Przedsiębiorstwo Wodociągów i Kanalizacji w Ząbkach Sp. z o.o.

DOKUMENTACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA (DIWZ)

Nazwa przedmiotu zamówienia:

Dostawa i uruchomienie NGFW z oprogramowaniem, serwera NAS oraz zarządzalnych urządzeń aktywnych sieci w ramach projektu: KPOD.05.10-CW.01-0001/25 Konkurs grantowy pn. "Cyberbezpieczne Wodociągi"

Ilość części w postępowaniu: JEDNA

Oznaczenie sprawy: PWIK- ZP / 14 / 2026

Zatwierdzam: PREZES ZARZĄDU Janusz Tomasz Czarnogórski

Ząbki, dnia 20 listopada 2026 r.

Oznaczenie sprawy: PWIK- ZP / 14 / 2026

I. Zamawiający: Przedsiębiorstwo Wodociągów i Kanalizacji w Ząbkach Sp. z o.o.

z siedzibą: ul. Hubalczyków 1, 05-091 Ząbki,
tel. 22 7-816-816, fax: 22 690-04-90
adres e-mail: przetargi@pwikzabki.pl
adres strony internetowej: https://platformazakupowa.pl/wodociagi_zabki
Godz. pracy: poniedziałek w godz. 10:00 – 18:00,
od wtorku do czwartku w godz. 08:00 – 16;00
piątek w godz. 07:00 – 15:00

II. Tryb udzielenia zamówienia

1. Niniejsze zamówienie jest sektorowym zamówieniem, którego wartość jest mniejsza niż kwota określona w art. 15 dyrektywy Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającej dyrektywę 2004/17/WE (Dz.Urz. UE L 94 z 28.03.2014, str. 243, z późn. zm.), zgodnie z informacją Prezesa Urzędu Zamówień Publicznych, ogłoszoną zgodnie z art. 3 ust 3 ustawy z dnia 11 września 2019 roku — Prawo zamówień publicznych (Dz.U. z 2024 r., poz. 1320 z późn. zm.), w związku z czym stosownie do art. 2 ust. 1 pkt 2 do jego udzielenia nie stosuje się przepisów tej ustawy.
2. Postępowanie o udzielenie niniejszego zamówienia prowadzone jest w trybie procedury zamkniętej do wielu Wykonawców, na podstawie Regulaminu udzielania zamówień publicznych w Przedsiębiorstwie Wodociągów i Kanalizacji w Ząbkach Sp. z o.o., zwanego dalej Regulaminem, z ogłoszeniem w Bazie Konkurencyjności oraz opcją składania wniosków o dopuszczenie do udziału w postępowaniu.

III. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa i uruchomienie firewalli NGFW, przełączników sieciowych, serwera NAS oraz oprogramowania do monitorowania infrastruktury informatycznej, w ramach projektu: KPOD.05.10-CW.01-0001/25 Konkurs grantowy pn. "Cyberbezpieczne Wodociągi" pod nazwą ,,Podniesienie cyberodporności systemów IT/OT PWiK Ząbki" dalej zwany „Projektem", realizowana na podstawie Umowy o powierzenie grantu o numerze KPOD.05.10-CW.01-001/25/0107/KPOD.05.10-CW.01-001/25/2026.
2. Ilości:
    a. NGFW typ 1 – 2 sztuki
    b. NGFW typ 2 – 3 sztuki
    c. Pakiet oprogramowania / licencji IPS typ 1 – 1 sztuka
    d. Pakiet oprogramowania / licencji IPS typ 2 – 1 sztuka
    e. Serwer NAS – 1 sztuka
    f. Switch zarządzalny – 10 sztuk
3. Opis przedmiotu zamówienia z zakresu dostawy i uruchomienia sprzętu komputerowego, zawarty jest w załącznikach do DIWZ.
4. Dostarczony sprzęt musi być fabrycznie nowy, nieużywany przed dniem dostawy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostawy, wolny od wad fizycznych i prawnych, a także pochodzić z oficjalnych kanałów dystrybucji.
5. Sprzęt musi posiadać deklarację zgodności UE wystawioną przez Producenta lub jego uprawnionego Przedstawiciela – jako załącznik do oferty Wykonawca złoży odpowiedni dokument potwierdzający spełnianie wymogu dla każdego z modeli serwerów oddzielnie.
6. Serwis sprzętu musi być realizowany bezpośrednio przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – jako załącznik do oferty Wykonawca złoży oświadczenie Producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez producenta.
7. W przypadku niewywiązywania się przez Wykonawcę lub Autoryzowanego Partnera Serwisowego Producenta z obowiązków gwarancyjnych, Producent przejmie na siebie wszelkie zobowiązania związane z serwisem - jako załącznik do oferty Wykonawca złoży oświadczenie Producenta serwera potwierdzające spełnienie tego warunku.

17. Pozostałe informacje:

1) Przedmiotem niniejszego postępowania nie jest zawarcie umowy ramowej;
2) Zamawiający nie dopuszcza składania oferty wariantowej;
3) Zamawiający nie dopuszcza składania ofert częściowych;
4) Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej;
5) Zamawiający nie przewiduje organizowania spotkania z Wykonawcami;
6) Zamawiający przewiduje udzielenie zamówień uzupełniających;

7) Zamawiający w zakresie świadczenia usług serwisowych dopuszcza możliwości powierzenia części zamówienia podwykonawcom (Autoryzowany Partner Producenta lub Producent).

Kod CPV:

32420000-3 (Urządzenia sieciowe),

48823000-3 (Serwery plików),

48219100-7 (Pakiety oprogramowania bramowego),

48730000-4 (Pakiety oprogramowania zabezpieczającego).

IV. Termin wykonania zamówienia

Termin realizacji zamówienia: **do 14 dni od daty podpisania umowy.**

W terminie 14 dni od poinformowania o wyborze oferty Wykonawca zobowiązany jest do podpisania umowy.

V. Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny spełnienia tych warunków:

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

1. Spełniają warunki udziału w postępowaniu dotyczące:

a) posiadania uprawnienia do wykonywania działalności lub czynności objętych niniejszym zamówieniem:

➔ Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać w sposób szczególny;

b) posiadania wiedzy i doświadczenia:

➔ Warunek ten zostanie spełniony, jeżeli Wykonawca wykaże* że:

➔ w okresie nie dłuższym niż 3 lata, zrealizował co najmniej dwie umowy o wartości minimum 200 tys. PLN netto na dostawę sprzętu komputerowego – Wykonawca złoży wykaz umów oraz referencje od Zamawiających,

* Wykonawca wykaże dostawy zrealizowane samodzielnie przez siebie, oznacza to, że Zamawiający nie uzna jako referencji Wykonawcy i poświadczeń wystawionych całościowo np. na grupę wykonawców, konsorcjum lub wykonawcę głównego obejmujących całość przedsięwzięcia / umowy / kontraktu, a uzna wyłącznie konkretny zakres faktycznego wkładu zrealizowanego przez Wykonawcę w danym zamówieniu, poświadczony przez przedstawiciela Inwestora. W związku z powyższym referencje powinny zawierać faktyczny zakres dostaw zrealizowanych przez danego Wykonawcę, ich wartość, czas i miejsce, oraz to, że zostały wykonane zgodnie z umową i prawidłowo ukończone.

c) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia:

➔ Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać w sposób szczególny;

d) sytuacji ekonomicznej i finansowej:

- ➔ warunek ten zostanie spełniony, jeżeli Wykonawca wykaże, że posiada opłaconą polisę, a w przypadku jej braku inny dokument potwierdzający, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na kwotę nie mniejszą niż 350 000,00 zł (słownie: trzysta pięćdziesiąt tysięcy złotych) wraz z dokumentem potwierdzającym opłacenie polisy.

2. Podlegają wykluczeniu z postępowania.

2.1 Z postępowania o udzielenie Zamówienia Sektorowego Podprogowego wyklucza się:

a) Wykonawców, którzy w ciągu ostatnich trzech lat przed dniem wszczęcia postępowania nie wykonali Zamówienia udzielonego im przez PWIK lub wykonali je nienależycie;
b) Wykonawców, którzy znajdują się w sporze z PWIK, w szczególności, jeżeli spór dotyczy dostaw, usług lub robót budowlanych wykonywanych przez danego Wykonawcę na rzecz PWIK;
c) Wykonawców, którzy nie złożyli wymaganych dokumentów, oświadczeń lub nie spełnili innych wymagań koniecznych dla udziału w postępowaniu określonych przez Zamawiającego;
d) Wykonawców, których upadłość bądź likwidację ogłoszono, lub w stosunku do których wszczęto postępowanie upadłościowe bądź likwidacyjne;

2.2 Informację o wykluczeniu wraz z uzasadnieniem Zamawiający przekazuje Wykonawcy.

3. W celu wspólnej realizacji zamówienia objętego niniejszym postępowaniem, zamawiający dopuszcza możliwość złożenia oferty wspólnej przez podmioty działające wspólnie. Każdy z warunków określonych w pkt. 1 winien spełniać co najmniej jeden z tych Wykonawców albo wszyscy ci Wykonawcy wspólnie, natomiast warunek dotyczący braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego – powinien spełniać każdy z Wykonawców samodzielnie.

4. Zamawiający przy ocenie ofert będzie się kierował regułą „spełnia" – „nie spełnia". Wykonawcy, którzy nie spełnią, choć jednego z warunków zostaną wykluczeni z postępowania, a ich oferty zostaną odrzucone.

5. Zamawiający odrzuca ofertę jeżeli:

a) jest niezgodna z DIWZ i nie da się poprawić omyłek w jej treści lub Wykonawca nie zgodził się na ich poprawienie;
b) jest niezgodna z przepisami prawa;
c) jej złożenie stanowi czyn nieuczciwej konkurencji zgodnie z zapisami Ustawy o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 Nr 153 poz. 1503 ze zmianami);
d) zawiera rażąco niską cenę w stosunku do przedmiotu Zamówienia Sektorowego Podprogowego.

Informację o odrzuceniu oferty wraz z uzasadnieniem Zamawiający przekazuje Wykonawcy, który ją złożył.

VI. Wykaz oświadczeń lub dokumentów, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełnienia warunków udziału w postępowaniu:

1. W zakresie wykazania spełniania przez Wykonawcę warunków, oprócz oświadczeń w formularzu postępowania należy przedłożyć:

1.1 **Wykaz dostaw** w zakresie niezbędnym do wykazania spełniania warunku wiedzy i doświadczenia, wykonanych w okresie ostatnich trzech lat przed upływem składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, z podaniem ich rodzaju i wartości, daty i miejsca wykonania oraz z załączeniem dokumentu potwierdzającego, że dostawy zostały zrealizowane – **Załącznik Nr 1**;

1.2 **Opłaconą polisę**, w przypadku jej braku inny dokument potwierdzający, że Wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia;

2. W zakresie potwierdzenia niepodlegania wykluczeniu z postępowania o udzielenie zamówienia:

2.1. **oświadczenia** o braku podstaw do wykluczenia – **aktywne pola w formularzu postępowania**;

3. Inne dokumenty:
Pełnomocnictwo do podpisania oferty musi być załączone do oferty, o ile nie wynika ono z przepisów lub innych dokumentów załączonych do oferty. Pełnomocnictwo musi być podpisane przez osoby uprawnione do reprezentowania Wykonawcy i określać jego zakres.

4. W przypadku składania oferty przez Wykonawców ubiegających się wspólnie, oświadczenie o spełnianiu każdego z warunków o których mowa rozdziale X niniejszej DIWZ pkt 1 składa co najmniej jeden z tych Wykonawców albo wszyscy ci Wykonawcy wspólnie. Natomiast dokumenty potwierdzające, że Wykonawca nie podlega wykluczeniu składa każdy z Wykonawców oddzielnie.
5. Wykonawca powołujący się przy wykazywaniu spełnienia warunków udziału w postępowaniu na potencjał innych podmiotów, przedkłada pisemne zobowiązanie innych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.

6. Oferta składana przez Wykonawców mających siedzibę lub miejsce zamieszkania poza terytorium Rzeczpospolitej Polskiej:

Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast wymaganego odpisu z właściwego rejestru albo zaświadczenia o wpisie do ewidencji działalności gospodarczej składa dokument lub dokumenty, wystawione zgodnie z prawem kraju, w którym ma siedzibę lub miejsce zamieszkania, zawierające dane aktualne na dzień składania ofert potwierdzające odpowiednio prawo Wykonawcy do występowania w obrocie prawnym i stwierdzające, że zakres jego działalności odpowiada profilowi zamówienia, że nie otwarto jego likwidacji ani nie ogłoszono upadłości, a także wskazujące osoby upoważnione do reprezentowania Wykonawcy.

7. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 z późn. zm.), które Wykonawca pragnie zastrzec przed dostępem dla innych uczestników postępowania, winny być wykazane w aktywnym polu formularza.

VII. Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

1. Osobami uprawnionymi przez Zamawiającego do kontaktów z Wykonawcami jest:
   a) Mirosław Sobiecki – przedmiot zamówienia - e-mail: przetargi@pwikzabki.pl
   b) Mirosław Sobiecki - dokumentacja przetargowa - e-mail: przetargi@pwikzabki.pl

2. Postępowanie prowadzone jest w języku polskim.

3. W postępowaniu o udzielenie zamówienia oświadczenia, wnioski, zawiadomienia oraz informacje, zamawiający i wykonawcy przekazują drogą elektroniczną za pośrednictwem www.platformazakupowa.pl.

4. Jeżeli zamawiający lub wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.

5. W przypadku braku potwierdzenia otrzymania wiadomości przez wykonawcę, zamawiający domniema, że pismo wysłane przez zamawiającego e-mail podany w ofercie przez wykonawcę, zostało mu doręczone w sposób umożliwiający zapoznanie się wykonawcy z treścią pisma.

6. Wszelką pisemną korespondencję do Zamawiającego, związaną z niniejszym postępowaniem należy kierować drogą elektroniczną za pośrednictwem www.platformazakupowa.pl

VIII. Wyjaśnienia i modyfikacje DIWZ

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści DIWZ lub jej zmianę. Zamawiający udziela odpowiedzi, jeżeli pisma Wykonawcy wpłynęły nie później niż na 3 dni przed terminem składania ofert, oraz w przypadkach gdy Zamawiający uzna, że odpowiedzi mogą mieć wpływ na wynik postępowania.

2. Zamawiający przekaże treść wyjaśnienia wszystkim wykonawcom, bez ujawnienia źródła zapytania, za pośrednictwem www.platformazakupowa.pl
3. Zamawiający nie przewiduje zebrania wszystkich wykonawców w celu wyjaśnienia treści DIWZ.

4. Zamawiający może w każdym czasie, przed upływem terminu składania ofert, dokonać zmiany treści DIWZ oraz terminu składania ofert. Informację o dokonanych zmianach Zamawiający zamieszcza za pośrednictwem www.platformazakupowa.pl.

IX. Wymagania dotyczące wadium

NIE DOTYCZY

X. Termin związania ofertą

1. Wykonawca pozostaje związany ofertą przez okres 60 dni

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

3. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

XI. Opis sposobu przygotowania ofert

1. Na ofertę składają się następujące dokumenty:
1) Aktywny formularz oferty na stronie www.platformazakupowa.pl/wodociagi_zabki zawierający oświadczenia Wykonawcy;
2) Wszystkie wymagane dokumenty wymienione w rozdziale VI niniejszej DIWZ;

2. Wykonawca zobowiązany jest przygotować ofertę zgodnie z wymaganiami DIWZ.

3. Załączniki muszą być podpisane kwalifikowanym podpisem elektronicznym przez osobę uprawnioną do składania oświadczeń woli w imieniu Wykonawcy.
4. Aktywny Formularz Oferty oraz załączniki zamieszczane w formie skanów należy wypełnić w języku polskim pod rygorem nieważności.
5. Wzory formularzy należy wypełnić ściśle według wskazówek określonych w DIWZ nie pomijając żadnego pola formularza. Zamawiający nie dopuszcza dokonywania w treści załączonych formularzy jakichkolwiek zmian ich treści.
6. Ofertę należy składać za pomocą e-platformy zakupowej Zamawiającego dostępnej pod adresem www.platformazakupowa.pl/wodociagi_zabki
7. Zeskanowane dokumenty takie jak referencje/uprawnienia, czyli elektroniczne kopie muszą być poświadczone przy użyciu kwalifikowanego podpisu elektronicznego przez osobę uprawnioną do składania oświadczeń woli w imieniu Wykonawcy.
8. Zamawiający zażąda przedstawienia oryginału lub notarialnie potwierdzonej kopii dokumentu wyłącznie wtedy, gdy przedstawiona przez Wykonawcę kopia dokumentu jest nieczytelna lub budzi wątpliwości, co do jej prawdziwości.
9. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę. Tłumaczenie nie jest wymagane, jeżeli Zamawiający wyraził zgodę.
10. Złożenie przez jednego Wykonawcę więcej niż jednej oferty lub oferty zawierającej rozwiązania alternatywne spowoduje jej odrzucenie.
14. Wykonawca wskaże w ofercie tę część zamówienia, której wykonanie powierzy podwykonawcom.

XII. Miejsce oraz termin składania i otwarcia ofert

1. Ofertę należy złożyć WYŁĄCZNIE za pomocą e-platformy zakupowej Zamawiającego dostępnej pod adresem www.platformazakupowa.pl/wodociagi_zabki w terminie **do dnia 30.11.2026 r. do godz. 09:55**

2. Wykonawca może przed upływem terminu do składania ofert, wycofać ofertę.

3. Wykonawca po upływie terminu składania ofert nie ma możliwości dokonania złożenia oraz wycofania oferty.

4. Odszyfrowanie i otwarcie ofert jest **niejawne** i nastąpi w siedzibie Przedsiębiorstwa Wodociągów i Kanalizacji w Ząbkach **w dniu 30.11.2026 r. po godz. 10:00**

XIII. Opis sposobu obliczenia ceny

1. Cenę należy podać jako cenę netto (cena brutto zostanie wyliczona automatycznie). Cena winna być wyrażona w złotych polskich do dwóch miejsc po przecinku. Cena za całość zamówienia będzie ceną ryczałtową.

2. Cenę oferty stanowi suma wartości wszystkich jej elementów, zawierająca wszystkie koszty niezbędne do wykonania zamówienia. Cena określona przez wykonawcę zostanie ustalona na okres ważności umowy i nie będzie podlegała zmianom. Wyklucza się możliwość roszczeń wykonawcy z tytułu błędnego skalkulowania ceny.

XIV. Informacja dotycząca walut obcych

Rozliczenia między Zamawiającym i Wykonawcą będą prowadzone w złotych polskich.

XV. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów.

1. Zamawiający uzna ofertę za ważną i przyjmie do szczegółowego rozpatrywania, jeżeli oferta spełnia wymagania określone niniejszą specyfikacją,
2. Stosowanie matematycznych obliczeń przy ocenie ofert, stanowi podstawową zasadę oceny ofert, które oceniane będą w odniesieniu do najkorzystniejszych warunków przedstawionych przez Wykonawców w zakresie kryteriów oceny.
3. Przy wyborze oferty Zamawiający kierował się będzie następującymi kryteriami i ich wagą:

   Cena (brutto) - 60%
   Okres gwarancji - 40%

   Ocena ofert zostanie przeprowadzona w oparciu o przedstawione wyżej kryteria oraz ich wagę. Oferty oceniane będą punktowo. Maksymalna ilość punktów jaką, po uwzględnieniu wagi, może osiągnąć oferta wynosi 100 pkt.

   W trakcie oceny ofert kolejno rozpatrywanym i ocenianym ofertom przyznane są punkty za powyższe kryteria według następujących zasad:

   Kryterium Cena (C) – znaczenie 60% (maksymalnie 60 pkt.)

$$C = \frac{\text{najniższa cena oferowana brutto spośród wszystkich badanych ofert}}{\text{cena badanej oferty brutto}} \times 60$$

Kryterium okres gwarancji (G) – znaczenie 40% (maksymalnie 40pkt.)

Sposób liczenia punktów okresu realizacji:

1) 1 rok - oferta otrzyma 0 punktów
2) 2 lata - oferta otrzyma 40 punktów

Sposób liczenia bilansu punktów:

Bilans punktów = C + G

4. Każda oferta, według podanego wyżej kryterium, podlega ocenie przez członków komisji przetargowej.

5. Oferta, która uzyska najwyższy bilans punktów według powyższego wzoru zostanie uznana przez Zamawiającego za najkorzystniejszą.

6. Zamawiający informuje, że w przypadku gdy najwyższy bilans punktów uzyska więcej niż jedna oferta, Zamawiający spośród tych ofert wybierze ofertę z najniższą ceną.

7. Zamawiający informuje, że w przypadku gdy najwyższy bilans punktów uzyska więcej niż jedna oferta i spośród tych ofert co najmniej dwie oferty będą zawierać identyczną najniższą cenę, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Wykonawcy składający oferty dodatkowe, nie mogą zaoferować ceny wyższej niż zaoferowane w złożonych ofertach.

8. Zamawiający przyzna zamówienie Wykonawcy, którego oferta odpowiada z wymaganiom określonym w DIWZ oraz została uznana za najkorzystniejszą.

9. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej w celu wyboru najkorzystniejszej oferty.

XVI. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. O wyborze oferty lub o unieważnieniu zamawiający zawiadomi niezwłocznie Wykonawców, którzy ubiegali się o udzielenie zamówienia.

2. W przypadku gdyby wyłoniona w prowadzonym postępowaniu oferta została złożona przez dwóch lub więcej Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego Zamawiający zażąda umowy regulującej współpracę tych podmiotów przed przystąpieniem do podpisania umowy o zamówienie publiczne.

3. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający wybierze ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej.

4. Podpisanie umowy z wybranym w ramach postępowania Wykonawcą nastąpi w terminie nie krótszym niż trzy dni lecz nie dłuższym niż siedem dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.

XVII. Projektowane postanowienia umowy

Projektowane postanowienia umowy stanowią - **Załącznik Nr 4 do DIWZ.**

Zamawiający przewiduje możliwość zmiany postanowień niniejszej umowy w przypadku zajścia okoliczności, których nie można było przewidzieć w chwili zawarcia umowy, a które powodują konieczność dostosowania umowy do nowych okoliczności,

w szczególności: awarii, klęski żywiołowej, stanu wyjątkowego, siły wyższej, zmiany obowiązujących przepisów.

XVIII. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenia zamówienia.

a) Wykonawca, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego zasad udzielania zamówień określonych w specyfikacji lub w *Regulaminie*, o którym mowa w pkt. II DIWZ oraz w przypadku zaniechania przez Zamawiającego obowiązkowych czynności, może przed zawarciem umowy poinformować Zamawiającego o nieprawidłowości czynności podjętych w toku postępowania lub nieprawidłowym zaniechaniu czynności, składając „Zażalenie" wskazujące czynność lub zaniechanie czynności Zamawiającego, której zarzuca się nieprawidłowość oraz zawierającą przedstawienie zarzutów z uzasadnieniem.

b) „Zażalenie" można złożyć w terminie 3 dni od dnia przesłania zawiadomienia o czynności Zamawiającego stanowiącej podstawę jej złożenia.

c) W przypadku wpłynięcia informacji dotyczącej nieprawidłowej treści ogłoszenia lub postanowień specyfikacji istotnych warunków zamówienia Zamawiający może przedłużyć termin składania ofert.

d) W przypadku wpłynięcia Zażalenia po upływie terminu składania ofert bieg terminu związania ofertą zostaje wstrzymany do czasu udzielenia odpowiedzi (rozstrzygnięcia) w sprawie zgłoszonych nieprawidłowości. O wtrzymaniu terminu Zamawiający zawiadamia wszystkich Wykonawców, którzy złożyli nieodrzucone oferty; w takiej sytuacji Zamawiający nie zawiera umowy do czasu rozstrzygnięcia zarzutów.

e) Zamawiający odpowiada na podniesione zarzuty, jeśli postanawia je uwzględnić (uznać). W takiej sytuacji w terminie 5 dni od otrzymania informacji przesyła rozstrzygnięcie (odpowiedź) Wykonawcy, który ja złożył. Zamawiający może również odpowiedzieć Wykonawcy składającemu informację oddalając podniesione zarzuty lub stwierdzając, że informacja pochodzi od podmiotu nieuprawnionego względnie złożono ją po upływie terminu określonego w specyfikacji. Brak rozstrzygnięcia w 5-dniowym terminie lub zawarcie umowy uznaje się za nieuwzględnienie podniesionych zarzutów.

f) W przypadku uwzględnienia zarzutów Zamawiający powtarza zakwestionowaną czynność lub dokonuje czynności bezprawnie zaniechanej niezwłocznie po rozstrzygnięciu. O powtórzeniu czynności lub wykonaniu czynności zaniechanych Zamawiający niezwłocznie zawiadamia wszystkich Wykonawców, którzy złożyli nieodrzucone oferty.

g) Od rozstrzygnięcia w sprawie podniesionych w informacji zarzutów albo braku ich rozpatrzenia w terminie przez Zamawiającego nie przysługuje odwołanie ani skarga do Sądu. Decyzja Zamawiającego w tej sprawie jest ostateczna.

XIX. Ochrona Danych Osobowych

1. Na potrzeby realizacji niniejszej Umowy Strony jako niezależni administratorzy danych udostępniać będą sobie nawzajem dane osobowe swoich reprezentantów lub przedstawicieli wskazanych w Umowie oraz innych osób w związku z realizacją Umowy w zależności od potrzeb wynikających z postanowień niniejszej Umowy, obejmujące następujące kategorie odnośnych danych: dane identyfikacyjne (m.in. imię i nazwisko, stanowisko, miejsce zatrudnienia, ewentualne nieobecności w pracy), kontaktowe (m.in. służbowy adres e-mail, numer telefonu, miejsce wykonywania pracy).

2. Strony zobowiązują się do poinformowania osób wymienionych w ust. 1 w terminie najpóźniej miesiąca po pozyskaniu danych osobowych lub przy pierwszej komunikacji z osobą, której dane dotyczą o konieczności przekazania ich danych na potrzeby realizacji Umowy, w tym o celu i zakresie przekazania danych, wskazanych w ust. 4-12 oraz źródle pozyskania danych osobowych.
3. Każda ze Stron zobowiązuje się do zabezpieczenia danych osobowych poprzez podjęcie odpowiednich środków technicznych i organizacyjnych wymaganych obowiązującymi przepisami prawa w zakresie ochrony danych osobowych, jak też ponosi wszelką odpowiedzialność za szkody wyrządzone w związku z przetwarzaniem danych osobowych.
4. Administratorem danych osobowych w rozumieniu art. 4 pkt 7 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 – zwane dalej „RODO"), przekazanych PWiK na potrzeby zawarcia i realizacji Umowy jest Przedsiębiorstwo Wodociągów i Kanalizacji w Ząbkach sp. z o.o. (PWiK), ul. Hubalczyków 1, 05-091 Ząbki, tel. 22 781-68-16.
5. W PWiK został wyznaczony Inspektor ochrony danych – P. Radosław Wasilewski, z którym można się skontaktować poprzez email daneosobowe@zabki.pl, telefonicznie 783-220-250 lub pisemnie na adres PWiK, ul. Hubalczyków 1, 05-091 Ząbki.
6. Zebrane dane osobowe będą przetwarzane w celach związanych z zawarciem i realizacją Umowy, jej obsługą oraz ewentualnym dochodzeniem lub odpieraniem roszczeń z niej wynikających, jak też w związku z wypełnieniem obowiązków prawnych ciążących na PWiK. Dane wskazane w ust. 1 zostały pozyskane przez PWiK od podmiotu, będącego Stroną niniejszej Umowy.
7. Podstawą prawną przetwarzania przez PWiK danych osobowych przekazanych przez drugą Stronę w celach wskazanych powyżej jest: wypełnianie obowiązków prawnych ciążących na PWiK, zgodnie z art. 6 ust. 1 lit. c RODO związanych m. in. z przepisami podatkowymi oraz przepisami o rachunkowości.
8. Dane osobowe przekazane PWiK mogą być przekazywane następującym kategoriom odbiorców:
   a) podmiotom przetwarzającym dane osobowe na zlecenie PWiK, w tym m.in. obsługującym systemy informatyczne wykorzystywane na potrzeby realizacji Umowy, świadczących usługi prawne, archiwizacyjne,
   b) podmiotom świadczącym usługi na rzecz danej Strony, w tym kurierom i firmom pocztowym (w związku z koniecznością dokonania zawiadomień określonych w Umowie), doradcom prawnym i finansowym oraz audytorom Stron (w związku ze świadczeniem usług doradztwa przy zawarciu, wykonaniu i egzekucji roszczeń wynikających z Umowy), przy czym takie podmioty przetwarzają dane na podstawie Umowy z PWiK i wyłącznie zgodnie z jej poleceniami. Dane mogą być także udostępniane podmiotom uprawnionym na podstawie prawa, w tym organom uprawnionym do kontrolowania PWiK.

9. Dane przetwarzane będą przez czas realizacji Umowy, a po jej zakończeniu przez czas związany z wygaśnięciem roszczeń związanych z Umową oraz przez czas zastrzeżony przepisami prawa, w tym przepisów o archiwizacji, przepisów podatkowych i przepisów dotyczących sprawozdawczości finansowej.
10. Każda osoba, której dane osobowe zostaną udostępnione pomiędzy Stronami w związku z zawarciem i realizacją Umowy ma prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania oraz prawo wniesienia sprzeciwu z przyczyn związanych z jej szczególna sytuacją, w przypadku, kiedy PWiK przetwarza dane w oparciu o swój prawnie uzasadniony interes. Sprzeciw taki można wyrazić w dowolnym momencie na adres poczty elektronicznej daneosobowe@zabki.pl lub pisemnie na adres PWiK, ul. Hubalczyków 1, 05-091 Ząbki.
11. Każda osoba ma również prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
12. Dane osobowe nie będą profilowane i nie będą służyły zautomatyzowanemu podejmowaniu decyzji.

XX. Postanowienia końcowe

W innych sprawach nieuregulowanych w DIWZ mają zastosowanie odpowiednie przepisy prawa polskiego oraz Regulaminu udzielania zamówień publicznych w Przedsiębiorstwie Wodociągów i Kanalizacji w Ząbkach Sp. z o.o. (Zarządzenie Nr 29/2011 Prezesa Zarządu z dnia 29. 07. 2011 r.).

XXI. Załączniki do DIWZ

Załączniki składające się na integralną cześć niniejszej DIWZ:
1) Załącznik Nr 1 - Wykaz dostaw;
2) Załącznik Nr 2 - Lista podmiotów należących do tej samej grupy kapitałowej;
3) Załącznik Nr 3 - Zobowiązanie do oddania do dyspozycji niezbędnych zasobów;
4) Załącznik Nr 4 - proponowane postanowienia umowy.
5) Załącznik Nr 5 – specyfikacje dostaw
9) Załącznik Nr 9 – specyfikacja zakresu uruchomienia.

Załącznik Nr 1 do DIWZ
PWIK- ZP/14/2026

.....
/Pieczątka adresowa Wykonawcy/

WYKAZ DOSTAW

Składając ofertę w przetargu na ***Dostawa i uruchomienie NGFW z oprogramowaniem, serwera NAS oraz zarządzalnych urządzeń aktywnych sieci w ramach projektu: KPOD.05.10-CW.01-0001/25 Konkurs grantowy pn. "Cyberbezpieczne Wodociągi"*** oświadczam, że moja firma zrealizowała w ciągu ostatnich ..... lat zrealizowała następujące zamówienia:

Lp.	Rodzaj zamówienia	Całkowita wartość	Czas realizacji - początek	Czas realizacji –Zakończenie	Nazwa Zamawiającego	Uwagi

Uwaga: Należy dołączyć dowody potwierdzające, że każda z wykazanych dostaw została wykonana i prawidłowo ukończona. W przypadku gdy zamawiający jest podmiotem, na rzecz którego dostawy wskazane w wykazie zostały wcześniej wykonane, wykonawca nie ma obowiązku przedkładania dowodów.

.....
(Miejscowość, data)

.....
(podpis upoważnionego przedstawiciela)

Załącznik Nr 2 do DIWZ
PWIK- ZP/14/2026

.....
/Pieczątka adresowa firmy/

Lista podmiotów należących do tej samej grupy kapitałowej.

Przystępując do postępowania o udzielenie zamówienia na ***Dostawa i uruchomienie NGFW z oprogramowaniem, serwera NAS oraz zarządzalnych urządzeń aktywnych sieci w ramach projektu: KPOD.05.10-CW.01-0001/25 Konkurs grantowy pn. "Cyberbezpieczne Wodociągi"***, *reprezentując Wykonawcę*

.....

(nazwa wykonawcy)

składamy listę podmiotów, razem z którymi należymy do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. nr 2021 poz. 275 z późn. zm.).

Lp.	Nazwa podmiotu	Adres podmiotu
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
.....		

.....
(miejscowość, data)

.....
podpis osoby uprawnionej do reprezentowania wykonawcy

.....
/Pieczęć firmowa Wykonawcy/

Załącznik Nr 3 do DIWZ
PWIK- ZP/14/2026

ZOBOWIĄZANIE
do oddania do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia

.....
(nazwa i adres Wykonawcy – podmiotu oddającego do dyspozycji zasoby)

zobowiązuję/my się do oddania na rzecz

.....
(nazwa i adres Wykonawcy, któremu inny podmiot oddaje do dyspozycji zasoby)

do dyspozycji niezbędne zasoby[1].....

.....
(zakres udostępnianych zasobów)

na okres .....
(okres na jaki udostępniane są zasoby)

Sposób wykorzystania ww. zasobów przez wykonawcę przy wykonywaniu zamówienia[2]:
.....

.....

Charakteru stosunku, jaki będzie łączył nas z wykonawcą[3]:
.....

.....

.....
(miejscowość, data)

.....
(podpis upoważnionego przedstawiciela)

---

1. Zakres udostępnianych zasobów niezbędnych do potwierdzenia spełniania warunku:
   - wiedza i doświadczenie
   - potencjał techniczny (rodzaj, nazwa, model)
   - osoby zdolne do wykonania zamówienia (imię i nazwisko, funkcja lub zakres wykonywanych czynności)
   - zdolności finansowe i ekonomiczne
2. np. podwykonawstwo, konsultacje, doradztwo. W sytuacji gdy przedmiotem udzielenia są zasoby nierozerwalnie związane z podmiotem ich udzielającym, niemożliwe do samodzielnego obrotu i dalszego udzielenia ich bez zaangażowania tego podmiotu w wykonanie zamówienia, taki dokument powinien zawierać wyraźne nawiązanie do uczestnictwa tego podmiotu w wykonaniu zamówienia.
3. np. umowa cywilno-prawna, umowa o współpracy.

PROPONOWANE POSTANOWIENIA UMOWY

zawarta w dniu ..... 2026 r. pomiędzy:

Przedsiębiorstwo Wodociągów i Kanalizacji w Ząbkach Sp. z o.o., z siedzibą w Ząbkach, Hubalczyków 1, 05-091 Ząbki, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XIV Wydział Gospodarczy Krajowego Rejestru pod numerem KRS: 0000321312, NIP: 1251516782, REGON: 141684012, posiadającą kapitał zakładowy w wysokości 16.464.000,00 zł którą reprezentuje Janusz Tomasz Czarnogórski – Prezes Zarządu,
zwaną w dalszej treści Umowy **„Zamawiającym”,**

a

..... z siedzibą w ..... przy ul. ..... wpisanym/ną do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy .....Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem: ...../ wpisanym/ną Centralnej Ewidencji i Informacji o Działalności Gospodarczej, posiadającym/cą NIP..... REGON ..... lub (imię i nazwisko), adres , PESEL
reprezentowanym/ną przez:
.....
zwanym dalej **„Wykonawcą”.**

łącznie zwanymi „STRONAMI”.

Zgodnie z wynikiem przeprowadzonego postępowania o udzielenie sektorowego zamówienia, którego wartość jest mniejsza niż kwota określona w art. 15 dyrektywy Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającej dyrektywę 2004/17/WE (Dz.Urz. UE L 94 z 28.03.2014, str. 243, z późn. zm.), zgodnie z informacją Prezesa Urzędu Zamówień Publicznych, ogłoszoną zgodnie z art. 3 ust 3 ustawy z dnia 11 września 2019 roku — Prawo zamówień publicznych (Dz.U. z 2024 r., poz. 1320 z późn. zm.), Strony zawierają umowę następującej treści:

§ 1.
PRZEDMIOT UMOWY

1. Przedmiotem zamówienia jest dostawa i uruchomienie firewalli NGFW, przełączników sieciowych, serwera NAS oraz oprogramowania do monitorowania infrastruktury informatycznej, w ramach projektu: KPOD.05.10-CW.01-0001/25 Konkurs grantowy pn. “Cyberbezpieczne Wodociągi” pod nazwą „Podniesienie cyberodporności systemów IT/OT PWiK Ząbki” dalej zwany „Projektem”, realizowana na podstawie Umowy o powierzenie grantu o numerze KPOD.05.10-CW.01-001/25/0107/KPOD.05.10-CW.01-001/25/2026 w następujących ilościach
   A. NGFW typ 1 – 2 sztuki
   B. NGFW typ 2 – 3 sztuki
   C. Pakiet oprogramowania / licencji IPS typ 1 – 1 sztuka
   D. Pakiet oprogramowania / licencji IPS typ 2 – 1 sztuka
   E. Serwer NAS – 1 sztuka
   F. Switch zarządzalny – 10 sztuk
2. Przedmiot Umowy realizowany jest w ramach projektu grantowego „Cyberbezpieczne Wodociągi”, realizowanego w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo”, finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) oraz Instrumentu na rzecz Odbudowy i Zwiększania Odporności (RRF) – NextGenerationEU, zgodnie z Umową o powierzenie grantu nr KPOD.05.10-CW.01-001/25/0107/KPOD.05.10-CW.01-001/25/2026.

3. Przedmiot Umowy obejmuje w szczególności realizację dostaw, oraz czynności niezbędnych do osiągnięcia celu zamówienia, w tym wszelkich prac wdrożeniowych, konfiguracyjnych, integracyjnych, konsultacyjnych, serwisowych oraz dokumentacyjnych, o ile są wymagane dla prawidłowej i kompletnej realizacji przedmiotu Umowy.
4. Szczegółowy zakres, wymagania funkcjonalne i techniczne, warunki realizacji oraz parametry jakościowe przedmiotu Umowy określa - Dokumentacja Istotnych Warunków Zamówienia („DIWZ") wraz z załącznikami, zwany dalej DIWZ, stanowiący integralną część niniejszej Umowy.
5. Wykonawca oświadcza, że zapoznał się z dokumentacją zamówienia, w szczególności z DIWZ, oraz że posiada wiedzę, zasoby techniczne, organizacyjne i kadrowe niezbędne do należytej realizacji przedmiotu Umowy, bez konieczności ponoszenia przez Zamawiającego dodatkowych kosztów poza wynagrodzeniem określonym w Umowie.

§ 2
OBOWIĄZKI STRON

1. Zamawiający zobowiązuje się do zapewnienia Wykonawcy stosownych upoważnień, dostępów oraz zgód niezbędnych do realizacji przedmiotu Umowy, a działania podejmowane przez Wykonawcę w granicach udzielonego umocowania uznaje za wykonywane za wiedzą i zgodą Zamawiającego.
2. Wykonawca jest zobowiązany w szczególności do:
   1) Realizacji przedmiotu zamówienia zgodnie z DIWZ oraz złożoną ofertą z zachowaniem należytej jakości i staranności;
   2) Umożliwienia Zamawiającemu bieżącego weryfikowania należytego wykonywania zamówienia oraz udzielania Zamawiającemu niezbędnych informacji;
   3) Współpracy w Zamawiającym, w zakresie umożliwienia spełnienia przez Zamawiającego obowiązków Grantobiorcy, w szczególności w zakresie:
      a) trwałości projektu,
      b) wymagań cyberbezpieczeństwa,
      c) zasad DNSH,
      d) obowiązków dokumentacyjnych,
      e) obowiązków kontrolnych,
      f) wymagań systemu s46,
      g) monitoringu moje.cert.pl,
      h) obowiązków promocyjnych KPO,
      i) archiwizacji dokumentacji projektowej;
   4) Informowania Zamawiającego o wszystkich znanych Wykonawcy okolicznościach mogących wpłynąć na realizację przedmiotu zamówienia;
   5) Niezwłocznego udostępniania do wglądu na żądanie Instytucji Pośredniczącej oraz innych podmiotów uprawnionych do kontroli wszelkich dokumentów związanych z realizacją przedmiotu zamówienia dotyczącego realizowanego Projektu;
   6) Realizacji przedmiotu zamówienia z zachowaniem wszelkich zasad bezpieczeństwa i higieny pracy;
   7) Realizacji przedmiotu zamówienia z poszanowaniem zasad:
      a) zasady równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami,
      b) zasady równości kobiet i mężczyzn,
      c) zasady zrównoważonego rozwoju,
      d) zasady „nie czyń poważnych szkód" (DNSH - Do No Significant Harm) oraz z przestrzeganiem Karty Praw Podstawowych Unii Europejskiej (KPP) oraz Konwencji ONZ o Prawach Osób Niepełnosprawnych (KPON);
   8) Stosowania przepisów o ochronie danych osobowych, zgodnie z rozporządzeniem 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) oraz z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych;
   9) Udziału w czynnościach kontrolnych, audytowych i wyjaśniających prowadzonych przez CPPC, NASK, instytucje krajowe, unijne oraz inne podmioty uprawnione do kontroli projektu;
   10) Zapewnienia kompatybilności wdrażanych rozwiązań z wymaganiami moje.cert.pl oraz systemu s46;
   11) Współpracy przy realizacji obowiązków związanych z utrzymaniem efektów projektu przez okres 3 lat od zakończenia projektu.

3. Wykonawca ponosi wobec Zamawiającego pełną odpowiedzialność z tytułu niewykonania lub nienależytego wykonania obowiązków wskazanych powyżej.
4. Wykonawca zobowiązany jest przekazać Zamawiającemu najpóźniej w dniu odbioru końcowego kompletną dokumentację powdrożeniową.
5. Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do dokumentacji powdrożeniowej.

§ 3.
ODPOWIEDZIALNOŚĆ WYKONAWCY

1. Wykonawca oświadcza i gwarantuje, że osoby uczestniczące w realizacji przedmiotu Umowy posiadają wszelkie wymagane uprawnienia, kwalifikacje, wiedzę specjalistyczną oraz doświadczenie zawodowe niezbędne do należytego i terminowego wykonania Umowy.
2. Wykonawca zobowiązuje się do realizacji przedmiotu Umowy z najwyższą starannością, zgodnie z profesjonalnym charakterem prowadzonej działalności, obowiązującymi standardami branżowymi oraz na najwyższym poziomie merytorycznym i jakościowym.
3. Wykonawca zobowiązuje się do niezwłocznego, nie później jednak niż w terminie 2 (dwóch) dni kalendarzowych od dnia powzięcia informacji, poinformowania Zamawiającego o wszelkich okolicznościach, zdarzeniach lub ryzykach, które mają lub mogą mieć wpływ na prawidłowe wykonanie Umowy, w szczególności w zakresie terminów realizacji lub zakresu rzeczowego przedmiotu Umowy.
4. Wykonawca ponosi pełną i wyłączną odpowiedzialność za prawidłowość, jakość, kompletność oraz terminowość wykonania przedmiotu Umowy.
5. Wykonawca oświadcza, że dysponuje odpowiednim potencjałem technicznym, organizacyjnym oraz kadrowym, umożliwiającym prawidłową i terminową realizację przedmiotu Umowy.
6. Wykonawca zobowiązuje się, że osoby wskazane imiennie w ofercie oraz dokumentach złożonych na potwierdzenie spełniania warunków udziału w postępowaniu będą faktycznie uczestniczyć w realizacji przedmiotu Umowy. Zmiana tych osób wymaga uprzedniej pisemnej zgody Zamawiającego oraz wykazania, że osoba zastępująca spełnia wymagania co najmniej równoważne osobie zastępowanej.

§4. TERMINY

1. Przedmiot umowy będzie realizowany w terminie ..... (zgodnie z terminem realizacji wskazanym przez Wykonawcę w Formularzu oferty), z zastrzeżeniem możliwości jego aktualizacji w trakcie realizacji projektu.
2. Zamawiający zastrzega możliwość zmiany harmonogramu realizacji na skutek wystąpienia okoliczności niezależnych i niezawinionych przez Zamawiającego, w tym zmian w harmonogramie realizacji projektu lub potrzeb uczestników projektu.
3. Wykonawca zobowiązany jest realizować Umowę w sposób zapewniający terminowe rozliczenie projektu grantowego przez Zamawiającego zgodnie z Umową o powierzenie grantu

§ 5.
WYNAGRODZENIE

1. Całkowite maksymalne wynagrodzenie Wykonawcy z tytułu wykonania umowy wynosi ..... zł netto, (podatek VAT - ...% w wysokości ..... zł), ... zł brutto.
2. Faktura, może zostać wystawiona po pełnej realizacji przedmiotu zamówienia oraz potwierdzeniu przez Strony.
3. Strony zgodnie postanawiają, że potwierdzeniem realizacji przedmiotu umowy będzie podpisany protokół odbioru przedmiotu zamówienia bez zastrzeżeń.
4. Strony postanawiają, że faktury VAT będą wystawiane zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług oraz z przepisami regulującymi funkcjonowanie Krajowego Systemu e-Faktur (KSeF), w tym przepisami dotyczącymi trybów szczególnych (offline/awaryjnych), o ile mają zastosowanie.
5. Przez fakturę ustrukturyzowaną strony rozumieją fakturę wystawioną w KSeF, która uzyskuje walor

faktury ustrukturyzowanej z chwilą nadania jej numeru identyfikującego w KSeF (numer KSeF).

6. Zamawiający zapewnia możliwość odbioru ustrukturyzowanych faktur elektronicznych za pośrednictwem KSeF.
7. Zamawiający zastrzega, że płatność nastąpi w terminie 14 dni na podstawie prawidłowo wystawionej faktury VAT, za którą strony uznają fakturę wystawioną zgodnie z przepisami prawa oraz prawidłową pod względem formalnym i rachunkowym, a także zawierającą w swojej treści nr umowy. Jeżeli faktura nie zawiera danych niezbędnych do jej przyporządkowania do umowy (w szczególności numeru umowy) albo zawiera błędy rachunkowe lub formalne uniemożliwiające dokonanie płatności, termin płatności biegnie od dnia otrzymania faktury korygującej lub faktury wystawionej prawidłowo.
8. Wykonawca nie ma prawa zbywania wierzytelności wynikających z niniejszej Umowy osobom trzecim bez pisemnej zgody Zamawiającego, pod rygorem nieważności.

1. Wykonawca odpowiada za pełną kompatybilność i poprawność licencyjną wszystkich dostarczonych komponentów oprogramowania.

§ 6.
KARY UMOWNE

1. W przypadku nieprzystąpienia do wykonania umowy zgodnie z harmonogramem Zamawiający będzie miał prawo do odstąpienia od Umowy oraz prawo żądać od Wykonawcy zapłaty kary umownej.
2. Zamawiający wprowadzi kary umowne w następujących wypadkach i wysokościach:
   1) w przypadku odstąpienia od Umowy w całości z przyczyn leżących pod stronie Wykonawcy – w wysokości 10 % Wynagrodzenia brutto;
   2) w przypadku odstąpienia od Umowy w części, z przyczyn leżących po stronie Wykonawcy – w wysokości 10 % części Wynagrodzenia należnego brutto za niewykonaną część Przedmiotu Umowy;
   3) za wykonanie przedmiotu umowy niezgodnie z umową i opisem przedmiotu zamówienia, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 3 % wartości wynagrodzenia brutto należnego za zrealizowaną część, za każdy stwierdzony przypadek.
   4) za zwłokę w realizacji przedmiotu Umowy — 0,2% wynagrodzenia brutto za każdy dzień zwłoki;
   5) za brak przekazania dokumentacji powdrożeniowej — 1% wynagrodzenia brutto za każdy przypadek;
   6) za naruszenie obowiązków bezpieczeństwa informacji — 5% wynagrodzenia brutto za każdy stwierdzony przypadek.
3. Niezależnie od naliczenia kar umownych, Zamawiającemu przysługuje prawo dochodzenia na zasadach ogólnych odszkodowania przewyższającego wysokość kar umownych do wartości poniesionej przez Zamawiającego szkody.
4. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne Przedmiotu Umowy lub jakiejkolwiek jego części, a w szczególności za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej, w tym w szczególności za nieprzestrzeganie przepisów ustawy o prawie autorskim i prawach pokrewnych, w związku z realizacją Przedmiotu Umowy.
5. W przypadku wystąpienia przez osoby trzecie z roszczeniami związanymi z realizacją Przedmiotu Umowy, Wykonawca zobowiązuje się do współdziałania z Zamawiającym oraz do podjęcia niezbędnych działań w celu ochrony interesów Zamawiającego.
6. Naliczone przez Zamawiającego kary umowne mogą być dochodzone kumulatywnie. Kary naliczone do dnia odstąpienia od Umowy są należne niezależnie od kary za odstąpienie.
7. Łączna wysokość kar umownych naliczonych przez Zamawiającego nie przekroczy równowartości 30 % Wynagrodzenia.

§ 7.
ODSTĄPIENIE OD UMOWY

1. Poza przypadkami przewidzianymi przepisami prawa, Zamawiający ma prawo odstąpić od Umowy w całości lub w części w następujących przypadkach:
   1) Wykonawca w sposób nienależyty wykonuje zobowiązania umowne i pomimo uprzedniego dwukrotnego wezwania do zaprzestania tych naruszeń nie rozpoczął należytego wykonania

Umowy.

2) Stwierdzenia braku wymaganej dokumentacji z realizacji przedmiotu umowy.

2. Odstąpienie od Umowy powinno nastąpić w formie pisemnej, w terminie 14 dni od dnia powzięcia przez Zamawiającego informacji o zaistnieniu okoliczności uzasadniającej złożenie takiego oświadczenia, z podaniem przyczyny oświadczenia.
3. Strony postanawiają, iż w przypadku odstąpienia od Umowy, po rozpoczęciu realizacji Umowy, odstąpienie zarówno na podstawie postanowień umownych, jak również przepisów ustawy, będzie miało skutek *ex nunc* – będzie dotyczyło niewykonanej części Przedmiotu Umowy.
4. Odstąpienie od Umowy nie pozbawia Zamawiającego prawa dochodzenia kar umownych i innych odszkodowań za szkody wynikłe w związku z niewykonaniem lub nienależytym wykonaniem Umowy przez Wykonawcę.
5. Oświadczenie o odstąpieniu od umowy Zamawiający może złożyć nie później niż w terminie ostatniego dnia obowiązywania umowy

§ 8.
ZMIANY UMOWY

1. Zamawiający na podstawie pkt 3.2.4 ppkt 4 lit. a Wytycznych dotyczących kwalifikowalności wydatków na lata 2021-2027, przewiduje możliwość dokonania następujących zmian Umowy:
   1) W zakresie zmiany terminu realizacji Przedmiotu Umowy i/lub wynagrodzenia, stosownie do przypadku:
      a) w sytuacji wystąpienia okoliczności wynikających ze zmiany jakichkolwiek rozporządzeń, przepisów, umowy o dofinansowanie, wniosku o dofinansowanie i innych dokumentów, w tym dokumentów programowych dotyczących Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" Krajowego Planu Odbudowy i Zwiększania Odporności, mających wpływ na realizację umowy,
      b) w sytuacji zmiany terminu realizacji umowy o dofinansowanie, w szczególności w sytuacji wydłużenia terminu realizacji projektu przez Beneficjenta. Termin realizacji umowy zostanie wydłużony odpowiednio o czas wydłużenia terminu realizacji projektu,
      c) w przypadku zmiany obowiązujących przepisów prawa, odnoszących się do niniejszego zamówienia, w tym zmiany stawki podatku VAT. Zmianie ulegnie wyłącznie kwota VAT w stopniu wynikającym z wprowadzonej zmiany, przy zachowaniu stałej ceny netto,
      d) w przypadku wystąpienia siły wyższej, rozumianej jako zdarzenie zewnętrzne, niezależne od Stron, niemożliwe do przewidzenia lub zapobieżenia przy zachowaniu należytej staranności, w szczególności obejmujące awarie infrastruktury teleinformatycznej, długotrwałe przerwy w dostępie do sieci Internet, ataki cybernetyczne, awarie systemów lub usług zewnętrznych, przerwy w dostawie energii elektrycznej, działania dostawców usług chmurowych lub hostingowych, a także inne zdarzenia mogące uniemożliwić lub istotnie utrudnić realizację Umowy,
      e) kiedy realizacja Przedmiotu Umowy była niemożliwa z przyczyn nie leżących po stronie Wykonawcy oraz następstw tego zdarzenia w przypadku napotkania przez Wykonawcę lub Zamawiającego okoliczności niemożliwych do przewidzenia i niezależnych od nich,
      f) konieczności ewentualnej zmiany zakresu Przedmiotu Umowy wprowadzonej na podstawie postanowień Wytycznych dotyczących kwalifikowalności wydatków na lata 2021- 2027 umożliwiających dokonanie takiej zmiany, jeśli zmiana ta powodowała będzie konieczność zmiany terminu realizacji umowy, przy czym każda zmiana może nastąpić tylko o czas niezbędny do wykonania Przedmiotu Umowy, nie dłużej jednak niż o okres trwania okoliczności będących podstawą zmiany oraz ich następstw;
   2) Zamawiający dopuszcza możliwość zmiany umowy we wszystkich jej zakresach także w przypadku wystąpienia następujących okoliczności:
      a) trwania wojny napastniczej przeciwko Rzeczypospolitej Polskiej lub działań zbrojnych na terytorium Rzeczypospolitej Polskiej, terytorium państwa członkowskiego Unii Europejskiej, terytorium Państwa-Strony Traktatu Północnoatlantyckiego albo na terytorium innego państwa graniczącego z Rzecząpospolitą Polską lub okupacji na tych terytoriach lub
      b) obowiązywania na obszarze Rzeczypospolitej Polskiej stanu klęski żywiołowej, stanu wyjątkowego albo stanu wojennego;
   3) Strony umowy wzajemnie informują się o wpływie okoliczności, o których mowa w pkt. 2 na

należyte wykonanie umowy potwierdzając ten wpływ oświadczeniami lub dokumentami.

2. Przedłużenie terminów realizacji przedmiotu umowy z przyczyn wskazanych w ust. 1 pkt. 2 Umowy może nastąpić wyłącznie o czas trwania przeszkody, tj. czas, w jakim wyżej wskazane okoliczności wpłynęły na termin wykonania Umowy przez Wykonawcę, to jest uniemożliwiły Wykonawcy terminową realizację przedmiotu Umowy.
3. Inicjatorem zmian w Umowie może być każda ze Stron, z tym, że ostateczna decyzja, co do wprowadzenia zmian i ich zakresu należy do Zamawiającego. Wystąpienie którejkolwiek z okoliczności mogących powodować zmianę Umowy, nie stanowi zobowiązania Zamawiającego do dokonania zmian, ani nie może stanowić podstawy do jakichkolwiek roszczeń Wykonawcy do ich dokonania.
4. Niezależnie od postanowień niniejszego paragrafu, Strony dopuszczają możliwość zmian redakcyjnych Umowy oraz zmian danych Stron ujawnionych w rejestrach publicznych, niestanowiących zmiany istotnej.

§ 9.
RODO

Zamawiający oświadcza, że w związku z wejściem w życie z dniem 25 maja 2018 roku przepisów 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 – Dziennik Urzędowy UE L 119, zwane w dalszej części RODO) Przedsiębiorstwo Wodociągów i Kanalizacji w Ząbkach Sp. z o.o. zapewniał będzie określone w tych przepisach standardy ochrony i właściwego postępowania z danymi osobowymi.
Zgodnie z art. 13 ust. 1 i 2 RODO Zamawiający informuje, że:

1. Przedsiębiorstwo Wodociągów i Kanalizacji w Ząbkach Sp. z o.o. – siedziba: 05-091 Ząbki, ul. Hubalczyków 1 jest Administratorem Danych Osobowych;
2. Pozyskane dane osobowe będą przetwarzane przez Przedsiębiorstwo Wodociągów i Kanalizacji w Ząbkach Sp. z o.o. jako Administratora Danych w celu związanym z realizacją niniejszego zamówienia;
3. dane osobowe będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli w wyniku postępowania zostanie zawarta umowa – do czasu przedawnienia roszczeń związanych z realizacją umowy;
4. w odniesieniu do zgromadzonych danych osobowych w związku z postępowaniem, decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
5. Zamawiający wyznaczył Inspektora Ochrony Danych, pana Radosława Wasilewskiego, z którym skontaktować można się:
   1) telefonicznie: pod nr +48 783 220 250
   2) pocztą tradycyjną: na adres: PWIK 05-091 Ząbki, ul. Hubalczyków 1
   3) pocztą elektroniczną: na adres e-mail daneosobowe@zabki.pl
   4) osobiście: w siedzibie PWiK w Ząbkach przy ul. Hubalczyków 1.
6. Posiada Pani/Pan:
   1) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   2) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych*;
   3) 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**;
   4) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
7. Nie przysługuje Pani/Panu:
   1) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   2) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   3) 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.

* Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.
** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

§10.
BEZPIECZEŃSTWO INFORMACJI I POUFNOŚĆ, TRWAŁOŚĆ PROJEKTU I ARCHIWIZACJA

1. Wykonawca zobowiązuje się do zachowania poufności wszelkich informacji uzyskanych w związku z realizacją Umowy.
2. Wykonawca zobowiązuje się stosować środki bezpieczeństwa adekwatne do charakteru infrastruktury krytycznej Zamawiającego.
3. Wykonawca zobowiązuje się do:
   1) niezwłocznego zgłaszania incydentów bezpieczeństwa;
   2) zabezpieczenia danych i konfiguracji;
   3) stosowania zasad minimalnych uprawnień;
   4) niewykorzystywania danych Zamawiającego poza realizacją Umowy.
4. Obowiązek poufności obowiązuje również po zakończeniu Umowy.
5. Wykonawca zobowiązuje się realizować Umowę w sposób zapewniający utrzymanie efektów projektu przez okres wymagany Umową o powierzenie grantu.
6. Wykonawca zobowiązuje się przechowywać dokumentację związaną z realizacją Umowy przez okres wymagany przepisami dotyczącymi projektów finansowanych ze środków KPO.
7. Wykonawca zobowiązuje się udostępniać dokumentację na każde żądanie Zamawiającego lub instytucji kontrolnych.

§ 11.
POSTANOWIENIA KOŃCOWE

1. Zamawiający i Wykonawca podejmą starania, aby rozstrzygnąć ewentualne spory wynikające z Umowy ugodowo poprzez bezpośrednie negocjacje lub w drodze mediacji, o której mowa w przepisach o postępowaniu cywilnym.
2. Jeżeli Zamawiający i Wykonawca nie będą w stanie rozstrzygnąć sporu ugodowo, wszelkie spory związane z Umową rozstrzygać będzie sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
3. Umowę zawarto w formie pisemnej pod rygorem nieważności. Wszelkie zmiany lub uzupełnienia Umowy wymagają formy pisemnej pod rygorem nieważności.
4. W sprawach nieuregulowanych Umową zastosowanie znajdują powszechnie obowiązujące przepisy prawa Rzeczypospolitej Polskiej, w tym w szczególności Kodeksu cywilnego.
5. Jeżeli którekolwiek z postanowień niniejszej Umowy okaże się lub stanie się w całości albo w części nieważne, bezskuteczne lub niewykonalne, nie wpływa to na ważność, skuteczność ani wykonalność pozostałych postanowień Umowy, które pozostają w mocy i są wiążące dla Stron. Strony zobowiązują się niezwłocznie podjąć negocjacje w dobrej wierze w celu zastąpienia postanowienia nieważnego, bezskutecznego lub niewykonalnego postanowieniem ważnym i skutecznym, które w możliwie najpełniejszy sposób będzie odpowiadało celowi gospodarczemu, funkcji oraz pierwotnemu zamiarowi Stron wyrażonemu w zastępowanym postanowieniu. Do czasu uzgodnienia nowego postanowienia zastosowanie znajdą odpowiednie przepisy prawa powszechnie obowiązującego, które w możliwie najbliższym zakresie realizują cel i ekonomiczny sens postanowienia uznanego za nieważne.

bezskuteczne lub niewykonalne.

6. Umowę zawarto w 2 jednobrzmiących egz. po 1 egz. dla każdej ze Stron

ZAMAWIAJĄCY **WYKONAWCA**

1 – Specyfikacja – Next Generation Firewall typ 1

Wymagania Ogólne

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

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

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

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

Funkcje Systemu Bezpieczeństwa:

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

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

12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

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

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

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

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

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

Ochrona przed atakami

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

Kontrola aplikacji

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

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

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

Zarządzanie

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

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

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

b) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres [36] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

2 – Specyfikacja – Next Generation Firewall typ 2

Wymagania Ogólne

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

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

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 5 portami Gigabit Ethernet RJ-45.

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

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

Funkcje Systemu Bezpieczeństwa:

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

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

12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

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

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

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

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

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

Ochrona przed atakami

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

Kontrola aplikacji

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

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

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

Zarządzanie

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

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

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

b) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres [36] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

3 – Specyfikacja – Wdrożenie rozwiązań NGFW

1. Dostarczenie trzech urządzeń Fortigate oraz ich fizyczna instalacja w siedzibie zamawiającego.
2. Aktualizacja oprogramowania wszystkich urządzeń do najnowszej, dostępnej w dniu wdrożenia wersji.
3. Ustawienie podstawowych parametrów dostępowych do urządzeń.
4. Analiza infrastruktury sieciowej i wymagań zamawiającego.
5. Konfiguracja podstawowych parametrów sieciowych urządzeń Fortigate.
6. Utworzenie profili bezpieczeństwa UTM dla każdego urządzenia na podstawie wytycznych zamawiającego, w tym: blokowanie niebezpiecznych stron www, blokowanie i monitorowanie aplikacji internetowych, ochrona przed DDoS, IPS, antywirus.
7. Konfiguracja tuneli IPSec typu site-to-site oraz dostępowych Remote Access.
8. Konfiguracja zbierania logów z urządzeń wg wytycznych zamawiającego.
9. Konfiguracja klastra HA dwóch urządzeń serii 60.
10. Testy działania profili bezpieczeństwa, przepustowości oraz obciążeń na urządzeniach.
11. Test klastra HA (wyłączenie dowolnego urządzenia i obserwacja przełączania się na drugie).
12. Migracja polityk bezpieczeństwa z dotychczas używanych urządzeń oraz weryfikacja zgodności nowej konfiguracji z wymaganiami operacyjnymi Zamawiającego.
13. Konfiguracja funkcjonalności SD-WAN dla ruchu między lokalizacjami, wraz z optymalizacją tras i priorytetyzacją ruchu krytycznego.
14. Wdrożenie i konfiguracja modułu Zero Trust Network Access (ZTNA) dla zdalnego dostępu użytkowników uprzywilejowanych.
15. Przeprowadzenie przeglądu (rule review) skonfigurowanych reguł bezpieczeństwa oraz optymalizacja zgodnie z zasadą najmniejszych uprawnień.
16. Opracowanie pełnej dokumentacji powdrożeniowej: schemat sieci, opis reguł, procedury eskalacyjne i awaryjne (runbook).
17. Opracowanie raportu zgodności wdrożonego rozwiązania z wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa dla operatora usługi kluczowej.
18. Przeprowadzenie dodatkowych testów odporności na awarie (symulacja: awaria łącza WAN, awaria zasilania, przeciążenie łącza).
19. Rozszerzone wsparcie powdrożeniowe (hypercare) przez okres 3 miesięcy od odbioru, z priorytetową obsługą zgłoszeń.

20. Utrzymanie i przegląd konfiguracji przez okres 24 miesięcy od odbioru, obejmujące: aktualizacje sygnatur i oprogramowania, kwartalny przegląd polityk bezpieczeństwa oraz wsparcie przy zmianach konfiguracji.

4 – Specyfikacja – przełącznik sieciowy zarządzalny z obsługą PoE

Parametr	Charakterystyka / wymagania minimalne
Typ urządzenia	Zarządzalny przełącznik sieciowy warstwy 3 przeznaczony do zastosowań profesjonalnych i korporacyjnych
Montaż	Przystosowany do montażu w szafie RACK 19"
Zarządzanie	Możliwość zarządzania urządzeniem lokalnie poprzez wbudowany interfejs WWW oraz CLI (SSH/port konsoli) bez konieczności korzystania z chmury producenta; dodatkowo możliwość centralnego zarządzania wieloma urządzeniami za pomocą dedykowanego oprogramowania/kontrolera sieciowego (lokalnego lub oferowanego przez producenta, w tym w modelu chmurowym jako funkcja opcjonalna) oraz aplikacji mobilnej wspierającej monitorowanie i konfigurację
Porty RJ-45	Minimum 48 portów Gigabit Ethernet RJ-45
Porty uplink	Minimum 4 porty SFP+ 10GbE
Obsługa PoE	Obsługa standardów PoE 802.3af, PoE+ 802.3at oraz PoE++ 802.3bt
Porty PoE+	Minimum 32 porty z obsługą PoE+
Porty PoE++	Minimum 16 portów z obsługą PoE++
Budżet mocy PoE	Minimum 600 W
Funkcje warstwy 2	VLAN 802.1Q, STP/RSTP/MSTP, LACP, IGMP Snooping
Funkcje warstwy 3	Routing statyczny IPv4/IPv6
QoS	Obsługa mechanizmów QoS i priorytetyzacji ruchu
Bezpieczeństwo	Obsługa ACL, DHCP Snooping, ochrona przed pętlami sieciowymi
Zarządzanie siecią	Obsługa SNMP, SSH, syslog oraz monitoringu ruchu i statystyk portów
Zarządzanie PoE	Możliwość monitorowania poboru mocy oraz zdalnego restartu urządzeń PoE
Funkcje dodatkowe	Obsługa Jumbo Frames oraz Auto MDI/MDIX
Aktualizacje	Możliwość aktualizacji oprogramowania z poziomu interfejsu zarządzania
Kopia konfiguracji	Możliwość eksportu i importu konfiguracji
Chłodzenie	Aktywne chłodzenie z automatyczną regulacją pracy wentylatorów
Tryb pracy	Przystosowany do pracy ciągłej 24/7
Sygnalizacja	Diody LED informujące o stanie pracy urządzenia i portów
Zasilanie	Zasilanie AC 230V
Gwarancja	Minimum 24 miesiące gwarancji producenta lub autoryzowanego dystrybutora

5 – Specyfikacja – Wdrożenie i utrzymanie rozwiązania Zarządzalny switch

1. Dostarczenie przełączników sieciowych oraz ich fizyczna instalacja w szafach dystrybucyjnych (RACK) w siedzibie zamawiającego.
2. Aktualizacja oprogramowania układowego (firmware) wszystkich przełączników do najnowszej, stabilnej wersji dostępnej w dniu wdrożenia.
3. Ustawienie podstawowych parametrów dostępowych i konfiguracyjnych urządzeń (w tym bezpiecznych haseł administratora, protokołów SSH/HTTPS oraz serwerów NTP).
4. Analiza obecnej infrastruktury sieciowej, schematu adresacji oraz wymagań zamawiającego w zakresie segmentacji ruchu.
5. Konfiguracja podstawowych parametrów sieciowych przełączników (w tym adresów IP zarządzania oraz tras domyślnych).
6. Utworzenie i konfiguracja wirtualnych sieci lokalnych (VLAN) dla poszczególnych segmentów sieci na podstawie wytycznych zamawiającego.
7. Konfiguracja portów przełączników w trybach dostępowych (Access) oraz magistralnych (Trunk) do przesyłania ruchu między urządzeniami.
8. Konfiguracja mechanizmów zapewniania niezawodności i ochrony przed pętlami w sieci (RSTP/MSTP) oraz agregacji linków (LACP).
9. Konfiguracja zbierania logów i monitorowania urządzeń (syslog, SNMP) według wytycznych zamawiającego.
10. Konfiguracja klastrowania lub łączenia przełączników w stos (Stacking) w celu zapewnienia wysokiej dostępności (HA) w warstwie dystrybucyjnej/rdzeniowej.
11. Testy prawidłowości działania przełączników, w tym weryfikacja poprawności routingu między sieciami VLAN, przepustowości łączy oraz testy redundancji.
12. Opracowanie szczegółowego planu migracji z dotychczasowej infrastruktury przełączającej, w tym harmonogramu prac minimalizującego przerwy w działaniu sieci.
13. Wdrożenie mechanizmów kontroli dostępu do sieci (NAC/802.1X) zintegrowanych z posiadaną usługą katalogową.
14. Konfiguracja dynamicznego przypisywania VLAN na podstawie tożsamości urządzenia/użytkownika, w powiązaniu z wdrożonym mechanizmem NAC.
15. Integracja przełączników z systemem monitorowania infrastruktury oraz z centralnym systemem logowania Zamawiającego.
16. Przeprowadzenie analizy obciążenia sieci oraz opracowanie planu rozbudowy/skalowania infrastruktury na kolejne 3 lata.
17. Opracowanie pełnej dokumentacji sieciowej: schemat logiczny i fizyczny, mapa VLAN, tabela adresacji IP.
18. Rozszerzony okres stabilizacji (hypercare) przez 2 miesiące od odbioru, z priorytetową obsługą zgłoszeń.

19. Przeprowadzenie testów akceptacyjnych w warunkach obciążenia zbliżonych do rzeczywistych (symulacja ruchu produkcyjnego).
20. Utrzymanie i przegląd konfiguracji przez okres 24 miesięcy od odbioru: aktualizacje firmware, przegląd konfiguracji VLAN/STP oraz wsparcie przy zmianach konfiguracji.

6 – Specyfikacja – Wdrożenie i utrzymanie rozwiązania styku sieci Internet z usługami wewnętrznymi

1. Analiza obecnej architektury sieci oraz wymagań Zamawiającego dotyczących udostępniania usług wewnętrznych do sieci Internet.
2. Opracowanie koncepcji strefy zdemilitaryzowanej (DMZ) uwzględniającej segmentację ruchu oraz separację usług publikowanych od sieci wewnętrznej.
3. Konfiguracja interfejsów i stref bezpieczeństwa (DMZ, LAN, WAN) na urządzeniach NGFW zgodnie z przyjętą koncepcją.
4. Instalacja i konfiguracja serwera pośredniczącego (reverse proxy) publikującego wskazane przez Zamawiającego usługi wewnętrzne.
5. Wdrożenie certyfikatów SSL/TLS dla publikowanych usług oraz konfiguracja automatycznego odnawiania certyfikatów.
6. Konfiguracja reguł translacji adresów (NAT) oraz polityk firewall ograniczających ruch wyłącznie do niezbędnych portów i protokołów.
7. Wdrożenie mechanizmów ochrony przed nadużyciami (m.in. ograniczenie liczby połączeń, ochrona przed atakami typu brute-force) dla publikowanych usług.
8. Konfiguracja logowania i przekazywania zdarzeń z punktu styku do centralnego systemu zbierania logów Zamawiającego.
9. Przeprowadzenie testów bezpieczeństwa opublikowanych usług, w tym weryfikacja poprawności segmentacji oraz testy podstawowego zakresu penetracyjnego.
10. Przeprowadzenie testów wydajnościowych oraz testów obciążeniowych łącza i punktu styku.
11. Przygotowanie dokumentacji powdrożeniowej zawierającej schemat połączeń, opis konfiguracji oraz procedury postępowania w sytuacjach awaryjnych.
12. Utrzymanie rozwiązania przez okres 12 miesięcy od odbioru, obejmujące: monitorowanie dostępności punktu styku, aktualizacje oprogramowania i certyfikatów, wsparcie przy zmianach konfiguracji oraz reakcję na zgłoszenia w ustalonym czasie SLA.
13. Wdrożenie i konfiguracja modułu Web Application Firewall (WAF) dla publikowanych aplikacji webowych.
14. Konfiguracja mechanizmów ochrony przed atakami DDoS na poziomie punktu styku.
15. Przeprowadzenie rozszerzonych testów penetracyjnych publikowanych usług przez niezależny zespół, w zakresie odpowiadającym metodyce OWASP Top 10.
16. Integracja logów punktu styku z systemem monitorowania/SIEM Zamawiającego w celu korelacji zdarzeń bezpieczeństwa.
17. Opracowanie planu ciągłości działania (BCP) oraz przeprowadzenie testu scenariusza awaryjnego (np. utrata łącza podstawowego i przełączenie na łącze zapasowe).

18. Opracowanie pełnej dokumentacji technicznej i proceduralnej zgodnej z wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa dla operatora usługi kluczowej.
19. Rozszerzone wsparcie powdrożeniowe (hypercare) przez okres 3 miesięcy od odbioru.
20. Wydłużenie okresu utrzymania rozwiązania do 24 miesięcy od odbioru, obejmujące: monitorowanie dostępności, aktualizacje, coroczny retest bezpieczeństwa oraz wsparcie przy zmianach konfiguracji.

7 – Specyfikacja - serwer NAS (Network Attached Storage)

Parametr	Charakterystyka / wymagania minimalne
Typ urządzenia	Sieciowy serwer plików (NAS) klasy biznesowej, przeznaczony do centralnego przechowywania, zabezpieczania i udostępniania danych w sieci lokalnej
Montaż	Obudowa RACK 19", wysokość maksymalnie 2U, przystosowana do montażu w szafie serwerowej Zamawiającego
Liczba zatok dyskowych	Minimum 8 zatok 3,5"/2,5" SATA z obsługą wymiany dysków bez wyłączania urządzenia (hot-swap)
Pojemność użytkowa	Minimum 30 TB przestrzeni użytkowej po skonfigurowaniu w trybie nadmiarowym zabezpieczającym przed jednoczesną awarią dwóch dysków
Dyski twarde	Dyski klasy NAS/Enterprise przeznaczone do pracy ciągłej 24/7/365, prędkość obrotowa minimum 7200 obr./min
Procesor	Minimum 4-rdzeniowy procesor architektury x86
Pamięć RAM	Minimum 4 GB ECC, z możliwością rozbudowy
Interfejsy sieciowe	Minimum 4 porty Gigabit Ethernet RJ-45 z obsługą agregacji łączy (LACP, standard 802.3ad); możliwość rozbudowy o karty sieciowe 10GbE
Zasilanie	Redundantne, wymienne moduły zasilania (minimum 2 szt.) zapewniające ciągłość pracy urządzenia w przypadku awarii jednego z nich
Obsługiwane poziomy RAID	RAID 0, 1, 5, 6, 10 oraz tryb dysku zapasowego (hot-spare)
Protokoły sieciowe	SMB/CIFS, NFS, FTP/FTPS, iSCSI
Zarządzanie	Zarządzanie poprzez przeglądarkę WWW (HTTPS), obsługa SNMP, powiadomienia e-mail/SMS o zdarzeniach i awariach, integracja z usługą katalogową Active Directory/LDAP
Ochrona danych	Obsługa migawek (snapshot) w trybie planowanym, replikacji danych oraz integracji z zewnętrznym oprogramowaniem do tworzenia i zarządzania kopiami zapasowymi
Bezpieczeństwo	Szyfrowanie danych na dyskach (AES), obsługa uwierzytelniania dwuskładnikowego (2FA) dla kont administracyjnych, kontrola dostępu na poziomie użytkowników i grup
Chłodzenie	Aktywne, z automatyczną regulacją pracy wentylatorów

Parametr	Charakterystyka / wymagania minimalne
Tryb pracy	Przystosowany do pracy ciągłej 24/7
Gwarancja	Minimum 24 miesiące gwarancji producenta lub autoryzowanego dystrybutora

8 – Specyfikacja - oprogramowanie do monitorowania infrastruktury informatycznej

Parametr	Charakterystyka / wymagania minimalne
Typ rozwiązania	Oprogramowanie klasy Network/Infrastructure Monitoring do centralnego monitorowania dostępności i wydajności infrastruktury informatycznej IT/OT
Architektura	Instalacja lokalna (on-premise) na serwerze Zamawiającego, bez konieczności przesyłania danych telemetrycznych poza infrastrukturę Zamawiającego
Liczba monitorowanych punktów	Minimum 500 sensorów/punktów pomiarowych w ramach jednej instalacji, z możliwością rozbudowy bez wymiany platformy
Obsługiwane protokoły i metody monitorowania	SNMP (v1/v2c/v3), WMI, ping (ICMP), SSH, HTTP/HTTPS, przepływy ruchu sieciowego (NetFlow/sFlow/jFlow), zapytania SQL
Zakres monitorowania	Dostępność i obciążenie urządzeń sieciowych, serwerów, macierzy dyskowych, środowisk wirtualizacji, usług sieciowych, aplikacji oraz wykorzystania łączy
Powiadomienia	Alarmowanie o zdarzeniach i przekroczeniach progów za pośrednictwem e-mail, SMS oraz powiadomień push/webhook
Wizualizacja	Konfigurowalne dashboardy oraz mapy sieci prezentujące stan monitorowanej infrastruktury w czasie rzeczywistym
Raportowanie	Automatyczne generowanie raportów okresowych (dziennych,

Parametr	Charakterystyka / wymagania minimalne
	tygodniowych, miesięcznych) w formatach PDF, HTML lub CSV
Historia danych	Przechowywanie danych historycznych z monitoringu przez okres minimum 12 miesięcy
Uprawnienia i role	Wielopoziomowy system uprawnień z możliwością tworzenia kont o ograniczonym zakresie dostępu (np. tryb tylko do odczytu)
Integracja	Możliwość integracji z systemami zewnętrznymi poprzez API oraz eksport danych do systemów SIEM/SOC
Licencjonowanie i wsparcie	Licencja obejmująca aktualizacje oraz wsparcie techniczne producenta przez okres minimum 12 miesięcy