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
Aktualizacja Systemu	element Prac Planowych zgłoszonych przez Wykonawcę do Zamawiającego, których celem jest wykonanie aktualizacji elementów 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. Wystąpienie Awarii upoważnia Zamawiającego do dokonania Zgłoszenia. Do Awarii nie zalicza się czynności administracyjnych i serwisowych wykonywanych w Systemie przez Wykonawcę lub Zamawiającego;
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.
Błąd krytyczny	Działanie Systemu niezgodnie ze specyfikacją określoną w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.**y opis przedmiotu zamówienia, wpływające na zakres i jakość działania Systemu, skutkujące Awarią uniemożliwiającą wykonywanie co najmniej jednej z funkcji kluczowych (w szczególności takich jak: dostęp do sieci Internet, filtrowanie ruchu webowego, zapewnienie dostępności konsoli zarządzającej dla administratorów) przez System na rzecz wszystkich lub większości użytkowników tych funkcji, jak również uniemożliwiającą wykonywanie kluczowych funkcjonalności realizowanych przez System – niezależnie od liczby użytkowników dotkniętych taką nieprawidłowością; Błędem krytycznym jest również degradacja wydajności Systemu mającą wpływ na wszystkich lub znaczną część użytkowników; Błędem krytycznym jest również Awaria Urządzeń i ich modułów w wyniku, której System stracił redundancję;
Błąd niekrytyczny	Działanie Systemu niezgodnie ze specyfikacją określoną w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.**, wpływające na zakres i jakość działania Systemu, skutkujące Awarią powodującą zakłócenie wykonywania funkcji Systemu lub uniemożliwieniem wykonywania takich funkcji na rzecz pojedynczych użytkowników; Błędem niekrytycznym jest również degradacja wydajności Systemu mającą wpływ na pojedynczych użytkowników;
Błąd Systemu / Błąd	Przyczyna Awarii, za usunięcie której zgodnie z Umową odpowiedzialność ponosi Wykonawca. Do Błędów Systemu zalicza się Błąd krytyczny, Błąd niekrytyczny i Usterkę;
Centralny Węzeł Bezpieczeństwa	Węzeł Bezpieczeństwa zlokalizowany w węźle centralnym dostarczający mechanizmy ochrony Zasobów obliczeniowych OSE
Czas Naprawy	Czas, który upłynął od chwili przekazania Wykonawcy Zgłoszenia do chwili Naprawy;
Czas przywrócenia Systemu – zastosowanie Obejścia	Czas, który upłynął od chwili przekazania Wykonawcy Zgłoszenia do chwili zastosowania Obejścia;
Czas Reakcji	Czas liczony od chwili przekazania Wykonawcy Zgłoszenia do chwili potwierdzenia przyjęcia Zgłoszenia do realizacji;

DNS **(Domain Name System)**	Usługa obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową.
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.
Dostęp Fizyczny	wykonywanie przez Wykonawcę czynności na podstawie Umowy w lokalizacji Systemu;
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.
Dzień Roboczy	każdy dzień od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy w Polsce;
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
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.
Kategoryzacja strony	Proces realizowany za pomocą funkcjonalności dynamicznej analizy treści polegający na przypisaniu jednej z predefiniowanych kategorii do danego adresu URL na podstawie treści prezentowanych na stronie.
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.
Naprawa	Przywrócenie funkcjonowania Systemu poprzez usunięcie Błędu i doprowadzenie do działania zgodnego z parametrami eksploatacyjnymi, specyfikacją, dokumentacją lub ewentualnymi innymi uzgodnieniami pomiędzy Stronami. Naprawę uważa się za dokonaną z chwilą jej weryfikacji i potwierdzenia jej wykonania przez osobę zgłaszającą po stronie Zamawiającego;
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.
Obejście	Przywrócenie funkcjonowania Systemu poprzez usunięcie uciążliwości Błędu i doprowadzenie do działania zgodnego z odpowiednimi ustaleniami reprezentantów Stron, odpowiedzialnych za realizację Umowy. Obejście nie jest normalnym działaniem takiej funkcjonalności, zaś System działa poniżej oczekiwań wynikających z jego specyfikacji. Obejście nie jest Naprawą. Obejście pozwala realizować wszystkie procesy związane z prawidłowym działaniem Systemu, jednak wymaga podejmowania przez użytkowników innych dodatkowych czynności lub powoduje działanie Systemu poniżej wymagań określonych parametrami eksploatacyjnymi. Obejściem może być również – pod warunkiem akceptacji reprezentanta Zamawiającego, odpowiedzialnego za realizację Umowy – zmianą realizacji przebiegu procesów Systemu;
Odbiór Systemu	Potwierdzenie wykonania przez Wykonawcę Etapu 0 Systemu zgodnie z Umową i Dokumentacją;
Osoba testująca	Osoba oddelegowana ze strony Wykonawcy do wykonywania testów.
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.
Prace Planowe	Prace zgłoszone przez Wykonawcę do Zamawiającego z wyprzedzeniem 3 Dni Roboczych, o zakresie i czasie trwania zaakceptowanym przez Zamawiającego, których celem jest konserwacja i Aktualizacja Systemu, i które mogą się wiązać z przerwaniem dostępności Systemu w całości (System nie jest dostępny i nie realizuje w tym czasie swoich funkcji) lub części (działanie Systemu jest ograniczone, np. nie pozwala na filtrowanie ruchu webowego, wykonywania inspekcji ruchu SSL, nie zapewnia możliwości zalogowania użytkownika do konsoli). Prace Planowe mogą być realizowane wyłącznie poza Godzinami Roboczymi;
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;
Priorytet	Nadawany Zgłoszeniu status, w oparciu o który definiowane są Czas Reakcji i Czas Naprawy;
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, RFC2866, RFC3579
Regionalny Węzeł Bezpieczeństwa	Węzeł Bezpieczeństwa zlokalizowany w węźle regionalnym i dostarczający mechanizmy ochrony szkół podłączonych do danego węzła regionalnego.
Re-lokacja Systemu	Przeniesienie Systemu wdrożonego w ramach realizacji Etapu 0 lub Etapu 0 i 1 z pierwotnej platformy wirtualizacyjnej dostarczonej przez Zamawiającego na inną wskazaną przez Zamawiającego, wykonane przez Wykonawcę na zlecenie Zamawiającego, jeden raz w czasie trwania Umowy; Re-lokacja może być wykonana wyłącznie poza Godzinami Roboczymi;
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 (Język 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 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 **(NG**FW – 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 / System (Security Web Gateway)	Oprogramowanie będące przedmiotem niniejszego postępowania, 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.

System zarządzający	Zbiór urządzeń i oprogramowania, zapewniający Zamawiającemu możliwość zarządzania dostarczanym Systemem SWG w pełnym zakresie funkcjonalnym wymaganym w pkt 3.7 niniejszego dokumentu
Usługa Asysty Technicznej	Wykonywanie przez Wykonawcę konsultacji i prac dodatkowych w zakresie funkcjonowania Systemu;
Usługa Instruktażu	Instruktaż dla operatorów i administratorów Systemu po stronie Zamawiającego.
Usługa Wsparcia Serwisowego	Obsługa przez Wykonawcę Zgłoszeń Zamawiającego, mająca na celu Naprawę Błędów i Usterek Systemu;
Usługi	• Usługi Wdrożenia Systemu • Usługi Instruktażu • Usługi Relokacji Systemu • Usługi Udostępniania Systemu • Usługi Wsparcia Serwisowego - Usuwanie błedów • Usługi Asysty Technicznej (zmiany konfiguracji / godziny)
Ustawa OSE	Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej
Usterka	Działanie Systemu niezgodnie ze specyfikacją określoną w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.**y opis przedmiotu zamówienia, wpływające na zakres i jakość działania Systemu, skutkujące niedogodnościami w działaniu Systemu nieograniczającymi możliwości wykonywania funkcji Systemu, ale utrudniającymi pracę użytkowników Systemu;
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 Systemu;
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 t.j. procesory, pamięć RAM, przestrzeń dyskowa wybudowana na potrzeby systemów i usług OSE. Zasoby dla realizacji Etapu 0 są umieszczone w lokalizacji Warszawa. Zasoby do realizacji pozostałych Etapów są zlokalizowane we wszystkich węzłach wojewódzkich.
Zgłoszenie	Poinformowanie Wykonawcy o wystąpieniu Awarii, Błędu lub Usterki, a także poinformowanie Zamawiajacego o Pracach planowych.

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 obliczeniowymi OSE. Węzły te będą także zapewniały łączność do sieci Internet.

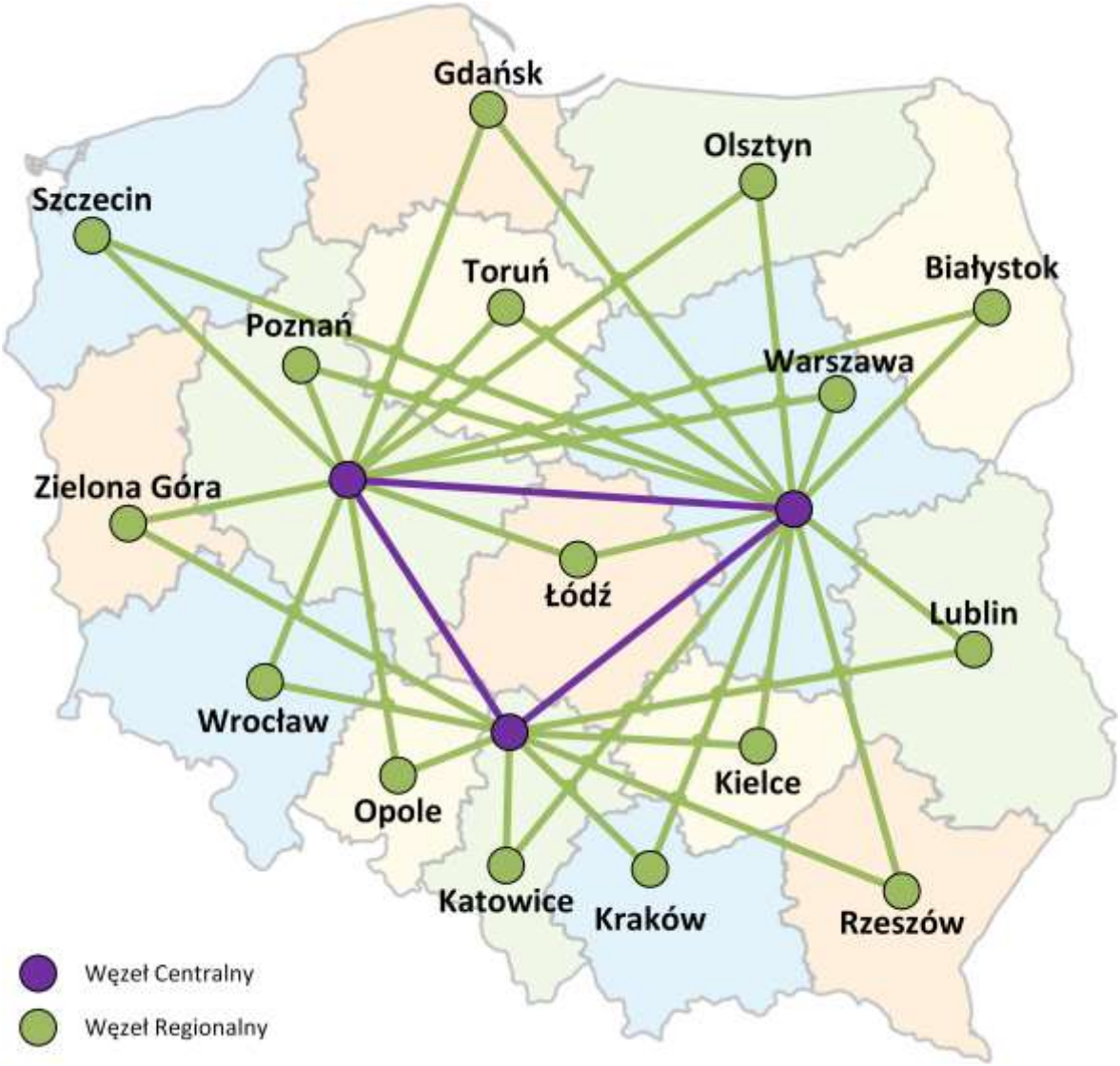
Centralny Węzeł Bezpieczeństwa będzie zlokalizowany tylko w dwóch Węzłach Centralnych, w ramach Obiektów w Warszawie i Poznaniu.

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 świadczenie na rzecz Zamawianego:

- Usługi Wdrożenia Systemu
- Usługi Instruktażu
- Usługi Relokacji Systemu
- Usługi Udostępniania Systemu– zgodnie z Gwarantowanym Poziomem Świadczenia Usług
- Usługi Wsparcia Serwisowego - Usuwanie błędów
- Usługi Asysty Technicznej (zmiany konfiguracji / godziny)

Aby zrealizować wymagane funkcjonalności opisane w niniejszym dokumencie, Wykonawca zobowiązany jest do dostarczenia Oprogramowania niezbędnego do zbudowania całego rozwiązania, stanowiącego System SWG, instalowanego na platformie wirtualizacyjnej Zamawiającego.

1) Dostarczane 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 wygania „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 dokona doboru odpowiedniego Oprogramowania do realizacji wymagań Zamawiającego w zakresie budowy Systemu SWG w Regionalnych Węzłach Bezpieczeństwa. Zamawiający dopuszcza oferowanie wielu komponentów realizujących zadania Systemu SWG w węzłach lub też jednego komponentu realizującego wszystkie niezbędne funkcje przy zachowaniu parametrów niezawodnościowych (HA). Jednocześnie proponowane rozwiązania powinny być zunifikowane.
7) Wykonawca jest zobowiązany do Wdrożenia Systemu SWG w każdym z 16 Regionalnych Węzłów Bezpieczeństwa oraz 1 węzła laboratoryjnego z uwzględnieniem podziału na Etapy.

Wdrożenie Systemu SWG obejmuje dostawę Oprogramowania, jego instalację, konfigurację, uruchomienie i przeprowadzenie procedury odbiorów, a następnie świadczenie na rzecz Zamawiającego usługi udostępniania Systemu SWG przez okres 12 miesięcy od daty protokolarnego odbioru Etapu 0, z zastrzeżeniem realizacji prawa opcji określonego w ust. 10 i 11 poniżej

8) Wykonawca jest zobowiązany do współpracy z innymi dostawcami wskazanymi przez Zamawiającego przy integracji Systemu SWG z innymi systemami wskazanymi przez Zamawiającego.
9) W ramach oferowanego przedmiotu zamówienia Wykonawca dostarczy również System zarządzający, umożliwiający Zamawiającemu konfigurację i administrację udostępnionym Systemem SWG w pełnym zakresie opisanym w ramach rozdziału 3 „Szczegółowy opis przedmiotu zamówienia".
10) Zamawiający przewiduje możliwość skorzystania z prawa opcji. Korzystanie z prawa opcji będzie polegało na:
    a) zamówieniu przez Zamawiającego Etapu 3 realizacji przedmiotu zamówienia,
    b) przedłużeniu okresu obowiązywania Umowy o okres 6 miesięcy, 2 razy po 6 miesięcy lub o 12 miesięcy

11. Szczegółowe regulacje dotyczące prawa opcji znajdują się w Załączniku nr 2 (wzór umowy) do Zapytania.

3.1. Funkcjonalności Systemu SWG

System SWG zainstalowany w każdym z 16 Regionalnych Węzłów Bezpieczeństwa będzie zawierać komponenty realizujące podstawowe funkcjonalności, m.in:

- zapewnienie mechanizmów ochrony Użytkowników na podstawie porównywania odwołań HTTP/HTTPS ze specjalizowaną bazą danych dostarczoną przez producenta i w oparciu o mechanizmy dynamicznej analizy treści
- zapewnienie mechanizmów analizy plików przesyłanych pobieranych z Internetu w celu poszukiwania wirusów
- zapewnienie mechanizmów przypisania polityk kontroli treści użytkownikom,
- monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do logów.

W ramach realizacji przedmiotu zamówienia, Wykonawca zainstaluje Węzeł laboratoryjny realizujący wszystkie funkcje wskazane dla Centralnych i Regionalnych Węzłów Bezpieczeństwa w zakresie dostarczenia Systemu SWG. Węzeł laboratoryjny pozwoli na przeprowadzenie:

- Testów aktualizacyjnych oprogramowania
- Testów przy większych zmianach konfiguracyjnych.

3.2. Architektura Infrastruktury Bezpieczeństwa

3.2.1. Podział funkcjonalny

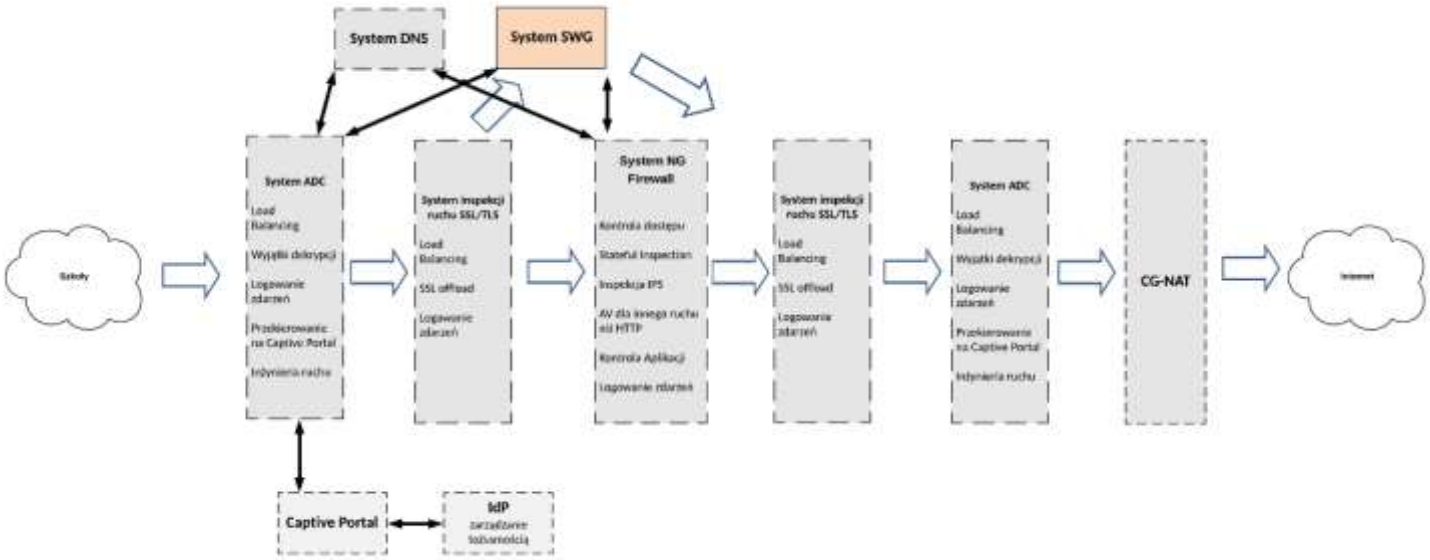
System SWG realizuje następujące funkcjonalności

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

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

3.2.2. Przepływ ruchu w węźle

Poniżej zaprezentowano schemat blokowy przepływu danych w Regionalnych Węzłach Bezpieczeństwa. Schemat przedstawia System SWG i pozostałe elementy Infrastruktury bezpieczeństwa w otoczeniu innych systemów Zamawiającego, które będą wymagały integracji z dostarczonym przez Wykonawcę przedmiotem zamówienia. Schemat blokowy przedstawiony poniżej jest wymaganiem Zamawiającego w zakresie architektury rozwiązania Infrastruktury Bezpieczeństwa.



- Cały ruch (100%) od CPE, po przejściu przez Węzeł agregacyjny, przechodzi przez System ADC, który rozkłada ruch na urządzenia dedykowane do wykonywania dekrypcji SSL (F5 BIG-IP SSL Orchestrator). Inspekcji podlega 100% ruchu SSL/TLS z pominięciem wybranych domen, pobranych z pól SNI lub CN certyfikatu, należących do kategorii treści określonych przez Zamawiającego. Informację na temat kategorii do jakiej należy dana domena, System ADC uzyska poprzez współpracę z Systemem DNS.
- Po dokonaniu deszyfracji, cały ruch zostanie przekierowany do Systemu NG Firewall, gdzie będą zdefiniowane polityki dotyczące ruchu warstwy 3/4 modelu ISO/OSI i uruchomione zostaną funkcjonalności IPS (100% ruchu), AV (9% ruchu - inspekcji AV będzie podlegał ruch niezwiązany z ruchem webowym HTTP/HTTPS) i Kontroli aplikacji (100% ruchu). System ADC przekieruje cały ruch webowy (HTTP, HTTPS) do Systemu SWG.
- System SWG dokona analizy treści w oparciu o specjalizowaną bazę URL i mechanizmy dynamicznej analizy treści (w przypadku, jeśli strona będzie zakwalifikowana do jednej z kategorii zdefiniowanych przez Zamawiającego w polityce filtrowania). Na podstawie wyników wspomnianej analizy, System SWG dokona weryfikacji wspomnianego wyniku z polityką filtrowania określoną przez Zamawiającego i przepuści lub zablokuje odwołanie do danej strony www. W drugim przypadku System SWG przekieruje użytkownika na stronę blokowania komunikującą powód blokady. Oprócz filtracji treści System SWG przeprowadzi również analizę AV dla wszystkich plików przesyłanych w ramach ruchu HTTP.
- Po dokonaniu inspekcji treści, ruch jest kierowany ponownie do urządzenia dedykowanego do obsługi ruchu SSL/TLS, w celu ponownej szyfracji SSL.
- Przed wyjściem ruchu z Regionalnego Węzła Bezpieczeństwa dokonywana jest translacja CGNAT do adresacji publicznej, po wykonaniu której ruch kierowany jest zgodnie z tablicą routingu do Węzła szkieletowego i dalej do sieci Internet.
- Ruch zarządzania (zarówno dla 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 nastąpi na poziomie VFR, logical system lub podobnym.

Zamawiający zakłada wyjątki od powyższego przepływu, które zostaną doprecyzowane przez strony (Wykonawcę i Zamawiającego) na etapie tworzenia projektu technicznego.

3.3. Skalowanie Systemu SWG

Poniższe dane mają charakter danych projektowych i zostały przedstawione w celu umożliwienia Wykonawcy zaoferowania optymalnego rozwiązania w postaci Systemu SWG spełniającej wszystkie wymagania Zamawiającego i parametry zawarte w niniejszym dokumencie.

Poniżej przedstawiono tabelę wskazującą maksymalne wartości, co do mocy obliczeniowej (liczba fizycznych rdzeni CPU), pamięci RAM (GB) i przestrzeni dyskowej (GB), jakie Zamawiający przewiduje na potrzeby instalacji i działania Systemu SWG w poszczególnych Węzłach, na dostarczonej przez Zamawiającego platformie wirtualnej.

	CPU [Liczba fizycznych rdzeni procesora]	RAM [GB]	Przestrzeń dyskowa [GB]
MAZOWIECKIE	1 134	4 032	35 759
ŚLĄSKIE	618	2 496	14 600
WIELKOPOLSKIE	346	1 408	8 800
DOLNOŚLĄSKIE	394	1 600	9 800
KUJAWSKO-POMORSKIE	250	992	6 800
LUBELSKIE	234	928	6 000
LUBUSKIE	234	928	6 000
ŁÓDZKIE	234	928	6 000
MAŁOPOLSKIE	234	928	6 000
OPOLSKIE	234	928	6 000
PODKARPACKIE	202	800	5 800
PODLASKIE	184	736	5 000
POMORSKIE	184	736	5 000
ŚWIĘTOKRZYSKIE	184	736	5 000
WARMIŃSKO-MAZURSKIE	136	544	4 000
ZACHODNIOPOMORSKIE	136	544	4 000

Platforma wirtualizacyjna Zamawiającego wykorzystywać będzie jedną z wymienionych technologii: Hyper-V, AWS lub vSphere.

3.3.1. Wymagania wydajnościowe na System SWG zainstalowany w Regionalnych Węzłach Bezpieczeństwa

W poniższych tabelach przedstawiono skalowanie Systemu SWG w rozbiciu na poszczególne Regionalne Węzły Bezpieczeństwa. Wdrożenie Systemu SWG odbywać się będzie w czterech etapach. Wszystkie podane poniżej tabele mają charakter wymagań w zakresie pojemności Systemu SWG.

3.3.1.1. Etap 0 - wymagane skalowanie Systemu SWG:

Województwo	Przepustowość Systemu SWG [Mbps]*	Liczba zapytań [HTTP(s) na sekundę]
MAZOWIECKIE	41 111	82 218

3.3.1.2. Etap 1 - wymagane skalowanie Systemu SWG:

Województwo	Przepustowość Systemu SWG [Mbps]*	Liczba zapytań [HTTP(s) na sekundę]
MAZOWIECKIE	41 111	82 218
ŚLĄSKIE	12 409	24 817
MAŁOPOLSKIE	6 290	12 581
WIELKOPOLSKIE	7 765	15 530
PODKARPACKIE	4 474	8 947
LUBELSKIE	4 101	8 203
DOLNOŚLĄSKIE	3 925	7 850
ŁÓDZKIE	3 883	7 766
POMORSKIE	3 824	7 648
KUJAWSKO-POMORSKIE	3 437	6 875
ZACHODNIOPOMORSKIE	3 262	6 523
WARMIŃSKO-MAZURSKIE	2 713	5 425
ŚWIĘTOKRZYSKIE	2 654	5 308
PODLASKIE	2 654	5 308
OPOLSKIE	2 049	4 099
LUBUSKIE	1 677	3 354

3.3.1.3. Etap 2 - wymagane skalowanie Systemu SWG:

Województwo	Przepustowość Systemu SWG [Mbps]*	Liczba zapytań [HTTP(s) na sekundę]
MAZOWIECKIE	41 111	82 218
ŚLĄSKIE	20 681	41 362
MAŁOPOLSKIE	10 484	20 968
WIELKOPOLSKIE	12 942	25 883
PODKARPACKIE	7 456	14 912
LUBELSKIE	6 835	13 671
DOLNOŚLĄSKIE	6 541	13 083
ŁÓDZKIE	6 471	12 943
POMORSKIE	6 373	12 747
KUJAWSKO-POMORSKIE	5 729	11 459
ZACHODNIOPOMORSKIE	5 436	10 871
WARMIŃSKO-MAZURSKIE	4 521	9 042
ŚWIĘTOKRZYSKIE	4 423	8 846
PODLASKIE	4 423	8 846
OPOLSKIE	3 415	6 831

LUBUSKIE	2 795	5 590

3.3.1.4. Etap 3 - wymagane skalowanie Systemu SWG - opcja

Województwo	Przepustowość Systemu SWG [Mbps]*	Liczba zapytań [HTTP(s) na sekundę]
MAZOWIECKIE	41 111	82 218
ŚLĄSKIE	24 817	49 634
MAŁOPOLSKIE	12 581	25 162
WIELKOPOLSKIE	15 530	31 060
PODKARPACKIE	8 947	17 894
LUBELSKIE	8 202	16 405
DOLNOŚLĄSKIE	7 849	15 700
ŁÓDZKIE	7 765	15 532
POMORSKIE	7 648	15 296
KUJAWSKO-POMORSKIE	6 875	13 751
ZACHODNIOPOMORSKIE	6 523	13 045
WARMIŃSKO-MAZURSKIE	5 425	10 850
ŚWIĘTOKRZYSKIE	5 308	10 615
PODLASKIE	5 308	10 615
OPOLSKIE	4 098	8 197
LUBUSKIE	3 354	6 708

*) „Przepustowość Systemu SWG [Mbps]" liczona przy założeniu uruchomionej polityki bezpieczeństwa uwzględniającej zastosowanie:

- 1 globalnej whitelisty,
- 1 globalnej blacklisty,
- 1 whitelisty aplikowanej dla zadanej podsieci IP,
- 1 blacklisty aplikowanej dla zadanej podsieci IP,
- Mechanizmu filtrowania adresów URL na podstawie specjalizowanej bazy danych dostarczonej przez producenta rozwiązania
- Sygnaturowej analizy przesyłanych plików z wykorzystaniem silnika antywirusowego
- Mechanizmu dopasowywania polityki bezpieczeństwa w zależności od nazwy grupy użytkownika uzyskanej z niestandardowego pola nagłówka HTTP
- Mechanizmu filtrowania w oparciu o informacje uzyskane z funkcjonalności dynamicznej analizy treści włączonej dla co najmniej wszystkich kategorii:
  - media społecznościowe,
  - blogi,
  - usługi do przechowywania i synchronizacji plików

Zakładane wielkości ruchowe (parametry intensywności ruchu – przepustowość Systemu SWG [Mbps], liczba zapytań HTTPS(s) na sekundę) są parametrami wymaganymi dla odpowiedniego przygotowania wydajności Systemu SWG. W przypadku, gdy ruch rzeczywisty będzie się różnić od planowanego jak wskazano w tabeli Zamawiający wymaga, aby System SWG:

a) dalej realizował wszystkie wymagane funkcjonalności zgodnie z wymaganiami,

b) zapewniał obsługę poszczególnych parametrów ruchowych do wielkości wskazanych w powyższych tabelach (ruch nadmiarowy jeżeli nie może być obsłużony powinien być odrzucany)

3.3.2. Wymagania wydajnościowe na Węzeł laboratoryjny

Wydajność Węzła laboratoryjnego*	
Liczba zapytań HTTP(s) na sekundę	1000

*) minimalna wydajność przy założeniu realizacji wszystkich zakładanych funkcjonalności realizowanych w Regionalnych Węzłach Bezpieczeństwa dla całego wskazanego w tabeli ruchu.

3.4. Wymagania wspólne dla Systemu SWG i Systemu zarządzającego

3.4.1. Wymagania wspólne dla wszystkich Systemów

1) System SWG i System zarządzający musi obsługiwać ruch w ramach IPv4 oraz IPv6, w dowolnych proporcjach, w zakresie pełnej funkcjonalności w tym dla analizy ruchu.
2) Zarządzanie wszystkimi elementami Systemu SWG musi odbywać się bezpośrednio i z wykorzystaniem Systemu zarządzającego za pomocą linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW zabezpieczonej z wykorzystaniem protokołu TLS w wersji min 1.1 RFC 4346, 1.2 RFC 5246. Zamawiający wyraża zgodę na wdrożenie Systemu SWG o parametrach wymuszających konieczność instalacji dodatkowego oprogramowania na stacji administratora, w celu efektywnego zarządzania dostarczonym Systemem SWG, zgodnie z wymaganymi parametrami.
3) Wszystkie komponenty Systemu SWG i Systemu zarządzającego muszą zapewniać Zamawiającemu możliwość zarządzania bezpośrednio danym komponentem z wykorzystaniem protokołów: HTTPS oraz SSH, jak i muszą mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania w skazanymi poniżej w punkcie 3.7 "System zarządzający”.
4) System SWG i System zarządzający musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q (min. 1000 tag VLAN).
5) System SWG i System zarządzający musi zapewniać Zamawiającemu możliwość uwierzytelniania administratorów za pomocą bazy lokalnej i z wykorzystaniem dwóch z wymienionych mechanizmów: RADIUS lub LDAP lub SAML.

6) System SWG i System zarządzający musi zapewniać Zamawiającemu możliwość zarządzania dostępem w oparciu o przypisane role (RBAC), w tym możliwość definiowania przez Zamawiającego własnych ról administracyjnych.
7) Wszystkie elementy wchodzące w skład Systemu SWG i Systemu zarządzającego muszą współpracować z rozwiązaniami do monitorowania poprzez protokoły SNMP w wersjach 2c, 3 i wspierać SNMP TRAP
8) Wszystkie elementy wchodzące w skład Systemu SWG i Systemu zarządzającego muszą mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów.
9) Wszystkie elementy wchodzące w skład Systemu SWG i Systemu zarządzającego muszą obsługiwać protokół NTP.
10) Wszystkie bazy sygnatur, kategoryzacji i feedów dostarczone w ramach Systemu SWG i Systemu zarządzającego muszą być, na bieżąco, cyklicznie aktualizowane przez producenta oprogramowania, zgodnie z harmonogramem zdefiniowanym przez Zamawiającego, przez cały okres trwania gwarancji.
11) Wszystkie elementy wchodzące w skład Systemu SWG i Systemu zarządzającego muszą logować, dla wszystkich zdarzeń, co najmniej następujące informacje:
    a) Czas i data transakcji wg lokalnego czasu,
    b) IP adres źródłowy,
    c) Login użytkownika, jeśli nastąpiło uwierzytelnienie,
    d) IP adres docelowy,
    e) Pełen URL (cała ścieżka),
    f) Akcja podjęta przez element zgodnie ze skonfigurowana polityką.
    g) Przyczyna wykonania akcji, np. wyszczególnienie mechanizmu, który spowodował blokadę ruchu.
    h) Kategoria w jakiej został zaklasyfikowany dany adres URL
    i) Liczba takich zdarzeń w ciągu ostatnich 24h (tylko w przypadku zdarzeń zagregowanych)
12) Wszystkie elementy wchodzące w skład Systemu SWG i Systemu zarządzającego muszą wysyłać zdarzenia (logi) do serwera SIEM za pomocą protokołu Syslog, w formacie CEF lub LEEF lub równoważnym RFC 5424
    a) Muszą umożliwiać Zamawiającemu konfigurację polityk logowania do systemu SIEM Zamawiającego dane o każdej sesji związanej z ruchem dozwolonym, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy komponentu Systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
    b) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego elementu.
13) Wszystkie elementy wchodzące w skład Systemu SWG i Systemu zarządzającego muszą obsługiwać routing statyczny.
14) System SWG i System zarządzający muszą umożliwiać Zamawiającemu cykliczne wykonywanie kopi zapasowej konfiguracji, zgodnie ze zdefiniowanym przez Zamawiającego harmonogramem, za pomocą dowolnego protokołu. Zapisana kopia konfiguracji musi być w formie edytowalnej np. w notatniku.
15) Dane, takie jak np. klucze prywatne, hasła, muszą być zaszyfrowane.

16) Zaoferowany System SWG nie może wprowadzać dodatkowego narzutu na opóźnienie w transmisji większego niż 100 ms.
17) Licencje dostarczone wraz z Systemem SWG i Systemem zarządzającym nie mogą ograniczać liczby użytkowników, administratorów, korzystających jednocześnie z Systemu SWG i z Systemu zarządzającego lub muszą umożliwiać wykorzystanie Systemu SWG dla wszystkich uczniów i nauczycieli z całej Polski (bez ograniczenia liczby urządzeń), a Systemu Zarządzającego dla co najmniej 20 administratorów Zamawiającego.

3.5. Klastrowanie elementów Systemu SWG i Systemu zarządzającego

1) System SWG i System zarządzający muszą zapewniać pełną redundancję (Wysoką dostępność) dla wszystkich elementów krytycznych powiązanych z dostarczeniem wszystkich funkcjonalności. Zamawiający wymaga, aby w przypadku Awarii, wydajność Systemu SWG uległa degradacji o nie więcej niż 20% bazowej wydajności i pojemności, określonej dla Systemu SWG, zainstalowanego w ramach danego węzła i podanej w punkcie 3.3.1.
2) System SWG, zainstalowany w ramach każdego z Regionalnych Węzłów Bezpieczeństwa, musi zostać zbudowany z zachowaniem wysokiej dostępność (HA) na poziomie n+1 – dodanie co najmniej jednego dodatkowego komponentu względem minimalnej liczby komponentów koniecznych do obsługi ruchu i liczby zapytań HTTP na sekundę, z zachowaniem wymagania opisanego w pkt 1. Zamawiający nie wyraża zgody na zastosowanie klastra:
    a) Active / active
    b) Active / pasive
3) System zarządzający, zainstalowany w ramach każdego z Centralnych Węzłów Bezpieczeństwa, musi zostać zbudowany z zachowaniem wysokiej dostępność (HA), która musi być zrealizowana poprzez zastosowanie klastra:
    a) Active / active
    lub
    b) Active / pasive
4) System SWG musi zapewniać mechanizmy skalowania wydajności przez możliwość konfiguracji wielu identycznych komponentów w każdym z węzłów.

3.6. System SWG dla Regionalnego Węzła Bezpieczeństwa

3.6.1. Wymagania funkcjonalne rozwiązania

W ramach wdrożonego Systemu SWG w Regionalnym Węźle Bezpieczeństwa muszą być realizowane wszystkie poniższe funkcjonalności. Zamawiający wymaga, aby wszystkie poniższe funkcjonalności działały w skali całego ruchu określonego dla danego węzła w punkcie 3.3.1. „Wymagania wydajnościowe na System SWG zainstalowany w Regionalnych Węzłach Bezpieczeństwa”. Zamawiający wymaga dostarczenia w ramach przedmiotu zamówienia następujących funkcjonalności:

a. Funkcjonalność filtrowania adresów URL
b. Funkcjonalność dynamicznej analizy treści
c. Funkcjonalność AV

3.6.2. Funkcjonalność filtrowania adresów URL

W ramach wdrożonego Systemu SWG w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga, aby funkcjonalność filtrowania adresów URL działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.1. „Wymagania wydajnościowe na System SWG zainstalowany w Regionalnych Węzłach Bezpieczeństwa".

1) Funkcjonalność filtracji adresów URL musi być zrealizowana na maszynach wirtualnych zainstalowanych na platformie wirtualizacyjnej dostarczonej przez Zamawiajacego.
2) Producent dostarczający Funkcjonalność filtracji adresów URL musi być członkiem the Internet Watch Foundation (IWF) lub organizacji o analogicznym statusie i zasięgu działania.
3) Funkcjonalność filtrowania adresów URL musi posiadać feed dla bazy Internet Watch Foundation (IWF) lub równoważnej, który będzie mógł być użyty w zakresie filtrowania i raportowania.
4) Funkcjonalność filtrowania adresów URL musi posiadać możliwość blokowania dostępu do treści przedstawiających seksualne wykorzystywanie dziecka (z ang. CSAM-child sexual abuse materials) poprzez aktywną implementację listy IWF "The child abuse image content URL list (CAIC)" lub równoważnej.
5) Funkcjonalność filtrowania adresów URL musi realizować funkcję forward proxy w trybie explicit i transparent dla całego ruchu.
6) W wersji transparent Funkcjonalność filtrowania adresów URL musi pracować w trybie inline (fizycznie w ścieżce ruchu) dla całego ruchu.
7) Funkcjonalność filtrowania adresów URL musi obsługiwać w trybie proxy następujące protokoły: HTTP, HTTPS. Dla pozostałych protokołów musi być zapewniona możliwość przepuszczenia ruchu bez inspekcji (passthrough).
8) Dostarczona Funkcjonalność filtrowania adresów URL musi zapewniać możliwość stworzenia przez Zamawiającego co najmniej 50 dowolnie sformułowanych polityk filtrowania, rozumianych jako zbiór reguł definiujących sposób:
    a) filtrowania ruchu HTTP, HTTPS w oparciu o specjalizowaną bazę danych opisaną w pkt 11 i na podstawie własnej bazy kategorii Zamawianego opisanej w pkt 16 ppkt a, wraz z obsługą wyjątków (na podstawie własnej bazy kategorii opisanej w pkt. 16 ppkt b, w szczególności white i black listy). Obsługa wyjątków musi odbywać się per podany zakres adresów IP – zakres działania danej kategorii definiującej wykluczenia z procesu filtrowania stosowane są w podsieci A, a nie są aplikowane dla podsieci B,
    b) włączenia/wyłączenia funkcjonalności dynamicznej analizy treści, zgodnej z wymaganiami z rozdziału 3.6.3, dla dowolnej ilości wybranych przez Zamawiającego kategorii treści określonych w specjalizowanej bazie danych opisanej w pkt. 11,
    c) włączenia/wyłączenia analizy antywirusowej, zgodnie z rozdziałem 3.6.4 „Funkcjonalność AV".
9) Funkcjonalność filtrowania adresów URL musi zapewniać możliwość uruchomienia poszczególnych polityk filtrowania, o których mowa powyżej, dla określonych:
    a) zakresów adresów IP

b) grup użytkowników zdefiniowanych lokalnie, zgodnie z pkt 23, w oparciu o zewnętrzny System tożsamości lub zewnętrzne repozytoria użytkowników (co najmniej LDAP, RADIUS lub SAML),
c) nazw i grup użytkowników zapisanych w parametrach nagłówka HTTP (parametry te zostaną wcześniej wstrzyknięte do nagłówka przez System ADC).

10) Funkcjonalność filtrowania adresów URL musi zapewniać możliwość uruchomienia poszczególnych polityk filtrowania, o których mowa powyżej, dla określonych zakresów adresów IP, w liczbie nie mniejszej niż 25 015 odpowiadającej liczbie szkół wskazanej w pkt 3.3.1, i grup użytkowników zdefiniowanych zgodnie z pkt 23.
11) Funkcjonalność filtrowania adresów URL musi filtrować ruch HTTP/HTTPS, porównując odwołania stron www i adresów IP ze specjalizowaną bazą danych (dostarczaną, utrzymywaną i rozwijaną przez producenta Systemu SWG), podzieloną na kategorie treści stron www i musi zawierać informacje o domenach i adresach URL.
12) Specjalizowana baza opisana w pkt 11 musi posiadać co najmniej 50 kategorii treści stron www, uwzględniających co najmniej kategorie wskazane w pkt 28, które mogą być użyte przez Zamawiającego w dowolny sposób w celu stworzenia polityki filtrowania.
13) Zamawiający musi mieć zapewnioną możliwość stworzenia własnej bazy kategorii, zawierającej:
    a) nie mniej niż 10 zdefiniowanych przez Zamawiającego nowych kategorii dotyczących zagadnień wykraczającej poza zakres wskazany w ramach bazy opisanej w pkt 11,
    b) nie mniej niż 30 000 kategorii rozumianych jako lista adresów URL, które będą służyć do obsługi wyjątków zgłoszonych przez użytkowników do polityki filtrowania, (black i white listy),
14) Funkcjonalność filtrowania adresów URL musi zapewniać możliwość cyklicznego importowania z zewnętrznych repozytoriów własnej bazy kategorii do polityk filtrowania.
15) Funkcjonalność filtrowania adresów URL musi zapewniać mechanizm kontroli dostępu do takiej bazy, uwzględniający logowanie aktywności poszczególnych operatorów i możliwość porównywania wersji takiej bazy.
16) Specjalizowana baza opisana w pkt 11 musi być nieprzerwanie aktualizowana przez producenta Oprogramowania, poprzez stosowanie każdorazowo łącznie co najmniej niżej wymienionych mechanizmów:
    a) mechanizmów przeszukujących i analizujących zasoby sieci Internet,
    b) zaawansowanych mechanizmów dokonujących klasyfikacji zawartości stron wykorzystując co najmniej mechanizmy machine learning i analizę leksykalną,
    c) zespół ludzi weryfikujących poprawność klasyfikacji.
17) Specjalizowana baza opisana w pkt 11 musi zawierać kategorię typu „Uncategorized", która może zostać wykorzystana przez Zamawiającego w polityce filtrowania.
18) Funkcjonalność filtrowania adresów URL musi umożliwiać Zamawiającemu definiowanie różnych akcji w przypadku wykrycia co najmniej poniższych typów zdarzeń:
    a. naruszenia polityki filtrowania tzn.:
        1. zarejestrowania strony, która powinna być zablokowana, w oparciu o specjalizowaną bazą danych opisaną w pkt 11,
        2. zarejestrowania strony, która powinna być zablokowana, w oparciu o własną bazę kategorii opisaną w pkt 13,

3. zarejestrowania próby połączenia metodą HTTP CONNECT,
4. zarejestrowania strony, która powinna być zablokowana przez funkcjonalność dynamicznej analizy treści opisaną w pkt 3.6.3,
5. zarejestrowania przesyłanego pliku, który powinien być zablokowany przez funkcjonalność AV, opisaną w pkt 3.6.4, w związku ze znalezionym wirusem,
6. zarejestrowania pliku, który powinien być zablokowany przez funkcjonalność AV, opisaną w pkt 3.6.4, w związku ze zdefiniowanym przez Zamawiającego zabronionym formatem pliku,

b. błędu w odpowiedzi serwera WWW,
c. błędu po stronie klienta, np. niepoprawna treść żądania,
d. problemu z połączeniem, np. brak możliwości połączenia z serwerem WWW,
e. problemu technicznego z funkcjonalnością filtrowania adresów URL, np. brak dostępności specjalizowaną bazą danych opisanej w pkt 11,

19) Funkcjonalność filtrowania adresów URL musi zapewniać Zamawiającemu możliwość zdefiniowania wszystkich wymienionych akcji, które System wykona względem użytkownika:
    a. blokowanie dostępu do strony www,
    b. publikację użytkownikowi ostrzeżenia przed wejściem na stronę, ale umożliwi mu otwarcie wspomnianej strony po wykonaniu przez niego wskazanej akcji, np. naciśnięcie przycisku
    c. publikację użytkownikowi strony blokowania umożliwiającej mu podanie danych logowania służących do uwierzytelnienia jego sesji, w oparciu o mechanizmy opisane w pkt 23 prowadzące do zmiany polityki filtrowania, na określony okres czasu definiowany jako czas życia obiektu cookie wstrzykiwanego do przeglądarki, z której korzysta użytkownik (cookie override),
    ~~d. przekierowanie użytkownika na zewnętrzny portal uwierzytelniający.~~
20) Funkcjonalność filtrowania adresów URL musi zapewniać Zamawiającemu możliwość przypisywania akcji opisanej w pkt 19 do poszczególnych kategorii lub listy kategorii, np. jeśli strona na która próbuje wejść użytkownik jest zakwalifikowana jako kategoria „Narkotyki” to zawsze wykonaj ”blokowanie dostępu do strony www” (akcja nr 1), jeśli zaś dana strona jest zakwalifikowana jako „alkohol” to wykonaj „publikację użytkownikowi ostrzeżenia przed wejściem na stronę, ale następnie możliwość wejścia na daną stronę” (akcja nr 2).
21) Proces klasyfikacji kategorii strony musi uwzględniać mechanizm oceny reputacji danego adresu URL co najmniej w dwupoziomowej skali.
~~22) Funkcjonalność filtrowania adresów URL musi umożliwiać Zamawiającemu blokowanie dla użytkowników połączeń do sieci TOR, nawet w przypadku wykorzystania pluggable transport protocol.~~
23) Funkcjonalność filtrowania adresów URL musi zapewniać definiowanie i uwierzytelnianie użytkowników i administratorów z wykorzystaniem lokalnej bazy danych i zewnętrznego systemu tożsamości zintegrowanego z Systemem z wykorzystaniem mechanizmów: LDAP, RADIUS lub SAML.
24) Funkcjonalność filtrowania adresów URL musi zapewniać Zamawiającemu możliwość definiowania polityk dla nieuwierzytelnionych użytkowników.

~~25) Funkcjonalność filtrowania adresów URL musi zapewniać Zamawiającemu możliwość (z opcją włącz / wyłącz) wykrywanie i blokowanie tunelowania w protokołach HTTP/HTTPS np., choć nie wyłącznie, blokowanie sesji SSH na porcie 443.~~

26) Funkcjonalność filtrowania adresów URL musi zapewniać możliwość stosowania przez Zamawiającego mechanizmu Safe Search, w pełnym zakresie funkcjonalności udostępnianym przez dostawcę narzędzia, w wyszukiwarkach internetowych, co najmniej Google, Youtube, Bing.
27) Funkcjonalność filtrowania adresów URL musi zapewniać możliwość filtrowania stron www na podstawie, nie mniej niż 20 zdefiniowanych przez Zamawiającego fraz, np. „dopalacze", „twitter porn", „niebieski wieloryb".
28) Funkcjonalność filtrowania adresów URL musi mieć możliwość rozpoznawania treści dotyczących co najmniej zagadnień opisanych poniżej. Funkcjonalność filtrowania adresów URL musi zapewnić możliwość wykorzystania rozpoznanych treści do budowy polityki filtrowania z wykorzystaniem kategorii. Wykonawca jest zobowiązany do wdrożenia Funkcjonalności filtrowania adresów URL, w którym wszystkie podane niżej treści będą rozpoznawane i zagregowane w nie mniej niż czterech rozłącznych kategoriach (Typ A, Typ B, Typ C i Typ D):
    a) Kategoria treści - Typ A:
        I. Treści określone w przepisach polskiego prawa, których publikacja lub publiczna prezentacja jest zabroniona, w tym:
            1. treści pornograficzne z udziałem małoletnich określane jako materiały przedstawiające seksualne wykorzystywanie dziecka (z ang. CSAM-child sexual abuse materials),
            2. treści zawierające materiały o charakterze pedofilskim oraz propagowanie i pochwalanie tych treści,
            3. treści zawierające uwodzenie małoletnich w Internecie,
            4. treści zawierające publiczne propagowanie faszystowskiego lub innego totalitarnego ustroju państwa lub nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość,
            5. treści zawierające publicznie rozpowszechniane i prezentowane informacje, które mogą ułatwić popełnienia przestępstwa terrorystycznego,
            6. treści zawierające publiczne znieważanie grupy ludności albo poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości,
            7. treści zawierające informacje o narkotykach, dopalaczach – witryny, które omawiają, zachęcają, promują, oferują, sprzedają, dostarczają lub w inny sposób promują użycie, hodowlę, produkcję lub dystrybucję narkotyków i dopalaczy, rozumianych jako między innymi: niefarmaceutyczne leki, rośliny odurzające, rozpuszczalniki, lub inne substancje chemiczne, oraz związanych z nimi akcesoriów,

8. strony służące do oferowania gier hazardowych niezgodnie z ustawą o grach hazardowych.

II. pornografia – witryny przedstawiające treści pornograficzne, takie jak tekst, obrazy lub wideo zawierające wizerunek osób lub przedmiotów o cechach jednoznacznie seksualnych,

III. przemoc – witryny, których celem jest przedstawianie fizycznych lub innych szkód wyrządzanych ludziom, zwierzętom lub mieniu, lub które dostarczają instrukcji, jak spowodować takie szkody,

IV. dla dorosłych – witryny przedstawiające materiały przeznaczone dla dorosłych odbiorców, ale nie zakwalifikowane w kategorii pornografia i przemoc. Witryny te zawierają często wulgarne, erotyczne, lub inne treści, które nie są odpowiednie dla dzieci,

V. alkohol i tytoń – witryny i materiały promujące alkohol i tytoń, jego sprzedaż i spożywanie, w tym, ale nie wyłącznie, piwo, wino i inne wysokoprocentowe napoje alkoholowe,

VI. broń i materiały wybuchowe – witryny i materiały promujące broń, jej produkcję, używanie i modyfikacje, w tym, ale nie wyłącznie, pistolety, karabiny oraz materiały wybuchowe,

VII. anoreksja i inne zaburzenia odżywiania – witryny i materiały promujące niezdrowy i niewłaściwy tryb życia, związany z zaburzeniami odżywiania,

VIII. samookaleczenia – witryny i materiały promujące niebezpieczny, niezdrowy i niewłaściwy tryb życia, związany z umyślnym uszkodzeniem własnego ciała w wyniku autoagresji lub depresji,

IX. treści zawierające elementy psychomanipulacji, czyli sterowania cudzymi uczuciami, którego celem jest wyłudzenie korzyści materialnych lub zmuszenie do niewłaściwych, często ryzykownych zachowań.

b) Kategoria treści - Typ B:

I. nielegalne oprogramowanie, lub inne nielegalne treści - witryny, które nielegalnie udostępniają oprogramowanie lub materiały chronione prawami autorskimi, np. muzyka i filmy, lub dostarczają informacje dotyczące źródeł takich materiałów, np. peer-to-peer,

II. gry online – witryny umożliwiające dostęp do gier sieciowych (z wyłączeniem gier wykorzystywanych w procesie edukacji),

III. przekleństwa – witryny i materiały zawierające treści, których celem jest eksponowanie wyrazów i zwrotów powszechnie uważanych za nieprzyzwoite, obsceniczne i wulgarne,

IV. zakłady online - witryny nie znajdujące się Rejestrze domen służących do oferowania gier hazardowych niezgodnie z ustawą, na których użytkownik może postawić zakład lub wziąć udział w puli zakładów, wziąć udział w loterii lub otrzymać informacje, pomoc, zalecenia lub przeszkolenie w takich działaniach,

V. portale randkowe - witryny, które umożliwiają poznanie innych ludzi w celach matrymonialnych lub towarzyskich, wymianę informacji pomiędzy użytkownikami w celu umówienia spotkania (w Internecie lub w poza nim) w celu nawiązania trwałej (lub nie) relacji towarzyskiej (czasami tylko seksualnej),

VI. czaty online - witryny, które udostępniają możliwość lub oprogramowanie pozwalające na prowadzenie czatów internetowych, komunikacji głosowej, wideokonferencji,
VII. różnorodny kontent dla dorosłych - witryny zawierające treści przeznaczone dla dorosłych, które nie stanowią oddzielnej kategorii,
VIII. wandalizm i przemoc – witryny i materiały zawierające treści, których celem jest promowanie zachowań łamania porządku prawnego, aktów wandalizmu, witryny o treściach pseudokibicowskich (np. nawoływanie do przemocy, etc.).
IX. uncategorized / none – strony nieznalezione w bazie Wykonawcy albo takie, których nie potrafiły jednoznacznie skategoryzować silniki klasyfikacyjne Wykonawcy,

Ponadto dla celów badawczo-rozwojowych w zamkniętym środowisku testowym Wykonawca zaoferuje rozwiązania filtracji z uwzględnieniem następujących treści:

c) Kategoria treści – Typ C:
   I. organizacje psychomanipulacyjne – witryny, które promują i dostarczają informacji na temat organizacji psychomanipulacyjnych na tle parareligijnym,
   II. zagrożenia zdrowia i życia – treści promujące, sprzedające, reklamujące lub omawiające wszelkie modyfikacje ciała, takie jak tatuaże i piercing oraz inne zachowania niebezpieczne dla zdrowia i życia osób nieletnich,
d) Kategoria treści – Typ D:
   I. witryny społecznościowe oraz blogi i fora w zakresie niebezpiecznych i nielegalnych treści,
   II. witryny oferujące możliwość udostępniania, magazynowania i wymiany plików,
   III. witryny udostępniające użytkownikom możliwość zakupu towarów i usług, takie jak aukcje i sklepy internetowe, w zakresie niebezpiecznej i nielegalnej oferty.

UWAGA: Powyższa klasyfikacja treści jest podana w dokumencie oraz w procesie zakupowym JEDYNIE w celach przeprowadzenia postępowania zakupowego na System SWG, co oznacza, że Funkcjonalność filtrowania adresów URL działająca w ramach Systemu SWG wybranego w ramach postępowania będzie jedynie umożliwiała rozróżnienie podanych treści i ochronę użytkowników przed nimi. Decyzję o włączeniu usługi będzie podejmował dyrektor szkoły na etapie jej podłączenia do sieci OSE. Będzie on też miał możliwość dostosowania poziomu ochrony poprzez definiowanie *white* i *black list* zawierających adresy URL, które będą traktowane w sposób specjalny w ramach usługi świadczonej na terenie podległej mu placówki. Jednocześnie należy podkreślić, że system ochrony użytkowników w żadnym zakresie nie będzie obejmować witryn z obszarów: bankowość i finanse, opieka zdrowotna i poczta elektroniczna. Zamawiający dopuszcza aby treści, dotyczące zagadnień określonych w powyższych kategoriach, były rozpoznawane z wykorzystaniem specjalistycznej bazy danych opisanej w pkt 3.6.2 ppkt. 11) lub Funkcjonalności dynamicznej analizy treści. W drugim przypadku Wykonawca jest zobowiązany do wskazania w Załączniku nr 8 do Zapytania Ofertowego lub w Koncepcji rozwiązania, które treści będą rozpoznawane za pomocą Funkcjonalności dynamicznej analizy treści.

29) Funkcjonalność filtrowania adresów URL musi zapewniać Zamawiającemu możliwość (opcji włącz / wyłącz) zablokowania dostępu do hostów numerycznych.
30) Funkcjonalność filtrowania adresów URL musi zapewniać Zamawiającemu możliwość dostosowania komunikatów o błędach lub komunikatów informacyjnych wyświetlanych użytkownikom, takich jak strona blokowania, a w szczególności wyświetlanie informacji powiązanych z sesją jak:
    a) nazwa uwierzytelnionego użytkownika,
    b) treść błędu,
    c) IP adres źródłowy,
    d) powód zablokowania danej strony www (nazwa kategorii, wskazanie dynamicznych mechanizmów klasyfikacyjnych jako źródło decyzji o zablokowaniu danej strony),
    e) adres IP lub nazwa komponentu blokującego.
31) Funkcjonalność filtrowania adresów URL musi odczytywać niestandardowe parametry nagłówka HTTP, np. informacje o nazwie użytkownika i przypisanej do niego grupie
32) Mechanizmy wymienione w pkt 16 ppkt b i pkt 16 ppkt c muszą analizować zawartość stron www w zakresie umieszczonego na stronie tekstu w tym jego kontekstu, umieszczonych na stronie zdjęć i filmów w tym ich treści oraz umieszczonych na stronach linków i ich reputacji.
33) Funkcjonalność filtrowania adresów URL musi zapewniać Zamawiającemu możliwość zaznaczenia kategorii opisanych w pkt 12, w celu przekierowania treści stron zaklasyfikowanych dookreślonych kategorii, do funkcjonalności dynamicznej analizy treści z wykorzystaniem co najmniej protokołu ICAP. Zamawiający wybierze nie więcej niż 15 kategorii spośród kategorii określonych w specjalizowanej bazie danych opisanej w pkt 11 i we własnej bazie kategorii określonej w pkt 13, w tym co najmniej kategorie wymienione w pkt 28 ppkt d.
34) Funkcjonalność filtrowania adresów URL musi umożliwiać Zamawiającemu blokowanie stron na podstawie odpowiedzi uzyskanych z funkcjonalności dynamicznej analizy treści. Odpowiedź uzyskana z funkcjonalności dynamicznej analizy treści ma priorytet wyższy niż kategoryzacja strony uzyskana ze specjalizowanej bazy danych opisanej w pkt 11.

3.6.3. Funkcjonalność dynamicznej analizy treści

W ramach wdrożonego Systemu SWG w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga, aby funkcjonalność dynamicznej analizy treści działała w skali 40% całego ruchu określonego dla danego węzła w punkcie 3.3.1. „Wymagania wydajnościowe na System SWG zainstalowany w Regionalnych Węzłach Bezpieczeństwa”.

1) Funkcjonalność dynamicznej analizy treści musi analizować treść stron www w celu oceny i klasyfikacji treści aktualnie prezentowanych na danej stronie www. Wynik analizy musi być przekazywany do funkcjonalności filtrowania adresów URL, która zablokuje odwołania do stron zaklasyfikowanych do kategorii wskazanych w polityce bezpieczeństwa.
2) Funkcjonalność dynamicznej analizy treści musi działać w czasie rzeczywistym.
3) Funkcjonalność dynamicznej analizy treści musi być zintegrowana z funkcjonalnością filtrowania adresów URL. Funkcjonalność filtrowania adresów URL wysyła do funkcjonalności

dynamicznej analizy treści, treść strony oglądanej przez użytkownika, poprzez co najmniej protokół ICAP

4) Opóźnienie ruchu wynikające z analizy wykonywanej przez funkcjonalność dynamicznej analizy treści nie może być większe niż 100 ms dla 60% analizowanych stron www i 250 ms dla 40% analizowanych stron www. Funkcjonalność dynamicznej analizy treści musi umożliwiać Zamawiającemu definiowanie sposobu zachowania systemu w momencie, kiedy czas analizy przekroczy 250 ms, np. przepuszczenie ruchu bez blokady.
5) Mechanizm Dynamicznej analizy treści musi analizować treść stron www z wykorzystaniem analizy leksykalnej lub dynamicznych mechanizmów Machine Learning lub sztucznej inteligencji. Zamawiający nie dopuszcza, aby mechanizmy analityczne wykorzystywane w ramach funkcjonalności dynamicznej analizy treści bazowały jedynie na wyrażeniach regularnych (Regex). Wykonawca musi zapewnić Zamawiającemu możliwość rozwoju mechanizmów analitycznych wykorzystywanych w ramach funkcjonalności dynamicznej analizy treści, w szczególności poprzez definiowanie nowych słowników lub szkolenie algorytmów Machine Learning.
6) Mechanizm Dynamicznej analizy treści musi dokonywać analizy treści napisanych co najmniej w języku polskim i angielskim.
7) Wykonawca musi zapewniać Zamawiającemu możliwość sterowania czułością mechanizmów analitycznych wykorzystywanych w ramach funkcjonalności dynamicznej analizy treści poprzez ustalanie progu, po przekroczeniu którego strony o danej treści są blokowane lub nie.

3.6.4. Funkcjonalność AV

W ramach wdrożonego Systemu SWG w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga, aby funkcjonalność AV działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.1 „Wymagania wydajnościowe na System SWG zainstalowany w Regionalnych Węzłach Bezpieczeństwa”.

1) Funkcjonalność AV musi być realizowana dla 100% ruchu związanego z ruchem HTTP i HTTPS. Wartości w tabeli w rozdziale 3.3.1.
2) Funkcjonalność AV musi umożliwiać skanowanie i blokowanie archiwów, w tym co najmniej: zip. W przypadku plików, których analiza jest nie możliwa w związku z wielokrotnym zabezpieczeniem hasłem, Funkcjonalność AV musi umożliwiać Zamawiającemu definicję akcji podejmowanej w przypadku zarejestrowania takiego pliku, w tym co najmniej: block lub allow
3) Funkcjonalność AV musi posiadać moduł inspekcji antywirusowej uruchamiany dla aplikacji wykorzystujących co najmniej następujące dekodery obsługujące protokoły HTTP, HTTPS, kontrolujący ruch bez konieczności uzupełniania o jakiekolwiek komponenty.
4) Baza sygnatur anty-wirus musi być dostarczana i wspierana przez producenta, na bieżąco cyklicznie aktualizowana i uzupełniana, przez dostawcę bazy (w przypadku bazy komercyjnej) lub przez community (w przypadku rozwiązań opensource), o nowe sygnatury definiujące profil zachowania znanych wirusów i musi być przechowywana na komponencie Systemu pełniącym funkcję Inspekcji AV. Baza ta posiada nie mniej 900 000 sygnatur antywirusowych lub baza ta posiada nie mnie niż 6000 sygnatur typów zagrożeń. Alternatywnie, o ile rozmiar

bazy sygnatur przekracza 5 000 000 dopuszcza się rozwiązania w których lokalna baza komponentu Systemu stanowi podzbiór bazy utrzymywanej przez producenta rozwiązania, na bieżąco aktualizowany przez producenta.

5) Funkcjonalność AV musi zapewniać możliwość wykrywania, śledzenia i blokowania transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe
    b. pliki graficzne
    c. pliki PDF
    d. pliki wykonywalne
    e. pliki multimedialne
    f. pliki pakietu Office
    g. pliki skompresowane
    h. inne pliki, które mogą służyć do propagacji wirusów
6) Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
7) Funkcjonalność AV musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, HTTPS w obu kierunkach – upload/download.
8) Funkcjonalność AV musi umożliwiać Zamawiającemu definiowanie wielkości pliku powyżej, którego funkcjonalność AV nie będzie przeprowadzała inspekcji danego pliku.

3.7. System zarządzający

System zarządzający, składający się z konsoli zarządzającej i konsoli raportującej, umożliwia Zamawiającemu zarządzanie dostarczanymi przez Wykonawcę funkcjonalnościami należącymi do Systemu SWG, zgodnie z przedstawionymi poniżej wymaganiami funkcjonalnymi, i umożlwiający na konfigurację wszystkich funkcji opisanych w ramach rozdziału 3.

Zamawiający wymaga wdrożenia Systemu zarządzającego w ramach Etapu 0.

3.7.1. Konsola zarządzająca

1) Konsola zarządzająca musi umożliwiać Zamawiającemu konfigurację wszystkich elementów składowymi Systemu SWG z wykorzystaniem co najmniej wszystkich następujących interfejsów administracyjnych:
    a. GUI przy wykorzystaniu protokołu HTTPS
    b. CLI przy wykorzystaniu protokołu SSH
    c. API, co najmniej poprzez wykorzystanie protokołu HTTP (REST API)
2) Konsola zarządzająca musi być dostarczona w postaci platformy wirtualizacyjnej (rozumianej jako maszyny wirtualnej wdrażanej na udostępnionej przez Zamawiającego paltfomie wirtulizacyjnej
3) Oprogramowanie zainstalowane w ramach platformy opisanej w pkt 3, musi być kompatybilne z każdym elementem Systemu SWG występującym w Centralnym i Regionalnym Węźle Bezpieczeństwa.

4) Konsola zarządzająca musi umożliwiać Zamawiającemu zarządzanie wszystkimi elementami składowymi Systemu SWG w pełnym zakresie funkcjonalnym określonym w niniejszym dokumencie
5) Konsola zarządzająca musi umożliwiać Zamawiającemu na centralne zarządzanie regułami bezpieczeństwa zdefiniowanymi na Systemie SWG
6) Komunikacja elementów składowych Systemu SWG z konsolą zarządzającą musi być realizowana z wykorzystaniem szyfrowanych protokołów.
7) Konsola zarządzająca musi umożliwić integrację z nadrzędnym systemem zarządzania Zamawiającego poprzez standardowe protokoły i otwarte mechanizmy integracyjne (w szczególności poprzez interfejs typu API lub modyfikację plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym) lub bezpośrednią komunikację z komponentem Systemu co najmniej poprzez protokół SSH), do których Wykonawca dostarczy dokumentację. Wykonawca w ramach Wdrożenia będzie zobowiązany do uczestniczenia w integracji konsoli zarządzającej z nadrzędnym systemem zarządzania Zamawiającego. Integrację, o której wspomniano powyżej, Zamawiający planuje zakończyć do końca 2020 roku.
8) Konsola zarządzająca musi umożliwiać Zamawiającemu uzupełnianie mechanizmów analitycznych funkcjonalności dynamicznej analizy treści o nowe, niedopuszczalne treści, na podstawie danych zaprezentowanych na statystykach wygenerowanych przez konsolę raportującą
9) Konsola zarządzająca musi umożliwiać Zamawiającemu uzupełnianie bazy adresów URL w Systemie SWG służącej do filtracji ruchu web (co najmniej globalnych whitelist oraz blacklist), na podstawie danych zaprezentowanych na statystykach wygenerowanych przez konsolę raportującą
10) Konsola zarządzająca musi zapewniać Zamawiającemu uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera RADIUS lub LDAP lub SAML,
11) Konsola zarządzająca musi zapewniać Zamawiającemu możliwość szczegółowego określenia ról i przypisania uprawnień poszczególnym administratorom (RBAC),
12) Konsola zarządzająca musi zapewnić podgląd stanu komponentów monitorowanych elementów Systemu SWG (m.in. interfejsy, moduły)
13) Konsola zarządzająca musi zapewnić odbieranie komunikatów SNMP Trap z zarządzanych elementów należących do Systemu SWG lub zapewnić równoważne mechanizmy zbierania danych zawartych w bazie MIB
14) Konsola zarządzająca musi umożliwiać Zamawiającemu monitorowanie Awarii i pokazanie aktualnych alarmów. Minimalny zakres monitorowania elementów Systemu SWG:
    a. Zbieranie danych z komponentów Systemu w tym co najmniej alarmy, warningi,
    b. Wizualizacja w postaci dashboardu informacji o stanie:
        1. wszystkich elementów Systemu SWG, w tym co najmniej wykorzystanie interfejsów sieciowych, aktualne wykorzystanie dysków i pamięci RAM
        2. przekroczenia zadanego poziomu obciążenia interfejsów, CPU, RAM, ilości sesji Systemu, utraty pakietów
        3. działaniem każdej ze skonfigurowanych i uruchomionych funkcjonalności danego elementu Systemu SWG
    c. Monitorowanie dostępności, wydajności, pojemności wszystkich elementów Systemu SWG

d. Analiza przepustowości i ruchu na bazie logów oraz ogólnego stanu i efektywności pracy Systemu SWG
e. Zarządzenie komunikatami
f. Przechwytywanie komunikatów sprzętowych i systemowych

15) Konsola zarządzająca musi zapewniać szczegółowy wgląd w stan pracy elementów składowych Systemu SWG
16) Konsola zarządzająca musi zapewnić tworzenie, usuwanie, edycję backupu i wersjonowanie szablonów konfiguracji oraz ich późniejsze wykorzystanie. Konsola zarządzająca musi przechowywać co najmniej 10 ostatnich wersji szablonów konfiguracji i umożliwiać ich przywrócenie, tzn. nadpisanie aktualnie działającej konfiguracji przez wskazaną przez Zamawiającego wersję
17) Konsola zarządzająca musi umożliwiać Zamawiającemu na odtworzenie backupu konfiguracji każdego elementu Systemu SWG
18) Konsola zarządzająca musi zapewniać archiwizację i wersjonowanie plików konfiguracyjnych
19) Konsola zarządzajaca musi zapewnić na przeglądanie logów w trybie rzeczywistym z podziałem na logi aktywności użytkowników i logów systemowych Systemu SWG oraz przeglądanie logów maksymalnie 8 godzin wstecz.
20) Konsola zarządzająca musi zapewniać dystrybucję (w tym aktualizację) oprogramowania systemowego na wszystkie elementy składowe Systemu SWG. W szczególności System musi zapewniać dostęp administracyjny w trybie Read-Only (widoczne wszystkie opcje konfiguracyjne w trybie monitorującym).

3.7.2. Konsola raportująca

Konsola raportująca składa się z modułów: analityczno- raportowego, diagnostycznego i z kolektora danych.

3.7.2.1. Wymagania wspólne dla wszystkich modułów

1) Konsola raportująca musi być dostarczona w postaci oprogramowania instalowanego na udostępnionej przez Zamawiającego platformie wirtualizacyjnej
2) Zarządzanie musi być dostępne z poziomu przeglądarki internetowej za pomocą jednego interfejsu graficznego umożliwiającego na konfigurację wszystkich modułów w pełnym zakresie funkcjonalnym. Zamawiający dopuszcza, żeby część konfiguracji odbywała się z wykorzystaniem CLI. Interfejs graficzny musi automatycznie dostosowywać się do zmiany wyglądu i rozmiaru aplikacji/raportów dla dowolnego współczynnika kształtu ekranu
3) Konsola raportująca musi umożliwiać skalowanie modułów kolektora, analitycznego, raportowego, diagnostycznego na wiele serwerów w celu podniesienia dostępności i wydajności – klaster HA.
4) Moduły kolektora danych, analityczno-raportowy oraz diagnostyczny muszą posiadać mechanizm backupu konfiguracji dający możliwość exportu i importu ustawień
5) Konsola raportująca musi umożliwiać Zamawiającemu tworzenie grup praw dostępu i zapewnienia dostępu na różnych poziomach uprawnień i zapewniać bezpieczeństwo na różnych poziomach definiowane per użytkownik/grupa/rola, oraz zapewniać dostępność

pełnych ram zarządzania umożliwiających kontrolowanie tego, co każdy administrator jest w stanie zrobić.

6) Konsola raportująca umożliwiać korzystanie z zewnętrznych repozytoriów danych o użytkownikach z wykorzystaniem co najmniej protokołów LDAP lub RADIUS, w procesie autentykacji i autoryzacji użytkownika
7) Konsola raportująca musi umożliwiać dodawanie zewnętrznych oraz edycji istniejących oraz tworzenia własnych rozszerzeń do wizualizacji danych (dashboardy, raporty)
8) Konsola raportująca musi udostępniać otwarty i udokumetowany interfejs REST API, aby tworzyć niestandardowe rozszerzenia do integracji z istniejącymi systemami Zamawiającego
9) Konsola raportująca musi umożliwiać definiowanie warunków/reguł dla danych, o które mogą odpytywać za pomocą API systemy zewnętrzne, np. lista zdarzeń, która ma się w systemie trzecim pokazać jako krytyczne lub związane z jakąś kategorią tematyczną/klasą urządzeń.
10) Konsola raportująca musi obsługiwać wszystkie dane przyjęte przez moduł kolektora danych, maksymalnie do 70k EPS.
11) Konsola raportująca musi umożliwiać na płynną pracę dla min. 100 mln unikalnych rekordów i wyświetlanie na dowolnej wizualizacji, określonej przez użytkownika, min. 1 mln rekordów oraz wyniku działania na tych rekordach jakiś funkcji, np. top 10 lub temu podobnej, w średnim czasie poniżej 30 sek zakładając jednoczesną pracę do 5 użytkowników systemu analityczno-raportowego.
12) Konsola raportująca nie może posiadać ograniczeń licencyjnych dotyczących ilości analizowanych danych.
13) Konsola raportująca musi umożliwiać jednoczesną pracę 10 użytkownikom.

3.7.2.2. Moduł kolektora danych

1) Kolektor danych musi umożliwiać przyjęcie za pośrednictwem protokołu syslog, przetworzenie i przechowywanie przez okres do 30 dni logów w ilości do 70k EPSów.
2) Kolektor danych musi umożliwiać przetworzenie logów przed przyjęciem ich w MODULE ANALITYCZNO-RAPORTOWYM w tym co najmniej na:
    a. filtrowanie logów
    b. modyfikację , np. unifikacji, w locie, zawartych w logach danych.
    c. Kategoryzację logów
    d. Routing logów do systemów zewnętrznych
3) Kolektor danych musi wykonywać normalizację logów – dane pochodzące z różnych źródeł i zachowujące informacje w różnych formatach muszą być dostępne do analizy/przeglądania w ujednoliconej postaci, np. data i czas, adresy, identyfikatory, nazwy, etc.
4) Kolektor danych musi umożliwiać transformację przychodzących logów za pomocą co najmniej następujących metod:
    a. przyrównania
    b. grupowania/agregacji
    c. modyfikacji (dodanie/zmiana wartości pola)
    d. dodawania informacji do zdarzeń z zewnętrznych źródeł danych

    Za pomocą wyżej wymienionych warunków, np. operatorów przyrównania, administrator musi mieć możliwość zdefiniowania zachownia Kolektora danych określającego co ma się stać

z danym wpisem, w ten sposób filtrując niepotrzebne logi lub decydować do jakiego miejsca przechowywania mają one trafić. Moduł powinien obsługiwać następujące rodzaje docelowych kontenerów: plik, baza danych, syslog, API. Moduł, na podstawie wyżej opisanych reguł i transformacji, musi potrafić dostarczyć inne logi do MODUŁU ANALITYCZNO-RAPORTOWEGO i inne do MODUŁU DIAGNOSTYCZNEGO.

5) Kolektor danych musi umożliwiać tworzenie zaawansowanych parserów (również własnych) w celu ekstraktowania danych i wykonywania transformacji na tych danych.

3.7.2.3. Moduł analityczno-raportowy

1) Moduł analityczno-raportowy musi umożliwiać użycie dowolnego pola z logów zebranych przez moduł kolektora danych, w celu przeprowadzenia analiz (użycia go jako wymiaru lub miary) do tworzenia wizualizacji oraz interaktywnego filtrowania i drążenia danych, opisanego poniżej, do 30 dni wstecz.
2) Moduł analityczno-raportowy musi umożliwiać pokazywanie danych na różnego rodzaju wizualizacjach
3) Moduł analityczno-raportowy musi umożliwiać przeszukiwanie wszystkich danych z poziomu interfejsu graficznego z pojedynczego pola wyszukiwania. Wyszukiwanie powinno przeszukiwać wszystkie rodzaje treści, w tym dane (wartości pól)
4) Moduł analityczno-raportowy musi umożliwiać interaktywne drążenie oraz filtrowanie danych na wszystkich dostępnych rodzajach wizualizacji danych.
5) Moduł analityczno-raportowy musi umożliwiać łatwą i elastyczną edycję i tworzenie widoków/dashboardów analitycznych
6) Moduł analityczno-raportowy musi umożliwiać przedstawianie dużych wolumenów danych (np. za długi okres czasu) w formie zagregowanej na widokach wyboru, które pozwalają zidentyfikować, wyfiltrować i załadować odpowiednie podzbiory danych (np. wycinek czasowy, zakres adresów IP, rodzaj przeprowadzonej akcji) do szczegółowej analizy na danych surowych (bez agregacji).
7) Moduł analityczno-raportowy musi umożliwiać przeprowadzanie analizy porównawczej na różnych wykresach w obrębie tej samej strony pulpitu nawigacyjnego.
8) Moduł analityczno-raportowy musi umożliwiać zdefiniowanie warunków logicznych dla wyświetlania się poszczególnych komponentów wizualizujących dane lub konkretnych jej elementów, np. kolumn w tabelach.
9) Moduł analityczno-raportowy musi umożliwiać wykonywanie przyrostowego zaczytywania / odświeżania danych.
10) Moduł analityczno-raportowy musi umożliwiać tworzenie i eksportowania danych z modułu analitycznego do postaci statycznych raportów dostępnych w różnych formatach zarówno ad-hoc na żądanie jak i wg ustalonego harmonogramu z poziomu interfejsu graficznego użytkownika jak i poprzez API. Zamawiający wymaga dostosowanie modułu analityczno-raportowego do obsługi co najmniej 30 raportów na godzinę. Stopień skomplikowania i złożoność raportów ustalona zostanie w trybie roboczym po podpisaniu umowy. Zamawiający wymaga aby raporty były generowane w formacie co najmniej: pdf, xls lub csv. Raporty będą przekazywane do odbiorców poprzez API i udostępnienie na współdzielonym zasobie dyskowym. Odbiorcą raportów może być każdy użytkownik Konsoli raportującej oraz zewnętrzne systemy wysyłające zapytania do Konsoli raportującej poprzez interfejs API.

Raporty mają być definiowane przez użytkowników Konsoli zarządzającej z poziomu interfejsu graficznego wskazanego w pkt 3.7.2.3 ppkt. 3). Zakres danych znajdujących się w raportach definiowany będzie poprzez definiowanie zapytania definiującego wyszukanie określone w pkt 3.7.2.3 ppkt. 3)

11) Musi być zapewniona możliwość archiwizacji logów do zewnętrznych systemów archiwizacyjnych
12) Moduł analityczno-raportowy musi umożliwiać tworzenie raportów z danych zebranych w ciągu 7 dni.
13) Moduł analityczno-raportowy musi udostępniać Zamawiającemu widok przedstawiający listę wszystkich adresów URL wraz z podaniem liczby wejść na dany adres URL, zarejestrowanych przez funkcjonalność dynamicznej analizy treści.
14) Moduł analityczno-raportowy musi umożliwiać Zamawiającemu przeglądanie następujących statystyk zebranych w ciągu ostatnich 7 dni:
    a. Wyświetlanie co najmniej 50 najpopularniejszych fraz i słów znajdujących się w treściach pobieranych przez użytkowników (dla wszystkich użytkowników oraz dla poszczególnych grup – np. podział geograficzny).
    b. Wyświetlanie fraz i słów „trendujących" – takich których ilość wystąpień znacząco wzrosła w ostatnim okresie (dla wszystkich użytkowników oraz dla poszczególnych grup – np. podział geograficzny).
    c. Wyświetlenie kontekstu dla fraz i słów umożliwiające określenie z jakimi zwrotami dana fraza występowała najczęściej na stronach pobieranych przez użytkowników.
    d. Wskazanie na jakich stronach wystąpiły dane frazy i słowa.

3.7.2.4. Moduł diagnostyczny

1) Moduł diagnostyczny musi umożliwiać przeglądanie, w czasie zbliżonym do rzeczywistego, logów systemu SWG z okresu do 24 godzin wstecz zebranych przez moduł kolektora danych.
2) Moduł diagnostyczny musi umożliwiać analizę surowych logów dostępowych oraz debugowych pochodzących z wszystkich elementów Systemu SWG w celu diagnozy problemów z działaniem systemu.
3) Moduł diagnostyczny musi umożliwiać zaawansowane wyszukiwanie danych w ww logach, tj:
    a. Stosowania operacji logicznych (OR, AND, NOT itp.),
    b. Zagnieżdżania zapytań,
    c. Stosowania w zapytaniach wyrażeń regularnych.

    z możliwością bieżącej modyfikacji tych kryteriów
4) Moduł diagnostyczny musi umożliwiać przeszukiwanie zawartość wszystkich zdarzeń jednocześnie, niezależnie od czasu ich wystąpienia, źródła pochodzenia czy formatu
5) Moduł diagnostyczny musi umożliwiać szybkie wyszukanie wystąpienia dowolnych wyrażeń w dowolnych zdarzeniach bez konieczności stosowania mechanizmów optymalizacji zapytań w zależności od typu przeszukiwanych danych.
6) Wyniki zapytań muszą być prezentowane w sposób umożliwiający interaktywne przeglądanie zdarzeń, spełniających warunki zawarte w zapytaniu (niezależnie od formatu tych zdarzeń) lub

automatycznego wykonywania dalszych zapytań inicjowanych za pomocą kliknięć poszczególnych elementów obrazujących wyniki.

3.8. Węzeł laboratoryjny

Węzeł laboratoryjny opisany poniżej musi odzwierciedlać pod kątem funkcjonalnym System SWG pracujący w Regionalnym Węźle Bezpieczeństwa. Wydajność Węzła laboratoryjnego musi być zgodna z tabelą podaną w pkt. 3.3.2 „Wymagania wydajnościowe na Węzeł laboratoryjny ”, z zachowaniem funkcjonalności uruchomionych w Regionalnym Węźle Bezpieczeństwa. Węzeł laboratoryjny zostanie zainstalowany na platformie wirtualizacyjnej Zamawiającego zlokalizowanej w Mazowieckim Regionalnym Węźle Bezpieczeństwa.

3.8.1. Wymagania na testową instancję Systemu SWG

Wykonawca w ramach kontraktu jest zobowiązany do dostarczenia do Węzła laboratoryjnego takiego samego co do wersji i rodzaju licencji Oprogramowania, jak to zainstalowane w Regionalnych Węzłach Bezpieczeństwa. Celem ww. środowiska będzie możliwość odtworzenia dowolnego fragmentu funkcjonalności Systemu SWG na potrzeby rozwiązywania problemów, a także na potrzeby testowania nowych wersji oprogramowania przed jego wdrożeniem w sieci OSE.

Wykonawca musi dostarczyć po jednym z dostarczonych modeli:

a) Oprogramowania SWG
b) Oprogramowania realizującego Funkcjonalność AV*
c) Oprogramowania realizującego dynamiczną analizę treści*

*) dostarczenie tych komponentów jest obligatoryjne w przypadku jeśli Wykonawca w ramach realizacji przedmiotu zamówienia dostarczy dedykowane komponenty realizujące wymagania postawione dla tych systemów w pkt 3.6

3.8.2. Wymagania na testową instalację Systemu zarządzającego

Zamawiający dostarczy oprogramowanie identyczne z oferowanym Systemem zarządzającym (możliwe jest nałożenie ograniczeń wydajnościowych) wraz z licencją umożliwiającą wykorzystanie tego oprogramowania wyłącznie do celów rozwojowo-testowych (bez prawa do wykorzystania w sieci eksploatowanej komercyjnie).

Oferowane oprogramowanie (wraz z licencją) musi zapewniać możliwość współpracy z oferowanym testowym środowiskiem fizycznym i wirtualnym oraz współpracy z systemami testowymi OSS/BSS Zamawiającego wyszczególnionymi w pkt 3.14.

3.9. Relokacja Systemu

Na zlecenie Zamawiającego, jednokrotnie w toku obowiązywania Umowy, Wykonawca może być zobowiązany do wykonania Relokacji Systemu na inną platformę wirtualizacyjną. Zamawiający przekaże zlecenie do Wykonawcy na co najmniej 30 dni przed ustaloną datą Relokacji Systemu. Wykonawca potwierdzi otrzymanie zlecenia i przystąpi do realizacji w uzgodnionym z Zamawiającym terminie. Relokacja Systemu wykonywana będzie w asyście Zamawiającego.

Relokacji muszą podlegać wszystkie komponenty Systemu wymienione w zleceniu, z uwzględnieniem Oprogramowania i danych zebranych w trakcie działania Systemu (w szczególności wszystkie logi).

Relokacja Systemu musi odbywać po za Godzinami Roboczymi i trwać nie dłużej niż 2 dni. Czas wykonania przez Wykonawcę Relokacji systemu liczony jest od wyłączenia Systemu do ponownego uruchomienia Systemu, potwierdzonego testami.

Po zainstalowaniu przenoszonych komponentów systemu w nowym i po podłączeniu ich do sieci teleinformatycznej Zamawiającego, Wykonawca przeprowadzi testy zgodne ze scenariuszami testowymi wykonywanymi na etapie Odbioru Systemu, w celu potwierdzenia poprawności działania Systemu w nowej lokalizacji lub na nowej platformie wirtualizacyjnej Zamawiającego.

Zamawiający nie gwarantuje, że pierwotna i docelowa platforma wirtualizacyjna zostaną zrealizowane w oparciu o tą samą technologię wirtualizacji. W zleceniu wykonania Relokacji Systemu Zamawiający przekaże Wykonawcy informację o technologii uzytej do budowy docelowej platformy wirtualizyjnej – jednej z: Hyper-V, KVM lub vSphere.

3.10. Usługa Asysty Technicznej

Usługa Asysty Technicznej polegać będzie na świadczeniu przez okres obowiązywania Umowy konsultacji lub wykonywaniu prac dodatkowych w zakresie funkcjonowania Systemu, przy czym nie dłużej niż do chwili wyczerpania puli 500 godzin roboczych przewidzianych dla realizacji tych usług lub prac. Usługa Asysty Technicznej będzie obsługiwana w terminach określonych dla Zgłoszeń z Priorytetem 3. Czynności wchodzące w zakres Usługi 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 Usługi Asysty Technicznej oraz możliwy termin ich wykonania. Wykonawca przystępuje do wykonania Usługi Asysty Technicznej po zaakceptowaniu przez Zamawiającego ustalonej pracochłonności oraz terminu wykonania. Po wykonaniu czynności wchodzących w zakres Usługi Asysty Technicznej Strony sporządzą protokół odbioru czynności wraz ze wskazaniem liczby godzin roboczych przeznaczonych na wykonanie Usługi.

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

Przedmiotem Usługi Asysty Technicznej mogą być w szczególności:

1) rekonfiguracja Systemu,
2) integracja z innymi systemami Zamawiającego,
3) uruchamianie nowych funkcjonalności Systemu według dyspozycji Zamawiającego,
4) czynności wynikające z rozbudowy Systemu.

3.11. Usługa Wsparcia Serwisowego

Świadczenie Usługi Wsparcia Serwisowego polegać będzie na obsłudze Zgłoszeń przekazywanych w ustalony sposób przez delegowanych pracowników Zamawiającego do Wykonawcy. W trakcie obsługi danego Zgłoszenia Wykonawca będzie zobowiązany do przeprowadzenia czynności diagnostycznych poprzez analizowanie przyczyny i okoliczności wystąpienia Awarii, w szczególności pod kątem wystąpienia Błędów Systemu oraz dostarczenia Obejścia i Naprawy. Wyniki tych prac będą przekazywane Zamawiającemu. W czasie diagnozy Zgłoszenia zespół Wykonawcy ma prawo kontaktować się z Zamawiającym w celu uzyskania dodatkowych informacji, pocztą elektroniczną lub telefonicznie.

Zgłoszenia będą dokonywane telefonicznie lub mailowo na wskazany adres Wykonawcy, przy czym Zgłoszenie telefoniczne powinno być następnie potwierdzone drogą mailową. Zgłoszenia Błędów Krytycznych muszą zostać potwierdzone przez Kierownika Projektu Zamawiającego. Zamawiający może wskazać inny sposób przekazywania i obsługi Zgłoszeń, w szczególności poprzez udostępnienie Wykonawcy dostępu do określonego systemu Zamawiającego.

Wykonawca świadczy Usługę Wsparcia Serwisowego w modelu 24/7 – 24 godziny dziennie, od poniedziałku do niedzieli – przez cały okres trwania Umowy.

Priorytety Zgłoszeń:

1) Błąd krytyczny – objawy wskazują na występowanie w systemie Błędu krytycznego,
2) Błąd niekrytyczny – objawy wskazują na występowanie w systemie Błędu niekrytycznego,
3) Usterka – objawy wskazują na występowanie w systemie Usterki.

Priorytet Zgłoszenia ustala Zamawiający.
Podczas prowadzenia przez Wykonawcę weryfikacji kompletności Zgłoszenia, Wykonawca może wnioskować do Kierownika Projektu Zamawiającego o obniżenie jego Priorytetu. Kierownik Projektu Zamawiającego powiadomi Wykonawcę o obniżeniu Priorytetu Zgłoszenia lub odrzuci wniosek Wykonawcy.

Zastosowanie zaakceptowanego przez Zamawiającego Obejścia powoduje odpowiednie obniżenie Priorytetu Zgłoszenia.

W wyniku przeprowadzonej diagnozy zespół Wykonawcy jest zobowiązany:

1) w przypadku stwierdzenia, że przyczyną Zgłoszenia jest Błąd w Systemie – potwierdzić jego priorytet (zgodnie z zasadą priorytet 1 (błąd krytyczny), priorytet 2 (niekrytyczny), priorytet 3 (usterka)) i zainicjować proces jego Naprawy siłami Wykonawcy lub z wykorzystaniem Wsparcia technicznego producenta,

2) w przypadku stwierdzenia, że przyczyną Zgłoszenia nie jest Błąd w Systemie – rozwiązać zgłoszenie na etapie diagnozy ze wskazaniem przyczyny (źródła) wystąpienia lub udzielić konsultacji,
3) w każdym przypadku realizacji Zgłoszenia dotyczącego Błędu krytycznego i Błędu niekrytycznego, zespół Wykonawcy zastosuje Obejście.

Gwarantowane czasy reakcji i naprawy

Priorytet zgłoszenia	Opis pozycji	Czas reakcji (godz)	Czas przywrócenia Systemu – zastosowanie Obejścia (godz)	Czas Naprawy (godz)
Priorytet 1	Błąd krytyczny	2	12	48
Priorytet 2	Błąd niekrytyczny	4	12	72
Priorytet 3	Usterka	6	-	96

Jeśli Błąd dotyczy Oprogramowania i Wykonawca uzyska od producenta Oprogramowania diagnozę problemu wskazującą, że naprawa wymaga instalacji nowej wersji oprogramowania, Wykonawca zobowiązany jest przekazać Zamawiającemu treść diagnozy i zastosować Obejście. Po przesłaniu do Zamawiającego diagnozy otrzymanej od producenta Oprogramowania, zostanie wstrzymany upływ Czasu Naprawy do czasu zainstalowania przez Wykonawcę nowej wersji oprogramowania wskazanej przez producenta Oprogramowania.

Wykonywanie Prac Planowych

Prace planowe wykonywane są przez Wykonawcę w Systemie pod warunkiem powiadomienia i uzyskania zgody Zamawiającego na co najmniej 5 dni przed datą ich rozpoczęcia. Prace Planowe mogą być wykonywane wyłącznie poza Godzinami Roboczymi.

W zakres Prac Planowych mogą wchodzić w szczególności:
1) Aktualizacja Systemu.
2) konserwacja Systemu.
3) inne związane z Systemem czynności serwisowe wymagające wtrzymania działania Systemu.

3.12. Usługa Instruktażu

W ramach Umowy Wykonawca zobowiązany jest do wykonania instruktaży, zgodnie z następującym zakresem:

3.12.1 Instruktaż w zakresie zastosowanych rozwiązań projektowych

1) Zakres instruktażu będzie obejmował co najmniej:

a) informacje umożliwiające uruchomienie wymienionych w niniejszym dokumencie funkcjonalności, w tym konfiguracje, rekonfiguracje, administracja użytkownikami oraz wszelkie inne kwestie związane z administracją Systemem,
b) używane protokoły routingu wraz z użytymi politykami, itp.,
c) używane polityki bezpieczeństwa,
d) używane ścieżki ruchu dla polityk bezpieczeństwa,
e) używane wyjątki w Systemie SWG,
f) sposoby konfiguracji usług na Systemie SWG wraz z podstawowymi mechanizmami i technikami diagnostycznymi,
g) wiedza przekazana w trakcie instruktażu musi być wystarczająca do konfiguracji usług dla szkół oraz kreowanie nowych usług.

2) Warunki przeprowadzenia instruktażu będą następujące:
a) instruktaż odbędzie się w siedzibie Zamawiającego (lub w miejscu wskazanym przez Zamawiającego na terenie Warszawy), wszelkie sprawy organizacyjne (w tym opłaty) związane z przygotowaniem sali szkoleniowej pozostają w gestii Zamawiającego,
b) instruktaż będzie zawierał część praktyczną z poruszanych zagadnień wykonywaną w laboratorium na miejscu lub zdalnie,
c) instruktaż odbędzie się na bazie zainstalowanego w ramach Umowy Systemu,
d) instruktaż będzie przeprowadzony dwukrotnie, w okresie pomiędzy realizacją Etapu 0 i realizacją Etapu 1,
e) każdorazowo w instruktażu będzie uczestniczyło do 10 osób,
f) każdorazowo instruktaż będzie trwał nie krócej niż 2 dni,
g) materiały dydaktyczne do ww. instruktażu zostaną przekazane w wersji elektronicznej, umożliwiającej NASK wydrukowanie dowolnej liczby kopii ww. materiałów.

3.12.2 Instruktaż zaawansowany z zakresu rozwiązań technicznych wchodzących w skład Systemu

1) Instruktaż w zakresie każdego z rozwiązań użytych do budowy Systemu SWG
2) Warunki przeprowadzenia instruktażu będą następujące:
a) instruktaże zostaną zrealizowane w autoryzowanym przez producentów ośrodkach szkoleniowych (preferowane ośrodki na terenie Warszawy lub Polski),
b) każdy z instruktaży odbędzie się w więcej niż 1 terminie, przy czym pierwszy instruktaż odbędzie się w terminie nie późniejszym, niż w ciągu czterech miesięcy od podpisania umowy,
c) w instruktażach będzie uczestniczyło do 10 osób wskazanych przez Zamawiającego,
d) każdy z instruktaży będzie zrealizowany na poziomie podstawowym oraz zaawansowanym (łącznie 2 instruktaże na każdą osobę).

3.12.3 Instruktaż z Utrzymania

1) Zakres instruktażu będzie obejmował co najmniej:

a) informacje umożliwiające podstawową weryfikację działania usług, opis działania całego Systemu,
b) monitoringu rozwiązania przez narzędzie wystawione i zapewnione przez Wykonawcę,
c) kwestii procedur operacyjnych w zakresie wymiany informacji,
d) ogólne informacje o systemie/technologii przekazane w takiej formie, aby uczestnik instruktażu był w stanie zdiagnozować, że zgłoszona awaria dotyczy tego konkretnego systemu.
e) informacje umożliwiające skonfigurowanie wymienionych w specyfikacji Systemu funkcjonalności. Instruktaż w tym zakresie jest przeznaczony dla osób zajmujących się konfiguracją Systemu,
f) konfiguracje, rekonfiguracje, administracja użytkownikami oraz wszelkie inne kwestie związane z administracją Systemem,
g) Analiza, klasyfikacja zgłoszeń,
h) tips&tricks w zakresie znanych obejść,
i) Aktualizacje dokumentacji stworzonej przez Wykonawcę.

2) Warunki przeprowadzenia instruktażu będą następujące:
a) instruktaż odbędzie się w siedzibie Zamawiającego (lub w miejscu wskazanym przez Zamawiającego), wszelkie sprawy organizacyjne (w tym opłaty) związane z przygotowaniem sali szkoleniowej pozostają w gestii Zamawiającego,
b) instruktaż odbędzie się na bazie zainstalowanego w ramach Umowy Systemu,
c) instruktaż będzie zawierał część praktyczną z poruszanych zagadnień wykonywaną w laboratorium na miejscu lub zdalnie,
d) instruktaż będzie przeprowadzony dwukrotnie, w okresie pomiędzy instalacją pierwszego węzła, a instalacją ostatniego węzła,
e) każdorazowo w instruktażu będzie uczestniczyło do 20 osób,
f) każdorazowo instruktaż będzie trwał nie krócej niż 2 dni,
g) materiały dydaktyczne do ww. instruktażu zostaną przekazane w wersji elektronicznej, umożliwiającej NASK wydrukowanie dowolnej liczby kopii ww. materiałów.

3.13. Wdrożenie

Szczegołowy przebieg wdrożenia został opisany w § 8 Wzoru Umowy

3.14. Integracje z systemami Zamawiającego

3.14.1. System zarządzania tożsamością

Zamawiający planuje w przyszłości wdrożenie Systemu zarządzania tożsamością. W przypadku wdrożenia takiego rozwiązania, każdy z Użytkowników sieci OSE będzie uwierzytelniany w celu doboru odpowiedniego polityki bezpieczeństwa, w tym poziomu filtrowania. W przypadku zakupu Systemu zarządzania tożsamością, każdy Użytkownik przy dostępie do sieci zostanie przekierowany przez System ADC na captive portal, dostarczony w ramach osobnego postępowania, gdzie nastąpi proces uwierzytelnienia i autoryzacji. Informacja o użytkowniku i przypisanej do niego grupie zostanie przekazana do Systemu ADC, z wykorzystaniem protokołu RADIUS lub innej metody

integracyjnej ustalonej z dostawcami na etapie integracji. System ADC przekaże informację, nt. uwierzytelnionego Użytkownika, do Systemów SWG. Jedynie Systemy ADC i SWG będą wykorzystywały tożsamość Użytkowników.

W przypadku podjęciu decyzji przez Zamawiającemu o konieczności wykorzystania informacji nt. tożsamości użytkowników na Systemie SWG, System ADC przekaże informację nt. uwierzytelnionego użytkownika (co najmniej: nazwę użytkownika i nazwę grupy do której użytkownik należy) poprzez wstrzyknięcie dodatkowych parametrów do nagłówka HTTP. Na podstawie tych informacji, System SWG dopasuje do danego ruchu odpowiednią politykę blokowania.

3.14.2. System provisioningu

Zamawiający planuje realizować procesy związane z uruchamianiem usług dla szkół, zmianą konfiguracji usług w sposób zautomatyzowany z wykorzystaniem udostępnionych przez niego metod integracji (w szczególności poprzez interfejs typu API, modyfikację plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym), bezpośrednią komunikację z wszystkimi komponentami Systemu co najmniej poprzez protokół SSH) wystawianych przez System zarządzający. System zarządzający dostarczony przez Wykonawcę zostanie zintegrowanyz centralnymi systemami nadzorującymi działanie wszystkich elementów sieci OSE.

Proces podłączenia szkoły zakłada dodanie adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły, do predefiniowanych na etapie wdrożenia polityk skonfigurowanych na Systemie SWG.

Proces zmiany konfiguracji usług zakłada modyfikację parametrów polityk zdefiniowanych per szkoła na poszczególnych systemach, w tym w szczególności choć nie wyłącznie:

- Na Systemie ADC:
    - Wyjątki definiujące jaki ruch ma nie podlegać dekrypcji SSL, np. na podstawie źródłowych lub docelowych adresów IP, adresów URL zawartych w parametrach certyfikatu (pola: SNI lub CN)
- Na Systemie NG Firewall:
    - Tworzenie dedykowanych polityk per szkoła blokujących lub przepuszczających ruch z/do zadanych adresów IP, nawiązywany na określonych portach TCP/UDP
    - Włączanie i wyłączanie ruchu mailowego (m.in. protokoły IMAP, POP3) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej
- Na Systemie DNS:
    - Włączenie / wyłączenie lub zmiana listy kategorii treści przypisanych do polityk określających poziom ochrony użytkowników OSE
- Na Systemie SWG:
    - Tworzenie dedykowanych polityk per szkoła

- Dodawanie i usuwanie kategorii blokowanych, skonfigurowanych w polityce dla danej szkoły
- Dodawanie i usuwanie zawartości statycznych list, zawierających adresu URL, definiujących wyjątki od polityki blokowania dla danej szkoły
- Włączanie i wyłączanie ruchu mailowego (protokoły HTTP i HTTPS) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej

➢ Na Systemie SIEM:

- Generowanie raportu dla danej szkoły, na podstawie predefiniowanych przez Zamawiającego szablonów
- Określenie harmonogramu generowania raportów dla danej szkoły

Oferowany System SWG musi umożliwiać Zamawiającemu automatyzację wyżej wymienionych procesów realizowanych na Systemie SWG. Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanym przez Wykonawcę Systemie SWG.

3.14.3. System Fault Management

Wykonawca jest zobowiązany do integracji Systemu SWG z systemami Fault Management z wykorzystaniem protokołów SYSLOG i SNMP (w tym SNMP Trap). Szczegółowy zakres integracji zostanie doprecyzowany na etapie Projektu technicznego.

3.14.4. System Performance Management

Wykonawca jest zobowiązany do integracji Systemu SWG z systemami Performance Management z wykorzystaniem co najmniej protokołu SNMP, w zakresie monitorowania i pobierania co najmniej następujących danych:

a) Pesistent Conections
b) CPU – Idle time
c) CPU – current overall CPU usage
d) Memory – Total Free
e) Memory – Total Real
f) Memory – Avail. Swap
g) Storage – disk usage

3.14.5. System Inventory

Wykonawca jest zobowiązany do integracji Systemu SWG z systemem Inventory z wykorzystaniem co najmniej protokołu SNMP. W ramach integracji Zamawiający zamierza pobierać w sposób automatyczny co najmniej następujące dane:

a) Numer seryjny komponentu Systemu

b) Producent, model komponentu Systemu
c) wersje oprogramowania
d) MAC adresy przypisane interfejsów sieciowych

Szczegółowy zakres integracji zostanie określony na etapie Projektu Technicznego.

3.14.6. System Config Management

Wykonawca jest zobowiązany do integracji Systemu SWG z systemem Config Management z wykorzystaniem co najmniej SNMP, bezpośredniej komunikacji z komponentami Systemu co najmniej poprzez protokół SSH. Zakres integracji zakłada pobieranie przez system Config Management informacji dotyczących konfiguracji każdego z elementów Systemu SWG i utrzymywanie go jako repozytorium aktualnej konfiguracji systemów.

Szczegółowy zakres integracji zostanie określony na etapie Projektu Technicznego.

3.14.7. Infrastruktura bezpieczeństwa

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

W szczególności Wykonawca jest zobowiązany do przedstawienia wytycznych konfiguracyjnych dla systemu wykonującego dekrypcję ruchu SSL/TLS – F5 BIG-IP SSL Orchestrator. Ruch rozszyfrowany na wskazanym urządzeniu zostanie przekazany do Systemu SWG, a następnie po wykonaniu analizy System SWG przekaże go ponownie do dekrypora celem ponownego zaszyfrowania komunikacji. Wytyczne konfiguracyjne dostarczone przez Wykonawcę muszą umożliwiać realizację wszystkich wymagań postawionych przez Zamawiającego w rozdziale 3.

3.14.8. System SIEM

Wykonawca jest zobowiązany do integracji Systemu SWG z systemem SIEM w zakresie przekazywania zdarzeń do, wskazanego przez Zamawiającego, kolektora SIEM. Zamawiający zakłada, że czas buforowania zdarzeń przed przekazaniem ich do Systemu SIEM nie będzie dłuższy niż 48h. System zarządzający będzie przekazywał do Systemu SIEM zdarzenia o wszystkich zablokowanych sesjach użytkowników oraz zagregowane informacje z ostatnich 24h o liczbie wejść na poszczególne adresy URL znajdujące się w określonej kategorii.

Szczegółowy zakres integracji, w tym poziomy logowania, zostanie określony na etapie Projektu Technicznego.

3.14.9. System parental control

Zamawiający planuje w przyszłości wdrożenie Systemu parental control. Zostanie on zrealizowany w postaci bezpłatnej aplikacji udostępnionej w ramach sklepów Google Play i AppStore oraz aplikacji desktopowej realizującej funkcjonalności:

- ochrony użytkowników przed nielegalnymi i szkodliwymi treściami dostępnymi w sieci Internet
- udostępnienie treści edukacyjnych
- dostarczenie konsoli zarządzającej umożliwiającej na wgląd w aktywność i kontrolę urządzenia dziecka w zakresie, wyboru profilu ochrony, czasu wykorzystania telefonu i wielu innych

System parental control zostanie zrealizowany przez Zamawiającego w ramach osobnego postępowania.

Wykonawca jest zobowiązany do integracji wszystkich komponentów Systemu z System parental control. W ramach integracji dostarczony System SWG będzie odpowiadał na zapytania, dotyczące kategoryzacji zadanego adresu URL, zadane za pomocą interfejsu REST API lub za pomocą protokołu ICAP z wykorzystaniem Funkcjonalności filtrowania adresów URL i Funkcjonalności dynamicznej analizy treści. W odpowiedzi System SWG przekaże do Systemu parental control, informację jaką kategorię posiada dany adres URL. Informacja ta zostanie utrwalona w Systemie parental control w postaci pamięci podręcznej (cache). Model licencjonowania Systemu SWG musi umożliwiać na wskazany powyżej sposób wykorzystania dostarczonego Systemu.

Alternatywnym modelem integracji z systemem parental control będzie zestawienie połączenia VPN pomiędzy urządzeniami użytkowników, a siecią OSE. Model ten jest natywnym sposobem wykorzystania Systemu SWG i nie będzie wymagał dodatkowych prac po stronie Wykonawcy.

Szczegółowy zakres integracji zostanie określony na etapie Projektu Technicznego.

3.15. Wytyczne dla Dokumentacji Technicznej

3.15.1. Ogólne założenia Projektu Technicznego

Dokument Projektu Technicznego powinien zawierać ogólną koncepcję realizacji całego Systemu z podziałem na Oprogramowanie w ramach każdego z Węzłów.

Dokument Projektu Technicznego powinien zawierać opisy wystarczający do zbudowania Systemy spełniającego wymagania opisane w Szczegółowym Opisie Przedmiotu Zamówienia (Załącznik nr 1 do Umowy)

Dokument Projektu Technicznego powinien zawierać opisy poszczególnych rozwiązań zaimplementowanych na Systemie SWG niezbędnych do realizacji Przedmiotu Zamówienia wraz z uzasadnieniem ich wyboru.

Dokument Projektu Technicznego powinien zawierać opisy każdego komponentu oraz funkcjonalności komponentu opisanej w Szczegółowym Opisie Przedmiotu Zamówienia, w szczególności dla Systemu SWG; Funkcjonalności filtracji adresów URL; Funkcjonalności AV; Funkcjonalności dynamicznej analizy treści; Systemu zarządzającego.

Dokument Projektu Technicznego powinien zawierać opis mechanizmów wysokiej dostępności (high availability) dla Systemu SWG i Systemu zarządzającego. Opisy powinny zawierać wyczerpujące scenariusze ich działania.

Dokument Projektu Technicznego powinien zawierać opis integracji Systemu SWG z Infrastrukturą bezpieczeństwa Zamawiającego, w sposób szczególny dokładny opis połączenia z systemem F5 BIG-IP SSL Orchestrator wraz z wytycznymi konfiguracynymi dla tego systemu. Opisy powinny zawierać wyczerpujące scenariusze ich działania.

Założenia konfiguracyjne zawarte w dokumencie Projektu Technicznego powinny zawierać rzeczywiste wyliczenie użytych zasobów dla każdego Węzła oraz pozostałych wolnych zasobów, biorąc pod uwagę zakładaną konfigurację, ilość zainstalowanych elementów oraz uruchomionych serwisów Systemu SWG i Systemu zarządzającego.

3.15.2. Zakres Projektu Technicznego:

a) Słownik zastosowanych pojęć,
b) Spis dostarczonego oprogramowania
c) Opis koncepcji oraz przyjętych założeń,
d) Plan wdrożenia/ Implementacji z podziałem na Węzły,
e) Opis architektury każdego węzła z rysunkami przedstawiającymi wysokopoziomową architekturę zastosowaną we wdrożeniu z uwzględnieniem integracji z Infrastrukturą bezpieczeństwa Zamawiającego,
f) Opis zastosowanych technologii, wraz z ich szczegółowym opisem oraz wyjaśnieniami doboru parametrów konfiguracyjnych,
g) Opis zastosowanych komponentów oraz połączeń pomiędzy nimi (topologie sieci, węzłów itp.),
h) Opis założeń ruchowych dla poszczególnych komponentów,
i) Opisy pojemnościowe / skalowalność każdego Węzła i komponentu,
j) Opis zastosowanych mechanizmów redundancji oraz mechanizmów detekcji awarii,
k) Opis zastosowanych protokołów routingu,
l) Opis zastosowanych mechanizmów zabezpieczenia komponentów Systemu i sieci jako całości (ochrona Control i Data Plane, dostęp Out of Band itp.)
m) Opis podłączenia i konfiguracji Systemu Zarządzania,
n) Opis przepływu ruchu przez System, przejścia ruchu przez poszczególne komponenty Systemu, kolejność, funkcje, opis dla różnych zastosowanych wariantów,
o) Dokumentacja producenta do wszystkich komponentów Systemu.
p) Wytyczne konfiguracyjne dla systemu F5 BIG-IP SSL Orchestrator
q) Logika rozwiązania:
   - Logiczny rysunek warstwy drugiej z podziałem na sieci VLAN, a także opis i zastosowanie w/w,
   - Opis i zastosowanie protokołów warstwy drugiej,
   - Opis zastosowanych adresacji IP / podział na klasy IP wraz ze szczegółowym rysunkiem węzłów i lokalizacji,
   - Opis routingu dynamicznego / statycznego zastosowanego we wdrożeniu,

- Opis polityk bezpieczeństwa zastosowanych na każdym z komponentów dostarczonego rozwiązania:
    1. Systemu SWG,
    2. Funkcjonalności filtracji adresów URL,
    3. Funkcjonalności dynamicznej analizy treści,
    4. Funkcjonalności AV,

r) Warstwa funkcjonalna

- Opis szczegółowy poszczególnych komponentów Systemu z wyszczególnieniem funkcjonalności i pełnionych funkcji z perspektywy architektury:
    5. Systemu SWG,
    6. Funkcjonalności filtracji adresów URL,
    7. Funkcjonalności dynamicznej analizy treści,
    8. Funkcjonalności AV,
    9. Systemu zarządzającego.
- Opis szczegółowy konfiguracji poszczególnych elementów Systemu,
- Opis zastosowanych mechanizmów bezpieczeństwa środowiska,
- Opis jak budować polityki bezpieczeństwa – rekonfiguracja, aktualizacja Funkcjonalności dynamicznej analizy treści w oparcio o dane z Konsoli raportującej
- Opis jak dodawać wyjątki na poziome Systemu SWG dla ruchu który nie podlega filtrowaniu (*white / black listy*)
- Opis zarzadzania i zdalnego dostępu do platformy,
- Opis połączeń do systemów zewnętrznych.

3.15.3. Zakres Dokumentacji powykonawczej

Do każdego zainstalowanego komponentu Systemu w Węźle Regionalnym powinna zostać wykonana osobna dokumentacja powykonawcza zawierająca między innymi:

- Lista zainstalowanych wszystkich komponentów Systemu oraz opis wykonanej instalacji.
- Kopie konfiguracji komponentów Systemu (tylko w wersji elektronicznej).
- Procedury do administrowania Węzłem (wyszczególnienie poniżej).

W zakresie dokumentacji powykonawczej Wykonawca powinien dostarczyć również zaktualizowany Projekt Techniczny (zmiany wynikłe podczas Wdrożenia i Testów Odbiorczych).

Procedury administracyjne opisujące czynności dla Systemu w danym Węźle jak i z perspektywy całego Systemu, powinny zawierać takie opisy jak:

- Procedury instalacji każdego elementu Systemu.
- Procedury włączania / wyłączania zasilania elementu Systemu.
- Procedury włączania / wyłączania elementu Systemu do sieci Zamawiającego.
- Procedury tworzenia i odtwarzania backupu dla każdego elementu Systemu.
- Procedura przyłączania poszczególnych elementu Systemu do Oprogramowania System Zarządzania.
- Procedury utrzymaniowe Oprogramowania.

- Procedury przyłączania Systemu SWG do systemów Zamawiającego, z którymi wykonano Integrację.
- Procedury diagnostyczne w przypadku Awarii, Błędów i Usterek.