Załącznik nr 1 do Zapytania Ofertowego/ Umowy …..

Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

1. Definicje

ADC (Application Delivery Controller)	System realizujący równomierne rozłożenie obciążenia na Urządzenia należące do Systemów ADC, NG Firewall, inspekcji ruchu SSL/TLS.
Asysta techniczna	Wykonywanie przez Wykonawcę konsultacji i prac dodatkowych w zakresie funkcjonowania Systemu.
AV (Antivirus)	Funkcjonalność, której celem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych w komunikacji sieciowej.
AV dla HTTP	Funkcjonalność, której celem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych w komunikacji sieciowej ruchu http(s).
Awaria	Każda nieprawidłowość w działaniu Systemu, niezależnie czy powstała z przyczyn, za które odpowiada Wykonawca, w wyniku której zostaje spełniona jedna z wymienionych niżej przesłanek: - nie jest możliwe korzystanie przez Zamawiającego z jakiejkolwiek funkcjonalności lub elementów Systemu; - istnieją zakłócenia w działaniu funkcjonalności Systemu mające wpływ na świadczenie przez Zamawiającego usług OSE; - nie jest zapewniona lub jest zakłócona redundancja poszczególnych elementów Systemu; - System wykazuje niestabilność, która może wpłynąć na utratę wydajności Systemu lub pogorszenie jakości usług;. - stwierdzenie stanu Systemu jest utrudnione
BGP	Zewnętrzny protokół trasowania (routingu) EGP. BGP w wersji czwartej jest podstawą działania współczesnego Internetu. Istnieje wiele rozszerzeń BGP stosowanych przy implementacji MPLS VPN, IPv6 czy Multicast VPN. Jest protokołem wektora ścieżki umożliwiającym tworzenie niezapętlonych ścieżek pomiędzy różnymi systemami autonomicznymi. Obecny otwarty standard protokołu BGP jest opisany w dokumentach RFC 4271 i 1771. Protokół ten nie używa tradycyjnych metryk - analogiczną funkcję (determinanty wyboru trasy) pełnią atrybuty i algorytm wyboru. BGP pozwala na pełną redundancję w połączeniu z Internetem, jest również używany do połączenia dwóch systemów

	autonomicznych, do wymiany ruchu między tymi systemami. Protokół BGP funkcjonuje w oparciu o protokół warstwy 4 modelu OSI (port TCP o numerze 179). Zapewnia to, że aktualizacje są wysyłane w sposób niezawodny, dzięki czemu w BGP niepotrzebne są mechanizmy retransmisji, segmentacji, itp. Routery zestawiają pomiędzy sobą sesje BGP, dzięki którym mogą wymieniać się informacjami o dostępnych trasach (prefiksach) i wyznaczać najlepszą niezapętloną ścieżkę do sieci docelowych.
Centralny Węzeł Bezpieczeństwa	Węzeł Bezpieczeństwa zlokalizowany w węźle centralnym dostarczający mechanizmy ochrony Zasobów obliczeniowych OSE.
DNS Firewall	System realizujący funkcję serwera DNS odpowiadającego na zapytania opisane w RFC 1035, posiadający możliwość blokowania części z nich w oparciu o reputacje poszczególnych domen lub w oparciu o przypisane do nich kategorie treści, dzięki temu zapewniając ochronę przed szkodliwym oprogramowaniem i/lub dostępem do treści nielegalnych i szkodliwych.
DNS resolver	System realizujący funkcję serwerów DNS dla sieci OSE. Jego zadaniem jest usprawnienie oraz przyśpieszenie procesu dostarczania odpowiedzi systemom i użytkownikom OSE na zapytania dotyczące adresów sieciowych.
Dynamiczna analiza treści	Funkcjonalność Systemu SWG, której celem jest zapewnienie użytkownikom OSE ochrony przed niebezpiecznymi treściami, poprzez mechanizm dynamicznej analizy treści dostępnych na stronach www, oparty o analizę leksykalną lub dynamiczne mechanizmy uczenia maszynowego.
Filtrowanie treści adresów URL	Funkcjonalność Systemu SWG, której celem jest zapewnienie ochrony użytkownikom OSE poprzez analizę zapytań HTTP i porównywanie adresów URL z specjalizowaną bazą danych dostarczoną i aktualizowaną przez producenta Systemu, mające na celu rozróżnienie dobrych i złych treści oraz zablokowanie tych drugich zgodnie z ustaloną polityka filtrowania.
FTP	Protokół transferu plików typu klient-serwer wykorzystujący TCP wykorzystujący dwukierunkowy transfer plików. FTP jest zdefiniowany przez RFC 959.

FW (Firewall)	Funkcjonalność zapewniająca kontrolę ruchu sieciowego na poziomie połączeń z sieciami o różnych poziomach zaufania, zapewniająca separację niechcianego ruchu sieciowego w celu uniemożliwienia dostępu nieuprawnionym osobom z sieci zewnętrznych do sieci chronionej.
Godzina Robocza	Pełna godzina zegarowa pomiędzy 8.00 – 17.00 w Dniu Roboczym.
IdP (Identity Provider)	System służący do tworzenia, utrzymywania i udostępniania tożsamości dla celów uwierzytelniania i autoryzacji dla zewnętrznych podmiotów.
IMAP	Internetowy protokół wykorzystywany do zarządzania wieloma folderami pocztowymi oraz pobieranie i operowanie na listach znajdujących się na zdalnym serwerze. Opisany w dokumentach RFC 3501, 4466, 4469, 4551, 5032, 5182, 5738, 6186, 6858, 7817, 8314, 8437, 8474.
Infrastruktura bezpieczeństwa	Zbiór Urządzeń i Oprogramowania zapewniających bezpieczeństwo teleinformatyczne OSE. Składa się z systemów NG Firewall, ADC, DNS, inspekcji ruchu SSL/TLS, SWG zainstalowanych w Regionalnych i Centralnych Węzłach Bezpieczeństwa.
Instruktaż	Instruktaż dla operatorów i administratorów Systemu po stronie Zamawiającego.
Inżynieria ruchu	Funkcjonalność zapewniająca możliwość decydowania o różnych metodach przetwarzania ruchu sieciowego ze względu na jego parametry, np. przepuszczenie ruchu do stron instytucji finansowych bez dekrypcji ssl.
Kierownik Projektu	Osoba działająca w imieniu powołującej ją Strony (odpowiednio przez Zamawiającego i przez Wykonawcę), której zadaniem jest nadzór nad wykonywaniem Umowy i wykonywanie innych uprawnień i obowiązków wskazanych w Umowie.
Kontrola aplikacji (Application control)	Funkcjonalność zapewniająca możliwość rozpoznawania aplikacji sieciowych i decydowania o dopuszczaniu możliwości ich komunikacji z siecią Internet.
LDAP (Lightweight Directory Access Protocol)	Protokół przeznaczony do korzystania z usług katalogowych. Jest to również nazwa własna usługi katalogowej przechowującej informacje o użytkownikach i ich atrybutach.
Monitorowanie urządzeń pod względem obciążenia	Funkcjonalność zapewniająca wykrywanie przeciążeń działania urządzeń (serwerów), świadczących usługi.

MPLS	Technika stosowana przez routery, w której trasowanie pakietów zostało zastąpione przez tzw. przełączanie etykiet. MPLS nazywany jest "protokołem warstwy 2,5", ponieważ korzysta z zalet warstwy 2 (modelu OSI) – wydajności i szybkości oraz warstwy 3 – skalowalności. Łącząc je, poprawia działanie usług dostarczanych w sieciach IP. Umożliwia rezerwacje pasma dla przepływu ruchu, gwarantuje rozróżnienie wymagań Quality of Service i implementowanie VPN.
NTP	Protokół synchronizacji czasu w sieci pakietowej. Najbardziej aktualna wersja protokołu to wersja czwarta kompatybilna wstecz z wersją trzecią. Obie wersje zostaly opisane w RFC , odpowiednio wersja trzy 1305 wersja cztery 5905.
Oprogramowanie	Oprogramowanie instalowane na Urządzenu i sprzęcie Zamawiającego w ramach realizacji Umowy wraz z dokumentacją, modyfikacjami, uaktualnieniami (SW update) i nowymi wersjami (SW upgrade), spełniające wymagania opisane w niniejszym Załączniku, które ma być dostarczone przez Wykonawcę na rzecz Zamawiającego w celu realizacji przedmiotu zamówienia
OSPF	Protokół trasowania dynamicznego oparty o analizę stanu łącza. Został oparty głównie o algorytm przeliczania trasy Dijkstry - gdzie każdy router wewnątrz obszaru komunikuje się ze swoimi sąsiadami, wymieniając z nimi informacjami o nawiązanych sąsiedztwach i łączach pomiędzy nimi. Oznacza to, że w ramach pojedynczego obszaru wszystkie routery znają całą jego topologię i wymieniają się między sobą informacjami o stanie łączy. Cechami protokołu OSPF są: trasowanie wielościeżkowe, trasowanie najmniejszym kosztem i Równoważenie obciążenia. Zdefiniowany on został jako OSPF wersja 2. w RFC 2328 dla IPv4, a aktualizacja dla IPv6 jako OSPF wersja 3. w RFC 5340.
POP3	Protokół internetowy wykorzystywany do pobierania poczty elektronicznej ze zdalnego serwera do komputera lokalnego. Działa poprzez port 110 TCP, a jego wersja szyfrowana poprzez port 995 Popisany w RFC 1734. Dodatkowo Wersja SSL została opisana w RFC 3207. Dokumenty opisujące dodatkowe funkcjonalności POP3

	RFC 1939 – Post Office Protocol – Version 3, RFC 2449 – POP3 Mechanizm Rozszerzania, RFC 1734 – Polecenia uwierzytelniania POP3 AUTH, RFC 2222 – Uwierzytelnianie SASL, RFC 3206 – Kody błędów SYS oraz AUTH POP.
Portal OSE	Portal udostępniający użytkownikom informację o stanie usług OSE oraz umożliwiający sterowanie tymi usługami dla użytkowników końcowych.
Pracownicy Stron	Osoby zatrudnione przez każdą ze Stron lub spółki powiązane w rozumieniu – art. 4 § 1 pkt 5 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych, jak też osoby zatrudnione przez Strony lub spółki powiązane na innej niż umowa o pracę podstawie.
Protokół HTTP	Protokół warstwy aplikacyjnej obsługujący w sieci komunikację ruchu webowego związanego z przestrzenią WWW (World Wide Web). Obecną definicję HTTP stanowi RFC 2616. Za pomocą protokołu HTTP przesyła się żądania udostępnienia dokumentów WWW i informacje o kliknięciu odnośnika oraz informacje z formularzy. Zadaniem stron WWW jest publikowanie informacji – natomiast protokół HTTP właśnie to umożliwia. HTTP standardowo korzysta z portu nr 80 (TCP).
Protokół HTTPS	Szyfrowana wersja protokołu HTTP, w przeciwieństwie do komunikacji niezaszyfrowanego tekstu w HTTP klient-serwer, HTTPS szyfrował dane przy pomocy protokołu SSL, natomiast obecnie używany jest do tego celu protokół TLS. HTTPS działa domyślnie na porcie nr 443 w protokole TCP, opisuje go RFC 2660.
RADIUS	Remote Authentication Dial In User Service – usługa zdalnego uwierzytelniania użytkowników, używana głównie z systemami telekomunikacyjnymi. Zdefiniowana w następujących RFC: RFC 2865, RFC 2866, RFC 3579.
Regionalny Węzeł Bezpieczeństwa	Węzeł Bezpieczeństwa zlokalizowany w węźle regionalnym i dostarczający mechanizmy ochrony szkół podłączonych do danego węzła regionalnego.
Równoważenie obciążenia (LB - Load Balancers)	Funkcjonalność zapewniająca sterowanie ruchem sieciowym na bazie polityk definiowanych przez Zamawiającego, w celu m.in. równoważenia obciążenia i przełączania awaryjnego zarówno pomiędzy systemami w jednym węźle, jak i pomiędzy systemami zlokalizowanymi w różnych węzłach sieci.

SAML (Security Assertion Markup Language)	Protokół służący do wymiany danych uwierzytelniania i autoryzacji w domenach zabezpieczeń. W modelu domeny SAML dostawca tożsamości jest specjalnym typem urzędu uwierzytelniania. Dostawca tożsamości SAML jest jednostką systemową, która wydaje zapewnienie uwierzytelniania w połączeniu z profilem SSO SAML. Strona ufająca, która zużywa te zapewnienie uwierzytelniania, jest nazywana dostawcą usług SAML.
Sieć OSE (Ogólnopolska Sieć Edukacyjna)	Publiczna sieć telekomunikacyjna służąca świadczeniu publicznie dostępnych usług telekomunikacyjnych szkole w rozumieniu art. 2 pkt 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2017 r. poz. 59 i 949), z wyjątkiem szkół dla dorosłych, zwanej dalej „szkołą”.
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, retencję logów oraz przeszukiwanie, raportowanie i tworzenie reguł korelacyjnych.
Siła wyższa	Wydarzenie lub okoliczność o charakterze nadzwyczajnym, na którą Wykonawca ani Zamawiający nie mają wpływu; wystąpieniu której Wykonawca ani Zamawiający, działając racjonalnie, nie mogli zapobiec przed zawarciem Umowy; której, w przypadku jej wystąpienia, Wykonawca ani Zamawiający, działając racjonalnie, nie mogli uniknąć lub jej przezwyciężyć; oraz która nie może być zasadniczo przypisana Wykonawcy ani Zamawiającemu.
SMTP	Protokół internetowy wykorzystywany do przekazywania poczty elektronicznej w Internecie . Standard został zdefiniowany w dokumencie RFC 821, a następnie zaktualizowany w 2008 roku w dokumencie RFC 5321.
SNMP	Rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi i serwerami za pośrednictwem sieci IP . Do transmisji wiadomości SNMP wykorzystywany jest głównie protokół UDP: standardowo port 161 wykorzystywany jest do wysyłania i odbierania żądań, natomiast port 162 wykorzystywany jest do przechwytywania sygnałów *trap* od urządzeń. Protokół znany jest i wykorzystywany w następujących wersjach:

	SNMPv1 – pierwsza wersja, która została opublikowana w 1988 roku w dokumencie RFC 1067 (z późniejszymi zmianami w RFC 1098 oraz RFC 1157. W tej wersji protokołu bezpieczeństwo oparte jest na tak zwanych *communities*, które są pewnego rodzaju nieszyfrowanymi hasłami umożliwiającymi zarządzanie urządzeniem. SNMPv2 – eksperymentalna wersja protokołu, określana także SNMPv2c, opisana w dokumencie RFC 1901. SNMPv3 – obsługująca uwierzytelnianie oraz szyfrowaną komunikację wykorzystującą szyfrowanie SHA i MD5.
SSH	Standard protokołów szyfrowania komunikacji typu klient-serwer , a także serwer-klient Protokoły z rodziny SSH korzystają zwykle z portu 22 protokołu TCP. Protokół SSH jest zaimplementowany na warstwie aplikacji modelu OSI w ramach połączenia TCP. Protokół SSH jest opisany szczegółowo w RFC 4251 i 4254.
SSL VPN dla DC (SSL-VPN – skrót od ang. Secure Socket Layer i Virtual Private Network)	System służący do bezpiecznej, szyfrowanej transmisji danych w ramach „wirtualnej prywatnej sieci". W sieci OSE wykorzystywany do umożliwienia bezpiecznego, zdalnego dostępu dla administratorów sieci OSE oraz zewnętrznych firm współpracujących z Operatorem OSE.
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.
System	Urządzenie wraz z Oprogramowaniem wchodzące w skład przedmiotu zamówienia
System DNS **(Domain Name System)**	System umożliwiający świadczenie usługi obsługującej rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową.
System inspekcji ruchu SSL/TLS	System odpowiedzialny za przeprowadzanie inspekcji ruchu szyfrowanego poprzez dekryptowanie i enkryptowanie ruchu, zabezpieczonego protokołami SSL/TLS (zgodnie z skonfigurowanymi politykami) i przesłanie go dalej do innych urządzeń bezpieczeństwa (NG Firewall i SWG).
System kontroli rodzicielskiej (System Parental Control)	Zbiór Urządzeń i Oprogramowania zapewniających funkcje ochrony użytkownika sieci OSE pod kątem filtracji treści nielegalnych i szkodliwych udostępnionych

	w Internecie, udostępniany w postaci aplikacji klienckiej na urządzenia należące do użytkowników końcowych, w tym w szczególności na urządzenia mobilne. System będzie się składał z dwóch aplikacji: klienta i konsoli zarządzającej pozwalającej na zarządzanie polityką bezpieczeństwa skonfigurowaną na kliencie, oraz z serwerów obsługujących żądania z aplikacji.
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 modelu OSI, z wykorzystaniem mechanizmów statefull packet inspection, intrusion prevetion system, application control, antivirus.
System SWG (Security Web Gateway)	Oprogramowanie zapewniające funkcje ochrony użytkownika sieci OSE pod kątem filtracji treści nielegalnych i szkodliwych udostępnionych w Internecie z wykorzystaniem funkcjonalności filtracji adresów URL, funkcjonalności dynamicznej analizy treści i funkcjonalności AV.
Urządzenie/Urządzenia	Urządzenie/urządzenia nabywane i dostarczone oraz zainstalowane i skonfigurowane w ramach umowy wraz z dokumentacją, koniecznym oprogramowaniem, licencjami, wyposażeniem, komponentami, akcesoriami, elementami zapewniającymi właściwą instalację i używanie Urządzenia zgodnie z przeznaczeniem; zwane dalej Urządzeniem
Ustawa OSE	Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej.
Użytkownicy Sieci OSE / Użytkownicy	Użytkownicy usług Sieci OSE w tym m.in.: uczniowie, nauczyciele, pracownicy administracyjni, osoby i systemy korzystające z usług OSE.
VPN	Tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi, za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa. Określenie "wirtualna" oznacza, że sieć ta istnieje jedynie jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z

	VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. Rozwiązania oparte na VPN stosowane są np. w sieciach korporacyjnych firm, których zdalni użytkownicy pracują ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie).
VRF	Technologia pozwalająca koegzystować wielu instancjom tablic routingu na tym samym routerze w tym samym czasie. Głównym aspektem tej funkcjonalności jest separacja wirtualnych tablic routingu wobec siebie bez potrzeby zastosowania wielu ruterów.
WAF (Web Application Firewall)	System Web Application Firewall zapewniający ochronę aplikacyjną dla udostępnianych przez Operatora OSE serwisów www, np. portal OSE, systemy udostępniane zewnętrznym firmom współpracującym z Operatorem OSE.
Wdrożenie Systemu	Dostawa, instalacja, integracja i uruchomienie Systemu w centrum przetwarzania danych wskazanym przez Zamawiającego wraz z dostarczeniem Dokumentacji, w tym wykonanie konfiguracji Systemu zgodnie z wytycznymi Zamawiającego. Wykonanie Wdrożenia Systemu zostanie potwierdzone w Protokole odbioru końcowego
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, SWG 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.
Wsparcie techniczne producenta	Zakupiony przez Wykonawcę u producenta razem z Systemem pakiet wsparcia technicznego, umożliwiający zgłoszenie i usuwanie błędów i usterek.
Wyjątki SSL	Funkcjonalność zapewniająca wykluczenie określonych kategorii, takich jak stron instytucji finansowych (banki, domy maklerskie, firmy ubezpieczeniowe), medycznych i

	innych przetwarzających dane wrażliwe, z procesu inspekcji ruchu SSL/TLS w sieci OSE.
Zasoby obliczeniowe OSE / chmura obliczeniowa OSE	Infrastruktura serwerowa udostępniona w celu zapewnienia mocy obliczeniowej tj. procesory, pamięć RAM, przestrzeń dyskowa wybudowana na potrzeby systemów i usług OSE.

2. Wstęp

2.1. Podstawa opracowania projektu

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, którym jest NASK Państwowy Instytut Badawczy.

2.2. Cele realizacji sieci OSE

W Polsce istnieje 25 015 szkół zlokalizowanych w 19 500 lokalizacjach. 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, w tym umożliwiających ochronę użytkowników,
3) Zapewnienie dostawcom treści edukacyjnych dostępu do użytkowników sieci OSE,
4) Umożliwienia wspomagania procesu kształcenia w szkole.

2.3. Założenia projektowe

Poniżej opisano główne założenia koncepcyjne, jak również zestaw wymagań, jakie musi spełniać Infrastruktura bezpieczeństwa, w celu umożliwienia realizacji usług zgodnie z założeniami.

2.3.1. Podstawowe założenia

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 jest z węzłów zlokalizowanych na terenie 16 województw.

2.3.2. Węzły sieci

W sieci OSE istnieją dwa funkcjonalne rodzaje węzłów:

- Węzeł Regionalny składa się z Węzła Agregacyjnego, do którego będą dołączone łącza ze szkół, oraz z Regionalnego Węzła Bezpieczeństwa.
- Węzeł Centralny, składa się z Węzła Szkieletowego, do którego będą dołączone Węzły Agregacyjne, oraz z Centralnego Węzła Bezpieczeństwa i z Zasobów obliczeniowych OSE. Węzły te będą także zapewniały łączność do sieci Internet.
  Centralny Węzeł Bezpieczeństwa będzie zlokalizowany tylko w dwóch Węzłach Centralnych, w ramach Obiektów w Warszawie i Poznaniu.

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

Obiekty, w których zainstalowane są Węzły sieci OSE, podano poniżej:

Województwo	Lokalizacja węzła	Regionalny Węzeł Bezpieczeństwa	Centralny Węzeł Bezpieczeństwa
MAZOWIECKIE	Warszawa	WAW	WAW Core
ŚLĄSKIE	Katowice	KAT	-
WIELKOPOLSKIE	Poznań	POZ	POZ Core
DOLNOŚLĄSKIE	Wrocław	WRO	-
KUJAWSKO-POMORSKIE	Toruń	TOR	-
LUBELSKIE	Lublin	LUB	-
LUBUSKIE	Zielona Góra	ZGO	-
ŁÓDZKIE	Łódź	LOD	-
MAŁOPOLSKIE	Kraków	KRA	-
OPOLSKIE	Opole	OPO	-
PODKARPACKIE	Rzeszów	RZE	-
PODLASKIE	Białystok	BIA	-
POMORSKIE	Gdańsk	GDA	-
ŚWIĘTOKRZYSKIE	Kielce	KIE	-
WARMIŃSKO-MAZURSKIE	Olsztyn	OLS	-
ZACHODNIOPOMORSKIE	Szczecin	SZC	-

Schemat połączeń Węzłów Centralnych i Regionalnych został pokazany poniżej.

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

Na potrzeby skalowania wszystkich komponentów Systemu należy przyjąć, że całość ruchu do / ze szkoły kierowana jest z / do sieci Internet.

Sumaryczna ilość ruchu z sieci Internet do szkół wyniesie 1 058 Gbps, a ze szkół do sieci Internet 385 Gbps (wartości określone dla sieci projektowanej na rok 2025).

Zakłada się, że ok. 60% ww. ruchu będzie wychodziło do Internetu przez węzeł WAW-Core, a pozostałe 40% będzie równomiernie rozłożone pomiędzy pozostałe dwa Węzły Centralne. W przypadku awarii dowolnego Węzła Centralnego, ruch przechodzący przez ten węzeł rozłoży się proporcjonalnie na pozostałe dwa Węzły Centralne.

2.3.3. Infrastruktura bezpieczeństwa

Architektura Infrastruktury bezpieczeństwa składa się z Systemu SWG wraz z Systemem zarządzającym oraz z Systemu ADC, Systemu inspekcji SSL/TLS, Systemu NG Firewall, Systemu DNS. (zakup systemów ADC, DNS, NG Firewall, inspekcji ruchu SSL/TLS jest realizowany w ramach osobnego postępowania). W ramach poszczególnych systemów realizowane są funkcjonalności zgodnie z tabelką.

SWG	
1	Filtrowanie adresów URL
2	Dynamiczna analiza treści
3	AV*

System ADC	
1	Inteligentne LB
2	Monitorowanie urządzeń pod względem obciążenia
3	Wyjątki SSL
4	Inżynieria ruchu
5	Dystrybucja tożsamości do system SWG
6	Funkcjonalność WAF**
7	Funkcjonlaność SSL VPN**
System inspekcji ruchu SSL/TLS	

1	Dekrypcja i ponowna enkrypcja ruchu szyfrowanego
System NG Firewall	
1	FW
2	Funkcjonalność IPS
3	Funkcjonalność AV***
4	Funkcjonalność Kontroli aplikacji
System DNS	
1	DNS resolver
2	DNS Firewall - ochrona antymalware
3	DNS Firewall – filtracja treści

*) Funkcjonalność AV na Systemie SWG jest realizowana jedynie dla plików przesyłanych w ramach protokołów HTTP i HTTPS).

**) Funkcjonalność jest realizowana tylko w Centralnych Węzłach Bezpieczeństwa.

***) Funkcjonalność AV na Systemie NG Firewall obsługuje 9% całego ruchu określonego dla danego węzła w zakresie obsługi protokołów SMTP, IMAP, POP3, FTP, SMB i inne (z pominięciem protokołów HTTP i HTTPS).

2.3.4. Koncepcja świadczenia usługi dla szkoły

W szkołach instalowane są urządzenia CPE, świadczące usługi dla sieci lokalnych w szkołach (urządzenia te w całości pozostają poza zakresem niniejszego zapytania).

Na urządzeniach tych lokalne adresy IPv4 z pul prywatnych zgodnych z RFC1918 / BCP5 translowane są (NAT 1:1) do adresów z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153). Jednocześnie dla klientów IPv6 zaalokowana jest pula adresów GUA z puli przydzielonej dla sieci OSE przez RIPE (w sieci OSE nie będą używane adresy prywatne IPv6).

Ruch od urządzeń CPE umieszczonych w szkołach przenoszony jest przez łącza, w technologii Ethernet, operatorów agregujących do Węzłów Agregacyjnych sieci OSE, gdzie jest oddawany do

urządzeń agregujących sieci OSE na interfejsach 10GE oraz 1GE. Ruch do każdego urządzenia CPE jest oddawany na oddzielnych VLANach, przy następujących założeniach:

- każda szkoła jest terminowana na oddzielnym VLANie lub VLANach,
- z każdej szkoły może być skreowanych kilka VLANów (do pięciu), przy czym każdy z nich terminowany jest po stronie szkoły w oddzielnym VRF, a od strony sieci OSE każdy traktowany jest jako oddzielne łącze z własną adresacją i routingiem; Separacja VLANów tworzona jest na potrzeby kreowania różnych usług, w tym usług posiadających różne polityki bezpieczeństwa;
- ruch zarządzania do urządzenia CPE jest oddzielony od ruchu produkcyjnego szkoły obsługiwanej przez to CPE i terminowany jest na oddzielnym VLANie,
- ww. VLANy mogą być oddane w jednym z dwóch modeli:
    - jako VLAN z pojedynczym tagowaniem, zgodnie ze standardem IEEE 802.1q lub,
    - jako VLAN z podwójnym tagowaniem, zgodnie ze standardem IEEE 802.1ad, przy czym ruch z pojedynczej szkoły ma wspólny S-TAG oraz EtherType = 0x88a8.

Ruch odebrany w Węźle Agregacyjnym kierowany jest do Regionalnego Węzła Bezpieczeństwa.

Następnie odebrany ruch z Regionalnego Węzła Bezpieczeństwa kierowany jest do Węzłów Szkieletowych, a następnie do sieci Internet. Pomiędzy Węzłem Bezpieczeństwa, a wyjściem do sieci Internet ruch IPv4 przechodzi przez instancję CG-NAT, gdzie jest translowany do publicznych adresów IPv4 przydzielonych dla sieci OSE.

2.3.4.1. Separacja ruchu

Ruch zarządzania (zarówno dla urządzeń CPE jak też urządzeń sieci OSE) traktowany jest jako ruch zaufany i jest oddzielony od ruchu produkcyjnego do / ze szkół. Separacja tego ruchu w sieci OSE powinna nastąpić na poziomie VFR, logical system lub podobnym (tj. zapewniającym separację tablic routingu oraz wykluczającym wzajemny dostęp do ruchu z poszczególnych strumieni).

2.3.4.2. QoS

W sieci OSE wdrożony został QoS z następującymi założeniami:

- klasyfikacja odbywa się na urządzeniu agregacyjnym sieci OSE,
- najwyższy priorytet w sieci ma ruch z klasy Network Control, obejmujący ruch kontrolny protokołów routingu (IGP, BGP, MPLS, itd.) – ruch ma zagwarantowane 3% pasma na interfejsach szkieletowych sieci (tj. interfejsach pomiędzy urządzeniami sieci OSE bez uwzględnienia urządzeń CPE);
- ruch w klasie MGMT (ruch zarządzania, w szczególności ruch do / z systemów OSS, ruch sesji terminalowych do urządzeń sieciowych, ruch do kolektorów logów) – ruch ma zagwarantowane 5% pasma na interfejsach sieci (w tym na interfejsach pomiędzy urządzeniami sieci OSE a urządzeniami CPE);
- ruch w klasie BE (Best Effort) obejmujący ruch produkcyjny do / ze szkół – ruch ma zagwarantowane 50% pasma na wszystkich interfejsach;
- w sieci OSE musi być przygotowana możliwość uruchomienia ruchu w klasach:
    - VOICE – ruch priorytetowy – nie więcej niż 5% pasma;

- INTVIDEO (Interactive Video) – ruch gorszy niż NC a lepszy niż MGMT – zagwarantowane 20% pasma;
- scavenger (less-than best-effort) – ruch bez gwarancji pasma.

3. Szczegółowy opis przedmiotu zamówienia

Przedmiotem zapytania jest dostarczenie Urządzenia i Oprogramowania niezbędnego do rozbudowania całego rozwiązania, stanowiącego System DNS oraz wdrożenie Urządzenia i Oprogramowania, zgodnie z przedstawionymi uwarunkowaniami. Przedmiot zamówienia obejmuje swoim zakresem:

- Wdrożenie Urządzenia i Oprogramowania zgodnie z koncepcją techniczną, przygotowaną przez Wykonawcę, przekazaną i zaakceptowaną przez Zamawiającego najpóźniej na 5 Dni roboczych przed rozpoczęciem prac,
- rozbudowę Systemu DNS o Urządzenie umożliwiające zbudowanie wysoko dostępnego środowiska posiadanego przez Zamawiającego komponentu Infoblox Grid Master oraz jego integracja z systemami Zamawiającego, wskazanymi przez Zamawiającego, wdrożonymi na potrzeby projektu OSE,
- przeprowadzenie instruktaży dla pracowników Zamawiającego,
- przeprowadzenie testów przy udziale Zamawiającego,
- świadczenie usług gwarancyjnych dla dostarczonego Urządzenia i Oprogramowania oraz usług zgodnie z wymaganiami Zamawiającego, w tym realizacja Asysty technicznej,
- zapewnienie w ramach serwisu gwarancyjnego usług Wsparcia technicznego producenta dla wdrożonego Systemu zgodnie z wymaganiami Zamawiającego przez cały okres trwania gwarancji,
- udzielenie licencji **na okres minimum 3 lat, od daty podpisania protokołu odbioru końcowego** na Oprogramowanie dostarczane i wdrażane w ramach realizacji przedmiotu zamówienia.

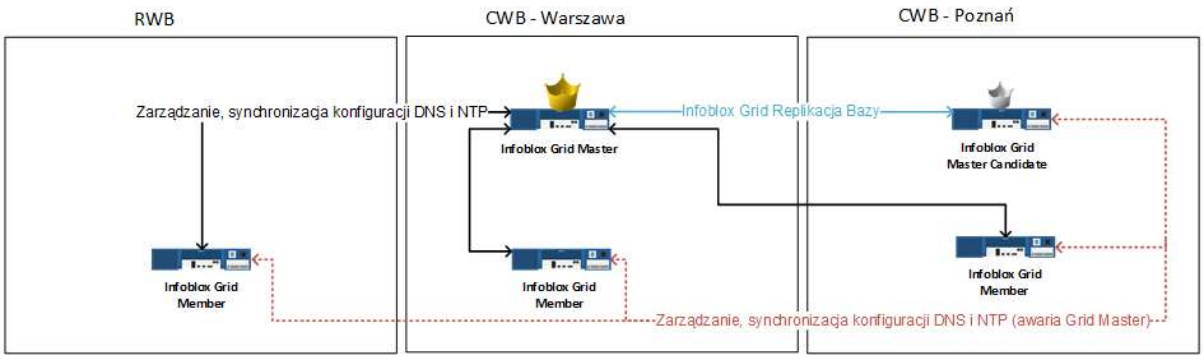
Aby zrealizować wymagane funkcjonalności opisane w niniejszym dokumencie, Wykonawca zobowiązany jest do dostarczenia Urządzenia wraz z Oprogramowaniem, niezbędnego do zbudowania całego rozwiązania, stanowiącego System.

1) Dostarczane Urządzenie i Oprogramowanie musi zostać wdrożone zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie.
2) Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny i Wykonawca zobowiązany jest do ich spełnienia w ramach oferowanego rozwiązania.
3) Wszystkie wymagania i parametry musza być spełnione łącznie.

4) Wszystkie wymagania podane w niniejszym dokumencie muszą być spełnione dla wielkości ruchu określonej w niniejszych wymaganiach, chyba że w opisie danej funkcjonalności podano inaczej.
5) W przypadku wymienienia wielu wymagań, konieczne jest spełniania wszystkich z nich (np. umieszczenie wymagania „Urządzenie musi obsługiwać multicast IPv4 (IGMPv2/3, PIM SM, SSM, MSDP)" oznacza konieczność obsługi przez urządzenie wszystkich wymienionych protokołów i ich wersji jednocześnie).
6) Wykonawca jest zobowiązany do doboru odpowiedniego Urządzenia do realizacji potrzeb Zamawiającego w zakresie budowy rozszerzenia funkcjonalności Centralnych Węzłów Bezpieczeństwa kompatybilnego z aktualnie posiadanym oprogramowaniem Infoblox GridMaster.
7) Wykonawca jest zobowiązany do współpracy z innymi dostawcami wskazanymi przez Zamawiającego przy integracji Systemu po dokonaniu jego rozbudowy z innymi systemami wskazanymi przez Zamawiającego.

3.1. Architektura systemu DNS w sieci OSE

Scentralizowane zarządzanie bazą IP Address Management (IPAM) i konfiguracją usług DNS oraz NTP na wszystkich posiadanych przez Zamawiającego urządzeniach Infoblox zostało realizowane poprzez Infoblox Grid Master. Role te będą obsługiwane przez będące w posiadaniu Zamawiającego dedykowane urządzenie Infoblox Trinzic TE-1425 w CWB Warszawa. W przypadku awarii Infoblox Grid Master w CWB Warszawa jego role przejmie posiadany przez Zamawiającego Infoblox Grid Master Candidate, który będzie zainstalowany w CWB Poznań na dedykowanym urządzeniu Infoblox Trinzic TE-1425.



3.2. Wymagania

3.2.1. Wymagania infrastrukturalne

1) Urządzenie musi być kompatybilne z aktualnie działającym u Zamawiającego systemem Infoblox Grid Master i musi umożliwiać zbudowanie klastra wykorzystującego obecnie posiadane przez Zamawiającego urządzenia Infoblox Trinzic 1425 oraz Urządzenie dostarczane przez Wykonawcę w ramach realizacji przedmiotu Umowy.

2) Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
3) Urządzenie musi być wyposażone w co najmniej trzy interfejsy Gigabit Ethernet 10/100/1000 (RJ45) i dodatkowy dedykowany interfejs Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania i minimum jeden interfejs Ethernet do dostępu typu IPMI 2.0.
4) Urządzenie posiada zasilanie prądem zmiennym 230V.
5) Urządzenie należy dostarczyć z dwoma redundantnymi zasilaczami z możliwością wymiany w trakcie pracy urządzenia (ang. Hot-swap).
6) Dostarczone Urządzenie musi być montowane w dostarczonych przez Zamawiającego szafach rack 19”.

3.2.2. Wymagania funkcjonalne

1) Pojemność bazy Systemu DNS/IP na minimum 800 000 rekordów.
2) Możliwość pełnienia funkcji zarządzania dla 40 urządzeń podsystemów usługowych.
3) Możliwość obsługi 35 administratorów Systemu jednocześnie.
4) Urządzenie musi dostarczać na bieżąco informacje o przyznawaniu adresów IP i urządzeniach, którym dany adres został przypisany (adres MAC, czas i data przyznania adresu, IP).
5) Urządzenie musi dostarczać usługę zarządzania adresami IP – IPAM (IP Address Management).
6) Urządzenie musi zarządzać adresami IPv4 i IPv6 pozwalając na graficzną (mapy sieci) oraz obiektową metodę zarządzania adresacją.
7) Urządzenie musi posiadać mechanizmy kontroli wprowadzania danych (poprawność adresów IP, masek itp.).
8) Urządzenie musi umożliwiać dodawanie opisów i własnych atrybutów dla obiektów sieci, adresów IP, domen. Atrybuty te muszą umożliwiać definicję typu i rozmiaru danego atrybutu. Musi być możliwość stosowania słowników atrybutów z wymuszeniem lub proponowaniem danego typu atrybutu dla danego rodzaju obiektu. Urządzenie musi umożliwiać dziedziczenie atrybutów w ramach struktury sieci i podsieci.
9) Urządzenie musi mieć możliwość rozbudowy o mechanizm skanowania sieci i hostów/adresów IP (ang. network discovery). Mechanizm ten musi działać w trybie na żądanie oraz musi umożliwiać zaplanowanie skanowania periodycznego.
10) Urządzenie musi posiadać mechanizmy typu „znajdź 10 nieużywanych adresów z sieci X” oraz „znajdź 10 nieużywanych podsieci rozmiaru np. /24 w podsieci np. a.b.c.d/16”. Funkcja musi być dostępna dla IPv4 i IPv6.
11) Urządzenie musi umożliwiać import danych w formacie CSV bezpośrednio z GUI i posiadać szczegółową dokumentację formatu danych importowanych. Urządzenie musi umożliwiać eksport danych w formacie CSV. Format pliku eksportu danych powinien mieć taką samą strukturę (nagłówki) jak format pliku importu danych w formacie CSV.
12) System musi udostępniać bezpłatnie narzędzie do importu danych z innych systemów DNS: Bind oraz Microsoft.
13) Urządzenie musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System).
14) Obsługa minimum 40 000 zapytań DNS na sekundę na pojedynczym Urządzeniu.

15) Urządzenie musi być zgodne z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Commnents, http://www.ietf.org/rfc.html)
16) Urządzenie musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136.
17) Urządzenie musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996.
18) Urządzenie musi wspierać protokoły DNS w wersji IPv4 i IPv6.
19) Urządzenie musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF).
20) Urządzenie musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS.
21) Urządzenie musi mieć możliwość świadczenia usługi DNS dla usług Active Directory.
22) Urządzenie musi wspierać usługę DDNS.
23) Urządzenie musi wspierać bezpieczną aktualizację rekordów DNS tzw. Secure Update, ze wsparciem dla protokołu GSS-TSIG.
24) Urządzenie musi wspierać obsługę MultiMaster DNS.
25) Urządzenie musi obsługiwać mechanizm IDN (Internationalized Domain Names) – (w tym polskie znaki) i posiadać wbudowany konwerter tzw. punycode.
26) Jeżeli oprogramowanie Urządzenia działa w oparciu o licencję czasową, to należy dostarczyć licencje na wymagane funkcjonalności na okres minimum 3 lat od daty podpisania protokołu odbioru końcowego.
27) Urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.
28) Zarządzanie Systemem musi odbywać się z jednego miejsca (IP) za pomocą jednolitego systemu graficznego.
29) Urządzenie musi posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian.
30) Zarządzanie Systemem musi się odbywać przez przeglądarkę WWW bez potrzeby instalacji specjalnego oprogramowania typu agent, klient itp.
31) Urządzenie musi dostarczać mechanizm REST API do kontroli systemu, wykonywania i automatyzacji zadań wykonywanych za pomocą GUI. Na etapie realizacji przedmiotu zamówienia, Wykonawca musi dostarczyć pełną dokumentację systemu API z przykładami zastosowania itp.
32) Urządzenie musi pracować jako platforma dystrybucji plików za pomocą protokołów TFTP, FTP, HTTP, oraz oferować usługi synchronizacji czasu za pomocą protokołu NTP (Network Time Protocol).
33) Urządzenie musi posiadać funkcję budowy Systemu rozproszonego z synchronizacją danych poprzez sieć IP z centralnym zarządzaniem całym systemem.
34) Urządzenie musi dostarczać informacje o wszystkich zmianach wprowadzanych przez administratorów (kto, kiedy, co zostało zmienione).
35) Urządzenie musi mieć możliwość wysyłania tych informacji do centralnego repozytorium za pomocą mechanizmu Syslog (TCP i UDP).
36) Urządzenie musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów. Granulacja uprawnień

powinna umożliwiać konfigurowanie uprawnień dla pojedynczych obiektów typu sieć, strefa DNS, rekord DNS.

37) Urządzenie musi wspierać uwierzytelnianie użytkowników poprzez: lokalną bazę użytkowników, protokół RADIUS, protokół TACACS+, LDAP, Microsoft Active Directory oraz sprzętowy moduł bezpieczeństwa (HSM): Safenet i Thales.
38) Urządzenie musi posiadać wbudowaną bazę danych. Baza danych nie może wymagać żadnych czynności administracyjnych związanych z jej konfiguracją i utrzymaniem.
39) Urządzenie musi mieć możliwość monitorowania parametrów urządzeń przy użyciu protokołu SNMP (Simple Network Management Protocol).
40) Dostęp do konsoli administracyjnej urządzeń Systemu powinien być możliwy poprzez: Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2 i Interfejs znakowy – dostępny poprzez port szeregowy, zabezpieczony hasłem dostępu, które jest powiązane z użytkownikiem.
41) Urządzenie musi umożliwiać wykonywanie planowanych kopii bezpieczeństwa do zewnętrznego serwera w celu uproszczenia procedur odzyskiwania w razie awarii (TFTP, FTP, SCP).

3.3. Asysta Techniczna

Asysta Techniczna polegać będzie na świadczeniu przez okres świadczenia serwisu gwarancyjnego konsultacji lub wykonywaniu prac dodatkowych w zakresie funkcjonowania Systemu, przy czym nie dłużej niż do chwili wyczerpania puli 800 Godzin Roboczych przewidzianych dla realizacji tych usług lub prac.

Czynności wchodzące w zakres Asysty Technicznej będą każdorazowo zlecane Wykonawcy drogą mailową przez Kierownika Projektu Zamawiającego lub pracownika Zamawiającego odpowiedzialnego za realizację Umowy wraz ze wskazaniem ich zakresu i oczekiwanego przez Zamawiającego rezultatu oraz terminu ich wykonania. W odpowiedzi na otrzymane zlecenie Wykonawca przekaże Zamawiającemu szacowaną pracochłonność zleconych czynności Asysty Technicznej oraz możliwy termin ich wykonania. Wykonawca przystępuje do wykonania Asysty Technicznej po zaakceptowaniu przez Zamawiającego ustalonej pracochłonności oraz terminu wykonania. Po wykonaniu czynności wchodzących w zakres Asysty Technicznej Strony podpiszą protokół odbioru czynności przygotowany przez Wykonawcę (zawierający wskazanie liczby Godzin roboczych przeznaczonych na wykonanie prac zleconych).

Zamawiający może wskazać inny sposób przekazywania i obsługi zleceń w ramach Asysty Technicznej, w szczególności poprzez udostępnienie Wykonawcy dostępu do określonego systemu Zamawiającego.

Przedmiotem Asysty Technicznej mogą być w szczególności:

1) rekonfiguracja aktualnie posiadanych przez Zamawiającego systemów bezpieczeństwa wchodzących w skład Infrastruktury bezpieczeństwa,
2) integracja z innymi systemami Zamawiającego,
3) uruchamianie nowych funkcjonalności Systemu według dyspozycji Zamawiającego,

4) uproszczenie administracji modyfikacjami kategorii Infoblox DNS Parental Control. Po wdrożeniu zmian DNS ParentalControl i Filtrowanie DNS Firewall będzie modyfikowane na podstawie zmiany atrybutu danej sieci w IPAM bez konieczności dodawania konfiguracji na poszczególnych urządzeniach,
5) zatrzymanie prób ominięcia usług DNS Parental Control i DNS Firewall poprzez użycie protokołu DNS over HTTPS (DoH),
6) czynności wynikające z rozbudowy Systemu.

3.4. Gwarancja

Urządzenie musi być objęte co najmniej 4 letnim serwisem gwarancyjnym świadczonym przez Wykonawcę w reżimie 24x7xNBD. Serwis gwarancyjny musi zapewnić usługę Wsparcia technicznego producenta rozwiązania, uprawniać do wymiany Urządzenia w przypadku zdiagnozowania jego Awarii, zapewniać wsparcie telefoniczne i www w języku angielskim lub polskim w zakresie rozwiązywania problemów z Urządzeniem i Oprogramowaniem oraz dostęp do poprawek i najnowszych komercyjnie dostępnych wersji Oprogramowania (upgrade).
Awarie będą zgłaszane na dedykowany adres mailowy Wykonawcy wymieniony w umowie.

3.5. Opis Instruktażu

W ramach Umowy Wykonawca zobowiązany jest do dostarczenia Instruktażu, zgodnie z następującym zakresem:

1) Zakres Instruktażu będzie obejmował co najmniej:
   a) sposoby konfiguracji usług na posiadanym przez Zamawiającego Systemie Infoblox Grid wraz z zaawansowanymi mechanizmami i technikami diagnostycznymi,
   b) wiedzę wystarczającą do konfiguracji usług dla szkół oraz kreowania nowych usług w zakresie wszystkich funkcjonalności udostępnianych przez wykorzystywany przez Zamawiajacego system Infoblox,
   c) informacje nt. zagrożeń jakich Zamawiający może się spodziewać w protokole DNS w kontekście posiadanego Systemu Infoblox Grid oraz automatyzacji funkcji bezpieczeństwa z wykorzystaniem posiadanych przez Zamawiającego rozwiązań Infoblox.
2) Warunki przeprowadzenia Instruktażu będą następujące:
   a) w instruktażach będzie uczestniczyło 6 osób wskazanych przez Zamawiającego - każda z osób zostanie przeszkolona na poziomie podstawowym oraz zaawansowanym (łącznie co najmniej 2 instruktaże na każdą osobę z danego zakresu),
   b) instruktaże zostaną zrealizowane w autoryzowanych przez producentów ośrodkach szkoleniowych (preferowane ośrodki na terenie Warszawy lub Polski),
   c) każdy z instruktaży odbędzie się w więcej niż 1 terminie,
   d) każdy z instruktaży musi być dostarczony Zamawiającemu w postaci voucher'ów ważnych przez 24 miesiące od daty podpisania Umowy.
   e) każdy z dostarczonych instruktaży musi być autoryzowany przez producenta dostarczanego Urządzenia

3.6. Wdrożenie

Szczegółowy przebieg wdrożenia został opisany w § 6 i § 7 Wzoru Umowy.

3.7. Integracje z systemami Zamawiającego

Wykonawca we współpracy z dostawcami systemów ADC, DNS, NG Firewall, inspekcji ruchu SSL/TLS należących do Infrastruktury bezpieczeństwa i Zamawiającym wykona testy integracyjne/odbiorcze mające na celu przetestowanie całego środowiska zainstalowanego w sieci Zamawiającego. Poprawne przejście tych testów będzie podstawą do dokonania odbioru końcowego.

W szczególności Wykonawca jest zobowiązany do rozbudowy istniejącego klastra systemu DNS oraz do uproszczenie administracji modyfikacjami kategorii Infoblox DNS Parental Control. Po wdrożeniu zmian DNS ParentalControl i Filtrowanie DNS Firewall będzie modyfikowane na podstawie zmiany atrybutu danej sieci w IPAM bez konieczności dodawania konfiguracji na poszczególnych urządzeniach oraz do zaimplementowania mechanizmu mającego na celu zatrzymanie prób ominięcia usług DNS Parental Control i DNS Firewall poprzez użycie protokołu DNS over HTTPS (DoH). Powyższe działania muszą zostać zrealizowane przez Wykonawcę w sposób nie wymagający od Zamawiającego wykonywania dodatkowych inwestycji w postaci zakupu dodatkowych licencji lub rozbudowy aktualnie posiadanych systemów.

3.8. Wymagany termin realizacji przedmiotu zamówienia

Wykonawca dostarczy i zainstaluje i skonfiguruje System w nieprzekraczalnym terminie do 45 dni kalendarzowych od daty zawarcia Umowy, pozostałe prace wchodzące w skład Przedmiotu zamówienia (wdrożenie, integracja z systemami Zamawiającego, przeprowadzenie testów, dostarczenie voucherów na instruktaże) w nieprzekraczalnym terminie do 90 dni kalendarzowych od daty podpisania Umowy.