania w okresie …….. od zawarcia umowy.
   (należy wstawić okres zgodny z formularzem rzeczowo-cenowym, w latach lub miesiącach, minimum 12 miesięcy/1 rok)

2. Oświadczamy, że cena oferty została wyliczona zgodnie z załączonym formularzem rzeczowo-cenowym (załącznik nr 3a) i obejmuje pełen zakres zamówienia określony w Załączniku nr 1 oraz Załączniku nr 2 do SIWZ jak również wszystkie koszty towarzyszące wykonaniu zamówienia, w tym podatek VAT.
3. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (w tym z Istotnymi Postanowieniami Umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
4. Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres 60 dni, którego bieg rozpoczyna się wraz z upływem terminu składania ofert.
5. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
6. Oświadczam, iż zapoznałem się z informacjami zawartymi w pkt 19.3 SIWZ, będącymi realizacją obowiązku informacyjnego określonego w art. 13 RODO, dotyczącymi przetwarzania moich danych osobowych przez Zamawiającego, a także znane są mi wszystkie przysługujące mi prawa, o których mowa w art. 15-16 oraz 18 RODO.
7. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 i/lub art. 14

RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. (W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO Wykonawca usuwa treść oświadczenia z niniejszego ustępu przez jego wykreślenie).

8. Oświadczamy, że nie zamierzamy powierzyć wykonania części zamówienia podwykonawcom* / zamierzamy powierzyć wykonanie następujących części zamówienia podwykonawcom*:

   1) ……. .....

   część (zakres) zamówienia nazwa (firma) podwykonawcy

   1) ……. .....
   część (zakres) zamówienia (nazwa) (firma) podwykonawcy

9. Kategoria przedsiębiorstwa Wykonawcy**:

.....

(wpisać: mikro, małe lub średnie przedsiębiorstwo)

10. Niniejszym informujemy, iż informacje składające się na ofertę, zawarte w załączniku nr ….. do oferty stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji i jako takie nie mogą być ogólnie udostępnione.

11. Numer rachunku bankowego, na który zostanie zwrócone wadium wpłacone w pieniądzu

……

12. Do oferty załączamy następujące dokumenty:

   1) …….
   2) …….
   3) …….

<u>Adres Wykonawcy, na który należy przesyłać ewentualną korespondencję:</u>

.....

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

Osoba uprawniona do kontaktów z Zamawiającym

.....

/wymagany kwalifikowany podpis elektroniczny/

* niepotrzebne skreślić

** Zgodnie z zaleceniem Komisji Europejskiej z dnia 6.05.2003 r. dot. definicji mikroprzedsiębiorstw, małych i średnich przedsiębiorstw (Dz. Urz. UE L 124 z 20.05.2003, str. 36):

- mikroprzedsiębiorstwo – to przedsiębiorstwo zatrudniające mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 mln. EUR;
- małe przedsiębiorstwo – to przedsiębiorstwo zatrudniające mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 mln. EUR;
- średnie przedsiębiorstwa – to przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 mln. EUR lub roczna suma bilansowa nie przekracza 43 mln. EUR.

Załącznik nr 3a do SIWZ

FORMULARZ RZECZOWO – CENOWY

(załączony plik EXCEL)

Znak: BDG.741.016.2020

Załącznik nr 4 do SIWZ

……
(nazwa i adres Wykonawcy)

....., dnia ..... 2020 r.

OŚWIADCZENIE WYKONAWCY

o przynależności albo braku przynależności do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych (t. j. Dz. U. z 2019 roku, poz. 1843)

Przystępując do postępowania o udzielenie zamówienia publicznego pt. **Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych – znak sprawy BDG.741.016.2020,** oświadczam, że reprezentowany przeze mnie Wykonawca:

☐ nie należy do grupy kapitałowej[4] w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t. j. Dz. U. z 2019 r., poz. 369 ze zm.) z Wykonawcami, którzy złożyli odrębne oferty w przedmiotowym postępowaniu o udzielenie zamówienia *

☐ należy do grupy kapitałowej[5] w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t. j. Dz. U. z 2019 r., poz. 369 ze zm.)* z nw. Wykonawcami[6], którzy złożyli odrębne oferty w przedmiotowym postępowaniu o udzielenie zamówienia:

1. …….. (*należy podać nazwę (firmę) podmiotu i siedzibę*)
2. …….. (*należy podać nazwę (firmę) podmiotu i siedzibę*)

/wymagany kwalifikowany podpis elektroniczny/

* właściwe zaznaczyć znakiem X

[4] Zgodnie z art. 4 pkt 14 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t. j. Dz. U. z 2019 r., poz. 369 ze zm.) przez grupę kapitałową rozumie się wszystkich przedsiębiorców, który są kontrolowani w sposób bezpośredni lub pośredni przez jednego przedsiębiorcę, w tym również tego przedsiębiorcę.

[5] j.w.

[6] Wraz ze złożeniem oświadczenia o przynależności do tej samej grupy kapitałowej z Wykonawcą/ami, który/ży złożył/li odrębną/e ofertę/y, Wykonawca może przedstawić dowody, że powiązania z ww. Wykonawcą/ami nie prowadzą do zakłócenia konkurencji w przedmiotowym postępowaniu o udzielenie zamówienia.

Załącznik nr 5 do SIWZ

....., dnia ..... 2020 r.

Pełnomocnictwo

w postępowaniu o udzielenie zamówienia publicznego pt. **Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych – znak sprawy BDG.741.016.2020**

.....
(nazwa Wykonawcy)

z siedzibą .....
(adres)

zarejestrowany przez .....

pod numerem.....

reprezentowany przez: .....

.....

upoważnia .....
(dane osoby upoważnionej)

zamieszkałego w .....

.....

legitymującego się .....
(nazwa i numer dokumentu: dowodu osobistego, paszportu)

do występowania w imieniu Wykonawcy w postępowaniu, w tym:

1. podpisania i złożenia w imieniu Wykonawcy oferty wraz z załącznikami*
2. składania w imieniu Wykonawcy wszelkich oświadczeń woli i wiedzy oraz dokonywania czynności przewidzianych przepisami prawa takich jak poświadczanie kopii dokumentów za zgodność z oryginałem, zadawania pytań, składania wyjaśnień itp.*
3. zawarcia Umowy w wyniku udzielenia zamówienia*

/wymagany kwalifikowany podpis elektroniczny/

** niepotrzebne skreślić*

Załącznik nr 6 do SIWZ

Jednolity Europejski Dokument Zamówienia
(załączony w oddzielnym pliku)

/wymagany kwalifikowany podpis elektroniczny

Załącznik nr 7 do SIWZ

……
(nazwa i adres Wykonawcy)

....., dnia ..... 2020 r.

WYKAZ WYKONANYCH LUB WYKONYWANYCH DOSTAW

Przystępując do postępowania o udzielenie zamówienia publicznego na **Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo przesyłanych danych – znak sprawy BDG.741.016.2020**

oświadczam, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie reprezentowany przeze mnie Wykonawca należycie wykonał lub wykonuje następujące dostawy:

Lp.	**Zakres dostawy**	**Podmiot, na rzecz którego dostawy zostały wykonane lub są wykonywane** (nazwa, adres)	**Data wykonania usługi** Początek (dd/mm/rr) – Koniec (dd/mm/rr)	**Wartość dostawy (brutto w PLN)**
1.				
2.				
(…)				

Do niniejszego wykazu należy dołączyć dowody, o których mowa w pkt 8.4.1 SIWZ.

/wymagany kwalifikowany podpis elektroniczny/

Załącznik nr 8 do SIWZ

……., dnia …… 2020 r.

……
(nazwa i adres Wykonawcy)

OŚWIADCZENIE WYKONAWCY

Przystępując do postępowania o udzielenie zamówienia publicznego na **Zakup urządzeń infrastruktury sieciowej podnoszących niezawodność i bezpieczeństwo danych – znak sprawy BDG.741.016.2020** oświadczam, że:

1. W stosunku do reprezentowanego przeze mnie Wykonawcy nie wydano prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne,

   w przypadku wydania takiego wyroku lub decyzji – załączam dokumenty potwierdzające dokonanie płatności tych należności, wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności,

2. W stosunku do reprezentowanego przeze mnie Wykonawcy nie orzeczono tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne,

/wymagany kwalifikowany podpis elektroniczny/

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI

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

……. (miejscowość), dnia ……. r.

/wymagany kwalifikowany podpis elektroniczny/