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
Kontrola aplikacji **(**Application control)	Funkcjonalność zapewniająca możliwość rozpoznawania aplikacji sieciowych i decydowania o dopuszczaniu możliwości ich komunikacji z siecią Internet.
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).
BFD	Protokół sieciowy wykrywający problemy pomiędzy dwoma procesami przekazującymi ruch połączonymi , między sobą. Wspierane protokoły trasowania to BGP, IS-IS ,OSPF. Został on opisany w RFC 5880.
BGP	Zewnętrzny protokół trasowania (routingu) EGP. BGP w wersji czwartej jest podstawą działania współczesnego Internetu. Istnieje wiele rozszerzeń BGP stosowanych przy implementacji MPLS VPN, IPv6 czy Multicast VPN. Jest protokołem wektora ścieżki umożliwiającym tworzenie niezapętlonych ścieżek pomiędzy różnymi systemami autonomicznymi. Obecny otwarty standard protokołu BGP jest opisany w dokumentach RFC 4271 i 1771. Protokół ten nie używa tradycyjnych metryk - analogiczną funkcję (determinanty wyboru trasy) pełnią atrybuty i algorytm wyboru. BGP pozwala na pełną redundancję w połączeniu z Internetem, jest również używany do połączenia dwóch systemów autonomicznych, do wymiany ruchu między tymi systemami. Protokół BGP funkcjonuje w oparciu o protokół warstwy 4 modelu OSI (port TCP o numerze 179). Zapewnia to, że aktualizacje są wysyłane w sposób niezawodny, dzięki czemu w BGP niepotrzebne są mechanizmy retransmisji, segmentacji, itp. Routery zestawiają pomiędzy sobą sesje BGP, dzięki którym mogą wymieniać się informacjami o dostępnych trasach (prefiksach) i

	wyznaczać najlepszą niezapętloną ścieżkę do sieci docelowych.
Centralny Węzeł Bezpieczeństwa	Wwęzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym dostarczający mechanizmy ochrony Zasobów obliczeniowych OSE
DDNS	Metoda, protokół lub usługa sieciowa umożliwiająca urządzeniom sieciowym lub systemom komputerowym, , zakomunikować w czasie rzeczywistym (ad-hoc) serwerowi nazw zmianę obecnej konfiguracji DNS w postaci skonfigurowanych domen, adresów oraz innych danych zamieszczonych w rekordach DNS.. Zgodna z standardem w ramach RFC 2136
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.
DNS tunneling	Podatność, która pozwala tunelować inne protokoły w ruchu protokołu DNS poprzez port 53 UDP
DNSSEC	Rozszerzenie systemu DNS mające na celu zwiększenie jego bezpieczeństwa poprzez uwierzytelnienie źródła danych DNS. Opisany w RFC 4033.
Dystrybucja tożsamości do system SWG	Funkcjonalność zapewniająca przekierowanie użytkownika OSE do systemu uwierzytelnienia i po poprawnym jego uwierzytelnieniu przekazanie informacji o użytkowniku i przypisanej mu grupie do systemów bezpieczeństwa SWG.
Fail-close	Mechanizm w którym urządzenie w trybie przeciążenia przerywa nowe połączenia.
Filtrowanie treści	Funkcjonalność SWG której celem jest zapewnienie ochrony użytkownikom OSE poprzez mechanizm

	dynamicznej analizy treści dostępnych na stronach www, oparty o analizę leksykalną lub dynamiczne mechanizmy uczenia maszynowego.
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.
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 / System	zbiór Urządzeń i Oprogramowania zapewniających bezpieczeństwo teleinformatyczne OSE, składa się z Regionalnych i Centralnych węzłów bezpieczeństwa, wraz z niezbędnymi licencjami i subskrypcjami, realizujące funkcje opisane w niniejszym dokumencie.
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.
IPS **(**Intrusion Prevention System)	Funkcjonalność zapewniająca detekcję i prewencję włamań do sieci lokalnych, daje możliwość monitorowania, wykrywania i blokowania ataków w ruchu dopuszczonym przez firewall'e
IPSEC	Zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia Wirtualnej Sieci Prywatnej (ang. VPN). VPN oparta na IPSEC składa się z dwóch kanałów komunikacyjnych pomiędzy połączonymi komputerami: kanał wymiany kluczy, za pośrednictwem którego przekazywane są dane związane

	z uwierzytelnianiem i szyfrowaniem (klucze) oraz kanał (jeden lub więcej), który niesie pakiety transmitowane poprzez sieć prywatną. Kanał wymiany kluczy jest standardowym protokołem UDP (port 500). Kanały przekazywania danych oparte są na protokole ESP (protokół numer 50) opisanym w dokumencie RFC 2406.
Kategoryzacja URL	Funkcjonalność SWG której celem jest zapewnienie ochrony użytkownikom OSE poprzez mechanizm porównywania odwołań do stron www wykonywanych przez użytkowników ze specjalizowaną bazą danych dostarczaną przez producenta SWG, podzieloną na kategorie treści stron www.
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. W sytuacji, awarii jednego z urządzeń, zadaniem systemu jest przekierowanie ruchu do innych sprawnych urządzeń, aby zapewnić wysoką dostępność całego systemu świadczącego 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 Virtual Private Network.
NETFLOW	Protokół wymyślony przez firmę Cisco na potrzeby zliczania przepływów i dający informacje na poziome trzeciej i czwartej warstwy modelu OSI. Istnieją jego wersje dla różnych producentów: Jflow or cflowd dla Juniper Networks, NetStream dla 3Com/H3C|HP, NetStream dla Huawei Technology, Cflowd dla Alcatel-Lucent, Rflow dla Ericsson, AppFlow Citrix. Ostatnio wyregulowany jako standard i nazwany IPFIX - RFC 5101, 5102
New CPS	Liczba nowo zestawianych połączeń na sekundę zestawianych w warstwie transportowej modelu OSI

NTP	Protokół synchronizacji czasu w sieci pakietowej. Najbardziej aktualna wersja protokołu to wersja czwarta kompatybilna wstecz z wersja trzecia. Obie wersje zostaly opisane w RFC , odpowiednio wersja trzy 1305 wersja cztery 5905.
Osoba testująca	Osoba oddelegowana ze strony Wykonawcy do wykonywania testów.
OSPF	Protokół trasowania dynamicznego oparty o analize stanu łącza . Został oparty glównie o algorytm przeliczania trasy Dijkstry - gdzie kazdy router wewnącz obszaru. 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 .
Persistent connection	Liczba utrzymywanych połączeń TCP w tablicy stanów Urządzeń
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 umożliwiający obsługę usług w sieci OSE, w tym zgłaszanie problemów technicznych, zmian w zakresie świadczonych usług.
Protokół HTTP	Protokół przesyłania dokumentów hipertekstowych to protokół sieci WWW . 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 , 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 obsługujący Szkoły podłączone do danego Węzła Regionalnego.
Równoważenie obciążenia (LB - Load Balancers)	Funkcjonalność zapewniająca równoważenie obciążenia i przełączanie awaryjne zarówno pomiędzy systemami w jednym węźle, jak i pomiędzy systemami zlokalizowanymi w różnych węzłach sieci.
RTSP	Protokół poziomu aplikacji, mający za zadanie sterowaniem dostarczaniem danych czasu rzeczywistego. Głównie wykorzystywany do dostarczenia tzw. strumieniowanych danych multimedialnych do użytkownika końcowego
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
SIP	SIP współgra z kilkoma innymi protokołami i jest zaangażowany jedynie w część sygnalizacyjną sesji komunikacyjnej. SIP występuje jako nośnik Session Description Protocol (SDP), który opisuje transportowane multimedia w sieci, np. używane porty IP, używany kodek itp. Pierwsza zaproponowana wersja standardu (SIP 2.0) została zdefiniowana w RFC 2543 . Protokół następnie uszczegółowiono w RFC 3261 , jakkolwiek wiele implementacji używa wskazówek z tymczasowych wersji próbnych (ang. *draft*).
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.
SWG (Security Web Gateway)	Zbiór urządzeń i oprogramowania,System zapewniających funkcję funkcje ochrony użytkownika sieci OSE związanąe z potencjalnym dostępem do treści nielegalnych i szkodliwych,.. pod kątem filtracji treści udostępnionych w Internecie.
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 (typu FW i SWG).
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 7w 4 i 7 warstwie OSI, z wykorzystaniem mechanizmów statefull packet inspection, intrusion prevetion system, application control, antivirus.
System zarządzający	Zbiór urządzeń i oprogramowania, zapewniający Zamawiającemu możliwość zarządzania dostarczaną Infrastrukturą bezpieczeństwa w pełnym zakresie

	funkcjonalnym wymaganym w pkt 3.7.8 niniejszego dokumentu
Tester	Urządzenie generujące testowy ruch zgodnie z wymaganiami opisanymi w załączniku nr 12 do Zapytania ofertowego.
Ustawa OSE	ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej
Użytkownicy Sieci OSE	użytkownicy usług Sieci OSE w tym m.in.: uczniowie, nauczyciele, pracownicy administracyjni, osoby i systemy korzystajcie 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 baz 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.

Węzeł Agregacyjny	węzeł do którego dołączone są łącza dostępowe do szkół, węzeł ten nie ma bezpośredniego połączenia do sieci Internet
Węzeł Bezpieczeństwa	zestaw Urządzeń wraz z Oprogramowaniem, realizujących funkcje bezpieczeństwa (m.in. dekrypcja SSL, funkcjonalność IPS, NG Firewall itd.), sposób działania tego węzła oraz jego budowa jest zakresem niniejszego zapytania. 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
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 są umieszczone w dwóch lokalizacjach Warszawa i Poznań.

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 PIB.

2.2. Przedmiot przedsięwzięcia

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 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 będzie z węzłów zlokalizowanych na terenie 16 województw.

2.3.2. Węzły sieci

W sieci OSE będą dwa funkcjonalne rodzaje węzłów:

- Węzeł Regionalny składa się z Węzła Agregacyjnego, do którego będą dołączone łącza ze szkół, oraz z Regionalnego Węzła Bezpieczeństwa.

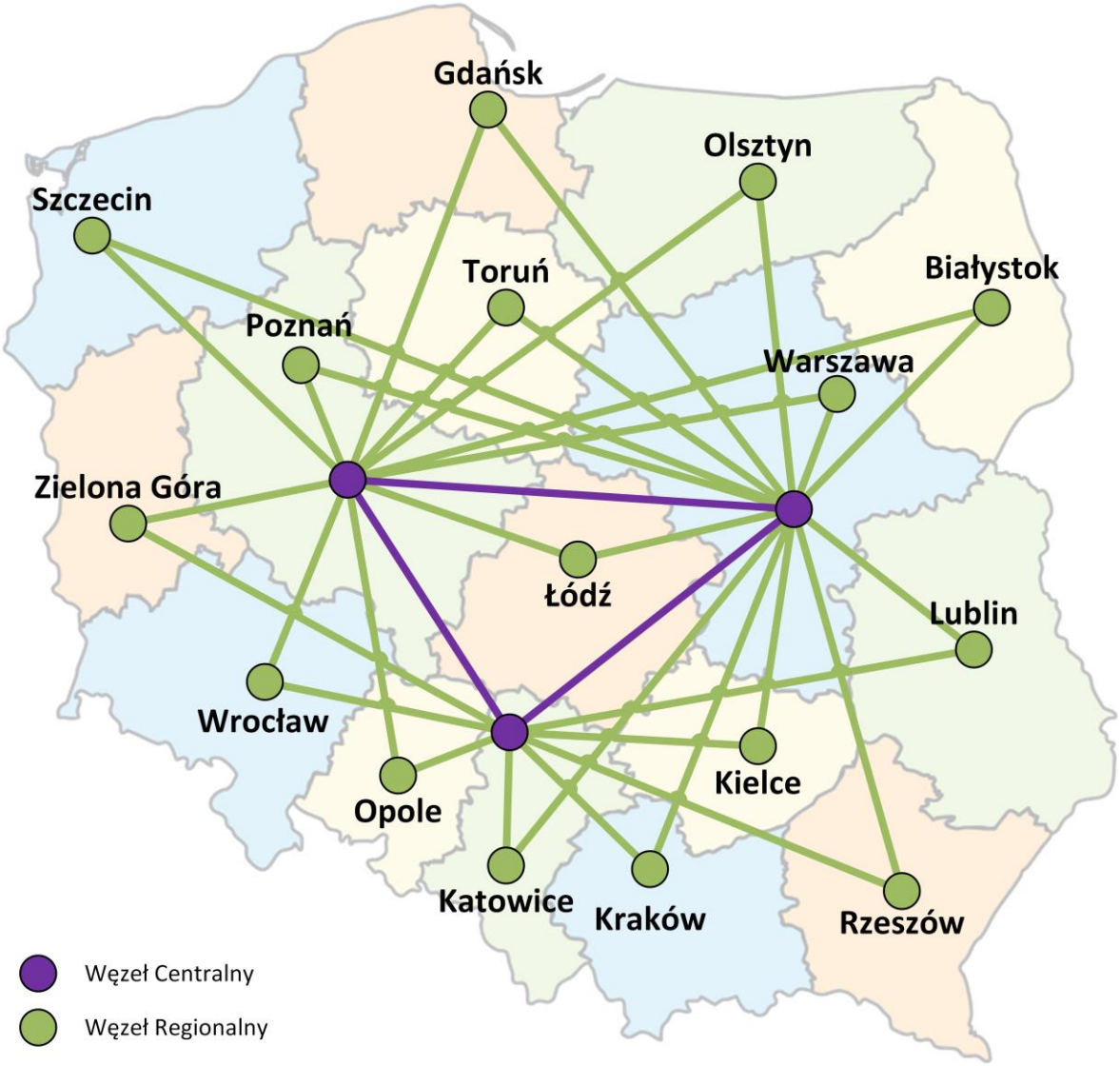
- Węzeł Centralny, składa się z Węzła Szkieletowego, do którego będą dołączone Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet oraz zapewnią połączenie z Zasobami obliczeniowymi OSE.
  Centralny Węzeł Bezpieczeństwa będzie zlokalizowany tylko w dwóch Węzłach Centralnych, w ramach Obiektów w Warszawie i Poznaniu. Wykonawca nie jest zobowiązany do dostarczenia Centralnego Węzła Bezpieczeństwa do Obiektu znajdującego się w Katowicach.

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

Obiekty, w których zainstalowane będą 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 zostanie 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 Urządzeń (zarówno w Węzłach Centralnych jak i Regionalnych) 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 szacowane 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. Koncepcja świadczenia usługi dla szkoły

W szkołach zainstalowane będą 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.

2.3.3.1. 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).

2.3.3.2. QoS

W sieci OSE wdrożony będzie QoS z następującymi założeniami:

- klasyfikacja odbywa się na urządzeniu agregacyjnym sieci OSE,
- najwyższy priorytet w sieci ma ruch z klasy Network Control, obejmujący ruch kontrolny protokołów routingu (IGP, BGP, MPLS, itd.) – ruch ma zagwarantowane 3% pasma na interfejsach szkieletowych sieci (tj. interfejsach pomiędzy urządzeniami sieci OSE bez uwzględnienia urządzeń CPE);
- ruch w klasie MGMT (ruch zarządzania, w szczególności ruch do / z systemów OSS, ruch sesji terminalowych do urządzeń sieciowych, ruch do kolektorów logów) – ruch ma zagwarantowane 5% pasma na interfejsach sieci (w tym na interfejsach pomiędzy urządzeniami sieci OSE a urządzeniami CPE);
- ruch w klasie BE (Best Effort) obejmujący ruch produkcyjny do / ze szkół – ruch ma zagwarantowane 50% pasma na wszystkich interfejsach;
- w sieci OSE musi być przygotowana możliwość uruchomienia ruchu w klasach:
    - VOICE – ruch priorytetowy – nie więcej niż 5% pasma;
    - INTVIDEO (Interactive Video) – ruch gorszy niż NC a lepszy niż MGMT – zagwarantowane 20% pasma;
    - scavenger (less-than best-effort) – ruch bez gwarancji pasma.

3. Szczegółowy opis przedmiotu zamówienia

Przedmiotem zapytania jest dostarczenie Urządzeń i Oprogramowania niezbędnych do zbudowania całego rozwiązania, stanowiącego Infrastrukturę bezpieczeństwa. Opis przedmiotu zamówienia obejmuje swoim zakresem:

- Przygotowanie Dokumentacji Technicznej zgodnie z opisem zawartym w Załączniku nr 11 do Umowy;
- Dostawa Urządzeń wraz z Oprogramowaniem, o cechach, funkcjonalności i parametrach technicznych szczegółowo wyspecyfikowanych w Szczegółowym Opisie Przedmiotu Zamówienia stanowiącym Załącznik nr 1 do Umowy;
- Udzielenie Gwarancji na Urządzenia z Oprogramowaniem oraz na wykonane Usługi, zgodnie z opisem w Załączniku nr 9 do Umowy;
- Wdrożenie Systemu, na które składają się wdrożenia poszczególnych Węzłów zgodnie z zatwierdzoną Dokumentacją Techniczną oraz wykonanie Integracji zgodnie z § 8 Umowy;
- Przygotowanie Planu Testów Odbiorczych na bazie wytycznych zawartych w Załączniku nr 10 do Umowy;
- Przeprowadzenie Instruktaży dla osób wskazanych przez Zamawiającego w zakresie opisanym w Załączniku nr 7 do Umowy;
- Przekazanie na czas nieokreślony licencji do Oprogramowania niezbędnego do prawidłowego funkcjonowania Urządzeń oraz praw autorskich dla utworów powstałych w trakcie realizacji niniejszej Umowy (w tym w szczególności dokumentacji projektowej dla Systemu oraz Dokumentacji powykonawczej);
- Przeprowadzenie Testów Odbiorczych;
- Realizacja obowiązków Wykonawcy w Okresie Stabilizacji, zgodnie z wymaganiami opisanymi w Załączniku nr 9 do Umowy;

- Wykonanie i przekazanie Zamawiającemu Dokumentacji Powykonawczej oraz jej aktualizacji, w przypadku zmian w Systemie, zgodnie z opisem w Załączniku nr 6 do Umowy;
- Utrzymywanie Systemu na warunkach określonych w Załączniku nr 13 do Umowy.

Wszystkie Urządzenia muszą zostać wdrożone zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie. 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. Wykonawca jest zobowiązany do takiego doboru Urządzeń, który zapewni efektywność energetyczną oferowanego rozwiązania i optymalizację ponoszonych przez Zamawiającego kosztów utrzymania rozwiązania.

Wszystkie wymagania i parametry musza być spełnione łącznie. Wszystkie wymagania podane w niniejszym dokumencie muszą być spełnione dla dowolnej wielkości ruchu określonej w niniejszych wymaganiach, chyba że w opisie danej funkcjonalności podano inaczej.

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).

Wykonawca jest proszony o dobór odpowiednich Urządzeń do realizacji potrzeb Zamawiającego w zakresie budowy Regionalnych i Centralnych Węzłów Bezpieczeństwa. Zamawiający dopuszcza oferowanie wielu urządzeń realizujących zadania węzłów lub też jednego urządzenia realizującego wszystkie niezbędne funkcje przy zachowaniu parametrów niezawodnościowych (HA). Jednocześnie proponowane rozwiązania dla poszczególnych węzłów powinny być zunifikowane.

Wykonawca jest zobowiązany do Wdrożenia Infrastruktury bezpieczeństwa w każdym z 16 Regionalnych Węzłów Bezpieczeństwa, 2 Centralnych Węzły Bezpieczeństwa oraz 1 węzła laboratoryjnego. Wdrożenie Infrastruktury bezpieczeństwa obejmuje dostawę Urządzeń i Oprogramowania, instalację, konfigurację, uruchomienie i przeprowadzenie procedury odbiorów, a następnie utrzymanie przez okres przejściowy. Wykonawca będzie również zobowiązany do współpracy z innymi dostawcami wskazanymi przez Zamawiającego przy integracji Infrastruktury bezpieczeństwa z innymi systemami wskazanymi przez Zamawiającego.

3.1. Funkcjonalności Węzłów Bezpieczeństwa

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

- Zapewniać bezpieczeństwo teleinformatyczne użytkownikom sieci OSE
- Wykrywać i zapobiegać włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym.
- Wykrywać i blokować zdefiniowane aplikacje webowe.
- Monitorować ruch sieciowy i zapisywać najważniejsze zdarzenia do logu.

Dwa Centralne Węzły Bezpieczeństwa będą zawierać komponenty realizujące funkcjonalności ochrony zasobów obliczeniowych:

- Zapewniać bezpieczeństwo teleinformatyczne zasobów obliczeniowych i systemów wsparcia
- Wykrywać i zapobiegać włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym

Ponad to w każdym Regionalnym Węźle Bezpieczeństwa zostaną zainstalowane mechanizmy ochrony użytkownika sieci OSE, realizowane w oparciu o systemy klasy SWG, których zakup Zamawiający planuje wykonać w ramach odrębnego postępowania.

W ramach wskazanego Węzła Centralnego Wykonawca zainstaluje Węzeł laboratoryjny realizujący wszystkie funkcje wskazane dla Centralnych i Regionalnych Węzłów Bezpieczeństwa. Węzeł laboratoryjny pozwoli na przeprowadzenie:

- Testów aktualizacyjnych oprogramowania
- Testów przy większych zmianach konfiguracyjnych.

3.2. Architektura Infrastruktury Bezpieczeństwa

3.2.1. Podział funkcjonalny

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

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
SWG	
1	Katagoryzacja URL
2	filtrowanie treści
3	AV dla HTTP

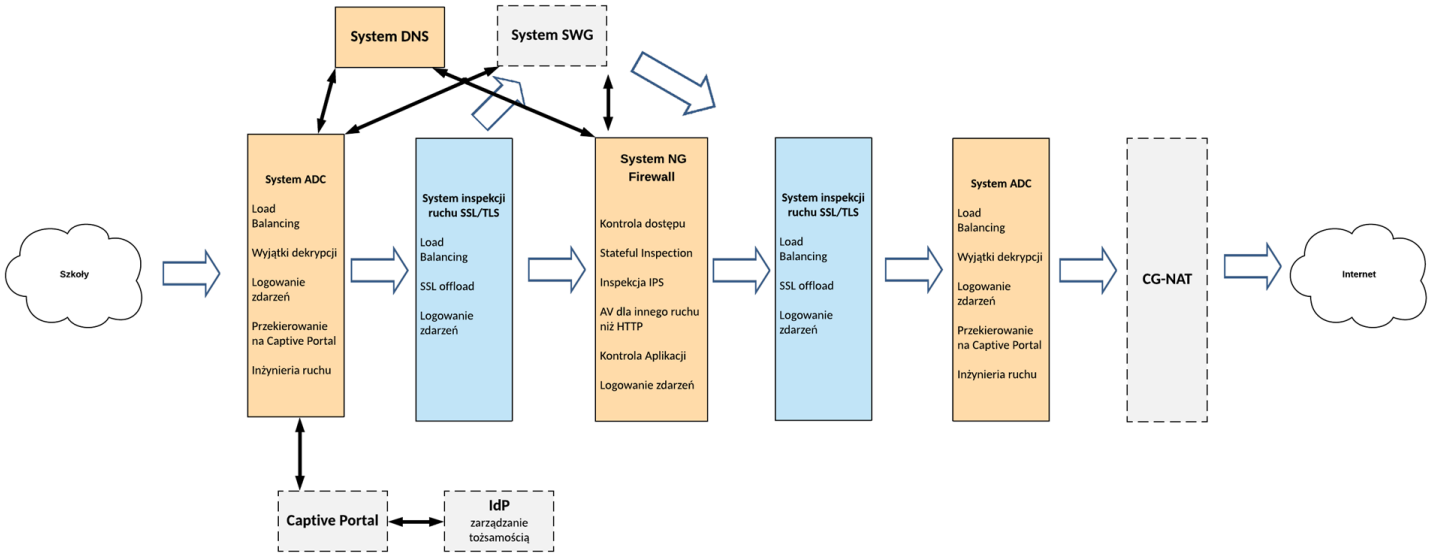
*) Funkcjonalność wymagana tylko w Centralnych Węzłach Bezpieczeństwa

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

3.2.2. Przepływ ruchu w węźle

Poniżej zaprezentowano schemat blokowy przepływu danych w Regionalnych Węzłach Bezpieczeństwa. Schemat przedstawia Infrastrukturę 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.

W wymiarowaniu Urządzeń potrzebnych do realizacji funkcji bezpieczeństwa należy wziąć pod uwagę potencjalne wielokrotne przejścia tych samych przepływów przez ten sam blok funkcjonalny np. System ADC lub System inspekcji ruchu SSL/TLS. W szczególności, na przedstawionym schemacie blokowym zarówno System ADC jak i System inspekcji ruchu SSL/TLS może być zrealizowany jako ta sama grupa Urządzeń.



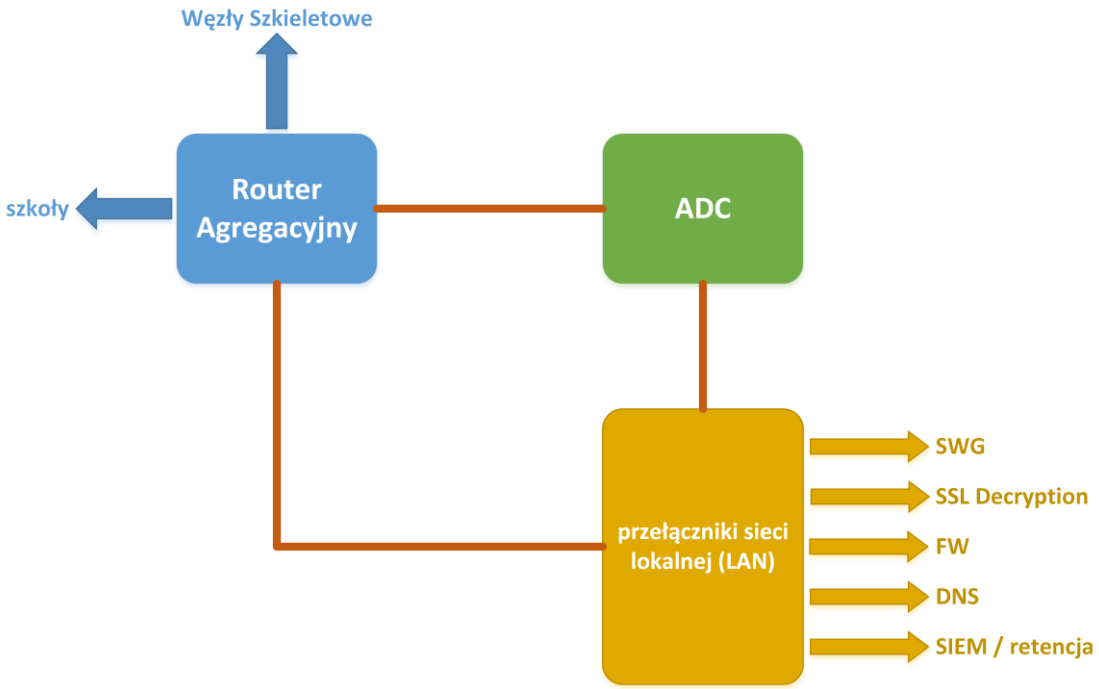
- Cały ruch (100%) od CPE, po przejściu przez Węzeł agregacyjny, przechodzi przez System ADC, który dokonuje deszyfracji SSL wewnętrznie lub z wykorzystaniem Urządzeń dedykowanych. Inspekcji podlega 100% ruchu SSL/TLS z pominięciem wybranych domen, pobranych z pól SNI lub CN certyfikatu, należących do kategorii treści określonych przez Zamawiającego. Informację na temat kategorii do jakiej należy dana domena, System ADC uzyska poprzez współpracę z Systemem DNS. Wykonawca na etapie realizacji przedmiotu zamówienia jest zobowiązany do konfiguracji Systemu ADC i Systemu DNS w sposób umożliwiający wykonanie tej funkcjonalności.
- Po dokonaniu deszyfracji, cały ruch zostanie przekierowany do Systemu NG Firewall, gdzie będą zdefiniowane polityki dotyczące ruchu warstwy 3 /4 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). W przypadku kiedy będzie to żądanie do serwisów web (HTTP, HTTPS), System przekieruje cały taki ruch do Systemu SWG.

- Po dokonaniu inspekcji treści, ruch jest kierowany ponownie do Systemu ADC, lub na urządzeniu dedykowanym do obsługi ruchu SSL/TLS, w celu ponownej szyfracji SSL.
- Ruch wychodzi z Regionalnego Węzła Bezpieczeństwa i kierowany jest zgodnie z tablicą routingu Węzła szkieletowego. W przypadku potrzeby skierowania ruchu do sieci Internet, przed opuszczeniem Węzła Centralnego, dokonywana jest translacja CGNAT do adresacji publicznej.
- 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 powinna nastąpić na poziomie VFR, logical system lub podobnym.

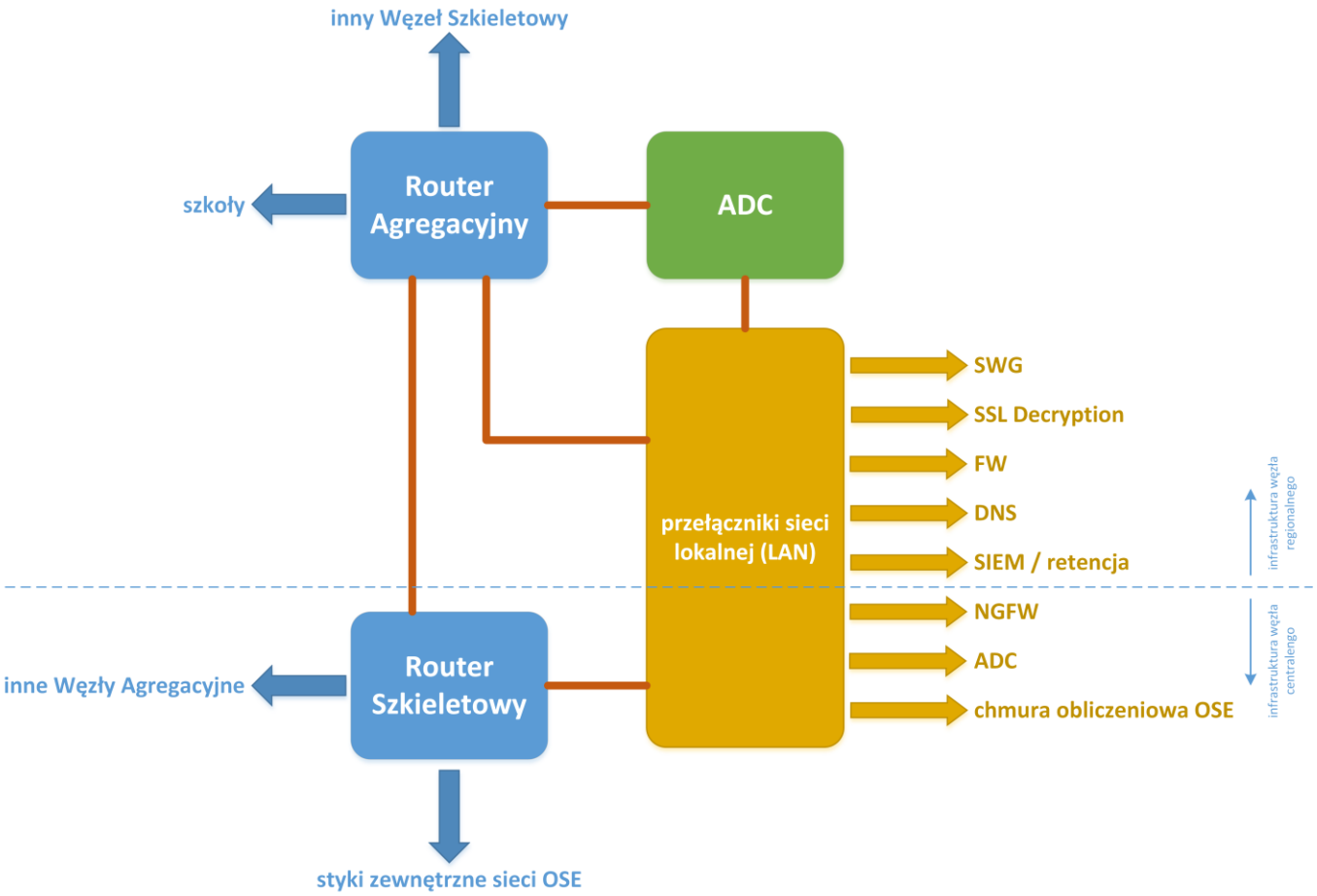
Zamawiający zakłada wyjątki od powyższego przepływu, które zostaną doprecyzowane przez strony (Wykonawcę i Zamawiającego) na etapie tworzenia projektu technicznego.

3.2.3. Schemat fizyczny podłączenia Infrastruktury Bezpieczeństwa do sieci Zamawiającego

Poniżej przedstawiono strukturę połączeń w Węźle Regionalnym. Przełączniki sieci lokalnej (LAN) zostaną dostarczone przez Zamawiającego. Schematy fizycznej realizacji Infrastruktury bezpieczeństwa jest wymaganiem Zamawiającego w tym zakresie.



Poniżej przedstawiono strukturę połączeń w Węźle Centralnym.



3.3. Skalowanie elementów Infrastruktury bezpieczeństwa

Poniżej przedstawiono ruchu z podziałem na protokoły. Poniższe dane mają charakter danych projektowych i zostały przedstawione w celu umożliwienia Wykonawcy zaoferowania optymalnego rozwiązania w postaci Infrastruktury bezpieczeństwa spełniającej wszystkie wymagania Zamawiającego i parametry zawarte w niniejszym dokumencie.

Protokół	%
HTTP	10%
HTTPS	80%
SMTP, IMAP, POP3, FTP, SMB i inne	9%
DNS	1%

Powyższa tabela pokazuje całościowy (UP/DOWN) rozkład procentowy ruchu z wydzieleniem wybranych protokołów. Zakładany rozkład proporcji ruchu dla poszczególnych protokołów jest elementem wymaganym dla odpowiedniego przygotowania wydajności Infrastruktury

bezpieczeństwa. W przypadku gdy ruch rzeczywisty będzie się różnić od planowanego podziału dla poszczególnych protokołów, jak wskazano w tabelce, Zamawiający wymaga aby Infrastruktura bezpieczeństwa:

a) realizowała, w dalszym ciągu, wszystkie wymagane funkcjonalności dla poszczególnych protokołów transmisyjnych, oraz

b) realizowała założenia wydajnościowe dla poszczególnych protokołów do wielkości wskazanych w powyższej tabeli

Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (throughputu), wymaganej na poszczególnych systemach zakładają profil całego ruchu typu IMIX (ang. Internet MIX według IETF RFC 6985 „IMIX Genome: Specification of Variable Packet Sizes for Additional Testing") zgodnie z parametrami przedstawionymi w poniższej tabeli.

Tabela Rozkład długości pakietów (przenoszonych w ramkach) w ruchu typu iMIX

Lp.	Długość pakietu IP [B]	Proporcja w całości	Udział w strumieniu [%]
1	64	3	30
2	128	1	10
3	1280	6	60

Zakładany rozkład wielkości pakietów jest elementem wymaganym dla odpowiedniego przygotowania wydajności Infrastruktury bezpieczeństwa. W przypadku gdy ruch rzeczywisty będzie się różnić od planowanego rozkładu, jak wskazano w tabelce powyżej, Zamawiający wymaga aby Infrastruktura bezpieczeństwa w dalszym ciągu realizowała:

a) wszystkie wymagane funkcjonalności oraz

b) założenia wydajnościowe dla poszczególnych wielkości pakietu do wielkości wskazanych w tabeli

Poniżej przedstawiono tabelę wskazującą maksymalne wartości, co do mocy (kW) i miejsca zajmowanego w szafie rack (RU), jakie Zamawiający przewiduje na potrzeby instalacji i działania Przedmiotu Zamówienia w poszczególnych Węzłach.

	Ilość miejsca w szafie [U]	Moc [kW]
MAZOWIECKIE	80	30
ŚLĄSKIE	60	20
WIELKOPOLSKIE	80	30
DOLNOŚLĄSKIE	42	17
KUJAWSKO-POMORSKIE	42	17

LUBELSKIE	45	18
LUBUSKIE	27	10
ŁÓDZKIE	47	18
MAŁOPOLSKIE	42	17
OPOLSKIE	27	10
PODKARPACKIE	47	18
PODLASKIE	30	12
POMORSKIE	47	18
ŚWIĘTOKRZYSKIE	30	12
WARMIŃSKO-MAZURSKIE	30	12
ZACHODNIOPOMORSKIE	40	18

3.3.1. Wymagania wydajnościowe na Regionalne Węzły Bezpieczeństwa

W poniższych tabelach przedstawiono skalowanie Infrastruktury bezpieczeństwa w rozbiciu na poszczególne Regionalne Węzły Bezpieczeństwa w rozbiciu na funkcjonalności Infrastruktury bezpieczeństwa. Wszystkie podane poniżej tabele mają charakter wymagań w zakresie pojemności Infrastruktury bezpieczeństwa

Liczba szkół z podziałem na poszczególne Węzły:

Województwo	Liczba Szkół
MAZOWIECKIE	3806
ŚLĄSKIE	3447
WIELKOPOLSKIE	2184
MAŁOPOLSKIE	2157
ŁÓDZKIE	1553
DOLNOŚLĄSKIE	1424
POMORSKIE	1363
LUBELSKIE	1348
PODKARPACKIE	1328
KUJAWSKO-POMORSKIE	1194
WARMIŃSKO-MAZURSKIE	1132
ZACHODNIOPOMORSKIE	942
ŚWIĘTOKRZYSKIE	921
PODLASKIE	921
LUBUSKIE	712
OPOLSKIE	582
Suma	25 015

Wymagane skalowanie Systemu DNS:

DNS query per second [DNS QPS]
200 000

Wymagane skalowanie Systemu ADC:

Województwo	Throughput Systemu ADC [Mbps]	New CPS	Persistent connection
MAZOWIECKIE	219 632	380 644	1 522 576
ŚLĄSKIE	198 880	344 679	1 378 717
WIELKOPOLSKIE	126 025	218 413	873 654
MAŁOPOLSKIE	124 454	215 692	862 767
ŁÓDZKIE	89 625	155 329	621 317
DOLNOŚLĄSKIE	82 166	142 401	569 605
POMORSKIE	78 632	136 278	545 110
LUBELSKIE	77 791	134 820	539 278
PODKARPACKIE	76 613	132 778	531 113
KUJAWSKO-POMORSKIE	68 873	119 364	477 457
WARMIŃSKO-MAZURSKIE	65 340	113 241	452 963
ZACHODNIOPOMORSKIE	54 347	94 189	376 756
ŚWIĘTOKRZYSKIE	53 169	92 148	368 591
PODLASKIE	53 169	92 148	368 591
LUBUSKIE	41 055	71 152	284 608
OPOLSKIE	33 595	58 224	232 897
Suma	1 443 366	2 501 500	10 006 000

Wymaganie na skalowanie Systemu inspekcji ruchu SSL/TLS:

Województwo	Throughput System inspekcji ruchu SSL/TLS [Mbps]	New CPS	Persistent connection
MAZOWIECKIE	197 668	342 580	1 370 318
ŚLĄSKIE	178 992	310 211	1 240 845
WIELKOPOLSKIE	113 422	196 572	786 288
MAŁOPOLSKIE	112 009	194 123	776 490
ŁÓDZKIE	80 662	139 796	559 185
DOLNOŚLĄSKIE	73 949	128 161	512 645
POMORSKIE	70 769	122 650	490 599
LUBELSKIE	70 012	121 338	485 350
PODKARPACKIE	68 952	119 500	478 002
KUJAWSKO-POMORSKIE	61 986	107 428	429 712
WARMIŃSKO-MAZURSKIE	58 806	101 917	407 666
ZACHODNIOPOMORSKIE	48 912	84 770	339 080
ŚWIĘTOKRZYSKIE	47 852	82 933	331 732
PODLASKIE	47 852	82 933	331 732
LUBUSKIE	36 949	64 037	256 147
OPOLSKIE	30 236	52 402	209 607
Suma	1 299 029	2 251 350	9 005 400

Wymagane skalowanie Systemu NG Firewall wraz z określeniem jaki procent ruchu ma być objęty funkcjonalnościami IPS, AV, Kontrola aplikacji.

Województwo	Throughput Systemu NG Firewall: IPS 100%, Kontrola Aplikacji 100%, AV 9% [Mbps]	New CPS	Persistent connection
MAZOWIECKIE	219 632	380 644	1 522 576
ŚLĄSKIE	198 880	344 679	1 378 717
WIELKOPOLSKIE	126 025	218 413	873 654
MAŁOPOLSKIE	124 454	215 692	862 767
ŁÓDZKIE	89 625	155 329	621 317
DOLNOŚLĄSKIE	82 166	142 401	569 605
POMORSKIE	78 632	136 278	545 110
LUBELSKIE	77 791	134 820	539 278
PODKARPACKIE	76 613	132 778	531 113
KUJAWSKO-POMORSKIE	68 873	119 364	477 457
WARMIŃSKO-MAZURSKIE	65 340	113 241	452 963
ZACHODNIOPOMORSKIE	54 347	94 189	376 756
ŚWIĘTOKRZYSKIE	53 169	92 148	368 591
PODLASKIE	53 169	92 148	368 591
LUBUSKIE	41 055	71 152	284 608
OPOLSKIE	33 595	58 224	232 897
Suma	1 443 366	2 501 500	10 006 000

3.3.2. Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa

W poniższej tabeli przedstawiono wymagane skalowanie Infrastruktury bezpieczeństwa dla poszczególnych Centralnych Węzłów Bezpieczeństwa :

Województwo	Wymaganie skalowanie Systemu SSL VPN [Liczba jednoczesnych użytkowników]*	Wymagania na skalowanie Systemu NG Firewall [Gbps]	Wymagania na skalowanie Systemu ADC [Gbps]	Wymagania na skalowanie Funkcjonalności WAF [Gbps]
MAZOWIECKIE	500	20	20	8
WIELKOPOLSKIE	500	20	20	8

*) Obsługa nie mniej niż 500 jednocześnie pracujących użytkowników z możliwością licencyjnej rozbudowy do 2 tysięcy licencji.

Zakładane wielkości ruchowe (ilość szkół , wolumen ruchu, parametry intensywności ruchu) są parametrami wymaganymi dla odpowiedniego przygotowania wydajności Infrastruktury bezpieczeństwa. W przypadku gdy ruch rzeczywisty będzie się różnić od planowanego jak wskazano w tabeli Zamawiający wymaga aby Infrastruktura bezpieczeństwa:

a) dalej realizowała wszystkie wymagane funkcjonalności zgodnie z wymaganiami, oraz

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

3.3.3. Wymagania wydajnościowe na Węzeł laboratoryjny

	Wydajność Węzła laboratoryjnego**
ADC	5 Gbps
NG Firewall	5 Gbps
Deszyfracji SSL/TLS	5 Gbps
DNS Firewall	200 DNS QPS***

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

***) w przypadku kiedy System DNS nie wymaga zakupu dedykowanej licencji per urządzenie, Zamawiający dopuszcza pominięcie tego parametru. W takim przypadku, Wykonawca jest zobowiązany do konfiguracji dedykowanego urządzenia realizującego funkcje produkcyjnego środowiska DNS z wykorzystaniem licencji produkcyjnej wyskalowanej na 200 000 DNS QPS.

3.4. Wymagania wspólne dla wszystkich elementów Infrastruktury bezpieczeństwa

a) Urządzenia składowe Infrastruktury bezpieczeństwa muszą być montowane w dostarczonych przez Zamawiającego szafach rack 19”.
b) Urządzenia składowe Infrastruktury bezpieczeństwa muszą być zasilane prądem przemiennym o napięciu 230V.
c) Infrastruktura bezpieczeństwa musi zapewniać wsparcie dla IPv4 oraz IPv6, w dowolnych proporcjach, w zakresie pełnej funkcjonalności w tym dla analizy ruchu jak i Systemu zarządzającego.

d) Zarządzanie wszystkimi elementami Infrastruktury bezpieczeństwa musi odbywać się z 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 Infrastruktury Bezpieczeństwa o parametrach wymuszających konieczność instalacji dodatkowego oprogramowania na stacji administratora, w celu efektywnego zarządzania dostarczoną Infrastrukturą Bezpieczeństwa, zgodnie z wymaganymi parametrami.
e) Infrastruktura bezpieczeństwa musi umożliwiać agregację łączy Ethernet statycznie lub w oparciu o protokół LACP, zarówno pomiędzy elementami składowymi Infrastruktury bezpieczeństwa jak i w podłączeniu z infrastrukturą sieciową Zamawiającego
f) Infrastruktura bezpieczeństwa musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q (min. 1000 tag VLAN).
g) Infrastruktura bezpieczeństwa musi zapewniać Zamawiającemu możliwość uwierzytelniania administratorów za pomocą bazy lokalnej i z wykorzystaniem dwóch z wymienionych mechanizmów: RADIUS lub TACACS+ lub LDAP lub SAML.
h) Infrastruktura bezpieczeństwa musi zapewniać Zamawiającemu możliwość zarządzania dostępem w oparciu o przypisane role (RBAC), w tym możliwość definiowania przez Zamawiającego własnych ról administracyjnych.
i) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą współpracować z rozwiązaniami do monitorowania poprzez protokoły SNMP w wersjach 2c, 3.
j) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą wspierać SNMP TRAP.
k) Wszystkie komponenty Infrastruktury bezpieczeństwa 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 3.7.8. "System zarządzający".
l) System zarządzający musi mieć możliwość zarządzania przez systemy firm trzecich z wykorzystaniem API lub innych metod wskazanych w rozdziale 3.11. Wykonawca w ramach Projektu Technicznego udostępni dokumentację opisującą API i ww. metody Integracji z systemami firm trzecich oraz w ramach wdrożenia będzie współpracował z innymi dostawcami wskazanymi przez Zamawiającego przy integracji Infrastruktury bezpieczeństwa z tymi systemami.
m) Wszystkie Urządzenia użyte do budowy Infrastruktury bezpieczeństwa muszą być wyposażone w dedykowany port konsoli zarządzającej.
n) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów.
o) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą posiadać dodatkowy port typu Ethernet (10/100/1000), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Zamawiający dopuszcza opcję alternatywną, którą jest możliwość skonfigurowania jednego z portów liniowych jako portu OOB.
p) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą posiadać port terminalowy do dołączenia konsoli (RS232 lub USB).

q) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą obsługiwać protokół NTP.

r) Wszystkie bazy sygnatur, kategoryzacji i feedów dostarczone w ramach Infrastruktury bezpieczeństwa muszą być, na bieżąco, cyklicznie aktualizowane, zgodnie z harmonogramem zdefiniowanym przez Zamawiającego, przez producenta oprogramowania przez cały okres trwania gwarancji.

s) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą logować, dla wszystkich zdarzeń, co najmniej następujące informacje:
   - Data transakcji wg lokalnego czasu,
   - IP adres źródłowy,
   - Login użytkownika, jeśli nastąpiło uwierzytelnienie,
   - IP adres docelowy,
   - Pełen URL (cała ścieżka),
   - Akcja podjęta przez Urządzenie zgodnie ze skonfigurowana polityką.
   - Przyczyna wykonania akcji, np. wyszczególnienie mechanizmu, który spowodował blokadę ruchu.

t) Wszystkie Urządzenia wchodzące w skład Infrastruktury bezpieczeństwa muszą wysyłać zdarzenia (logi) do serwera SIEM za pomocą protokołu Syslog, w formacie CEF lub LEEF lub równoważnym RFC 5424
   - Urządzenia 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 Urządzenia. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
   - Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego Urządzenia.

u) Infrastruktura bezpieczeństwa musi 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.

v) Dane, takie jak np. klucze prywatne, hasła, muszą być zaszyfrowane.

w) Zaoferowana Infrastruktura bezpieczeństwa nie może wprowadzać dodatkowego narzutu na opóźnienie w transmisji większego niż 100 ms.

x) Infrastruktura bezpieczeństwa musi umożliwiać Zamawiającemu na zarządzanie pasmem sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ) na Systemie ADC lub na Systemie NG Firewall

y) Infrastruktura bezpieczeństwa musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B

3.5. Klastrowanie elementów Infrastruktury bezpieczeństwa

a) Infrastruktura bezpieczeństwa musi zapewniać pełną redundancję (Wysoką dostępność) dla wszystkich elementów krytycznych powiązanych z dostarczeniem kluczowych funkcjonalności. Zamawiający wymaga aby w przypadku awarii, wydajność Infrastruktury Bezpieczeństwa ulega degradacji o nie więcej niż 20% bazowej wydajności i pojemności, określonej dla danego węzła w punkcie 3.3.

b) Wysoka dostępność (HA) musi być zrealizowana na poziomie n+1. Zamawiający nie wyraża zgody na zastosowanie klastra:
   - Active / active
   - Active / pasive

c) z wyłączeniem systemów:
   - zarządzających elementami Infrastruktury bezpieczeństwa
   - elementów Infrastruktury bezpieczeństwa, które będą tworzyć elementy Centralnego Węzła Bezpieczeństwa
   - elementów Węzła laboratoryjnego

d) Zamawiający dopuszcza realizację klastrów active/active i active/passive dla Systemu zarządzającego elementami Infrastruktury bezpieczeństwa i elementów Infrastruktury bezpieczeństwa, które będą tworzyć elementy Centralnego Węzła Bezpieczeństwa. W przypadku Systemu ADC Zamawiający dopuszcza zastosowanie klastra active/active i active/passive w przypadku kiedy Wykonawca zastosuje rozwiązania typu appliance, a wydajność pojedynczego Urządzenia wystarczy do spełnienia wymogów wydajnościowych postawionych dla danego Węzła w rozdziale 3.3.

e) Infrastruktura bezpieczeństwa musi zapewniać mechanizmy skalowania wydajności przez możliwość konfiguracji wielu identycznych Urządzeń w każdym z węzłów.

f) Zamawiający wymaga zastosowania Urządzenia typu ADC (load balancer), gwarantującego kontrolę sesji i monitorowanie dostępności poszczególnych urządzeń. Dostarczony System ADC musi spełniać wymogi opisane w punkcie 3.6.4 oraz 3.7.4.

3.6. Infrastruktura bezpieczeństwa dla Regionalnego Węzła Bezpieczeństwa

3.6.1. Wymagania funkcjonalne rozwiązania

W ramach wdrożonej Infrastruktury bezpieczeństwa 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. „Skalowanie elementów Infrastruktury bezpieczeństwa”. Zamawiający wymaga dostarczenia w ramach przedmiotu zamówienia następujących systemów:

a) System NG Firewall
   - Funkcjonalność AV
   - Funkcjonalność IPS
   - Funkcjonalność Kontrola aplikacji
   - Logowanie zdarzeń do centralnego systemu SIEM

b) System DNS
   - DNS resolver
   - DNS Firewall - ochrona antymalware
   - DNS Firewall – filtracja treści
   - Logowanie zdarzeń do centralnego systemu SIEM

c) System inspekcji ruchu SSL/TLS
   - Dekrypcja i ponowna enkrypcja ruchu szyfrowanego
   - Funkcjonalność logowania zdarzeń do centralnego systemu SIEM

d) System ADC
   - Przekierowanie nieuwierzytelnionych użytkowników na zewnętrzny captive portal, dostarczony w ramach osobnego postępowania, i dystrybucja informacji o uwierzytelnionym użytkowniku do Systemów SWG
   - Inteligentne rozkładanie ruchu na pozostałe urządzenie w danym Węźle Bezpieczeństwa, np. w oparciu o badanie ich bieżącej wydajności
   - Inżynieria ruchu na podstawie polityk definiowanych przez Zamawiającego, np. innego przepływu ruchu, który nie ma być poddawany dekrypcji SSL.
   - Logowanie zdarzeń do centralnego systemu SIEM

Infrastruktura bezpieczeństwa musi być zrealizowana w oparciu o dostarczoną przez Wykonawcę dedykowaną platformę sprzętową.

3.6.2. System NG Firewall

W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System NG Firewall działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa".

a) Zaoferowane rozwiązania dla Systemu NG Firewall musi opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Gartner Magic Quadrant for Enterprise Network Firewalls, lub analogicznych zestawieniach przygotowanych przez równoważne organizacje, przygotowanych w ciągu ostatnich trzech lat przed upływem terminu składania ofert.
b) System NG Firewall nie może posiadać ograniczenia na ilość jednocześnie pracujących Użytkowników w sieci chronionej.
c) System NG Firewall musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP).
d) System NG Firewall musi wspierać Equal Cost Multipath (ECMP) .
e) Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI). Funkcjonując w trybie transparentnym Urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych, jak również nie może wprowadzać segmentacji sieci na odrębne domeny rozgłoszeniowe.
f) System NG Firewall musi być dostarczony jako specjalizowane Urządzenie, lub grupa Urządzeń, zabezpieczeń sieciowych (appliance). W architekturze Systemu NG Firewall musi występować separacja modułu zarządzania i modułu przetwarzania danych.
g) System NG Firewall musi umożliwiać Zamawiającemu tworzenie i modyfikowanie polityk, które opisywać będą mechanizmy kontroli produkcyjnego ruchu sieciowego, pochodzącego ze szkół, pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
h) System NG Firewall musi umożliwiać Zamawiającemu definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików, Kontrola aplikacji) dla dowolnego strumienia danych definiowanego jak ruch wychodzący lub przychodzący z/do określonych podsieci IP na/z określonych porty TCP / UDP

i) Polityka zabezpieczeń Systemu NG Firewall musi umożliwiać Zamawiającemu konfigurację w oparciu o strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, adresy URL, użytkowników sieci.

j) System NG Firewall musi umożliwiać Zamawiającemu konfigurację, w ramach pojedynczej polityki:
   - Uruchamianie funkcjonalności AV, IPS i Kontroli aplikacji rozumiane jako przypisanie do polityki konkretnego profilu określającego działanie danej funkcjonalności zgodnie z wymaganiami postawionymi w pkt 3.6.2.1, 3.6.2.2 i 3.6.2.3.
   - Akcji, co najmniej blokady lub przepuszczenia transmisji, podejmowanej w ramach naruszenia określonych w polityce kryteriów i zabezpieczeń,
   - rejestrowanie wszystkich zdarzeń zakwalifikowanych przez daną politykę,
   - [Wykreślony podpunkt]

k) System NG Firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1Q.

l) System NG Firewall musi umożliwiać Zamawiającemu konfigurację i pracę każdego interfejsu sieciowego w trybie transparentnym, L2 i L3. Tryb pracy Systemu NG firewall musi być ustalany per interfejs sieciowy, a System NG firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji Systemu NG Firewall

m) Każdy z interfejsów sieciowych Systemu NG Firewall musi pozwalać na tworzenie subinterfejsów VLAN.

n) System NG Firewall musi obsługiwać min 1000 znaczników VLAN

o) System NG Firewall musi posiadać funkcję ochrony przed atakami typu DoS poprzez limitowanie ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP, wykorzystując co najmniej następujące mechanizmy:
   - Flood Protection
   - SYN Floods
   - Port scans

   Zamawiający dopuszcza, aby powyższa funkcjonalność została zrealizowana alternatywnie przez funkcjonalność IPS, opisaną w pkt 3.6.2.2. Szczegółowego opisu przedmiotu zamówienia.

p) System NG Firewall musi umożliwiać Zamawiającemu budowanie polityk uwierzytelniania dla Użytkowników i administratorów, definiujących rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów.

q) Polityki definiujące muszą umożliwiać wykorzystanie adresów źródłowych, docelowych, numerów portów usług oraz adresów URL. Minimalne wymagane przez Zamawiającego mechanizmy uwierzytelnienia to do wyboru dwa z trzech wymienionych: RADIUS, TACACS+, LDAP.

r) Polityka kontroli dostępu musi precyzyjnie definiować prawa dostępu Użytkowników i administratorów do określonych usług sieci i musi być utrzymywana nawet, gdy osoba zmieni lokalizację i adres IP. W przypadku Użytkowników i administratorów pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. System NG Firewall musi umożliwiać Zamawiającemu realizację wszystkich powyższych funkcji poprzez integrację z zewnętrznym systemem zarządzania tożsamością.

s) System NG Firewall musi pozwalać na konfigurowanie i wysyłanie logów, w formacie CEF lub LEEF lub równoważnym RFC 5424, do różnych serwerów Syslog min 2 serwerów typu Syslog.
t) System NG Firewall musi obsługiwać nie mniej niż 5 wirtualnych firewalli działających w trybie routed, posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji Systemu NG Firewall. Alternatywnie Zamawiający dopuszcza sytuację gdzie odrębne tablice routingu są realizowane poprzez dodatkowe wirtualne firewalle.
u) System NG Firewall musi obsługiwać protokoły routingu dynamicznego, nie mniej niż OSPF, BGP.
v) System NG Firewall musi posiadać możliwość dostosowania komunikatów o błędach lub komunikatów informacyjnych wyświetlanych Użytkownikom, w szczególności wyświetlanie informacji powiązanych z sesją dla poszczególnych funkcjonalności:
   - powód zablokowania danej sesji,
   - treść błędu,

   System NG Firewall musi umożliwiać Zamawiającemu definiowanie różnych statycznych stron blokowania dla poszczególnych powodów zablokowania danych sesji związanych np. z funkcjonalnością IPS lub funkcjonalnością Kontroli aplikacji.

3.6.2.1. Funkcjonalność AV

W ramach wdrożonej Infrastruktury bezpieczeństwa 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. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG firewall. Zamawiający dopuszcza realizację tej funkcjonalności w sposób równoważny z wykorzystaniem dedykowanych Urządzeń lub jedynie w Węzłach Centralnych przy założeniu realizacji funkcjonalności AV dla wszystkich Użytkowników obsługiwanych przez dany Węzeł.

a) Funkcjonalność AV musi być realizowana dla 9% ruchu związanego z ruchem SMTP, IMAP, POP3, FTP i inne. Wartości w tabeli w rozdziale 3.3.
b) Funkcjonalność AV musi posiadać silnik antywirusowy, który umożliwia skanowanie i blokowanie ruchu w obu kierunkach komunikacji dla protokołów działających również na niestandardowych portach (np. FTP na porcie 2021).
c) Funkcjonalność AV musi umożliwiać skanowanie i blokowanie archiwów, w tym co najmniej: zip.
d) Funkcjonalność AV musi posiadać moduł inspekcji antywirusowej uruchamiany dla aplikacji wykorzystujących co najmniej następujące dekodery obsługujące protokoły SMTP, IMAP, POP3, FTP, kontrolujący ruch bez konieczności uzupełniania o jakiekolwiek komponenty. 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 urządzeniu 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 urządzenia stanowi

podzbiór bazy utrzymywanej przez producenta rozwiązania, na bieżąco aktualizowany przez producenta.

e) Funkcjonalność AV musi zapewniać możliwość wykrywania, śledzenia i blokowania transferu następujących kategorii plików w ruchu sieciowym:
   - pliki systemowe
   - pliki graficzne
   - pliki PDF
   - pliki wykonywalne
   - pliki multimedialne
   - pliki pakietu Office
   - pliki skompresowane
   - inne pliki, które mogą służyć do propagacji wirusów
f) Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
g) Funkcjonalność AV musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: SMTP, FTP, IMAP, POP3 w obu kierunkach - upload/download.
h) Funkcjonalność AV w trybie proxy musi umożliwiać Zamawiającemu na definiowanie wielkości pliku powyżej, którego funkcjonalność AV nie będzie przeprowadzała inspekcji danego pliku.

3.6.2.2. Funkcjonalność IPS

W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność IPS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall .

a) Funkcjonalność IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
b) Funkcjonalność IPS musi posiadać dostarczoną i wspieraną przez producenta bazę sygnatur ataków, która musi zawierać minimum 10 000 wpisów i być aktualizowana automatycznie. Baza sygnatur musi być dostarczana i wspierana przez producenta, na bieżąco cyklicznie aktualizowana i uzupełniana, przez dostawcę bazy. Zamawiający dopuszcza że w momencie podpisania umowy baza zawiera co najmniej 5 000 sygnatur i w ciągu następnych 12 miesięcy baza zostanie rozbudowana do wielkości wymaganych 10 000 sygnatur
c) Funkcjonalność IPS musi umożliwiać Zamawiającemu definiowanie własnych wyjątków, określających dla jakich adresów IP (docelowych lub źródłowych) system IPS ma nie wykonywać analizy pakietów, oraz własnych sygnatur opisujących sposób zachowania znanych podatności (exploit'ów).
d) Funkcjonalność IPS musi zapewniać Zamawiającemu możliwość wykrywania i blokowania szerokiej gamy zagrożeń, takich jak min.:
   - złośliwe oprogramowanie,
   - skanowanie sieci,
   - ataki na usługę VoIP,

- próby przepełnienia bufora,
- ataki na aplikacje P2P,
- zagrożenia dnia zerowego, itp.

e) Funkcjonalność IPS musi zapewniać Zamawiającemu możliwość wykrywania zagrożeń za pomocą co najmniej łącznie wszystkich poniższych mechanizmów:
   - sygnatury
   - mechanizm wykrywania anomalii w protokołach
   - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego

f) Funkcjonalność IPS musi dobierać optymalny mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego DPI lub Funkcjonalność IPS musi dokonywać analizy danych strumieniowo i wspierać mechanizmy pełnej re-asemblacji ruchu sieciowego oraz braku selektywnego wyłączania sygnatur

g) Funkcjonalność IPS musi umożliwiać Zamawiającemu wykrywanie i blokowanie komunikacji Command&Control do sieci botnet.

h) Funkcjonalność IPS musi zapewniać Zamawiającemu możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez konieczności użycia zewnętrznych narzędzi i wsparcia producenta.

3.6.2.3. Funkcjonalność Kontrola aplikacji

W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność Kontroli aplikacji (udostępnianych poprzez sieć Internet) działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall .

a) Funkcjonalność Kontroli Aplikacji musi posiadać funkcję, która musi umożliwiać Zamawiającemu kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

b) Funkcjonalność kontroli aplikacji musi posiadać bazę Kontroli Aplikacji, która musi zawierać minimum 2500 sygnatur opisujących charakterystykę aplikacji lub która musi zawierać 5000 ich pojedynczych modułów. Baza sygnatur musi być dostarczana i wspierana przez producenta, na bieżąco cyklicznie aktualizowana i uzupełniana, przez dostawcę bazy.

c) Funkcjonalność Kontroli aplikacji musi umożliwiać Zamawiającemu Kontrolę aplikacji chmurowych (co najmniej: Facebook, Instagram, Youtube, Twitter, Google Docs, Dropbox) pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

d) Baza realizująca funkcjonalność kontroli aplikacji musi być podzielona na kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa, przynajmniej: proxy, P2P.

e) Funkcjonalność kontroli aplikacji musi umożliwiać Zamawiającemu definiowanie własnych sygnatur.

f) Funkcjonalność kontroli aplikacji musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z np. P2P i Instant Messaging). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury lub sygnatury i analizę heurystyczną.

3.6.3. System DNS

W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System inspekcji DNS działał w skali całego ruchu określonego w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa".

a) System DNS musi być dedykowaną platformą sprzętową lub być składową innego elementu Systemu.
b) System DNS musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System)
c) System DNS musi umożliwiać Zamawiającemu tworzenie własnych wpisów typu:
   - A
   - AAAA
   - CNAME
   - MX
   - PTR
   - NS
   - SOA
   - SRV
   - TXT

   Definicje typów wpisów są zgodne z RFC 1035 punkt 3.2.2.
d) System DNS musi być zgodny z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Commnents http://www.ietf.org/rfc.html)
e) System DNS musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136
f) System DNS musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996
g) System DNS musi wspierać protokoły DNS w wersji IPv4 i IPv6
h) System DNS musi wspierać obsługę MultiMaster DNS
i) System DNS musi wpierać cache DNS
j) System DNS musi wspierać usługę DDNS
k) System DNS musi wspierać usługę walidacji DNSSEC
l) System DNS musi mieć pojemność bazy na minimum 800 000 rekordów
m) System DNS musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF oraz protokołu BFD)
n) System DNS musi posiadać funkcjonalność filtrowania odpowiedzi DNS na podstawie cyklicznie aktualizowanej przez producenta bazy reputacji domen infekujących malware/botnet/SURBL nowo obserwowanych domen w sieci Internet oraz wykrywania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego (Machine Learning) pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych za pomocą protokołu DNS.
o) System DNS musi posiadać funkcjonalność wykrywania i blokowania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego bazującego na uczeniu maszynowym i pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych przez

protokół DNS. W tym celu urządzenie dla nazw FQDN w zapytaniach DNS (w tym dla zapytań o rekordy A) musi co najmniej: wyliczać entropię znaków, sprawdzać popularność występowania w językach naturalnych wszystkich 2- i 3-gramów, obliczać współczynnik liczby samogłosek do wszystkich znaków w nazwie, obliczać współczynnik liczby cyfr do wszystkich znaków w nazwie, analizować rozmiar zapytania, analizować częstotliwość zapytań DNS.

p) System DNS musi posiadać funkcjonalność DNS firewalla, tzn. na podstawie następujących zdarzeń:
   - zapytanie DNS od konkretnego adresu IP
   - zapytanie DNS o konkretną domenę
   - odpowiedź DNS zawierająca konkretny adres IP
   - odpowiedź DNS z konkretną nazwą i adresem IP w rekordzie NS dla danej domeny (NSDNAME i NSIP)

   musi mieć możliwość podjęcia następujących działań:

   - blokowanie dostępu z odpowiedzią NXDOMAIN
   - blokowanie dostępu z odpowiedzią NODATA
   - przekierowanie na inny adres
   - zezwolenie na dostęp z logowaniem zdarzenia
q) System DNS musi posiadać ochronę przed atakami związanymi z protokołami DNS, BGP OSPF, NTP, w tym co najmniej:
   - Na protokoły BGP i OSPF wykorzystywane do DNS Anycast (m.in. blokowanie niespodziewanych pakietów BGP/OSPF, czy zbyt dużej liczby pakietów BGP/OSPF w danym okresie czasu)
   - Na protokół NTP wykorzystywany do synchronizacji czasu (m.in. blokowanie nieprawidłowych żądań NTP)
r) System DNS musi umożliwiać Zamawiającemu na przekierowanie użytkownika sieci na stronę z informacją o zablokowaniu zapytania DNS
s) System DNS musi umożliwiać Zamawiającemu na dostosowanie komunikatów o błędach i komunikatów informacyjnych wyświetlanych Użytkownikom, w szczególności wyświetlanie informacji powiązanych z sesją jak:
   - treść błędu,
   - źródłowy adres IP,
   - powód zablokowania danej sesji bazujący na kategorii zablokowanej domeny
t) System DNS musi umożliwiać Zamawiającemu na blokowanie lub przekierowywanie domen ze względu na kategorię serwowanej treści.
u) Baza kategoryzacji zawiera co najmniej 100 kategorii treści, uwzględniających co najmniej kategorie , które mogą być użyte przez Zamawiającego w dowolny sposób w celu stworzenia polityki filtrowania. Zamawiający wymaga aby baza kategorii zawierała co najmniej kategorie zawierające domeny prezentujące treści pornograficzne, treści udostępniające możliwość uczestniczenia w grach hazardowych w szczególności znajdujących się w Rejestrze prowadzonym przez Ministerstwo finansów.
v) System musi filtrować zapytania DNS, porównując poszczególne requesty ze specjalizowaną bazą danych (dostarczaną przez producenta Systemu), podzieloną na kategorie treści zawierającą informacje o domenach.

w) System DNS musi umożliwiać Zamawiającemu blokowania zapytań DNS odwołujących się do domen znajdujących się w bazie dostarczanej przez Internet Watch Foundation (IWF) lub równoważnej organizacji,
x) System 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.
y) System DNS musi posiadać funkcjonalność blokowania zapytań DNS skorelowanych z domenami o niebezpiecznej treści: domeny wykorzystywane do propagacji złośliwego oprogramowania, domeny Phishing'owe, domeny wykorzystywane do zestawiania połączeń typu Command and Control z Botnetami
z) System DNS musi dać możliwość tworzenia listy domen dopuszczanych i listy domen zabronionych przez administratora systemu mających priorytet nad listami dostarczonymi wraz z systemem.
aa) System DNS musi umożliwiać Zamawiającemu na konfigurację polityki dostępu do treści zależnej od adresu IP, przy czym zachodzące na siebie przestrzenie adresowe są traktowane jako oddzielne, tzn. przykładowo adres 10.1.1.20/32 może mieć inną politykę dostępu do treści niż 10.1.1.1/24

3.6.4. System ADC

W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System ADC działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa".

a) Zaoferowane rozwiązania dla Systemu ADC muszą opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Gartner Magic Quadrant for Application Delivery Controllers lub Gartner Market Guide for Application Delivery Controllers, lub analogicznych zestawieniach przygotowanych przez równoważne organizacje, przygotowanych w ciągu ostatnich trzech lat przed upływem terminu składania ofert.
b) System ADC musi równoważyć obciążenie pomiędzy Urządzeniami do rozszywania ruchu SSL, Urządzeniami NG Firewall oraz Urządzeniami SWG (zarówno dla ruchu HTTP jak i rozszytej zawartości ruchu HTTPS. Urządzenia SWG zostaną dostarczone w ramach osobnego postepowania)
c) System ADC musi zapewniać Zamawiającemu możliwość zdefiniowania grupy Urządzeń tego samego typu, np. inspekcji ruchu SSL/TLS, NG Firewall, SWG
d) System ADC musi być dostarczony jako specjalizowane Urządzenie, lub grupa Urządzeń (appliance).
e) W architekturze Systemu ADC musi występować separacja modułu zarządzania i modułu przetwarzania danych.
f) System ADC musi zapewniać możliwość przesłania ruchu do Systemu inspekcji ruchu SSL/TLS, a następnie rozłożenie go na poziomie zdefiniowanej przez administratora grupy Urządzeń należących do poszczególnych Systemów dostarczanych w ramach Infrastruktury bezpieczeństwa oraz do Systemów SWG

g) System ADC musi monitorować, czy urządzenia w danej grupie funkcjonalnej pracują, a w razie niedostępności jednego automatycznie przesyłać ruch do pozostałych działających urządzeń.
h) System ADC musi zapewniać zamawiającemu możliwość konfiguracji sposobu zachowania Systemu ADC w sytuacji, kiedy w danej funkcjonalnej grupie urządzeń żadne urządzenia nie będzie działało – minimalnie pominięcie serwisu (fail open) lub odrzucenie połączenia (fail close).
i) System ADC musi realizować translację portu na czas przechodzenia przez strefy rozszytego ruchu, np. ruch przychodzący na porcie 443, który uległ rozszyfrowaniu, jest następnie przesyłany na porcie 8443 do grupy urządzeń NFGW, następnie przesyłany jest na porcie 3128 do grupy Urządzeń SWG, oraz ponownie ruch wychodzący zaszyfrowany jest na porcie 443.
j) System ADC musi zapewniać możliwość dodania przez Zamawiającego własnego nagłówka do protokołu HTTP w celu przekazania do innych urządzeń bezpieczeństwa.
k) System ADC należący do Infrastruktury bezpieczeństwa musi umożliwiać Zamawiającemu podłączenie z innymi elementami Infrastruktury bezpieczeństwa i sieci Zamawiającego z wykorzystaniem wszystkich poniższych sposobów:
   - bezpośredniego połączenia (połączenie punkt-punkt),
   - połączenie w ramach jednego VLAN'u (połączenie w warstwie 2 modelu ISO/OSI).,
   - połączenie z wykorzystaniem adresów IP (połączenie w warstwie 3 modelu ISO/OSI).
l) System ADC musi realizować równomierne rozłożenie całego ruchu na poziomie Regionalnego Węzła Bezpieczeństwa i zapewniać Zamawiającemu możliwość definiowania reguł określających kryteria, co najmniej: źródłowy i docelowy adres IP oraz źródłowy i docelowy port TCP/UDP, jaki ruch ma zostać przesłany do Systemu inspekcji SSL/TLS, Systemu NG firewall oraz do Systemu SWG.
m) System ADC musi zapewnić Zamawiającemu możliwość ustalenia kolejności wysyłanego rozszytego ruchu, tzn. podjęcie decyzji, czy najpierw trafia on do Systemu NG firewall czy do Systemu SWG. Zamawiający może określać kolejność, o której mowa poprzez definiowanie reguł określających kryteria (przynajmniej: adresów/adresów IP, geolokalizacji, portu).
n) System ADC musi również wspierać wysyłanie dowolnej, zdefiniowanej za pomocą reguł, wielkości ruchu:
   - do urządzeń działających w warstwie 2 (L2, np. IPS),
   - do systemów pasywnych (np. systemu IDS)
   - oraz z wykorzystaniem protokołu ICAP.
o) System ADC musi umożliwiać Zamawiającemu sprawdzanie kategoryzacji adresu URL zawartego w certyfikacie (pola SNI lub SNI i CN) poprzez współpracę z Systemem DNS. Alternatywnie Zamawiający dopuszcza zastosowanie wewnętrznej bazy kategoryzacji dostarczonej przez producenta ADC.
p) System ADC musi umożliwiać Zamawiającemu wykonywanie zapytań DNS na podstawie zawartości pól certyfikatu, którym podpisana jest dana sesja SSL/TLS.
q) System ADC musi posiadać wbudowany język skryptowy, posiadający co najmniej następujące cechy:
   - Analiza, zmiana oraz zastępowanie parametrów w nagłówku HTTP oraz w zawartości pakietów w skali całego ruchu obsługiwanego przez dane Urządzenie,
   - W budowanych skryptach można analizować, zmieniać oraz zastępować parametry w nagłówkach protokołów: HTTP, TCP, RTSP, SIP.

r) System ADC musi realizować analizę, zmianę oraz zastępowanie parametrów w nagłówku oraz w zawartości pakietów
s) Co najmniej dla protokołów: HTTP, TCP, RTSP, SIP
t) Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego
u) System ADC musi posiadać funkcjonalność równoważenia obciążenia (sterowania ruchem) na bazie:
   - mechanizmów równoważenia obciążenia: round robin, ważona, najmniejsza liczba połączeń, najszybsza odpowiedź, grupy priorytetów,
   - mechanizmów monitorowania stanu serwerów ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, HTTP/HTTPS, LDAP, FTP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi być zapewniona możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność wyżej wymienionych usług.
   - mechanizmów przywiązywania sesji: cookie (hash, rewrite, custom, insert, passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID
   - usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków HTTP, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi,
   - Informacji na temat grupy użytkownika (po wdrożeniu systemu zarządzania tożsamością)
v) System ADC musi zapewniać Zamawiającemu możliwość tworzenia reguł definiujących wyjątki od reguł określających domyślny przepływ ruchu i przesłania go do wskazanej funkcjonalnej grupy Urządzeń. Reguły określające wyjątki mogą być budowane przez Zamawiającego z wykorzystaniem źródłowego i docelowego adresu IP lub adresu podsieci oraz statycznej listy adresów URL.
w) System ADC musi posiadać funkcje przywiązywania sesji (Session persistence) do określonej ścieżku ruchu na podstawie konfiguracji przez Zamawiającego reguł wykorzystujących co najmniej następujące atrybuty:
   - Cookie (hash, rewrite, custom, insert, passive)
   - Adres źródła
   - Identyfikator sesji SSL
   - Adres docelowy
   - Tworzonych przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 3.6.4 ppkt. q
   - Badanie obciążenia poszczególnych nodów w klastrze pod względem obciążenia
x) System ADC musi umożliwiać Zamawiającemu przekierowanie ruchu pochodzącego od nieuwierzytelnionych Użytkowników na zewnętrzny captive portal, dostarczony w ramach osobnego postępowania.
y) System ADC musi posiadać co najmniej następujące interfejsy administracyjne:
   - GUI przy wykorzystaniu protokołu https
   - Zarządzanie poprzez SSH
   - Zarządzanie poprzez web API
z) System ADC musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych, przez dane Urządzenie, połączeń TCP/UDP. W przypadku przekroczenia zdefiniowanej wartości System

ADC musi umożliwiać Zamawiającemu określenie akcji pozwalającej na wysłanie użytkownikom sieci strony błędu lub przekierowanie ich na inny serwer.

aa) System ADC musi umożliwiać Zamawiającemu konfigurację poniższych funkcji na każdym Urządzeniu dostarczonym w ramach Systemu ADC:
- Obsługa protokołu SNMP v1/v2c/v3
- Zewnętrzny syslog
- Zbieranie danych i ich wyświetlanie
- Zbieranie danych zgodnie z ustawieniami administratora
- Osobna brama domyślna dla interfejsu zarządzającego
- [Wykreślony podpunkt]
- Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy)
- Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.

bb) System ADC musi obsługiwać sieci VLAN w standardzie 802.1Q.

cc) System ADC musi obsługiwać agregację linków w standardzie 802.3ad (LACP)

dd) System ADC musi obsługiwać Jumbo Frames

ee) System ADC musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding), które wykonuje separację ruchu sieciowego do różnych aplikacji. Musi zapewniać poprawne działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP.

ff) System ADC musi obsługiwać protokoły dynamicznego routingu BGP i OSPF.

3.6.5. System inspekcji ruchu SSL/TLS

W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność inspekcji ruchu SSL/TLS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający określa, że poprzez inspekcję ma na myśli deszyfrowanie i ponowne szyfrowanie ruchu SSL/TLS sklasyfikowanego na podstawie określonych przez Zamawiającego reguł.

a) System inspekcji ruchu SSL/TLS musi być dostarczony jako specjalizowane Urządzenie, lub grupa Urządzeń, (appliance) lub być składową innego elementu Infrastruktury bezpieczeństwa.

b) System inspekcji ruchu SSL/TLS musi zapewniać inspekcję całej komunikacji szyfrowanej protokołem SSL/TLS. System inspekcji ruchu SSL/TLS musi zapewniać możliwość deszyfracji ruchu SSL/TLS, skategoryzowanego jako „niezaufany", który zostanie wysłany dalej w celu poddania go właściwej inspekcji na Systemie NG firewall i Systemie SWG.

c) System inspekcji ruchu SSL/TLS musi posiadać zestaw polityk definiujący ruch SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji.

d) System inspekcji ruchu SSL/TLS posiada wbudowaną i automatycznie, cyklicznie aktualizowaną przez producenta oprogramowania listę serwerów, dla których niemożliwa jest deszyfracja ruchu (z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji. Realizacja funkcjonalności może być realizowana poprzez

mechanizmy uczące dodające wyjątki na podstawie obserwowanego ruchu lub może być wsparta skryptem wykonywanym na lub poza urządzeniem.

e) System inspekcji ruchu SSL/TLS musi zapewniać Zamawiającemu możliwość dodawania wyjątków w procesie deszyfracji TLS'a w oparciu, o co najmniej:
   - adres IP/FQDN źródłowy,
   - podsieć źródłowa/docelowa
   - zbiór adresów IP/FQDN

f) W trybie rozszywania ruchu TLS, System inspekcji ruchu SSL/TLS musi wykonywać kontrolę certyfikatu serwera do którego łączy się użytkownik tj. minimum sprawdzenia daty ważności i łańcucha certyfikacji. W przypadku wykrycia nieważnego certyfikatu lub niepoprawnego łańcuch certyfikacji, System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu zdefiniowanie reguły blokującej daną komunikację i wystawienie użytkownikowi sieci komunikatu o błędzie.

g) Podczas rozszywania ruchu TLS, System inspekcji ruchu SSL/TLS nie może używać różnych zestawów algorytmów szyfrowania dla komunikacji z klientem i serwerem, w szczególności niedopuszczalna jest sytuacja, gdzie klient używa słabszego kryptograficznie mechanizmu niż serwer.

h) System inspekcji ruchu SSL/TLS musi zapewniać Zamawiającemu możliwość blokowania sesji szyfrowanych, nawet jeśli mechanizm rozszywania TLS jest wyłączony, na podstawie analizy certyfikatu serwera np. blokowanie całej domeny (z poddomenami) tumblr.com bez deszyfracji TLS.

i) System inspekcji ruchu SSL/TLS musi umożliwiać deszyfrowanie i szyfrowanie ruchu TLS na Urządzeniu w oparciu o co najmniej następujące algorytmy: RSA, DH i ECDHE.

j) System inspekcji ruchu SSL/TLS musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów.

k) [Punkt wykreślony]

l) Klucze prywatne zapisane na Systemie inspekcji ruchu SSL/TLS muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.

m) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu tworzenie polityki pozwalającej na wykluczenia ruchu podlegającego deszyfrowaniu na podstawie:
   - Źródłowego i docelowego adresu IP
   - Grupy adresów IP/FGQDN

n) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu utworzenie portu sieciowego, który posłuży do przesłania rozszytego ruchu do innego urządzenia.
   - W trybie pasywnym
   - W trybie aktywnym
   - ICAP

o) System inspekcji ruchu SSL/TLS musi współpracować z infrastrukturą PKI Zamawiającego

p) System inspekcji ruchu SSL/TLS musi umożliwiać generowanie certyfikatów typu ROOT w celu podpisywania certyfikatów użytych do deszyfracji oraz posiadać możliwość integracji w zewnętrznymi systemami PKI Zamawiającego.

q) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu sprawdzanie kategoryzacji adresu URL zawartego w certyfikacie (pola SNI lub SNI i CN) poprzez współpracę z Systemem DNS.

r) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu wykonywanie zapytań DNS na podstawie zawartości pól certyfikatu, którym podpisana jest dana sesja SSL/TLS.

s) [Wykreślony Punkt]

3.7. Infrastruktura bezpieczeństwa dla Centralnego Węzła Bezpieczeństwa

3.7.1. Wymagania funkcjonalne rozwiązania

W ramach wdrożonej Infrastruktury bezpieczeństwa dla Zasobów obliczeniowych OSE, zlokalizowanej w dwóch Centralnych Węzłach Bezpieczeństwa, muszą być realizowane wszystkie poniższe funkcjonalności. Mogą one być zrealizowane w postaci osobnych lub pojedynczych, platform sprzętowych lub programowych z komercyjnym wsparciem Wykonawcy i producentów.

a) System NG Firewall
   - Funkcjonalność IPS
   - Funkcjonalność AV
   - Logowanie zdarzeń do centralnego systemu SIEM

b) System inspekcji DNS/ DNS Serwer
   - DNS resolver
   - DNS Firewall - ochrona antymalware
   - Logowanie zdarzeń do centralnego systemu SIEM

c) System ADC
   - Przekierowanie nieuwierzytelnionych użytkowników na zewnętrzny captive portal i dystrybucja informacji o uwierzytelnionym użytkowniku do Systemów SWG
   - Inteligentne rozkładanie ruchu na pozostałe urządzenie w danym Węźle Bezpieczeństwa, np. w oparciu o badanie ich bieżącej wydajności
   - Inżynieria ruchu na podstawie polityk definiowanych przez Zamawiającego, np. innego przepływu ruchu, który nie ma być poddawany dekrypcji SSL.
   - Logowanie zdarzeń do centralnego systemu SIEM

d) Funkcjonalność Web Application Firewall
   - Realizacja wymagań postawionych w rozdziale 3.7.6
   - Logowanie zdarzeń do centralnego systemu SIEM

e) SSL VPN
   - Realizacja wymagań postawionych w rozdziale 3.7.5
   - Logowanie zdarzeń do centralnego systemu SIEM

e) System inspekcji ruchu SSL/TLS
   - Dekrypcja i ponowna enkrypcja ruchu szyfrowanego
   - Funkcjonalność logowania zdarzeń do centralnego systemu SIEM

f) System zarządzający poszczególnymi elementami Infrastruktury bezpieczeństwa
   - Zarządzanie konfiguracją w pełnym zakresie funkcjonalnym określonym w rozdziale 3.7.8

- Logowanie zdarzeń do centralnego systemu SIEM

Infrastruktura bezpieczeństwa musi być zrealizowana w oparciu o dostarczoną przez Wykonawcę dedykowaną platformę sprzętową. Zamawiający dopuszcza, aby Systemy zarządzające i raportujące zostały zrealizowane postaci maszyny wirtualnej wspieranej na platformach np. takich jak Vmware, Hyper-V lub KVM.

3.7.2. System NG Firewall

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System NG Firewall działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2. „ Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa".

a) Zaoferowane rozwiązania dla Systemu NG Firewall muszą opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Gartner Magic Quadrant for Enterprise Network Firewalls, lub analogicznych zestawieniach przygotowanych przez równoważne organizacje, przygotowanych w ciągu ostatnich dwóch lat
b) System NG Firewall nie może posiadać ograniczenia na ilość jednocześnie pracujących Użytkowników w sieci chronionej.
c) System NG Firewall musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP).
d) System NG Firewall musi wspierać Equal Cost Multipath (ECMP) .
e) Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI). Funkcjonując w trybie transparentnym Urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych, jak również nie może wprowadzać segmentacji sieci na odrębne domeny rozgłoszeniowe.
f) System NG Firewall musi być dostarczony jako specjalizowane Urządzenie, lub grupa Urządzeń, zabezpieczeń sieciowych (appliance). W architekturze Systemu NG Firewall musi występować separacja modułu zarządzania i modułu przetwarzania danych.
g) System NG Firewall musi umożliwiać Zamawiającemu tworzenie i modyfikowanie polityk, które opisywać będą mechanizmy kontroli produkcyjnego ruchu sieciowego, pochodzącego ze szkół, pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
h) System NG Firewall musi umożliwiać Zamawiającemu definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików, Kontrola aplikacji) dla dowolnego strumienia danych definiowanego jak ruch wychodzący lub przychodzący z/do określonych podsieci IP na/z określonych porty TCP / UDP
i) Polityka zabezpieczeń Systemu NG Firewall musi umożliwiać Zamawiającemu konfigurację w oparciu o strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, adresy URL, użytkowników sieci.
j) System NG Firewall musi umożliwiać Zamawiającemu konfigurację, w ramach pojedynczej polityki:

- Uruchamianie funkcjonalności AV, IPS i Kontroli aplikacji rozumiane jako przypisanie do polityki konkretnego profilu określającego działanie danej funkcjonalności zgodnie z wymaganiami postawionymi w pkt 3.7.2.1, 3.7.2.2 i 3.7.2.3.
- Akcji, co najmniej blokady lub przepuszczenia transmisji, podejmowanej w ramach naruszenia określonych w polityce kryteriów i zabezpieczeń,
- rejestrowanie wszystkich zdarzeń zakwalifikowanych przez daną politykę,
- [Wykreślony podpunkt]

k) System NG Firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1Q.

l) System NG Firewall musi umożliwiać Zamawiającemu konfigurację i pracę każdego interfejsu sieciowego w trybie transparentnym, L2 i L3. Tryb pracy Systemu NG firewall musi być ustalany per interfejs sieciowy, a System NG firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji Systemu NG Firewall

m) Każdy z interfejsów sieciowych Systemu NG Firewall musi pozwalać na tworzenie subinterfejsów VLAN.

n) System NG Firewall musi obsługiwać min 1000 znaczników VLAN

o) System NG Firewall musi posiadać funkcję ochrony przed atakami typu DoS poprzez limitowanie ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP, wykorzystując co najmniej następujące mechanizmy:
   - Flood Protection
   - SYN Floods
   - Port scans

   Zamawiający dopuszcza, aby powyższa funkcjonalność została zrealizowana alternatywnie przez funkcjonalność IPS, opisaną w pkt 3.6.2.2. Szczegółowego opisu przedmiotu zamówienia.

p) System NG Firewall musi umożliwiać Zamawiającemu budowanie polityk uwierzytelniania dla Użytkowników i administratorów, definiujących rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów.

q) Polityki definiujące muszą umożliwiać wykorzystanie adresów źródłowych, docelowych, numerów portów usług oraz adresów URL. Minimalne wymagane przez Zamawiającego mechanizmy uwierzytelnienia to do wyboru dwa z trzech wymienionych: RADIUS, TACACS+, LDAP.

r) Polityka kontroli dostępu musi precyzyjnie definiować prawa dostępu Użytkowników i administratorów do określonych usług sieci i musi być utrzymywana nawet, gdy osoba zmieni lokalizację i adres IP. W przypadku Użytkowników i administratorów pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. System NG Firewall musi umożliwiać Zamawiającemu realizację wszystkich powyższych funkcji poprzez integrację z zewnętrznym systemem zarządzania tożsamością.

s) System NG Firewall musi pozwalać na konfigurowanie i wysyłanie logów, w formacie CEF lub LEEF lub równoważnym RFC 5424, do różnych serwerów Syslog min 2 serwerów typu Syslog.

t) System NG Firewall musi obsługiwać nie mniej niż 5 wirtualnych firewalli działających w trybie routed, posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji Systemu NG Firewall. Alternatywnie Zamawiający

dopuszcza sytuację gdzie odrębne tablice routingu są realizowane poprzez dodatkowe wirtualne firewalle.

u) System NG Firewall musi obsługiwać protokoły routingu dynamicznego, nie mniej niż OSPF, BGP.

v) System NG Firewall musi posiadać możliwość dostosowania komunikatów o błędach lub komunikatów informacyjnych wyświetlanych Użytkownikom, w szczególności wyświetlanie informacji powiązanych z sesją dla poszczególnych funkcjonalności:
   - powód zablokowania danej sesji,
   - treść błędu,

   System NG Firewall musi umożliwiać Zamawiającemu definiowanie różnych statycznych stron blokowania dla poszczególnych powodów zablokowania danych sesji związanych np. z funkcjonalnością IPS lub funkcjonalnością Kontroli aplikacji.

3.7.2.1. Funkcjonalność AV

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym 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. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG firewall. Zamawiający dopuszcza realizację tej funkcjonalności w sposób równoważny z wykorzystaniem dedykowanych Urządzeń lub jedynie w Węzłach Centralnych przy założeniu realizacji funkcjonalności AV dla wszystkich Użytkowników obsługiwanych przez dany Węzeł.

a) Funkcjonalność AV musi być realizowany dla 9% ruchu związanego z ruchem SMTP, IMAP, POP3, FTP i inne. Wartości w tabeli w rozdziale 3.3.

b) Funkcjonalność AV musi posiadać silnik antywirusowy, który umożliwia skanowanie i blokowanie ruchu w obu kierunkach komunikacji dla protokołów działających również na niestandardowych portach (np. FTP na porcie 2021).

c) Funkcjonalność AV musi umożliwiać skanowanie i blokowanie archiwów, w tym co najmniej: zip.

d) Funkcjonalność AV musi posiadać moduł inspekcji antywirusowej uruchamiany dla aplikacji wykorzystujących co najmniej następujące dekodery obsługujące protokoły SMTP, IMAP, POP3, FTP, kontrolujący ruch bez konieczności uzupełniania o jakiekolwiek komponenty. 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 urządzeniu 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 urządzenia stanowi podzbiór bazy utrzymywanej przez producenta rozwiązania, na bieżąco aktualizowany przez producenta.

e) Funkcjonalność AV musi zapewniać możliwość wykrywania, śledzenia i blokowania transferu następujących kategorii plików w ruchu sieciowym:
   - pliki systemowe
   - pliki graficzne
   - pliki PDF
   - pliki wykonywalne
   - pliki multimedialne
   - pliki pakietu Office
   - pliki skompresowane
   - inne pliki, które mogą służyć do propagacji wirusów
f) Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
g) Funkcjonalność AV musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: SMTP, FTP, IMAP, POP3 w obu kierunkach - upload/download.
h) Funkcjonalność AV w trybie proxy musi umożliwiać Zamawiającemu na definiowanie wielkości pliku powyżej, którego funkcjonalność AV nie będzie przeprowadzała inspekcji danego pliku.

3.7.2.2. Funkcjonalność IPS

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność IPS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall.

a) Funkcjonalność IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
b) Funkcjonalność IPS musi posiadać dostarczoną i wspieraną przez producenta bazę sygnatur ataków, która musi zawierać minimum 10 000 wpisów i być aktualizowana automatycznie. Baza sygnatur musi być dostarczana i wspierana przez producenta, na bieżąco cyklicznie aktualizowana i uzupełniana, przez dostawcę bazy. Zamawiający dopuszcza, że w momencie podpisania umowy baza zawiera co najmniej 5 000 sygnatur i w ciągu następnych 12 miesięcy baza zostanie rozbudowana do wielkości wymaganych 10 000 sygnatur

c) Funkcjonalność IPS musi umożliwiać Zamawiającemu definiowanie własnych wyjątków, określających dla jakich adresów IP (docelowych lub źródłowych) system IPS ma nie wykonywać analizy pakietów, oraz własnych sygnatur opisujących sposób zachowania znanych podatności (exploit'ów).
d) Funkcjonalność IPS musi zapewniać Zamawiającemu możliwość wykrywania i blokowania szerokiej gamy zagrożeń, takich jak min.:
   - złośliwe oprogramowanie,
   - skanowanie sieci,

- ataki na usługę VoIP,
- próby przepełnienia bufora,
- ataki na aplikacje P2P,
- zagrożenia dnia zerowego, itp.

e) Funkcjonalność IPS musi zapewniać Zamawiającemu możliwość wykrywania zagrożeń za pomocą co najmniej łącznie wszystkich poniższych mechanizmów:
   - sygnatury
   - mechanizm wykrywania anomalii w protokołach
   - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego

f) Funkcjonalność IPS musi dobierać optymalny mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego DPI lub Funkcjonalność IPS musi dokonywać analizy danych strumieniowo i wspierać mechanizmy pełnej re-asemblacji ruchu sieciowego oraz braku selektywnego wyłączania sygnatur

g) Funkcjonalność IPS musi umożliwiać Zamawiającemu wykrywanie i blokowanie komunikacji Command&Control do sieci botnet.

h) Funkcjonalność IPS musi zapewniać Zamawiającemu możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez konieczności użycia zewnętrznych narzędzi i wsparcia producenta

3.7.2.3. Funkcjonalność Kontrola aplikacji

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność Kontroli aplikacji (udostępnianych poprzez sieć Internet) działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall .

a) Funkcjonalność Kontroli Aplikacji musi posiadać funkcję, która musi umożliwiać Zamawiającemu kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

b) Funkcjonalność kontroli aplikacji musi posiadać bazę Kontroli Aplikacji, która musi zawierać minimum 2500 sygnatur opisujących charakterystykę aplikacji lub która musi zawierać 5000 ich pojedynczych modułów. Baza sygnatur musi być dostarczana i wspierana przez producenta, na bieżąco cyklicznie aktualizowana i uzupełniana, przez dostawcę bazy.

c) Funkcjonalność Kontroli aplikacji musi umożliwiać Zamawiającemu Kontrolę aplikacji chmurowych (co najmniej: Facebook, Instagram, Youtube, Twitter, Google Docs, Dropbox) pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

d) Baza realizująca funkcjonalność kontroli aplikacji musi być podzielona na kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa, przynajmniej: proxy, P2P.

e) Funkcjonalność kontroli aplikacji musi umożliwiać Zamawiającemu definiowanie własnych sygnatur.

f) Funkcjonalność kontroli aplikacji musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z np. P2P i Instant Messaging).

Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury lub sygnatury i analizę heurystyczną.

3.7.3. System DNS

W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System inspekcji DNS działał w skali całego ruchu określonego w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa".

a) System DNS musi być dedykowaną platformą sprzętową lub być składową innego elementu Systemu.
b) System DNS musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System)
c) System DNS musi umożliwiać Zamawiającemu tworzenie własnych wpisów typu:
   - A
   - AAAA
   - CNAME
   - MX
   - PTR
   - NS
   - SOA
   - SRV
   - TXT

   Definicje typów wpisów są zgodne z RFC 1035 punkt 3.2.2.
d) System DNS musi być zgodny z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Commnents http://www.ietf.org/rfc.html)
e) System DNS musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136
f) System DNS musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996
g) System DNS musi wspierać protokoły DNS w wersji IPv4 i IPv6
h) System DNS musi wspierać obsługę MultiMaster DNS
i) System DNS musi wpierać cache DNS
j) System DNS musi wspierać usługę DDNS
k) System DNS musi wspierać usługę walidacji DNSSEC
l) System DNS musi mieć pojemność bazy na minimum 800 000 rekordów
m) System DNS musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF oraz protokołu BFD)
n) System DNS musi posiadać funkcjonalność filtrowania odpowiedzi DNS na podstawie cyklicznie aktualizowanej przez producenta bazy reputacji domen infekujących malware/botnet/SURBL nowo obserwowanych domen w sieci Internet oraz wykrywania tunelowania w DNS (DNS

tunneling) za pomocą silnika analitycznego (Machine Learning) pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych za pomocą protokołu DNS.

o) System DNS musi posiadać funkcjonalność wykrywania i blokowania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego bazującego na uczeniu maszynowym i pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych przez protokół DNS. W tym celu urządzenie dla nazw FQDN w zapytaniach DNS (w tym dla zapytań o rekordy A) musi co najmniej: wyliczać entropię znaków, sprawdzać popularność występowania w językach naturalnych wszystkich 2- i 3-gramów, obliczać współczynnik liczby samogłosek do wszystkich znaków w nazwie, obliczać współczynnik liczby cyfr do wszystkich znaków w nazwie, analizować rozmiar zapytania, analizować częstotliwość zapytań DNS.
p) System DNS musi posiadać funkcjonalność DNS firewalla, tzn. na podstawie następujących zdarzeń:
   - zapytanie DNS od konkretnego adresu IP
   - zapytanie DNS o konkretną domenę
   - odpowiedź DNS zawierająca konkretny adres IP
   - odpowiedź DNS z konkretną nazwą i adresem IP w rekordzie NS dla danej domeny (NSDNAME i NSIP)

   musi mieć możliwość podjęcia następujących działań:

   - blokowanie dostępu z odpowiedzią NXDOMAIN
   - blokowanie dostępu z odpowiedzią NODATA
   - przekierowanie na inny adres
   - zezwolenie na dostęp z logowaniem zdarzenia
q) System DNS musi posiadać ochronę przed atakami związanymi z protokołami DNS, BGP OSPF, NTP, w tym co najmniej:
   - Na protokoły BGP i OSPF wykorzystywane do DNS Anycast (m.in. blokowanie niespodziewanych pakietów BGP/OSPF, czy zbyt dużej liczby pakietów BGP/OSPF w danym okresie czasu)
   - Na protokół NTP wykorzystywany do synchronizacji czasu (m.in. blokowanie nieprawidłowych żądań NTP)
r) System DNS musi umożliwiać Zamawiającemu na przekierowanie użytkownika sieci na stronę z informacją o zablokowaniu zapytania DNS
s) System DNS musi umożliwiać Zamawiającemu na dostosowanie komunikatów o błędach i komunikatów informacyjnych wyświetlanych Użytkownikom, w szczególności wyświetlanie informacji powiązanych z sesją jak:
   - treść błędu,
   - źródłowy adres IP,
   - powód zablokowania danej sesji bazujący na kategorii zablokowanej domeny
t) System DNS musi umożliwiać Zamawiającemu na blokowanie lub przekierowywanie domen ze względu na kategorię serwowanej treści.
u) Baza kategoryzacji zawiera co najmniej 100 kategorii treści, uwzględniających co najmniej kategorie , które mogą być użyte przez Zamawiającego w dowolny sposób w celu stworzenia polityki filtrowania. Zamawiający wymaga aby baza kategorii zawierała co najmniej kategorie zawierające domeny prezentujące treści pornograficzne, treści udostępniające możliwość

uczestniczenia w grach hazardowych w szczególności znajdujących się w Rejestrze prowadzonym przez Ministerstwo finansów.

v) System musi filtrować zapytania DNS, porównując poszczególne requesty ze specjalizowaną bazą danych (dostarczaną przez producenta Systemu), podzieloną na kategorie treści zawierającą informacje o domenach.

w) System DNS musi umożliwiać Zamawiającemu blokowania zapytań DNS odwołujących się do domen znajdujących się w bazie dostarczanej przez Internet Watch Foundation (IWF) lub równoważnej organizacji,

x) System 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.

y) System DNS musi posiadać funkcjonalność blokowania zapytań DNS skorelowanych z domenami o niebezpiecznej treści: domeny wykorzystywane do propagacji złośliwego oprogramowania, domeny Phishing'owe, domeny wykorzystywane do zestawiania połączeń typu Command and Control z Botnetami

z) System DNS musi dać możliwość tworzenia listy domen dopuszczanych i listy domen zabronionych przez administratora systemu mających priorytet nad listami dostarczonymi wraz z systemem.

aa) System DNS musi umożliwiać Zamawiającemu na konfigurację polityki dostępu do treści zależnej od adresu IP, przy czym zachodzące na siebie przestrzenie adresowe są traktowane jako oddzielne, tzn. przykładowo adres 10.1.1.20/32 może mieć inną politykę dostępu do treści niż 10.1.1.1/24

3.7.4. System ADC

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System ADC działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa".

a) Zaoferowane rozwiązania dla Systemu ADC muszą opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Gartner Magic Quadrant for Application Delivery Controllers lub Gartner Market Guide for Application Delivery Controllers, lub analogicznych zestawieniach przygotowanych przez równoważne organizacje, przygotowanych w ciągu ostatnich trzech lat przed upływem terminu składania ofert.

b) System ADC musi równoważyć obciążenie pomiędzy Urządzeniami lub serwerami aplikacyjnymi oraz ruch użytkownika do Aplikacji

c) System ADC musi zapewniać Zamawiającemu możliwość zdefiniowania grupy Urządzeń lub serwerów tego samego typu, np. Serwery WWW aplikacji 01, Serwery APP aplikacji 01

d) System ADC musi być dostarczony jako specjalizowane Urządzenie, lub grupa Urządzeń (appliance).

e) W architekturze Systemu ADC musi występować separacja modułu zarządzania i modułu przetwarzania danych.

f) System ADC musi zapewniać możliwość przesłania ruchu do Urządzeń lub serwerów , a następnie rozłożenie go na poziomie zdefiniowanej przez administratora grupy Urządzeń lub

serwerów należących do poszczególnych Systemów dostarczanych w ramach Infrastruktury bezpieczeństwa lub serwerów umieszczonych na Zasobach obliczeniowych OSE

g) System ADC musi monitorować, czy Urządzenia lub serwery w danej grupie funkcjonalnej pracują, a w razie niedostępności jednego automatycznie przesyłać ruch do pozostałych działających Urządzeń lub serwerów.

h) System ADC musi zapewniać zamawiającemu możliwość konfiguracji sposobu zachowania Systemu ADC w sytuacji, kiedy w danej funkcjonalnej grupie urządzeń żadne urządzenia nie będzie działało – minimalnie pominięcie serwisu (fail open) lub odrzucenie połączenia (fail close).

i) System ADC musi realizować translację portu na czas przechodzenia przez strefy rozszytego ruchu, np. ruch przychodzący na porcie 443, który uległ rozszyfrowaniu, jest następnie przesyłany na porcie 8443 do grupy Urządzeń lub serwerów oraz ponownie ruch wychodzący zaszyfrowany jest na porcie 443.

j) System ADC musi zapewniać możliwość dodania przez Zamawiającego własnego nagłówka do protokołu HTTP w celu przekazania do innych Urządzeń lub serwerów.

k) System ADC należący do Infrastruktury bezpieczeństwa musi umożliwiać Zamawiającemu podłączenie z innymi elementami Infrastruktury bezpieczeństwa i sieci Zamawiającego z wykorzystaniem wszystkich poniższych sposobów:
   - bezpośredniego połączenia (połączenie punkt-punkt),
   - połączenie w ramach jednego VLAN'u (połączenie w warstwie 2 modelu ISO/OSI).,
   - połączenie z wykorzystaniem adresów IP (połączenie w warstwie 3 modelu ISO/OSI).

l) System ADC musi realizować równomierne rozłożenie całego ruchu na poziomie Centralnego Węzła Bezpieczeństwa i zapewniać Zamawiającemu możliwość definiowania reguł określających kryteria, co najmniej: źródłowy i docelowy adres IP oraz źródłowy i docelowy port TCP/UDP.

m) [Wykreślony Punkt]

n) System ADC musi również wspierać wysyłanie dowolnej, zdefiniowanej za pomocą reguł, wielkości ruchu:
   - do urządzeń działających w warstwie 2 (L2, np. IPS),
   - do systemów pasywnych (np. systemu IDS)
   - oraz z wykorzystaniem protokołu ICAP.

o) [Wykreślony Punkt]

p) [Wykreślony Punkt]

q) System ADC musi posiadać wbudowany język skryptowy, posiadający co najmniej następujące cechy:
   - Analiza, zmiana oraz zastępowanie parametrów w nagłówku HTTP oraz w zawartości pakietów w skali całego ruchu obsługiwanego przez dane Urządzenie,
   - W budowanych skryptach można analizować, zmieniać oraz zastępować parametry w nagłówkach protokołów: HTTP, TCP, RTSP, SIP.

r) System ADC musi realizować analizę, zmianę oraz zastępowanie parametrów w nagłówku oraz w zawartości pakietów

s) Co najmniej dla protokołów: HTTP, TCP, RTSP, SIP

t) Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego

u) System ADC musi posiadać funkcjonalność równoważenia obciążenia (sterowania ruchem) na bazie:
   - mechanizmów równoważenia obciążenia: round robin, ważona, najmniejsza liczba połączeń, najszybsza odpowiedź, grupy priorytetów,
   - mechanizmów monitorowania stanu serwerów ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, HTTP/HTTPS, LDAP, FTP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi być zapewniona możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność wyżej wymienionych usług.
   - mechanizmów przywiązywania sesji: cookie (hash, rewrite, custom, insert, passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID
   - usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków HTTP, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi,
   - Informacji na temat grupy użytkownika (po wdrożeniu systemu zarządzania tożsamością)

v) System ADC musi zapewniać Zamawiającemu możliwość tworzenia reguł definiujących wyjątki od reguł określających domyślny przepływ ruchu i przesłania go do wskazanej funkcjonalnej grupy Urządzeń. Reguły określające wyjątki mogą być budowane przez Zamawiającego z wykorzystaniem źródłowego i docelowego adresu IP lub adresu podsieci oraz statycznej listy adresów URL.

w) System ADC musi posiadać funkcje przywiązywania sesji (Session persistence) do określonej ścieżku ruchu na podstawie konfiguracji przez Zamawiającego reguł wykorzystujących co najmniej następujące atrybuty:
   - Cookie (hash, rewrite, custom, insert, passive)
   - Adres źródła
   - Identyfikator sesji SSL
   - Adres docelowy
   - Tworzonych przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 3.6.4 ppkt. q
   - Badanie obciążenia poszczególnych nodów w klastrze pod względem obciążenia

x) System ADC musi umożliwiać Zamawiającemu przekierowanie ruchu pochodzącego od nieuwierzytelnionych Użytkowników na zewnętrzny captive portal, dostarczony w ramach osobnego postępowania.

y) System ADC musi posiadać co najmniej następujące interfejsy administracyjne:
   - GUI przy wykorzystaniu protokołu https
   - Zarządzanie poprzez SSH
   - Zarządzanie poprzez web API

z) System ADC musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych, przez dane Urządzenie, połączeń TCP/UDP. W przypadku przekroczenia zdefiniowanej wartości System ADC musi umożliwiać Zamawiającemu określenie akcji pozwalającej na wysłanie użytkownikom sieci strony błędu lub przekierowanie ich na inny serwer.

aa) System ADC musi umożliwiać Zamawiającemu konfigurację poniższych funkcji na każdym Urządzeniu dostarczonym w ramach Systemu ADC:
   - Obsługa protokołu SNMP v1/v2c/v3
   - Zewnętrzny syslog

- Zbieranie danych i ich wyświetlanie
- Zbieranie danych zgodnie z ustawieniami administratora
- Osobna brama domyślna dla interfejsu zarządzającego
- [Wykreślony podpunkt]
- Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy)
- Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.

bb) System ADC musi obsługiwać sieci VLAN w standardzie 802.1Q.

cc) System ADC musi obsługiwać agregację linków w standardzie 802.3ad (LACP)

dd) System ADC musi obsługiwać Jumbo Frames

ee) System ADC musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding), które wykonuje separację ruchu sieciowego do różnych aplikacji. Musi zapewniać poprawne działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP.

ff) System ADC musi obsługiwać protokoły dynamicznego routingu BGP i OSPF.

3.7.5. Funkcjonalność SSL VPN

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność SSL VPN działała dla liczby użytkowników określonej w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa".

a) Funkcjonalność SSL VPN musi działać we wszystkich trybach: portal dostępowy, tunel aplikacyjny, tunel szyfrowany SSL VPN

b) Funkcjonalność SSL VPN musi umożliwiać Zamawiającemu na definiowanie polityki dostępu poprzez graficzny edytor, który pozwoli Zamawiającemu wybierać konkretne obiekty konfiguracyjne (elementy uwierzytelnienia, konfiguracji dostępu, dostępnych zasobów, itp.) oraz najczęstsze powtarzające się konfiguracje kopiować do makr , alternatywnie definiowanie makr i ich sekwencji w sposób tekstowy.

c) [Wykreślony punkt]

d) Funkcjonalność SSL VPN musi obsługiwać OAuth 2.0 w trybie: klient, serwer zasobów (resource server) oraz serwer autoryzacji (authorization server)

e) Funkcjonalność SSL VPN musi zapewniać Zamawiającemu możliwość uwierzytelnienia użytkowników przy wykorzystaniu wszystkich wymienionych metod: formularzy, certyfikatów cyfrowych, SecurID, Kerberos SSO, tokenów RSA, Radius, LDAP, Oracle Access Manager, kart smart cards, uwierzytelnienia wieloskładnikowego

f) Funkcjonalność SSL VPN musi udostępniać klientów VPN działających na platformach: Windows, Mac, Linux, Android, iPad, iPhone oraz przeglądarek: IE, Firefox, Chrome

g) Funkcjonalność SSL VPN musi udostępniać klientów VPN umożliwiających Zamawiającemu na inspekcję stacji klienta sprawdzającą poprawność pracy aplikacji (antywirus, firewall, rejestrów, procesów) dla systemów Windows, Linux, Mac

h) Funkcjonalność SSL VPN musi zapewniać możliwość automatycznego aktualizowania wersji oprogramowania klienta dla systemów Windows

i) Funkcjonalność SSL VPN musi zapewniać możliwość utworzenia bezpiecznego wirtualnego pulpitu na czas trwania sesji użytkownika
j) Funkcjonalność SSL VPN musi zapewniać wsparcie dla CAPTCHA
k) Funkcjonalność SSL VPN musi zapewniać wsparcie dla tzw. "step-up authentication"
l) Funkcjonalność SSL VPN musi zapewniać wsparcie dla Microsoft ActiveSync oraz Outlook Anywhere z wykorzystaniem NTLM
m) Funkcjonalność SSL VPN musi zapewniać Zamawiającemu możliwość generacji jednorazowych tokenów (OTP) i wysyłanie ich mailem lub integrując się z zewnętrzną bramką poprzez SMS
n) Funkcjonalność SSL VPN musi zapewniać Zamawiającemu możliwość definiowania per grupa użytkowników (np. Active Directory)/lub per użytkownik limitu pasma przydzielonego dla użytkownika do ściągania informacji
o) [Wykreślony punkt]
p) Funkcjonalność SSL VPN musi zapewniać Zamawiającemu możliwość definiowania reguł dostępu użytkownika bazując na listach uwzględniających parametry warstwy 4 oraz 7 modelu ISO OSI.
q) Funkcjonalność SSL VPN musi zapewniać Zamawiającemu możliwość gromadzenia parametrów uwierzytelnienia użytkownika - credential caching.
r) Funkcjonalność SSL VPN musi zapewniać Zamawiającemu możliwość budowania dynamicznej strony www, w zależności od użytkownika, jego przynależności do danej grupy, zawierającej udostępnione aplikacje.
s) Funkcjonalność SSL VPN musi zapewniać wsparcie dla VMWare View oraz Citrix XenApp/XenDesktop
t) Funkcjonalność SSL VPN musi zapewniać obsługa funkcji szyfrowania site-to-site IPSec VPN. Alternatywnie Wykonawca może przenieść realizację tego wymagania na inny System dostarczany w ramach Infrastruktury bezpieczeństwa
u) Funkcjonalność SSL VPN musi obsługiwać tryb wymuszający nawiązanie połączenia VPN, tzw. tryb always-on dla systemu Windows
v) Funkcjonalność SSL VPN musi zapewniać wsparcie dla zewnętrznego uwierzytelnienia w dostępie SSL VPN tzw. captive portal
w) [Wykreślony punkt]
x) Funkcjonalność SSL VPN musi posiadać mechanizm raportowy. Zamawiający dopuszcza aby mechanizm raportowy został dostarczony w ramach Systemu zarządzającego. Mechanizm raportowy musi uwzględniać nie mniej niż:
    a. Błędne próby uwierzytelnienia
    b. Informacje o użytkownikach
    c. Zasoby, do których odwołują się użytkownicy
    d. Lokalizacja (Geolocation)
y) Licencjonowanie funkcjonalności SSL VPN musi odbywać się per ilość jednocześnie pracujących użytkowników z możliwością instalacji klienta na dowolnej ilości urządzeń/stacji roboczych.

3.7.6. Funkcjonalność Web Application Firewall

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby Funkcjonalność WAF

działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa”. Zamawiający zakłada realizację funkcjonalności Web application Firewall (WAF) na Systemie ADC lub jako dedykowane Urządzenie typu appliance..

a) Zaoferowane rozwiązania dla funkcjonalność WAF muszą opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Gartner Magic Quadrant for Web Application Firewalls, lub analogicznych zestawieniach przygotowanych przez równoważne organizacje, przygotowanych w ciągu ostatnich dwóch lat
b) Funkcjonalność WAF musi umożliwiać Zamawiającemu konfigurację następujących trybów pracy:
   - Tryb wykrywania, logowania i blokowania ataków
   - Tryb wykrywania i logowania ataków bez blokowania
   - Tryb uczenia się bez blokowania
   - Tryb uczenia się z blokowaniem i logowaniem
c) Funkcjonalność WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe, tzn. zostało określone w modelu aplikacji web, jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web i statycznie definiowanych polityk bezpieczeństwa.
d) Funkcjonalność WAF musi umożliwiać Zamawiającemu na tworzenie polityki bezpieczeństwa definiującej zestaw sygnatur, które mają być wykorzystane do ochrony całej aplikacji lub poszczególnych jej modułu (np. formularz rejestracyjny)
e) Funkcjonalność WAF musi umożliwiać Zamawiającemu zakres działania polityki bezpieczeństwa na podstawie:
   - Nazwy hosta źródłowego i docelowego
   - Wartości wszystkich parametrów z nagłówków HTTP
   - Wartości wszystkich parametrów cookie
f) Funkcjonalność WAF musi umożliwiać Zamawiającemu na ręczne konfigurowanie i modyfikację reguł polityki bezpieczeństwa
g) Funkcjonalność WAF musi identyfikować i blokować, zgodnie z polityka bezpieczeństwa, incydenty z wykorzystaniem bazy sygnatur (negatywny model zabezpieczeń)
h) Funkcjonalność WAF musi umożliwiać Zmawiającemu na automatyczne budowanie polityk w oparciu o informacje uzyskane w ramach integracji z skanerami aplikacji webowych udostępnianych przez zewnętrznych dostawców np. Cenzic, HP WebInspect, IBM AppScan, Qualys Guard, WhiteHat Sentinel.
i) Funkcjonalność WAF musi umożliwiać Zamawiającemu na blokowanie zapytań z danego obszaru geograficznego na podstawie dostarczonej w ramach rozwiązania bazy geolokacyjnej.
j) Funkcjonalność WAF musi umożliwiać Zamawiającemu definiowanie różnych akcji podejmowanych przez funkcjonalność WAF w przypadku wykrycia naruszenia polityki bezpieczeństwa, w tym co najmniej:
   - Wygenerowanie zdarzenia i zapisanie go do logu lub wysłanie do zewnętrznego serwera SIEM
   - Blokowanie danej sesji

- Wygenerowanie komunikatu o błędzie lub komunikatu informacyjnego, który zostanie wystawiony do Użytkownika

k) Funkcjonalność WAF musi posiadać możliwość dostosowania komunikatów o błędach lub komunikatów informacyjnych wyświetlanych Użytkownikom, w szczególności wyświetlanie informacji powiązanych z sesją jak:
   - treść błędu,
   - powód zablokowania danej sesji
   - Nazwa urządzenia

l) Funkcjonalność WAF musi umożliwiać Zamawiającemu konfigurację wyświetlana stron blokowania (błędu) w technologiach AJAX i JSON

m) Funkcjonalność WAF musi posiadać cyklicznie aktualizowaną przez producenta oprogramowania bazę sygnatur, podzieloną na kategorie zagrożeń, definiujących sposób wykrywania znanych ataków, co najmniej określonych w OWASP 10, wykorzystujących podatności znajdujące się na liście CVE (Common Vulnerabilities and Exposures)

n) Funkcjonalność WAF musi posiadać bazę przynajmniej 4500 sygnatur, które są zaprojektowane do wykrywania znanych problemów i ataków na aplikacje webowe.

o) Baza sygnatur wykorzystywana przez funkcjonalność WAF musi być podzielona na grupy umożliwiające wybór technologii stosowanych w aplikacji web, w szczególności choć nie wyłącznie:
   - Bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2
   - System Operacyjny: Windows, Linux, UNIX
   - Język aplikacji, frameworki: ASP, ASP .NET, PHP, Java, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Java Servlets/JSP, Lotus Domino, Macromedia ColdFusion, JRun, Outlook Web Access, SSI, WebDAV, JQuery, SSI, WebDAV, jQuery
   - Serwer WWW: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy.

p) Funkcjonalność WAF musi umożliwiać Zamawiającemu na tworzenie własnych sygnatur, co najmniej w oparciu o wyrażenia regularne

q) Funkcjonalność WAF musi pozwolić Zmawiającemu budować profil aplikacji, będący zapisem parametrów określających sposobu zachowania aplikacji (komunikacji pomiędzy modułami wewnątrz aplikacji oraz sposobu interakcji z użytkownikami), chronionej przez funkcjonalność WAF, w oparciu o co najmniej następujące parametry:
   - wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a.
   - typ widoku aplikacji (np. servlet) oraz format komunikacji (co najmniej: HTTP form, JSON, XML) pomiędzy komponentami aplikacji
   - przejścia, przełączenia widoku, pomiędzy URL-ami (servletami)
   - dopuszczalne metody HTTP opisane w RFC 2616,
   - dopuszczalne cookie,
   - dopuszczalne parametry w polityce bezpieczeństwa konfigurowanej na Funkcjonalności WAF wchodzącej w skład modelu bezpieczeństwa,
   - parametry dynamiczne, np. typy wartości przesyłane w formularzach (integer, string itd.)
   - typ/format parametrów (co najmniej: alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML,)
   - wystąpień i długość parametrów (per każdy parametr, co najmniej długość zapytań HTTP)

r) Funkcjonalność WAF musi umożliwiać Zamawiającemu na definiowanie dopuszczalnej sekwencji zapytań HTTP/HTTPS w obrębie realizacji poszczególnych usług dostarczanych przez aplikację web (*workflow*)
s) Funkcjonalność WAF musi tworzyć profil aplikacji web w sposób automatyczny, na podstawie analizy ruchu sieciowego do aplikacji, w szczególności sposobu interakcji użytkowników z aplikacją i sposobu komunikacji pomiędzy modułami aplikacji web
t) Funkcjonalność WAF musi umożliwiać Zamawiającemu na ręczną modyfikację profilu aplikacji web
u) Funkcjonalność musi umożliwiać Zamawiającemu na tworzenie wyrażeń regularnych (regexp) dla następujących celów:
   - definicje sygnatur
   - definicje wrażliwych danych
   - definicja rodzaju parametrów
   - nazwy Hosta i definicje prefixów URL
   - strojenie parametrów, których uczy się dynamicznie z profili aplikacji webowych"
v) Funkcjonalność WAF musi pozwolić Zamawiającemu wykorzystywać algorytmy służące do tworzenia profilu bezpieczeństwa do odrzucania zdefiniowanych przez administratora zachowań w procesie aktualizacji profilu.
w) Funkcjonalność WAF musi umożliwiać Zamawiającemu na definiowanie zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako zgodne z założonym przez sposobem działania aplikacji, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.
x) Funkcjonalność WAF musi pozwolić Zmawiającemu na automatyczne wykrywanie stron logowania Użytkowników (do aplikacji chronionych przez funkcjonalność WAF) oraz automatycznie włączać dla tych stron ochronę przed atakami typu brute force.
y) Funkcjonalność WAF musi umożliwiać Zamawiającemu na wykorzystanie mechanizmów ochrony aplikacji web (w szczególności sygnatur, mechanizmów behawioralnych, porównywanie ze zdefiniowanym profilem aplikacji web) w celu identyfikacji i blokowania ataków typu:
   - SQL Injection,
   - Cross-Site Scripting,
   - Cross-Site Request Forgery,
   - Session hijacking,
   - Command Injection,
   - Cookie/Session Poisoning,
   - Parameter/Form Tampering,
   - Forceful Browsing,
   - Brute Force Login,
   - Web Scraping
   - Cookie manipulation/poisoning
   - Dynamic Parameter tampering
   - Buffer Overflow
   - Stealth Commanding
   - Unused HTTP Methods

- Malicious File Uploads
- Hidden Field Manipulation
- Slow Loris

z) Funkcjonalność WAF musi umożliwiać Zamawiającemu na wstrzykiwanie do sesji nawiązanej miedzy aplikacją i przeglądarką, dodatkowych informacji (cookie, tokeny, JavaScript)

aa) Funkcjonalność WAF musi wykrywać i blokować ataki typu Denial of Service (DoS) ukierunkowanymi na warstwę aplikacyjną (np. zalewanie aplikacji web dużą ilością zapytań http).

bb) Funkcjonalność WAF musi umożliwiać Zamawiającemu na definiowanie zakresu działania mechanizmów odpowiedzialnych za wykrywanie i blokowanie ataków typu DoS per:
- Source IP,
- Obszar geolokacyjny,
- URL,
- Globalnie - website

cc) Funkcjonalność WAF musi posiadać mechanizmy automatycznego wykrywania i blokowania botów, zanim wywołają atak DDoS, web scraping lub brute force, wykorzystujące co najmniej trzy z poniższych metod:
- Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania
- Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless browser
- Sygnatur botów
- Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest Użytkownik).

dd) Funkcjonalność WAF musi umożliwiać Zamawiającemu na przypisywanie różnych poziomów mechanizmów odpowiedzialnych za wykrywanie i blokowanie ataków (D)DoS dla danych URL-i portalu, np. /infoportal/* musi posiadać luźniejszą politykę detekcji i zapobiegania ataków DDoS niż /sklep/*.

ee) Funkcjonalność WAF musi wykrywać i blokować ataki typu DDoS na tzw. ciężkie serwlety, czyli serwlety wywołujące złożone operacje obliczeniowe np. skomplikowane zapytania do baz danych.
- Wykrycie ataku na ciężkie serwlety musi bazować co najmniej na analizie liczby zapytań (TPS) oraz na badaniu czasu odpowiedzi

ff) Funkcjonalność WAF musi umożliwiać Zamawiającemu zapis ruchu do plików zgodnych z formatem TCP dump, w momencie wykrycia ataku (D)DoS.

gg) Funkcjonalność WAF musi posiadać cyklicznie aktualizowaną przez producenta oprogramowania bazę zawierającą kategoryzację programów typu bot i umożliwiać Zamawiającemu na blokowanie i przepuszczanie ruchu, wygenerowanego przez programy zaklasyfikowane w ramach poszczególnych kategorii, w szczególności przepuszczanie ruchu od komercyjnie używanych i uznanych za nieszkodliwe botów (np. search enginy i crawlery) oraz blokowanie ruchu od szkodliwych botów (np. UFONet).

hh) Funkcjonalność WAF musi posiadać mechanizmy ochrony dla aplikacji AJAX, JSON oraz aplikacji wykorzystujących Google Web Toolkit.

ii) Funkcjonalność WAF musi posiadać funkcję sprawdzania reputacji adresów IP, dostających się do chronionych aplikacji, w specjalizowanej bazie dostarczanej przez producenta Oprogramowania

jj) Baza reputacyjna, dostarczona w ramach funkcjonalności WAF, musi być automatycznie aktualizowana o nowe informacje o zagrożeniach nie rzadziej niż co 5 minut.

kk) Baza reputacyjna, dostarczona w ramach funkcjonalności WAF, musi zawierać informacje na temat co najmniej:
- Anonimowych proxy
- Sieci Botnet
- Aktywnych źródeł usług oferujących lub dystrybuujących malware, rootkity, robaki oraz wirusy
- Źródeł ataków DDoS/DoS
- Źródeł Exit Node sieci Tor
- Adresów IP zainfekowanych przez malware
- Adresów IP świadczących usługi hostingowe dla phishingu lub fraudów.
- Źródeł ataków cross-site scripting, iFrame injection, SQL injection, cross domain injection czy domain password brute force
- Źródłowych adresów IP skanerów służących do rekonesansu poprzez skanowanie hostów oraz domen
- Weryfikacja adresu źródłowego na podstawie X-Forwarded-For (XFF)

ll) Funkcjonalność WAF musi umożliwiać Zamawiającemu na wykorzystanie wbudowanych mechanizmów normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wykrywać:
- Directory traversal
- Kodowanie typu %u
- Kodowanie typu IIS backslash
- IIS Unicode codepoints
- Bare byte decoding
- Apache whitespace
- Wstrzykiwanie komentarzy (np. <!-- -->)

3.7.7. System inspekcja ruchu SSL/TLS

W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność inspekcji ruchu SSL/TLS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa". Zamawiający określa, że poprzez inspekcję ma na myśli deszyfrowanie i ponowne szyfrowanie ruchu SSL/TLS sklasyfikowanego na podstawie określonych przez Zamawiającego reguł.

a) System inspekcji ruchu SSL/TLS musi być dostarczony jako specjalizowane Urządzenie, lub grupa Urządzeń, (appliance) lub być składową innego elementu Infrastruktury bezpieczeństwa.

b) System inspekcji ruchu SSL/TLS musi zapewniać inspekcję całej komunikacji szyfrowanej protokołem SSL/TLS. System inspekcji ruchu SSL/TLS musi zapewniać możliwość deszyfracji ruchu SSL/TLS, skategoryzowanego jako „niezaufany", który zostanie wysłany dalej w celu poddania go właściwej inspekcji na Systemie NG firewall i Systemie SWG.

c) System inspekcji ruchu SSL/TLS musi posiadać zestaw polityk definiujący ruch SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji.

d) System inspekcji ruchu SSL/TLS posiada wbudowaną i automatycznie, cyklicznie aktualizowaną przez producenta oprogramowania listę serwerów, dla których niemożliwa jest deszyfracja ruchu (z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji. Realizacja funkcjonalności może być realizowana poprzez mechanizmy uczące dodające wyjątki na podstawie obserwowanego ruchu lub może być wsparta skryptem wykonywanym na lub poza urządzeniem.

e) System inspekcji ruchu SSL/TLS musi zapewniać Zamawiającemu możliwość dodawania wyjątków w procesie deszyfracji TLS'a w oparciu, o co najmniej:
   - adres IP/FQDN źródłowy,
   - podsieć źródłowa/docelowa
   - zbiór adresów IP/FQDN

f) W trybie rozszywania ruchu TLS, System inspekcji ruchu SSL/TLS musi wykonywać kontrolę certyfikatu serwera do którego łączy się użytkownik tj. minimum sprawdzenia daty ważności i łańcucha certyfikacji. W przypadku wykrycia nieważnego certyfikatu lub niepoprawnego łańcuch certyfikacji, System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu zdefiniowanie reguły blokującej daną komunikację i wystawienie użytkownikowi sieci komunikatu o błędzie.

g) Podczas rozszywania ruchu TLS, System inspekcji ruchu SSL/TLS nie może używać różnych zestawów algorytmów szyfrowania dla komunikacji z klientem i serwerem, w szczególności niedopuszczalna jest sytuacja, gdzie klient używa słabszego kryptograficznie mechanizmu niż serwer.

h) System inspekcji ruchu SSL/TLS musi zapewniać Zamawiającemu możliwość blokowania sesji szyfrowanych, nawet jeśli mechanizm rozszywania TLS jest wyłączony, na podstawie analizy certyfikatu serwera np. blokowanie całej domeny (z poddomenami) tumblr.com bez deszyfracji TLS.

i) System inspekcji ruchu SSL/TLS musi umożliwiać deszyfrowanie i szyfrowanie ruchu TLS na Urządzeniu w oparciu o co najmniej następujące algorytmy: RSA, DH i ECDHE.

j) System inspekcji ruchu SSL/TLS musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów.

k) [Wykreślony punkt]

l) Klucze prywatne zapisane na Systemie inspekcji ruchu SSL/TLS muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.

m) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu tworzenie polityki pozwalającej na wykluczenia ruchu podlegającego deszyfrowaniu na podstawie:
   - Źródłowego i docelowego adresu IP
   - Grupy adresów IP/FGQDN

n) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu utworzenie portu sieciowego, który posłuży do przesłania rozszytego ruchu do innego urządzenia.
   - W trybie pasywnym
   - W trybie aktywnym
   - ICAP

o) System inspekcji ruchu SSL/TLS musi współpracować z infrastrukturą PKI Zamawiającego

p) System inspekcji ruchu SSL/TLS musi umożliwiać generowanie certyfikatów typu ROOT w celu podpisywania certyfikatów użytych do deszyfracji oraz posiadać możliwość integracji w zewnętrznymi systemami PKI Zamawiającego.

q) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu sprawdzanie kategoryzacji adresu URL zawartego w certyfikacie (pola SNI lub SNI i CN) poprzez współpracę z Systemem DNS.

r) System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu wykonywanie zapytań DNS na podstawie zawartości pól certyfikatu, którym podpisana jest dana sesja SSL/TLS.

s) [Wykreślony Punkt]

~~s) System inspekcji ruchu SSL/TLS musi obsługiwać protokoły dynamicznego routingu BGP i OSPF~~

3.7.8. System zarządzający

System zarządzający umożliwia Zamawiającemu zarządzanie dostarczanymi przez Wykonawcę systemami należącymi do Infrastruktury bezpieczeństwa, zgodnie z przedstawionymi poniżej wymaganiami funkcjonalnymi, i umożlwiający na konfigurację wszystkich funkcji opisanych w ramach rozdziału 3. Zamawiający zakłada, że w ramach Systemu zarządzania, Wykonawca dostarczy oprogramowanie dedykowane dla każdego z wdrażanych systemów (w szczególności: System ADC, System NG firewall, System inspekcji SSL/TLS i System DNS), które musi być kompatybilne z każdym Urządzeniem danego rodzaju występującym w Centralnym lub Regionalnym Węźle Bezpieczeństwa. Zamawiający dopuszcza dostarczanie Systemu zarządzającego jako zestawu Urządzeń typu appliance lub jako maszyny wirtualne instalowane na infrastrukturze Zamawiającego.

Zamawiający dopuszcza wdrożenie Systemu zarządzającego w dwóch Węzłach Centralnych, w Warszawie i Poznaniu, lub we wszystkich Węzłach Regionalnych.

Wymagania:

a) System zarządzający musi realizować przynajmniej następujące funkcjonalności:
   - Zarządzanie konfiguracją elementów składowymi Infrastruktury bezpieczeństwa
   - Monitorowanie elementów Infrastruktury bezpieczeństwa
   - Raportowanie podstawowych elementów

b) Zarządzanie Systemem zarządzającym musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web i posiadać co najmniej następujące interfejsy administracyjne:
   - GUI przy wykorzystaniu protokołu HTTPS
   - CLI przy wykorzystaniu protokołu SSH
   - API, co najmniej poprzez wykorzystanie protokołu http (REST API)

c) Komunikacja elementów składowych poszczególnych systemów dostarczanych w ramach Infrastruktury bezpieczeństwa z Systemem zarządzającym musi być realizowana z wykorzystaniem szyfrowanych protokołów.

d) System zarządzający 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 Urządzeniami co najmniej poprzez protokół SSH), do których Wykonawca dostarczy dokumentację. Wykonawca w ramach Wdrożenia będzie zobowiązany do uczestniczenia w integracji Systemu zarządzania dostarczonego w ramach Infrastruktury bezpieczeństwa z nadrzędnym systemem zarządzania Zamawiającego. Integrację, o której wspomniano powyżej, Zamawiający planuje zakończyć do końca 2019 roku.

e) System zarządzający musi umożliwiać Zamawiającemu monitorowanie awarii i pokazanie aktualnych alarmów. Minimalny zakres monitorowania elementów Infrastruktury bezpieczeństwa:
   - Zbieranie danych z Urządzeń w tym co najmniej alarmy, warningi,
   - Generowanie i wizualizacja awarii związanych z:
     - wszystkimi elementami Infrastruktury bezpieczeństwa, w tym co najmniej interfejsów sieciowych, zasilaczy, wentylatorów, dysków, pamięci RAM
     - przekroczenie zadanego poziomu obciążenia interfejsów, CPU, RAM, ilości sesji Systemu, utraty pakietów
     - niepoprawnym działaniem każdej ze skonfigurowanych i uruchomionych funkcjonalności danego elementu Infrastruktury bezpieczeństwa
   - Monitorowanie dostępności, wydajności, pojemności wszystkich elementów Infrastruktury bezpieczeństwa
   - Analiza przepustowości i ruchu na bazie logów oraz ogólnego stanu i efektywności pracy Infrastruktury bezpieczeństwa
   - Zarządzenie komunikatami
   - Przechwytywanie komunikatów sprzętowych i systemowych
f) System zarządzający musi zapewniać Zamawiającemu możliwość generowania i exportowania raportów, co najmniej w formacie PDF. Zamawiający dopuszcza aby raporty prezentujące ogólną dostępność danego systemu były udostępnione w postaci dashboardów i system zarządzający nie musi umożliwiać ich exportu do pliku.
g) System zarządzający musi zapewniać Zamawiającemu możliwość generowania raportów co najmniej, w zakresie:
   - Ogólną dostępność danego systemu
   - Statystyki typu TOP 10 wybranych parametrów monitorowanych przez dany system, co najmniej:
     - Zablokowanych ataków przez funkcjonalność IPS
     - Zablokowanych typów malware'u wykrytych na funkcjonlaności AV
     - Zablokowanych aplikacji określonych w funkcjonalności Kontroli aplikacji
     - Adresów IP źródłowych generujących ataki wykryte przez funkcjonalność WAF
h) System zarządzający musi zapewniać Zamawiającemu możliwość generowania raportów z danych zebranych w ciągu ostatnich 48h.
i) System zarządzający musi zapewniać Zamawiającemu uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera RADIUS lub TACACS+
j) System zarządzający musi zapewnić `podgląd stanu komponentów monitorowanych Urządzeń (m.in. interfejsy, moduły, zasilacze)

k) System zarządzający musi zapewnić odbieranie komunikatów SNMP Trap z zarządzanych Urządzeń należących do Infrastruktury bezpieczeństwa lub zapewnić równoważne mechanizmy zbierania danych zawartych w bazie MIB
l) System zarządzający musi zapewnić tworzenie, usuwanie, edycję, tworzenie backupu i wersjonowanie szablonów konfiguracji oraz ich późniejsze wykorzystanie.
m) System zarządzający musi umożliwiać Zamawiającemu na odtworzenie backupu konfiguracji każdego elementu Infrastruktury bezpieczeństwa
n) System zarządzający musi zapewniać archiwizację i wersjonowanie plików konfiguracyjnych
o) System zarządzający musi zapewniać dystrybucję (w tym aktualizację) oprogramowania systemowego.
p) System zarządzający musi zapewniać Zamawiającemu możliwość szczegółowego określenia ról i przypisania uprawnień poszczególnym administratorom,
q) System zarządzający musi umożliwiać Zamawiającemu zarządzanie wszystkimi elementami składowymi Infrastruktury bezpieczeństwa w pełnym zakresie funkcjonalnym.
r) System zarządzający musi umożliwiać Zamawiającemu na centralne zarządzanie regułami bezpieczeństwa zdefiniowanymi na systemach dostarczonych w ramach Infrastruktury bezpieczeństwa
s) System zarządzający musi zapewniać szczegółowy wgląd w statystyki ruchu, stan pracy elementów składowych Systemu
t) Licencja dostarczona wraz z Systemem zarządzającym nie może ograniczać liczby użytkowników, administratorów korzystających jednocześnie z platformy Systemu zarządzającego.

3.8. Węzeł laboratoryjny

Węzeł laboratoryjny opisany poniżej musi odzwierciedlać pod kątem funkcjonalnym Infrastrukturę bezpieczeństwa pracującą w Regionalnym Węźle Bezpieczeństwa i Centralnym Węźle Bezpieczeństwa. Wydajność Węzła laboratoryjnego musi być zgodna z tabelą podaną w rozdziale 3.3.2 „Wymagania wydajnościowe na Węzeł laboratoryjny", z zachowaniem funkcjonalności uruchomionych w Regionalnym Węźle Bezpieczeństwa i Centralnym Węźle Bezpieczeństwa..

3.8.1. Wymagania na środowisko fizyczne

Wykonawca w ramach kontraktu jest zobowiązany do dostarczenia do Węzła laboratoryjnego fizycznym specjalizowanych Urządzeń typu appliance posiadających taką samą wersję Oprogramowania jak ta instalowana na Urządzeniach zainstalowanych w Centralnych i Regionalnych Węzłach Bezpieczeństwa. Celem ww. środowiska będzie możliwość odtworzenia dowolnego fragmentu funkcjonalności Infrastruktury bezpieczeństwa na potrzeby rozwiązywania problemów, a także na potrzeby testowania nowych wersji oprogramowania przed jego wdrożeniem w sieci OSE.

Wykonawca musi dostarczyć po jednym Urządzeniu z dostarczonych modeli:

a) Urządzeń NG Firewall,
b) Urządzeń ADC,
c) Urządzeń inspekcji SSL/TLS*

d) Urządzeń DNS*
e) Urządzeń Web Application Firewall*

*) dostarczenie tych Urządzeń jest obligatoryjne w przypadku jeśli Wykonawca w ramach realizacji przedmiotu zamówienia dostarczy dedykowane Urządzenia realizujące wymagania postawione dla tych systemów w pkt 3.6 i 3.7

Dostarczone Urządzenia zostaną podłączone do przełącznika sieciowego dostarczonego przez Zamawiającego.

3.8.2. Wymagania na środowisko wirtualne

Wykonawca dostarczy kompletne środowisko wirtualne zapewniające modelowanie sieci OSE.

Środowisko to musi zapewniać zamodelowanie całego Centralnego i Regionalnego Węzła Bezpieczeństwa.

W ramach środowiska wirtualnego, Wykonawca dostarczy odpowiednio wyskalowany serwer wraz ze wszystkimi wymaganymi licencjami.

3.8.3. Wymagania na testową instalację Systemu zarządzającego

Wykonawca 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 oraz współpracy z systemami testowymi OSS/BSS Zamawiającego wyszczególnionymi w pkt 3.10..

3.9. Wdrożenie

3.9.1. Przebieg wdrożenia

a) Przez cały okres trwania wdrożenia Wykonawca wydeleguje osobę odpowiedzialną za realizację przedmiotu Umowy (Kierownika Projektu), która będzie współpracowała z osobą o analogicznych odpowiedzialnościach ze strony Zamawiającego.
b) Przedstawiciele Stron, odpowiedzialni za realizację Umowy będą realizować cykliczne spotkania w celu m.in. wymiany informacji o postępach w pracach, rozwiązywania problemów. Szczegóły dotyczące częstości i miejsc spotkań zostaną uzgodnione w trybie roboczym pomiędzy Stronami.
c) Zamawiający, w ramach przygotowania do wdrożenia, jest zobowiązany do zapewnienia, z zachowaniem odpowiedniego wyprzedzenia w stosunku do planowanych dostaw Urządzeń, Obiektów wraz następującym wyposażeniem do uruchomienia Węzła:
   - powierzchnię kolokacyjną wraz z szafami telekomunikacyjnymi,

- zasilanie szaf w energię elektryczną,
- elementy pasywne umożliwiające budowę okablowania pomiędzy szafami,
- okablowanie stacyjne pomiędzy szafą a punktem koncentracji infrastruktury kablowej Obiektu oraz pomiędzy szafami,
- sieć szkieletową do komunikacji pomiędzy poszczególnymi węzłami OSE.

d) Zamawiający jest zobowiązany do uzyskania w terminach wynikających z Szczegółowego Harmonogramu Wdrożenia Węzła wszelkich niezbędnych zezwoleń i zgód umożliwiających prowadzenie instalacji i uruchomienia Urządzeń i Oprogramowania w Obiekcie.

e) Zamawiający jest zobowiązany do umożliwienia pracownikom Wykonawcy dostępu do Obiektu, w uzgodnionych godzinach, jednak nie krócej niż od 8.00 do 18.00 w Dniach roboczych oraz w szczególnych przypadkach w uzgodnionych przez Strony godzinach, a także dostęp do niezbędnych mediów (np. energia elektryczna).

f) Wykonawca jest zobowiązany do dostarczenia i instalacji Urządzeń i Oprogramowania wraz z licencjami oraz subskrypcjami niezbędnych do pełnego wdrożenia Infrastruktury bezpieczeństwa, w tym między innymi:
   - Wykonania Okablowania stacyjnego, łączącego ze sobą Urządzenia w obrębie szafy, zgodnie z Dokumentacją,
   - Zapewnienie kabli przyłączeniowych, do łączenia instalowanych Urządzeń ze sobą oraz z panelami połączeniowymi,
   - Zapewnienie osprzętu i materiałów instalacyjnych do montażu dostarczonych Urządzeń,
   - KVM over IP jeżeli będzie wymagany do zarządzania Infrastrukturą bezpieczeństwa.

g) Wykonawca dostarczy, w terminach wynikających ze Szczegółowego Harmonogramu Wdrożenia, Urządzenia i Oprogramowanie stanowiące kompletne wyposażenie Węzła Bezpieczeństwa, odpowiednio Centralnego lub Regionalnego, realizującego wszystkie założone funkcjonalności opisane w Załączniku nr 1 do Umowy, a następnie wykona prace instalacyjne w Obiekcie wskazanym przez Zamawiającego, w tym dokona montażu Urządzeń w szafach i okablowania

h) Wszystkie dostarczone Urządzenia zostaną przez Wykonawcę zainstalowane w szafach telekomunikacyjnych z zastosowaniem dedykowanych uchwytów mocujących, a następnie okablowane w sposób umożliwiający komunikację pomiędzy nimi, zgodnie z Projektem Technicznym.

i) Wykonawca dostarczy i zainstaluje kable połączeniowe, zapewniające połączenie pomiędzy Urządzeniami w tej samej szafie oraz pomiędzy Urządzeniami a panelem połączeniowym, w przypadku łączenia z Urządzeniami w innej szafie. Wykonawca ułoży wszystkie kable połączeniowe w sposób uporządkowany, z zastosowaniem dostarczonych przez siebie lub istniejących w szafie organizerów okablowania. Wykonawca przytwierdzi ułożone kable połączeniowe w sposób umożliwiający dostęp do poszczególnych Urządzeń w szafie, jak również w sposób umożliwiający wymianę uszkodzonych elementów Urządzeń (kart) bez konieczności deinstalacji okablowania.

j) Zainstalowane przez Wykonawcę kable połączeniowe zostaną w sposób czytelny oznaczone, a oznaczenie to zostanie udokumentowane w Dokumentacji Powykonawczej. Sposób oznaczania okablowania zostanie uzgodniony pomiędzy stronami w trybie roboczym.

k) Wykonawca po wykonaniu instalacji oraz podłączenia okablowania dokona podłączenia Urządzeń do zainstalowanych w szafach listew dystrybucji energii elektrycznej. Włączenie

Urządzeń do zasilania odbędzie się w oparciu o regulacje obowiązujące w zakresie podłączania odbiorników energii elektrycznej na terenie danego Obiektu. Pracownicy lub podwykonawcy Wykonawcy, realizujący podłączenie Urządzeń do zasilania, będą posiadali stosowne kwalifikacje.

l) Wykonawca wykona konfigurację dostarczonych Urządzeń i Oprogramowania zgodnie z uzgodnionym Projektem Technicznym. Zakres konfiguracji Urządzeń będzie obejmował pełen zakres Wdrożenia.

m) Wykonawca podłączy zainstalowane Urządzenia do dostarczonej w ramach innego projektu sieci telekomunikacyjnej OSE, realizując topologię Węzła zgodnie ze strukturą połączeń określoną w Rozdziale 3.2.

n) W trakcie prac instalacyjnych i konfiguracyjnych Wykonawca jest zobowiązany wysyłać Zamawiającemu cykliczne raporty z zaawansowania prac. prac. Raport musi zawierać informacje o stopniu zawansowania prac, planowanych pracach na kolejny okres oraz wskazywać ewentualne ryzyka i sposoby ich mitygacji. Raport będzie przekazywany podczas cyklicznych spotkań, o których mowa w pkt. b)

o) Zamawiający ma prawo uczestniczyć na każdym etapie prac instalacyjnych i konfiguracyjnych. W ramach uczestniczenia w pracach Wykonawca ma prawo m.in. kontrolować jakość wykonywanych prac instalacyjnych jak również dotrzymywanie zasad prowadzenia prac na Obiekcie.

p) Po zakończeniu prac wdrożeniowych Wykonawca przygotuje i przekaże do Zamawiającego Dokumentację Powykonawczą. Zakres dokumentacji powykonawczej został określony w Załączniku nr 6 do Umowy.

q) Zamawiający dostarczy platformę sprzętowo-programową do instalacji Oprogramowania System zarządzający o ile takie wymaganie będzie wynikać z Dokumentacji Technicznej.

r) Wykonawca zainstaluje i skonfiguruje wg Dokumentacji Technicznej Oprogramowanie System zarządzający. Wykonawca skonfiguruje Oprogramowanie wymienione w zdaniu poprzednim do współpracy z Urządzeniami.

s) Wykonawca będzie współpracował z Zamawiającym przy Integracji z systemami Zamawiającego w zakresie opisanym w Zapytaniu ofertowym.

t) Wykonawca przeprowadzi wspólnie z Zamawiającym Testy odbiorcze Węzła, w oparciu o zatwierdzony Plan testów.

u) Wykonawca zobowiązany jest zapewnić, aby wszystkie czynności odbiorcze, w tym również związane z uwzględnianiem uwag i zastrzeżeń Zamawiającego do Dokumentacji Powykonawczej zostały zakończone w terminach wynikających ze Szczegółowego Harmonogramu Wdrożenia Węzła.

3.9.2. Podział obowiązków stron przy realizacji Umowy

L.p.	Zadanie	Zamawiający	Wykonawca	Czas wykonania
1.	Podpisanie Umowy	x	x	
2.	Wyznaczenie Kierowników Projektu	x	x	2 dni
3.	Przygotowanie i przedstawienie do wypełnienia ankiety w zakresie HLD		x	

L.p.	Zadanie	Zamawiający	Wykonawca	Czas wykonania
4.	Wypełnienie ankiety w zakresie HLD wraz z konsultacjami	x		5 dni
5.	Przygotowanie Dokumentacji Technicznej w zakresie HLD i przekazanie do akceptacji		x	
6.	Akceptacja Dokumentacji Technicznej w zakresie HLD lub zgłoszenie uwag.	x		5 dni
7.	Przeprowadzenie instruktaży		x	
8.	Utrzymanie		x	
9.	Świadczenie gwarancji w okresie trwania umowy		x	
10.	Przekazanie listy uprawnionych przedstawicieli do dostępu zdalnego do systemu		x	
11.	Zapewnienie dostępu zdalnego uprawnionym przedstawicielom	x		
12.	Zapewnienie uprawnionym przedstawicielom Wykonawcy do urządzeń zainstalowanych w węzłach	x		

3.9.3. Podział obowiązków stron przy wdrożeniu Węzła

Wykonawca stworzy Szczegółowy Harmonogram Wdrożenia Węzła na podstawie następującego podziału obowiązków pomiędzy Strony:

L.p.	Zadanie	Zamawiający	Wykonawca	Czas wykonania
1.	Wydanie Polecenia Wdrożenia Węzła	x		
2.	Przygotowanie Szczegółowego Harmonogramu Wdrożenia Węzła		x	
3.	Przygotowanie i przedstawienie do wypełnienia ankiety w zakresie LLD		x	
4.	Wypełnienie ankiety w zakresie LLD wraz konsultacjami	x		5 dni
5.	Przygotowanie Dokumentacji Technicznej w zakresie LLD i przekazanie do akceptacji		x	
6.	Akceptacja Dokumentacji Technicznej w zakresie LLD lub zgłoszenie uwag	x		5 dni
7.	Przygotowanie i przedstawienie do akceptacji Planu Testów Odbiorczych		x	
8.	Weryfikacja i zatwierdzenie Planu Testów Odbiorczych lub zgłoszenie uwag	x		5 dni
9.	Przygotowanie Obiektów do instalacji Urządzeń zgodnie z Rozdziałem 11 ust. 3	x		60 dni od Polecenia wdrożenia Węzła
10.	Zgłoszenie gotowości dostawy Urządzeń		x	
11.	Potwierdzenie gotowości dostawy Urządzeń	x		2 dni

L.p.	Zadanie	Zamawiający	Wykonawca	Czas wykonania
12.	Dostawa i odbiór ilościowy	x	x	
13.	Przekazanie listy uprawnionych przedstawicieli do wstępu na obiekty, w których będą instalowane urządzenia		x	
14.	Zapewnienie dostępu uprawnionym przedstawicielom Wykonawcy.	x		3 dni
15.	Instalacja Urządzeń w szafach zgodnie z Rozdziałem 11 ust. 6		x	
16.	Podłączenie Urządzeń do zasilania i uziemienia		x	
17.	Uruchomienie Urządzeń		x	
18.	Konfiguracja Urządzeń		x	
19.	Zestawienie łączy szkieletowych do szafy	x		
20.	Dołączenie łączy szkieletowych do zainstalowanych urządzeń		x	
21.	Uczestniczenie w pracach instalacyjnych i wdrożeniowych	x		
22.	Zgłoszenie gotowości do Testów Odbiorczych		x	
23.	Testy Odbiorcze	x	x	2 tygodnie
24.	Przygotowanie dokumentacji powykonawczej		x	
25.	Akceptacja dostarczonej Dokumentacji, akceptacja wykonanych prac instalacyjnych węzła lub wniesienie uwag	x		5 dni
26.	Podpisanie Protokołu Odbioru Wstępnego	x	x	
27.	Stabilizacja		x	
28.	Zgłoszenie gotowości do Odbioru Końcowego		x	
29.	Weryfikacja poprawności zakończenia Okresu Stabilizacji lub wniesienie uwag	x		
30.	Odbiór Końcowy Węzła	x	x	
31.	Podpisanie Protokołu Odbioru Końcowego	x	x	

3.10. Integracje z systemami Zamawiającego

3.10.1. 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 -. System NG Firewall i System inspekcji ruchu SSL/TLS będą bazowały jedynie na adresacji IP przydzielonej do każdej ze szkół.

W przypadku podjęciu decyzji przez Zamawiającemu o konieczności wykorzystania informacji nt. tożsamości użytkowników na innych Systemach niż ADC i SWG, Oferowana Infrastruktura bezpieczeństwa musi umożliwiać Zamawiającemu rozbudowę mającą na celu dostosowanie Systemu NG Firewall i Systemu inspekcji ruchu SSL/TLS do obsługi tożsamości Użytkowników.

3.10.2. 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 Urządzeniami co najmniej poprzez protokół SSH) wystawianych przez System zarządzający dostarczony w ramach Infrastruktury Bezpieczeństwa. System dostarczony w ramach Infrastruktury bezpieczeństwa zostanie zintegrowany, na warunkach opisanych w Umowie, z 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 systemach dostarczonych w ramach Infrastruktury Bezpieczeństwa.

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

Oferowana Infrastruktura bezpieczeństwa musi umożliwiać Zamawiającemu automatyzację wyżej wymienionych procesów. Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanej przez Wykonawcę Infrastrukturze bezpieczeństwa.

3.10.3. System Fault Management

Wykonawca jest zobowiązany do integracji, na warunkach opisanych w Umowie, wszystkich Urządzeń z systemami Fault Management z wykorzystaniem protokołów SYSLOG i SNMP (w tym SNMP Trap). Szczegółowy zakres integracji zostanie doprecyzowany na etapie Projektu technicznego.

3.10.4. System Performance Management

Wykonawca jest zobowiązany do integracji, na warunkach opisanych w Umowie, wszystkich Urządzeń z systemami Performance Management z wykorzystaniem co najmniej protokołu SNMP, w zakresie monitorowania i pobierania co najmniej następujących danych:

a) Pesistent Conections
b) Current Throughput
c) CPS – new connections per second
d) CPU – Idle time
e) CPU – Percentage spent on processes in the user space
f) CPU – Percentage spent on process in the system space
g) Memory – Total Free
h) Memory – Total Real
i) Memory – Avail. Swap
j) Storage – disk usage
k) Obciążenie interfejsów sieciowych

3.10.5. System Inventory

Wykonawca jest zobowiązany do integracji, na warunkach opisanych w Umowie, wszystkich Urządzeń 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 urządzenia

b) Producent, model urządzenia
c) wersje oprogramowania
d) MAC adresy przypisane interfejsów sieciowych
e) Lista elementów składowych urządzenia tj. chassis, karty, interface'y, dyski, pamięć

Szczegółowy zakres integracji zostanie określony na etapie Projektu Technicznego.

3.10.6. System Config Management

Wykonawca jest zobowiązany do integracji, na warunkach opisanych w Umowie, wszystkich Urządzeń z systemem Config Management z wykorzystaniem co najmniej SNMP, bezpośredniej komunikacji z Urządzeniami co najmniej poprzez protokół SSH. Zakres integracji zakłada pobieranie przez system Config Management informacji dotyczących konfiguracji każdego z elementów Infrastruktury bezpieczeństwa i utrzymywanie go jako repozytorium aktualnej konfiguracji systemów.

Szczegółowy zakres integracji zostanie określony na etapie Projektu Technicznego.

3.10.7. System SWG

W szczególności Wykonawca we współpracy z dostawcą Systemu SWG i Zamawiającym wykona testy integracyjne mające na celu przetestowanie całego środowiska zainstalowanego w sieci Zamawiającego.

Szczegółowy zakres integracji zostanie określony po rozstrzygnięciu postępowania na System SWG.

3.10.8. System SIEM

Wykonawca jest zobowiązany do integracji, na warunkach opisanych w Umowie, wszystkich Urządzeń z systemem SIEM w zakresie przekazywania zdarzeń i przepływów do, wskazanego przez Zamawiającego, kolektora SIEM. Zamawiający zakłada, że czas buforowania zdarzeń przed przekazaniem ich do Systemu SIEM nie będzie dłuższy niż 48h.

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

3.11. Warunki dostawy

a) Wykonawca będzie dostarczał Urządzenia do każdego Węzła Bezpieczeństwa, odpowiednio Centralnego, Regionalnego oraz Laboratoryjnego, realizujących wszystkie opisane w wymaganiach funkcje, zapewniające określoną funkcjonalność oraz ilość portów o zdefiniowanych przepustowościach.

b) Dostarczane Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed dniem dostawy, w oryginalnych opakowaniach transportowych producenta. Zamawiający dopuszcza rozpakowanie urządzeń przez Wykonawcę w celu przeprowadzenia przez Wykonawcę testu sprawności Urządzeń i wykonania ich konfiguracji wstępnej. Po dostarczeniu

Urządzeń do miejsca ich instalacji i wykonaniu prac instalacyjnych Wykonawca jest zobowiązany do usunięcia opakowań transportowych na własny koszt.

c) Każde z dostarczonych urządzeń, musi mieć zainstalowane rekomendowane do stosowania przez producentów Urządzeń wersje Oprogramowania. Ww. Oprogramowanie nie może być wersją wytworzoną jedynie na potrzeby niniejszego postepowania, której używania nie rekomenduje się pozostałym użytkownikom Urządzeń. Oprogramowanie w dostarczonej wersji musi posiadać wsparcie techniczne producenta dostarczanych Urządzeń.

d) Wszystkie dostarczane Urządzenia, należące do jednej rodziny Urządzeń, będą wyposażone w tą samą (identyczną) wersję Oprogramowania. W przypadku gdyby producent urządzeń zmienił rekomendowaną wersje oprogramowania dla danej rodziny Urządzeń Wykonawca powiadomi o tym Zamawiającego, a następnie uzgodni z Zamawiającym wersję Oprogramowania, która będzie instalowana na Urządzeniach w ramach kolejnych dostaw.

e) Każde z dostarczonych Urządzeń, stanowiących elementy składowe poszczególnych Węzłów, będzie pochodzić z oficjalnego kanału dystrybucyjnego producenta, zapewniającego w szczególności realizację uprawnień gwarancyjnych oraz autoryzowanego serwisu. Na żądanie Zamawiającego Wykonawca dostarczy w ciągu 14 dni oficjalne potwierdzanie tego faktu wystawione przez producenta Urządzeń.

f) Dostarczone Urządzenia w dniu złożenia oferty nie będą znajdować się na liście sprzętu przeznaczonego do wycofania z produkcji lub sprzedaży na terenie Polski.