***„Zapotrzebowanie na dedykowaną moc obliczeniową dla projektu SWG w ramach projektu Budowa Ogólnopolskiej Sieci Edukacyjnej”,* znak postępowania ZZ.2131.630.2019.TKI [OSE2019]**

Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

1. Wprowadzenie

Ogólnopolska Sieć Edukacyjna ma na celu zapewnienie dostępu do szybkiego, bezpiecznego Internetu dla szkół. OSE jest publiczną siecią telekomunikacyjną, opartą o istniejącą infrastrukturę szerokopasmową wybudowaną w ramach inwestycji komercyjnych oraz dofinansowanych ze środków publicznych w ramach Programu Operacyjnego Polska Cyfrowa. Za uruchomienie i utrzymanie Sieci, oraz w szczególności za dostarczenie szkołom usługi dostępu do Internetu o symetrycznej przepustowości co najmniej 100 Mb/s wraz z kompleksowymi usługami bezpieczeństwa sieciowego, w tym ochrony przed zagrożeniami dla prawidłowego rozwoju uczniów, odpowiedzialny jest Operator OSE.

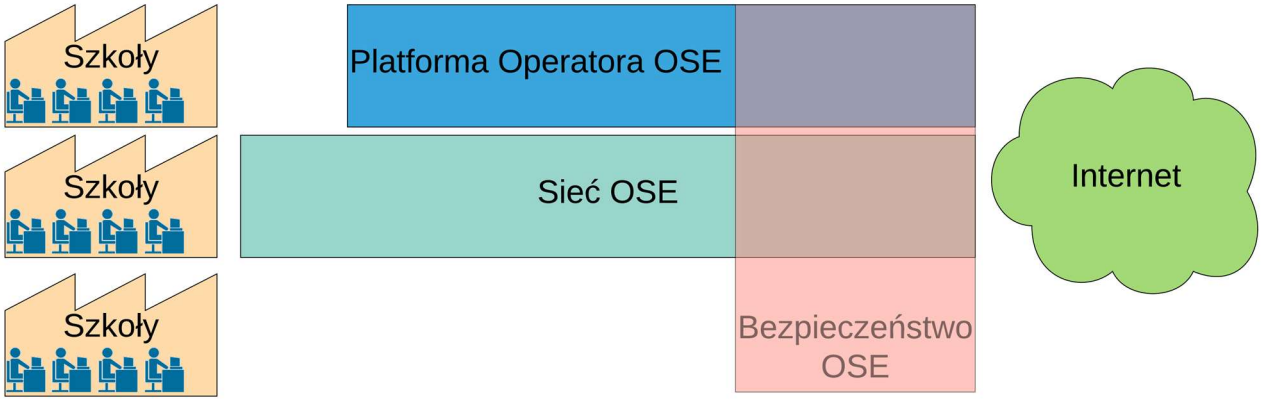
Operatorem OSE został NASK - Państwowy Instytut Badawczy (zwany dalej" „NASK"), nadzorowany przez Ministra Cyfryzacji.

Podstawowym zadaniem OSE ma być zapewnienie szkołom w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych wraz z szeregiem usług powiązanych, w tym:
1) Zapewnienie usług dostępu do sieci Internet o przepływności minimum 100 Mb/s symetrycznie,
2) Zapewnienie usług bezpieczeństwa umożliwiających ochronę użytkowników,
3) Zapewnienie dostawcom treści edukacyjnych dostępu do użytkowników sieci OSE.
4) Umożliwienia wspomagania procesu kształcenia w szkole.

W ramach budowy OSE planuje się uruchomienie sieci rozległej transmisji danych, systemów bezpieczeństwa wraz z systemami wsparcia obejmującymi m.in. systemy: zarządzania tożsamością, OSS, BSS, SIEM jak również urządzenia abonenckie (CPE), przełączniki, AP sieci bezprzewodowej. Usługi obejmować będą swoim zasięgiem terytorium Polski. Sieć OSE, zbudowana będzie z węzłów zlokalizowanych na terenie 16 województw.

1.1. Koncepcja OSE

NASK, jako operator OSE zapewniający dostęp do Internetu dla szkół realizuje swoje działania w oparciu o trzy podstawowe obszary:



1. Sieć OSE - Infrastruktura telekomunikacyjna wykorzystywana do świadczenia przez Operatora OSE usług dostarczanych klientom (takich jak m.in dostęp do Internetu).

2. Platforma Operatora OSE - platforma złożona z komponentów informatycznych, których celem jest wsparcie wszelkiej działalności NASK, jako Operatora OSE (w tym m.in. zarządzanie infrastrukturą sieciową, działania sprzedażowe czy rozliczanie wydatków) składające się z dwóch typów komponentów:
    a. Systemy OSE - systemy informatyczne tworzone lub rozwijane na potrzeby operatora OSE
    b. Systemy NASK - systemy informatyczne wykorzystywane w ramach podstawowej działalności NASK PIB, które zostaną zintegrowane z rozwiązaniem na potrzeby OSE
3. Bezpieczeństwo OSE - komponenty warstwy sieciowej, sprzęt oraz oprogramowanie, których celem jest zapewnienie bezpieczeństwa teleinformatycznego sieci OSE oraz jej użytkownikom.

2. Definicje

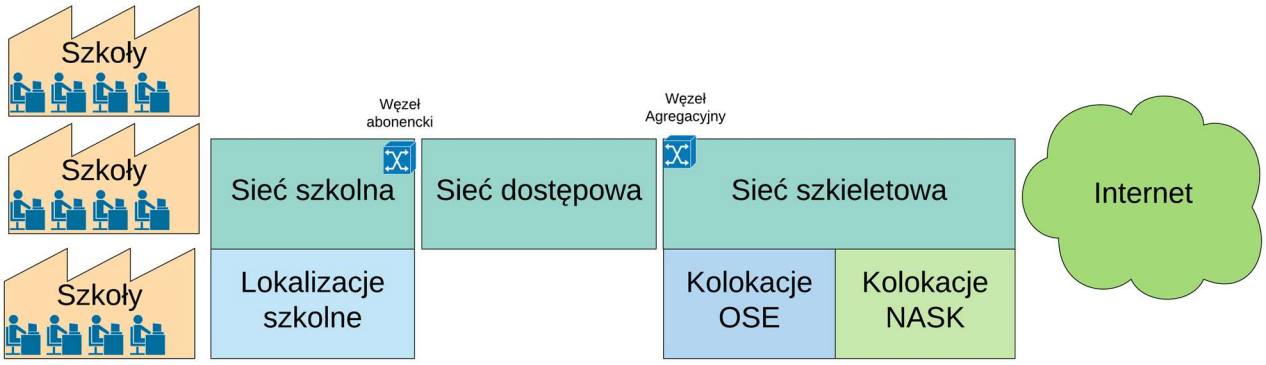
Definicja	Wyjaśnienie
ADC (Application Delivery Controller)	system realizujący równomierne rozłożenie obciążenia na Urządzenia należące do Systemów ADC, NG Firewall, inspekcji ruchu SSL/TLS
Administratorzy OSE	komórka organizacyjna odpowiadająca za utrzymanie sieci OSE
Centralny Węzeł Bezpieczeństwa	węzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym dostarczający mechanizmy ochrony Zasobów obliczeniowych OSE
Lokalizacja węzła / Kolokacja	miejsce fizyczne, powierzchnia kolokacyjna, w którym pracuje Węzeł sieci / Węzeł Bezpieczeństwa.
Węzeł agregacyjny	węzeł, do którego dołączone są łącza dostępowe do szkół, węzeł ten nie ma bezpośredniego połączenia do sieci Internet
Węzeł bezpieczeństwa	zestaw Urządzeń wraz z Oprogramowaniem, realizujących funkcje bezpieczeństwa (m.in. dekrypcja SSL, funkcjonalność IPS, NG Firewall itd.). Zamawiający wyróżnia dwa typy Regionalny Węzeł Bezpieczeństwa oraz Centralny Węzeł Bezpieczeństwa
Węzeł szkieletowy	węzeł zapewniający przeniesienie ruchu z węzłów agregacyjnych do sieci Internet, a także inżynierię ruchu, na styku sieci OSE z Internetem
Węzeł sieci	zespół urządzeń pracujących w jednej lokalizacji, zapewniających komunikację użytkownikom sieci (Szkołom) z siecią Internet. Węzeł wraz z innymi węzłami, z którymi jest połączony za pośrednictwem łączy szkieletowych, stanowi sieć OSE. Częścią węzła są Regionalne i Centralne Węzły Bezpieczeństwa.
Dostawca sieci szkieletowej	przedsiębiorca telekomunikacyjny, udostępniający swoją infrastrukturę na potrzeby budowy szkieletu OSE, czyli łączy pomiędzy węzłami OSE
Dostawca kolokacji	podmiot świadczący na rzecz Zamawiającego usługi kolokacji w centrum przetwarzania danych, w którym zlokalizowany jest Węzeł centralny i/lub Węzeł agregacyjny sieci OSE
Centralny Węzeł Bezpieczeństwa	węzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym, zapewniający ochronę Zasobów obliczeniowych OSE

Definicja	Wyjaśnienie
System NG Firewall(NGFW – Next Generation Firewall)	system kontrolujący dostęp do sieci w oparciu o polityki, klasyfikujące ruch bazujący na informacjach pozyskanych z protokołów działających w 4 i 7 warstwie OSI, z wykorzystaniem mechanizmów statefull packet inspection, intrusion prevetion system, application control, antivirus.
Ustawa OSE	ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej
Użytkownicy Sieci OSE	użytkownicy usług Sieci OSE w tym m.in.: uczniowie, nauczyciele, pracownicy administracyjni oraz inni upoważnieni przez administratora danych usług Sieci OSE
Zasoby obliczeniowe OSE	infrastruktura serwerowa udostępniona w celu zapewnienia mocy obliczeniowej t.j. procesory, pamięć RAM, przestrzeń dyskowa wybudowana na potrzeby systemów i usług OSE. Zasoby są umieszczone w dwóch węzłach centralnych OSE w lokalizacjach: Warszawa i Poznań.
SYSLOG	Program, który umożliwia rejestrowanie zachodzących zdarzeń przy pomocy scentralizowanego mechanizmu logowania. Działa on na porcie 514 udp / tcp. Cały mechanizm jest opisany w następujących RFC 5424 i 3164
SIEM	system tożsamy z funkcjami Log Management (LM) odpowiedzialny za logowanie zdarzeń z urządzeń sieciowych, systemów operacyjnych oraz aplikacji. System LM posiada funkcjonalności takie jak: zbieranie logów, agregację logów oraz przeszukiwanie, raportowanie i tworzenie reguł korelacyjnych
System	Infrastruktura serwerowa wraz z platformą wirtualizacyjną
System Retencji	system odpowiedzialny za zbieranie logów i zdarzeń z urządzeń sieciowych, posiada funkcjonalności takie jak: zbieranie logów, agregację logów, retencję logów oraz przeszukiwanie i raportowanie.
SWG (Platforma Security Web Gateway)	System zapewniający funkcje ochrony użytkownika sieci OSE związane z potencjalnym dostępem do treści nielegalnych i szkodliwych w Internecie.
Moc obliczeniowa	infrastruktura serwerowa zapewniająca odpowiednią sumaryczną pojemność w zakresie procesorów fizycznych, pamięć RAM, przestrzeni dyskowej.

3. Sieć OSE

Podstawowym zadaniem OSE jest zapewnienie jednostkom oświatowym w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych z przepustowością nie mniejszą niż 100Mb/s (symetrycznie).

W celu świadczenia usług szerokopasmowego dostępu do Internetu niezbędne jest zapewnienie odpowiedniej infrastruktury telekomunikacyjnej łączącej szkołę / lokalizację (wraz z jej siecią i sprzętem informatycznym) do zasobów sieci Internet. Cały przebieg tzw. Sieci OSE możemy podzielić na trzy segmenty zgodnie z poniższym rysunkiem.

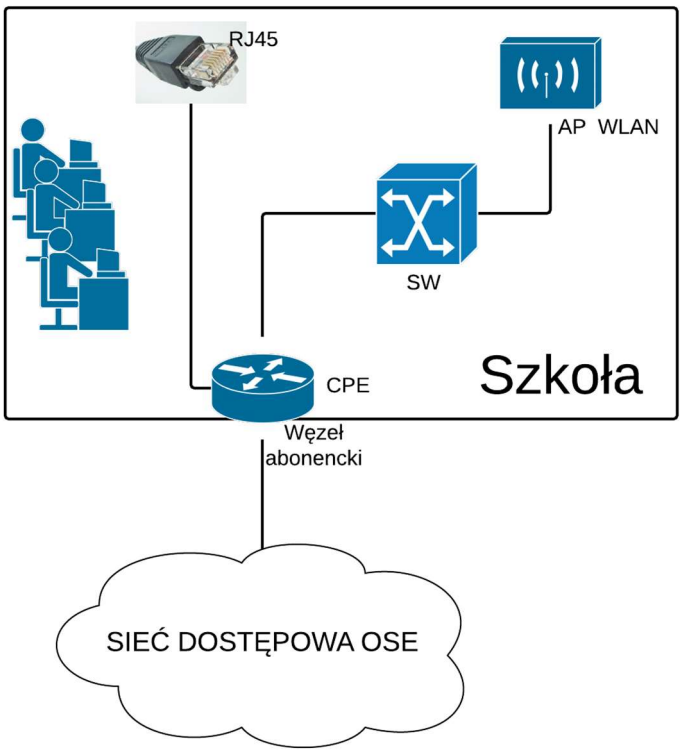


- Sieć szkolna - infrastruktura sieciowa znajdująca się w lokalizacjach szkolnych, której celem jest zapewnienie łączności dla urządzeń w szkole (zarówno klienckich jak i elementów sieciowych) z punktem dostępowym (CPE). Punkt styku sieci szkolnej z otoczeniem nazywany jest węzłem abonenckim. Zapewnienie odpowiedniej kolokacji dla infrastruktury szkolnej znajduje się w odpowiedzialności placówki szkolnej i jej dyrektora.
- Sieć dostępowa - infrastruktura sieciowa dostarczana przez innych operatorów telekomunikacyjnych zapewniająca łączność pomiędzy lokalizacją szkolną a siecią szkieletową.
- Sieć szkieletowa - Infrastruktura sieciowa zapewniająca łączność pomiędzy węzłami sieci OSE oraz siecią OSE a siecią Internet. Sieć szkieletowa znajduje się po części w ramach kolokacji dzierżawionych od podmiotów zewnętrznych, a w pewnej części w kolokacji NASK

3.1. Sieć szkolna

Sieci lokalne w jednostkach oświatowych, co do zasady, nie będą w ramach podłączania do OSE modernizowane, jednakże zakłada się możliwość przeprowadzenia ograniczonych prac rekonfiguracyjnych w celu umożliwienia korzystania z dostarczonych usług. Decyzja o wykonywaniu tych prac będzie podejmowana ad hoc, podczas wizyty partnera serwisowego.

Architektura sieci szkolnej z perspektywy OSE przedstawiona jest na poniższym obrazku:



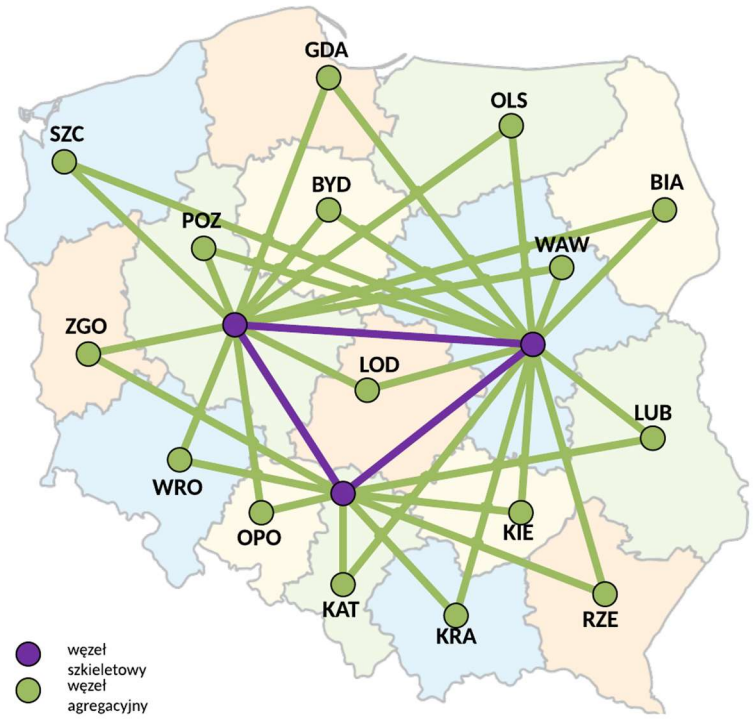
Infrastruktura telekomunikacyjna doprowadzana jest przez operatorów do poszczególnych lokalizacji, w jakich znajdują się szkoły. Należy jednakże zauważyć, że pomiędzy szkołą a lokalizacją zachodzi relacja wiele do wielu. Oznacza to, iż w lokalizacji może występować wiele szkół, lub szkoła może znajdować się w wielu lokalizacjach. Dodatkowo zdarzają się sytuacje, gdy szkoła w danej lokalizacji posiada więcej niż jeden budynek. Mogą się również zdarzyć sytuacje, że pod jednym adresem znajdować się będę szkoły o różnym modelu podłączania, czyli w danym adresie może występować więcej niż jedna lokalizacja (lokalizacja grupuje szkoły w jednym adresie podłączane i obsługiwane w tym samym modelu podłączania).

3.2. Sieć dostępowa

Połączenie pomiędzy lokalizacją szkolną (węzeł abonencki), a siecią szkieletową OSE (węzeł agregacyjny) realizowana jest za pośrednictwem tzw. sieci dostępowej.

3.3. Sieć szkieletowa

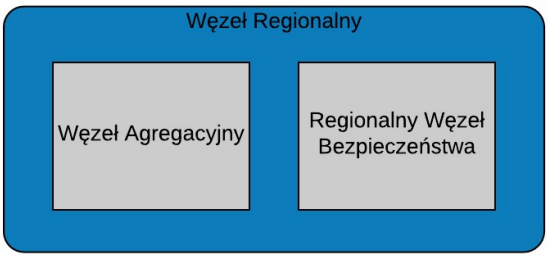
W zakresie sieci szkieletowej operator OSE opiera się na łączach dzierżawionych od operatorów telekomunikacyjnych, nie jest rozważana budowa własnej infrastruktury kablowej. Przeprowadzony przez NASK Dialog Techniczny z operatorami telekomunikacyjnymi wskazał na potrzebę budowy 16 węzłów OSE, zlokalizowanych w miastach wojewódzkich, w celu agregowania ruchu z jednostek oświatowych z terenu całego kraju (węzły agregacyjne). Trzy spośród tych węzłów pełnią również rolę węzłów centralnych (węzły szkieletowe). Pozostałe węzły są połączone do węzłów centralnych. Lokalizacje węzłów zostały wybrane przez NASK Państwowy Instytut Badawczy w ramach odrębnych, wewnętrznych procesów zakupowych, w wyniku których zostali wyłonieni dostawcy Usług kolokacji w poszczególnych centrach przetwarzania danych. Zamawiający planuje również objęcie wszystkich "kolokacji" jednym, wspólnym systemem zarządzania.

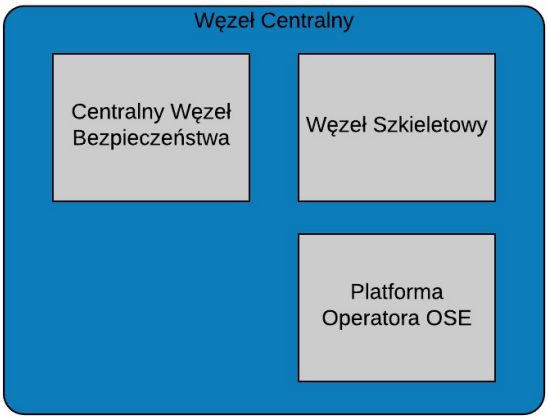


Węzły sieci

W sieci OSE istnieją dwa funkcjonalne rodzaje węzłów:

- Węzły Regionalne, w których skład wchodzą Węzły Agregacyjne (do których są dołączone łącza ze szkół) oraz Regionalne Węzły Bezpieczeństwa
- Węzły Centralne, w których skład wchodzą Węzły Szkieletowe, Centralne Węzły Bezpieczeństwa oraz Zasoby Obliczeniowe OSE (będące platformą dla systemów OSE). Do Węzłów Szkieletowych dołączone są Węzły Agregacyjne. Węzły te także zapewniają łączność do sieci Internet.





Węzły Szkieletowe są zlokalizowane w tych samych miejscach co Węzły Agregacyjne, za wyjątkiem węzła WAW / WAW Core, w którym Węzeł Agregacyjny jest umieszczony w innej lokalizacji niż Węzeł Szkieletowy (oba węzły będą zlokalizowane na terenie Warszawy). Urządzenia pełniące funkcje obu węzłów są oddzielne.

Każdy węzeł OSE wyposażony zostanie w urządzenia sieciowe, Infrastrukturę bezpieczeństwa, przełączniki sieci lokalnej, niezbędne zasoby obliczeniowe operatora OSE (komponenty systemów z grupy OSS: Systemu Retencji Logów, Systemy FP/PM), rutery shadow oraz urządzenia sieci zarządzającej, zapewniające dostęp administracyjny do wszystkich urządzeń zlokalizowanych w węźle. Infrastruktura sieciowa w węzłach OSE opiera się o następujące typy/modele urządzeń:

- rutery - Juniper MX (960 i 10003)
- Junos 18.2 (rutery MX)
- CG-NAT - Juniper SRX (4600)
- Junos 19.1 (SRX 4600)
- LAN - Juniper QFX (10008, 10003, 5110 i 5120)
- Junos 19.1 (Switche QFX 10008)
- Junos 17.2 (Switche QFX 10002)
- Junos 18.1 (Switche QFX 5000)
- rutery shadow - Juniper SRX320
- Junos Space ver.19.1R1
- Connectivity Services Director ver. 4.2R1

4. Bezpieczeństwo OSE

W sieci OSE istnieją funkcjonalne rodzaje węzłów:

- Węzeł Regionalny składa się z Węzła Agregacyjnego, do którego są dołączone łącza ze szkół, oraz z Regionalnego Węzła Bezpieczeństwa.
- Węzeł Centralny, składa się z Węzła Szkieletowego, do którego są dołączone Węzły Agregacyjne. Węzły te także zapewniają łączność do sieci Internet oraz zapewnią połączenie z Zasobami obliczeniowymi OSE. Centralny Węzeł Bezpieczeństwa jest zlokalizowany tylko w dwóch Węzłach Centralnych.

Węzły Centralne mogą być zlokalizowane w tych samych Obiektach, co Węzły Regionalne, ale Urządzenia pełniące funkcje obu węzłów są oddzielne.

Każdy węzeł OSE wyposażony zostanie w urządzenia sieciowe, elementy Infrastruktury bezpieczeństwa, przełączniki sieci lokalnej, systemy OSS, systemy BSS zlokalizowane w węźle oraz w urządzenia sieci zarządzania, zapewniające dostęp administracyjny do wszystkich Urządzeń zlokalizowanych w Węźle.

Każdy z 16 Regionalnych Węzłów Bezpieczeństwa zawiera komponenty realizujące podstawowe funkcjonalności, m.in:

- zapewnianie bezpieczeństwa teleinformatycznego użytkownikom sieci OSE,
- wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym,
- wykrywanie i blokowanie zdefiniowanych aplikacji webowych,
- monitorowanie ruchu sieciowego i zapisywanie najważniejszych wydarzeń do logu.

Dwa Centralne Węzły Bezpieczeństwa będą zawierać komponenty realizujące funkcjonalności ochrony Zasobów obliczeniowych OSE, tzn. będą:

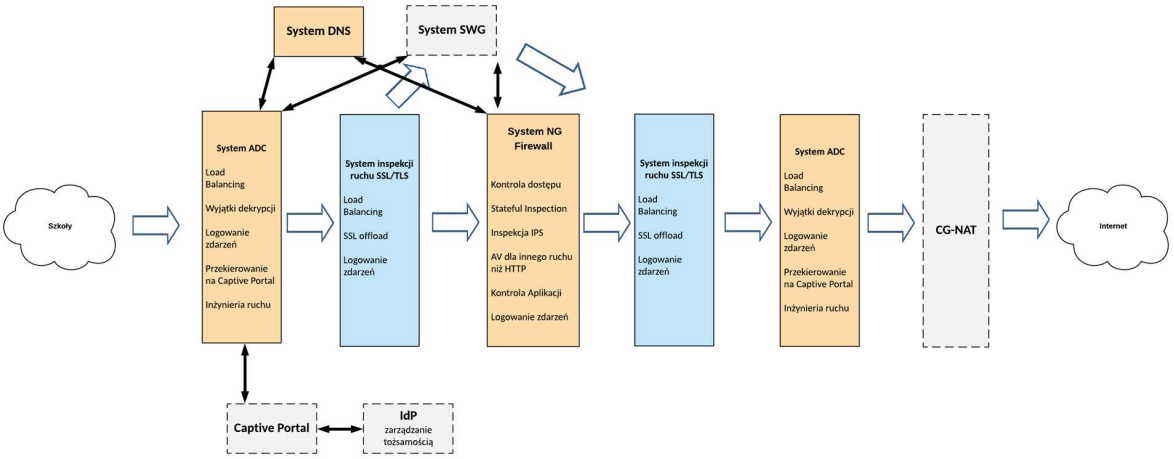
- zapewniać bezpieczeństwo teleinformatyczne Zasobów obliczeniowych OSE i systemów wsparcia
- wykrywać i zapobiegać włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym

Ponad to w każdym Regionalnym Węźle Bezpieczeństwa zostaną zainstalowane mechanizmy ochrony użytkownika sieci OSE, realizowane w oparciu o systemy klasy SWG.

4.1. Architektura Infrastruktury Bezpieczeństwa

Architektura Infrastruktury bezpieczeństwa składa się z Systemu ADC, Systemu inspekcji SSL/TLS, Systemu NG Firewall, Systemu DNS, Systemu zarządzającego oraz Systemu SWG.

Poniżej zaprezentowano schemat blokowy przepływu danych w Regionalnych Węzłach Bezpieczeństwa. Schemat zawiera systemy Zamawiającego, składające się na Infrastrukturę bezpieczeństwa.



Infrastruktura bezpieczeństwa zostanie oparta o urządzenia/systemy zastępujących producentów:

- ADC (LTM) – F5 Networks
- SSLO (deszyfracja) – F5 Networks
- SSL VPN, ADC, WAF – F5 Networks
- Firewall – Fortigate
- DNS – InfoBlox

Systemy Wsparcia

Zamawiający planuje większość procesów realizować w sposób zautomatyzowany. Systemy i infrastruktura objęte zostaną zintegrowane z centralnymi systemami nadzorującymi działanie wszystkich elementów sieci OSE.

5. Opis przedmiotu zamówienia

5.1. Opis ogólny

Przedmiotem zamówienia jest wdrożenie wraz z dostawą, instalacją, uruchomieniem dedykowanej mocy obliczeniowej dla projektu SWG w wyznaczonym przez zamawiającego miejscu, zgodnie z przedstawionymi w dokumencie uwarunkowaniami wdrożenia, do kolokacji. W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do:

- wykonania szczegółowego dokumentacji wdrożeniowej serwerów do infrastruktury zamawiającego z kolokacji zgodnie z wytycznymi zamawiającego (dokumentacja wdrożenia serwerów)
- wdrożenia (dostawa, instalacja, podłączenie, konfiguracja, instalacja warstwy wirtualizacyjnej wraz z zarządzaniem, uruchomienie i integracja) serwerów zapewniających moc obliczeniową w sposób maksymalnie zautomatyzowany dla skrócenia czasu implementacji

- dostarczenie opisu parametrów wydajnościowych dla dostarczonych serwerów obejmujących miedzy innymi: rodzaj procesowa liczbę rdzeni i taktowanie, suma pamięci RAM, liczba dysków w tym typ RAID i dostępna pamięć dyskowa
- świadczenie usług wsparcia serwisowego dla dostarczonych urządzeń, zgodnie z wymaganiami Zamawiającego
- realizacja czynności wchodzących w zakres utrzymania serwisowego w ramach wdrożonego rozwiązania w okresie obowiązywania umowy na warunkach opisanych w niniejszym dokumencie
- opcjonalnego wydłużeniu przez Zamawiającego czasu świadczenia usługi i wsparcia serwisowego

Serwery muszą zostać wdrożone zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie. Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne, ilościowe i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny. Wykonawca zobowiązany jest do spełnienia wymagań obligatoryjnych w ramach ceny oferowanego Rozwiązania.

Wykonawca jest zobowiązany do zaproponowania Rozwiązania optymalnego pod względem jak najmniejszej ilości komponentów różnych producentów.

6. Warstwa infrastruktury

6.1. Wstęp

Wymagane jest dostarczenie infrastruktury serwerowej, która będzie się składać na środowisko obliczeniowe.
Głównym celem dostawy dedykowanej mocy obliczeniowej jest zapewnienie zasobów dla:

- Platformy Security Web Gateway

Pozostałe wymagania dla Wykonawcy przy dostawie środowiska:

- zapewnienie odpowiedniej mocy obliczeniowej wraz z warstwą wirtualizacyjną i jej zarządzaniem;
- powierzchni do składowania danych dla powyższego systemu;
- wysoka skalowalność rozwiązania i efektywne wykorzystanie zasobów sprzętowych poprzez zgodność środowiska z platformą wirtualizacyjną;
- uproszczenie zarządzania infrastrukturą serwerową poprzez zastosowanie kart zarządzających;
- zapewnienie wirtualizatora zgodnego z wymaganiami na systemem SWG, zgodnie z opublikowanym ogłoszeniem na stronie https://bip.nask.pl/bip/zamowienia-publiczne/208,Usluga-wdrozenia-i-udostepnienia-Systemu-SWG-Secure-Web-Gateway-w-celu-swiadczen.html;

6.2. Założenia techniczne

Wymagana jest architektura serwerowa zbudowana w modelu prywatnej dedykowanej mocy obliczeniowej wraz warstwą wirtualizacyjną i jej zarządzaniem. Moc obliczeniowa ma być umieszczona w centrum przetwarzania danych w Warszawie. W celu zapewnienia odpowiedniej ciągłości działania, serwery zostaną zamontowane w minimum trzech szafach RACK w celu zminimalizowania wpływu zdarzeń losowych na ciągłość działania systemu. Wymaga się użycia rozwiązań pozwalających zarządzanie

infrastrukturą serwerową i wirtualizacją. Poniżej zebrano główne założenia techniczne infrastruktury dla dedykowanej mocy obliczeniowej, które Wykonawca musi spełnić w kontekście infrastruktury obliczeniowej:

1. Infrastruktura mocy obliczeniowej ma być jak najbardziej zintegrowana, jednolita i prosta w zarządzaniu oraz odporna na awarie, musi obejmować zarówno warstwę sprzętową, jak i niezbędne oprogramowanie.
2. Wszystkie elementy systemu SWG będą uruchamiane, jako maszyny wirtualne. Wymagane jest zapewnienie odpowiedniej ilości serwerów danego typu (opisano poniżej) spełniających minimalne wymagania, ilościowe pojemnościowe i wydajnościowe dla poszczególnych typów maszyn wirtualnych:
    a. Typ A - 46 serwerów po 2x CPU 8 rdzeni, 64 GB RAM, 2 x 900GB Dysk
    b. Typ B - 2 serwery po 2x CPU 8 rdzeni, 96 GB RAM, 2 x 900GB Dysk
    c. Typ C - 2 serwery po 2x CPU 8 rdzeni, 128 GB RAM, 2 x 900GB Dysk
    d. Typ D - 10 serwerów po 2x CPU 8 rdzeni, 128 GB RAM, 4 x 2TB Dysk
3. Serwery zostaną zamontowane w minimum trzech szafach zapewniając poziom nadmiarowości (umożliwiający zastąpienie dowolnego typu serwerów) min. N+1.
4. Wdrożone rozwiązanie informatyczne musi pracować w architekturze redundantnej. Zasoby dyskowe, muszą zapewniać poziom niezawodności minimum RAID 1,5,6 na których zostaną uruchomione usługi.
5. Serwery muszą dysponować minimum dwoma portami transmisyjnymi Ethernet 10Gbps SFP+ i należy je podłączyć do dwóch przełączników LAN-DC.
6. Serwery muszą być wyposażone w redundantne zasilacze i należy je podłączyć do dwóch torów zasilania.
7. Serwery muszą być zarządzane poprzez karty zarządzające.
8. Serwery będą posiadały zainstalowane i objęte licencją na czas usługi wirtualizatory wspierane przez system SWG.
9. System wirtualizacji będzie zarządzany z jednego graficznego interfejsu.

7. Opis wymaganych funkcjonalnych dla całego systemu

7.2. Platforma dedykowanej mocy obliczeniowej - wymagania funkcjonalne

7.2.1 Wirtualizacja mocy obliczeniowej

Identyfikator wymagania	Treść wymagania

O31.F1	Zapewnienie wirtualizatora zgodnego z wymaganiami na systemem SWG, zgodnie z opublikowanym ogłoszeniem na stronie https://bip.nask.pl/bip/zamowienia-publiczne/208,Usluga-wdrozenia-i-udostepnienia-Systemu-SWG-Secure-Web-Gateway-w-celu-swiadczen.html
O31.F2	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z przedziału od 1 do 128 procesorowych
O31.F3	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM
O31.F4	Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych
O31.F5	Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root
O31.F6	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
O31.F7	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii
O31.F8	UEFI virtual BIOS – wirtualne maszyny uruchomione na systemie do wirtualizacji z wykorzystaniem technologii - Unified Extended Firmware Interface (UEFI)
O31.F9	Dostarczone oprogramowanie musi zapewniać możliwość jednolitej wirtualizacji dla wszystkich dostarczonych w ramach przedmiotu zamówienia serwerów

7.3.2 Infrastruktura dla Platformy Security Web Gateway

O32.F4	Cała infrastruktura obliczeniowa w ośrodku przetwarzania danych dla Platformy Security Web Gateway powinna składać się z serwerów opisanych w punkcie 7.3.7. Środowisko dla Platformy Security Web Gateway będzie zainstalowane na warstwie wirtualizacyjnej. Warstwa wirtualizacyjna wymagana jest ze względu na zapewnienie możliwości instalowania wirtualnych maszyn z obrazów. Środowisko zaimplementowane na serwerach nie będzie wymagało backupu, a redundancja rozwiązania zapewniona zostanie za pomocą nadmiarowych hostów.

7.3.3 Wymagania ogólne dla serwerów platformy Security Web Gateway

W ramach oferowanego Rozwiązania Wykonawca jest zobowiązany dostarczyć serwery spełniające poniższe wymagania. Wszystkie serwery muszą zostać dostarczone w wymaganej konfiguracji, wraz z wkładkami SFP+ do kart sieciowych i przełączników potrzebnymi do podłączenia ich do sieci. Serwery należy dostarczyć z kablami zasilającymi.

Identyfikator wymagania		Treść wymagania w odniesieniu do każdego serwera
O32.5.F1	Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji min. 4 lub 8 dysków 2.5" lub 3,5”Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
O32.5.F2	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów.
O32.5.F3	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
O32.5.F4	Procesor	Zainstalowane dwa procesory, w tym każdy minimalnie ośmiordzeniowy klasy x86, 40 sztuk serwerów z zegarem minimum 2Ghz na rdzeń pamięcią Cache minimum 20MB 20 sztuk serwerów z zegarem minimum 2,3Ghz na rdzeń pamięcią Cache minimum 30MB
O32.5.F5	RAM	Minimum 64GB (dla Typu A) Minimum 96GB (dla Typu B) Minimum 128GB (dla Typu C i D) (w zależności od typu serwera opisanego w rozdziale 6.2 w punkcie 2) z możliwością rozbudowy do minimum 192GB.
		Oferowane serwery muszą dysponować odpowiednią konfiguracja do uruchomienia systemu SWG.
O32.5.F6	Diagnostyka	Panel LCD lub LED umieszczony w serwerze, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, zasilania lub za pomocą dedykowanego oprogramowania do zarządzania serwerem.
O32.5.F8	Interfejsy sieciowe	2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+
O32.5.F9	Dyski twarde	Możliwość instalacji dysków SAS, SATA
		Zainstalowane, minimum 2, lub 4 dysków twardych (w zależności od typu serwera opisanego w rozdziale 6.2 w punkcie 2), każdy o pojemności min 900GB lub minimum 2TB, skonfigurowane w RAID 1 lub 5, przeznaczone do instalacji sytemu wirtualizacyjnego.
O32.5.F10	Dyski capacity	Serwery wyposażone w dyski w wariantach (w zależności od typu serwera opisanego w rozdziale 6.2 w punkcie 2): min. 2 x 900GB Hot Swap SAS – (dla Typu A,B,C) min. 2 x 2TB Hot Swap – (dla Typu D)

O32.5.F11	Kontroler RAID	Kontroler obsługujący co najmniej następujące poziomy RAID 1, 5, 6. Wyposażony w min. 1GB pamięci nieulotnej cache.
O32.5.F13	Wbudowane porty	min. 2 porty USB 2.0 w obudowie, 1 port VGA
O32.5.F14	Video	Zintegrowana karta graficzna
O32.5.F15	Wentylatory	Redundantne
O32.5.F16	Zasilacze	Redundantne, Hot-Plug
O32.5.F17	Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
		· zdalny dostęp do graficznego interfejsu Web karty zarządzającej
		· zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera)
O32.5.F18	Certyfikaty	Serwer musi posiadać deklarację CE.
		Microsoft Windows Server min. w wersji 2008x64
		Vmware ESXi 6.0
O32.5.F19	Usługa Wsparcia Serwisowego-warunki	Usługa Wsparcia Serwisowego musi świadczona w modelu NBD z czasem skutecznej naprawy lub wymiany każdego z komponentów Systemu w ciągu 24 godzin liczonych od momentu zgłoszenia przez Zamawiającego do Wykonawcy, na adres Wykonawcy podany w Umowie. W ramach ww. Usługi Wykonawca jest zobowiązany do odbioru od Zamawiającego i dokonania instalacji i uruchomienia naprawionego bądź wymienionego komponentu Systemu w centrum przetwarzania danych Zamawiającego, w którym świadczona jest Usługa Udostępniania Systemu.
O32.5.F20	Elementy instalacyjne	Oferowane rozwiązanie musi być dostarczone z kompletem niezbędnych elementów do jego instalacji takich jak: szyny montażowe, przewody zasilające, kable Ethernet), 4 moduły SFP+ MultiMode (2 szt. w dostarczanym urządzeniu oraz 2 szt. w przełączników DC-LAN), 2 patchcordy światłowodowe duplex MMC LC/PC – LC/UPC do połączenia oferowanego rozwiązania z przełącznicą światłowodową ODF w szafie.
O32.5.F22	Wirtualizator	Serwer musi posiadać zainstalowany wirtualizator w wersji takiej samej na wszystkich serwerach pozwalając na instalowanie wirtualnych maszyn z obrazów maszyn wirtualnych. Wspierający możliwość uruchamiania maszyn wirtualnych o parametrach min. 16xCPU, min 128GB RAM, min. 4x2TB Dysk.
O32.5.F22	Licencja	Serwer musi posiadać licencję pozwalającą na uruchomienie nielimitowanej liczby wirtualizatorów w jednym centrum danych, jak również nielimitowanej

		liczby procesorów dostępnych na wirtualizatorze na potrzeby maszyn wirtualnych. Wykonawca dostarcza licencje zgodnie z modelem licencjonowania producenta do wirtualizacji. Liczoną od dnia 20.12.2019r.

7.5. Wymagania wdrożeniowe

7.5.1. Zakres prac

Wymagania w zakresie prac wdrożeniowych realizowanych przez Wykonawcę w ramach przedmiotu zamówienia:

Nr Wymagania	Treść Wymagania
O51.F1	dostarczenie sprzętu do wyznaczonej przez Zamawiającego kolokacji
O51.F2	zamontowanie i uruchomienie sprzętu w wyznaczonych szafach serwerowych (szyny montażowe i zasilanie redundantne)
O51.F3	konfiguracja sprzętu (zasoby dyskowe)
O51.F4	podłączenie sprzętu do wyznaczonych portów w przełącznicy ODF w szafie
O51.F5	instalacja i konfiguracja platformy wirtualizacyjnej wraz z jej zarządzaniem
O51.F8	podłączenie portów zarządzających do sieci zarządzającej
O51.F10	konfiguracja monitorowania i zarządzania infrastrukturą serwerową
O51.F11	przeprowadzenie testu dostępności serwera obejmującego redundancja zasilania i sieci LAN

7.5.2. Zakres opisu i dokumentacji przygotowanego systemu

Wykonawca przygotuje dokumentacją przedwdrożeniowa i po wdrożeniową zgodnie z opisem przedmiotu umowy i wsadem technicznym dostarczonym przez zamawiającego w ramach przedmiotu zamówienia:

Nr Wymagania	Treść Wymagania
O52.F1	Wsad techniczny zamawiający dostarczy w dniu podpisania umowy (lokalizację DC, liczbę szaf RACK, adresację IP, VLANy, porty na przełącznikach)

Nr Wymagania	Treść Wymagania
O52.F2	Dokumentacja powdrożeniowa Wykonawca dostarczy po zakończeniu wdrożenia usługi w dniu odbioru zamówienia.
O52.F3	Dokumentacja musi zawierać, listę dostarczonych komponentów serwerowych z podziałem na typy, schemat podłączenia portów Ethernet Data LAN-DC, adresacje IP i podział na VLANy w ramach dostarczonego środowiska, opis zarządzania serwerami fizycznymi, opis przygotowanego rozwiązania zapewniającego moc obliczeniową w modelu zwirtualizowanym.
O52.F4	Dokumentacja powdrożeniowa musi zawierać zbiór danych określających przygotowane konta dostępu: logiczny, hasła i sposób dostępu do platformy sprzętowej i wirtualnej.
O52.F5	Dokumentacja powdrożeniowa musi zawierać status przeprowadzonych testów odbiorczych obejmujących redundancję w obszarze zasilania i sieci LAN-DC.

7.5.3. Zakres usług wsparcia serwisowego

Wymagania na usługi wsparcia serwisowego realizowanych przez Wykonawcę w ramach przedmiotu zamówienia:

Nr Wymagania	Treść Wymagania
O53.F1	Możliwość zgłaszania wad i usterek w pracy środowiska będzie realizowana w godzinach 8:00-18:00 w tracie obowiązywania umowy pod wskazanym przez wykonawcę numerem tel. i adresem poczty elektronicznej email wskazany dokumentacji powdrożeniowej.
O53.F2	Przyjęcie zgłoszenie serwisowego musi nastąpić w ciągu 8 godz. od zgłoszenia.
O53.F3	Czas skutecznej naprawy lub obejścia problemu, musi nastąpić w ciągu 24h od zgłoszenia w dni robocze. Problem zgłoszony ostatniego dnia pracującego np. w piątek musi zostać rozwiązany w następnego dnia pracującego np. w poniedziałek.
O54.F4	Wymiana uszkodzonego serwera w kolokacji Zamawiającego obejmie: demontaż i montaż nowego sprzętu, podłączenie kabli i uruchomienie serwera, instalacja wirtualizatora i integracja z systemem zarządzania środowiskiem.
O53.F5	Dostęp do kolokacji zamawiającego realizowany jest w cyklu 24/7/365 i w tym okresie realizacji usług serwisowych w lokalizacji Zamawiającego. Wizyta w kolokacji wymaga zgłoszenia z wyprzedzeniem 8h.