

OPIS PRZEDMIOTU ZAMÓWIENIA

(po zmianach z dnia 17.02.2022 r.)

Przedmiot zamówienia: Dostawa do siedziby Zamawiającego fabrycznie nowych, nieużywanych urządzeń sieciowych wraz z konfiguracją, szkoleniem administratorów oraz niezbędnymi licencjami.

Tabela nr 1

Lp.	Charakterystyka, parametry techniczne, cechy funkcjonalne przedmiotu zamówienia	
I	Zarządzalny przełącznik L2 służący do podłączenia urządzeń operatora do klastra HA głównych firewall-i FortiGate 200F (model przykładowy: FortiSwitch 124F) – 1 szt.	
1.	Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:
2.	Parametry fizyczne platformy	a) Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. b) Zasilanie AC 230V. c) Maksymalny pobór mocy: 30 W. d) Minimalny zakres temperatury pracy: 0-40°C.
3.	Interfejsy sieciowe - wymagania minimalne	Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 24 porty GE RJ-45. b) 4 porty 10 GE SFP+.

4.	Zarządzanie	<ul style="list-style-type: none"> a) Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. b) Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). c) Wsparcie dla SNMP w wersjach 1-3 d) Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. e) Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. f) Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. g) Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). h) Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. i) Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. j) Automatycznie wykonywane rewizje konfiguracji.
5.	Parametry wydajnościowe	<ul style="list-style-type: none"> a) Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. b) Tablica adresów MAC o pojemności co najmniej 32k wpisów. c) Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6.	Wymagane funkcje	<ul style="list-style-type: none"> a) Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. b) Obsługa Jumbo Frames. c) Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). d) Agregacja portów zgodna ze standardem 802.3ad. e) Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. f) Port-mirroring. g) Uwierzytelnianie 802.1x na poziomie portu. h) Uwierzytelnianie 802.1x w oparciu o adres MAC. i) W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). j) W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. k) W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. l) Obsługa protokołu sFlow.
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego	<ol style="list-style-type: none"> 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf).

	zarządzania / NAC	<p>Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ol style="list-style-type: none">Centralne zarządzanie konfiguracją urządzeniaAktualizacja oprogramowania realizowana z systemu centralnego zarządzaniaCentralne zarządzanie sieciami VLAN.Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'uRozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.Automatyczna detekcja i rekomendacje konfiguracji.Przesyłanie logów na zewnętrzny serwer syslog.Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.Obsługa białych i czarnych list adresów MAC.Wykrywanie aplikacji komunikujących się w sieci. <ol style="list-style-type: none">Musi być możliwe redundantne połączenie z elementami zarządzającymi.W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ol style="list-style-type: none">System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
9.	Gwarancja oraz wsparcie	<p>System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p>
10.	Rozszerzone wsparcie serwisowe	<ol style="list-style-type: none">System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent

		<p>winien przedłożyć dokumenty:</p> <ol style="list-style-type: none"> a) Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
II	Główne firewall-e NGFW wykorzystane do podłączenia ITWL do sieci Internet (model przykładowy: FortiGate 200F) – 2 szt.	
1.	Wymagania ogólne	<ol style="list-style-type: none"> 1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 3. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. 4. System musi wspierać IPv4 oraz IPv6 w zakresie: <ol style="list-style-type: none"> a) Firewall. b) Ochrony w warstwie aplikacji. c) Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN. 5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

3.	Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none">1. System realizujący funkcję Firewall musi dysponować minimum:<ol style="list-style-type: none">a) 18 portami Gigabit Ethernet RJ-45.b) 8 gniazdami SFP 1 Gbps.c) 4 gniazdami SFP+ 10 Gbps.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.4. System musi być wyposażony w zasilanie AC.
4.	Parametry wydajnościowe	<ol style="list-style-type: none">1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę.2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps.4. Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.
5.	Funkcje Systemu Bezpieczeństwa	<ol style="list-style-type: none">1. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:<ol style="list-style-type: none">a) Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.b) Kontrola Aplikacji.c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.d) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.e) Ochrona przed atakami - Intrusion Prevention System.f) Kontrola stron WWW.g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.h) Zarządzanie pasmem (QoS, Traffic shaping).i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).j) Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu

		<p>client-to-site.</p> <ul style="list-style-type: none">k) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.l) Analiza ruchu szyfrowanego protokołem SSH.m) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
6.	Polityki, Firewall	<ul style="list-style-type: none">1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<ul style="list-style-type: none">a) Translację jeden do jeden oraz jeden do wielu.b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.<ul style="list-style-type: none">a) Amazon Web Services (AWS).b) Microsoft Azurec) Google Cloud Platform (GCP).d) OpenStack.e) VMware NSX.f) Nutanix

7.	Połączenia VPN	<ol style="list-style-type: none"> 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: <ol style="list-style-type: none"> a) Wsparcie dla IKE v1 oraz v2. b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) Obsługa protokołu Diffie-Hellman grup 19 i 20. d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tunel e) pomiędzy SPOKE w topologii HUB and SPOKE. f) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. g) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. h) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. i) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. j) Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: <ol style="list-style-type: none"> a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwi realizację połączeń IPSec VPN lub SSL VPN.
8.	Routing i obsługa łączy WAN	<ol style="list-style-type: none"> 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: <ol style="list-style-type: none"> a) Routingu statycznego. b) Policy Based Routingu. c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
9.	Funkcje SD-WAN	<ol style="list-style-type: none"> 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
10.	Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

		<ol style="list-style-type: none"> 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
12.	Ochrona przed atakami	<ol style="list-style-type: none"> 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
13.	Kontrola aplikacji	<ol style="list-style-type: none"> 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
14.	Kontrola WWW	<ol style="list-style-type: none"> 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla

		<p>adresów URL.</p> <ol style="list-style-type: none">5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
15.	Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none">1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<ol style="list-style-type: none">a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.
16.	Zarządzanie	<ol style="list-style-type: none">1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnił dokumentację.6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
17.	Logowanie	<ol style="list-style-type: none">1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

		<ol style="list-style-type: none">2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.4. Musi istnieć możliwość logowania do serwera SYSLOG.
18.	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: a) ICSA lub EAL4 dla funkcji Firewall.
19.	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 60 miesięcy.
20.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
21.	Rozszerzone wsparcie serwisowe AHB/SOS	<ol style="list-style-type: none">1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:<ol style="list-style-type: none">a) Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).b) Certyfikat ISO 9001 podmiotu serwisującego.

III	Zarządzalne światłowodowe przełączniki L3 wykorzystane w sieci szkieletowej (model przykładowy: FortiSwitch FS-1024D/FS-1024E) – 2 szt.	
1.	Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:
2.	Parametry fizyczne platformy	<ol style="list-style-type: none"> 1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Wymagany - z możliwością wymiany w czasie pracy - redundanthy zasilacz. 4. Maksymalny pobór mocy: 140 –180W. 5. Minimalny zakres temperatury pracy: 0-40°C.
3.	Interfejsy sieciowe - wymagania minimalne	Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: 24 porty 10 GE SFP+.
4.	Zarządzanie	<ol style="list-style-type: none"> 1. Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania. 2. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. 3. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 4. Wsparcie dla SNMP w wersjach 1-3 5. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 6. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 7. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 8. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 9. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 10. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 11. Automatycznie wykonywane rewizje konfiguracji.
5.	Parametry wydajnościowe	<ol style="list-style-type: none"> 1. Przepustowość urządzenia - min. 480 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 712 Mpps.

		<ol style="list-style-type: none"> 2. Tablica adresów MAC o pojemności co najmniej 64k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6.	Wymagane funkcje	<ol style="list-style-type: none"> 1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames. 3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Agregacja portów zgodna ze standardem 802.3ad. 5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. 6. Obsługa routingu statycznego. 7. Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP. 8. Port-mirroring. 9. Uwierzytelnianie 802.1x na poziomie portu. 10. Uwierzytelnianie 802.1x w oparciu o adres MAC. 11. W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN). 12. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 13. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. 14. Obsługa protokołu sFlow.
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<ol style="list-style-type: none"> 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: <ol style="list-style-type: none"> a) Centralne zarządzanie konfiguracją urządzenia. b) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania. c) Centralne zarządzanie sieciami VLAN. d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u. e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. g) Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. h) Automatyczna detekcja i rekomendacje konfiguracji. i) Przesyłanie logów na zewnętrzny serwer syslog. j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. k) Obsługa białych i czarnych list adresów MAC. l) Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

		3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
9.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
10.	Rozszerzone wsparcie serwisowe	<ol style="list-style-type: none"> 1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty: <ol style="list-style-type: none"> a) Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
IV	Zarządzalne miedziane przełączniki L3 wykorzystane w sieci szkieletowej do podłączenia użytkowników i urządzeń w obrębie tego samego budynku oraz sieci MGMT (model przykładowy: FortiSwitch 448E) – 2 szt.	
1.	Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:
2.	Parametry fizyczne platformy	<ol style="list-style-type: none"> 1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Wbudowany redundantny zasilacz.

		<ol style="list-style-type: none"> 4. Maksymalny pobór mocy: 50 W. 5. Minimalny zakres temperatury pracy: 0-50°C.
3.	Interfejsy sieciowe - wymagania minimalne	<ol style="list-style-type: none"> 1. Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: <ol style="list-style-type: none"> a) 48 porty GE RJ-45. b) 4 porty 10 GE SFP+.
4.	Zarządzanie	<ol style="list-style-type: none"> 1. Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania. 2. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. 3. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 4. Wsparcie dla SNMP w wersjach 1-3 5. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 6. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 7. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 8. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 9. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 10. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 11. Automatycznie wykonywane rewizje konfiguracji.
5.	Parametry wydajnościowe	<ol style="list-style-type: none"> 1. Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 32 k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

6.	Wymagane funkcje	<ol style="list-style-type: none">1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.2. Obsługa Jumbo Frames.3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).4. Agregacja portów zgodna ze standardem 802.3ad.5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.6. Wsparcie dla Private VLAN.7. Obsługa routingu statycznego.8. Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.9. Port-mirroring.10. Uwierzytelnianie 802.1x na poziomie portu.11. Uwierzytelnianie 802.1x w oparciu o adres MAC.12. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).13. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.14. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.15. Obsługa protokołu sFlow.
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<ol style="list-style-type: none">1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:<ol style="list-style-type: none">a) Centralne zarządzanie konfiguracją urządzeniab) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzaniac) Centralne zarządzanie sieciami VLAN.d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'ue) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.g) Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.h) Automatyczna detekcja i rekomendacje konfiguracji.i) Przesyłanie logów na zewnętrzny serwer syslog.j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.k) Obsługa białych i czarnych list adresów MAC.l) Wykrywanie aplikacji komunikujących się w sieci.2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

		3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ol style="list-style-type: none"> 1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. 2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
9.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
10.	Rozszerzone wsparcie serwisowe	<ol style="list-style-type: none"> 1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty: <ol style="list-style-type: none"> a) Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
V	10GBASE-SR SFP+ 850nm 300m DOM LC MMF Transceiver Module Wkładki światłowodowe do FortiGate 200F oraz FortiSwitch 448E oraz FortiSwitch 1024D (model przykładowy: FS-TRAN-SFP+SR) – 22 szt.	
VI	Kable światłowodowe duplex typ LC MMF 1.5m (model przykładowy: Patchcord FX) – 8 szt.	
VII	Kable światłowodowe duplex typ LC MMF 0.5m (model przykładowy: Patchcord FX) – 4 szt.	
VIII		

	Kable miedziane kat.7 1m (model przykładowy: Patchcord S/FTP) – 2 szt.
IX	Kable miedziane kat.7 0.5m (model przykładowy: Patchcord S/FTP) – 2 szt.
X	Prace wdrożeniowe
1.	<ol style="list-style-type: none">1. Audyt bieżącej konfiguracji,2. przygotowanie koncepcji wdrożenia i migracji usług wraz z Zamawiającym,3. montaż i instalacja urządzeń w siedzibie oraz w szafach rackowych należących do Zamawiającego,4. konfiguracja nowego rozwiązania z zachowaniem ciągłości działania obecnej infrastruktury klienta,5. testy konfiguracji i funkcjonalne,6. przełączenie usług na nową infrastrukturę,7. dokumentacja powykonawcza obejmująca opis podstawowych parametrów dostarczonego rozwiązania,8. szkolenie z obsługi i konfiguracji wdrożonych urządzeń,9. prace będą prowadzone w dni robocze w godzinach 7-16 w lokalizacji w Warszawie w siedzibie klienta,10. Modernizacja infrastruktury sieciowej oraz wdrożenia etapów 1+2 które powinny być realizowane łącznie (WAN+LAN):<ol style="list-style-type: none">a) Etap 1 WAN + Firewall : projekt, wdrożenie, szkolenie, dokumentacja,b) Etap 2 LAN: projekt, wdrożenie, szkolenie, dokumentacja.

1. Warunki realizacji zamówienia

Zamawiający wymaga, aby Wykonawca w zakresie realizacji zamówienia:

- a) dostarczył na własny koszt i ryzyko przedmiot zamówienia do siedziby Instytutu Technicznego Wojsk Lotniczych, ul. Księcia Bolesława 6, 01-494 Warszawa i przeprowadził rozładunek przedmiotu zamówienia w miejscu wskazanym przez Zamawiającego,
- b) dostarczył cały przedmiot zamówienia fabrycznie nowy oraz nieużywany,
- c) dostarczył wraz z przedmiotem zamówienia instrukcje obsługi w języku polskim lub angielskim,
- d) przeprowadził wdrożenie, konfigurację dostarczonego przedmiotu zamówienia oraz szkolenie administratorów.

2. Warunki prac wdrożeniowych

Zamawiający wymaga, aby Wykonawca w ramach prac wdrożeniowych wykonał:

- a) audyt bieżącej konfiguracji,
- b) przygotowanie koncepcji wdrożenia i migracji usług wraz z Zamawiającym,
- c) montaż i instalacja urządzeń w siedzibie oraz w szafach rackowych należących do Zamawiającego,

- d) konfiguracje nowego rozwiązania z zachowaniem ciągłości działania obecnej infrastruktury klienta,
- e) testy konfiguracji i funkcjonalne,
- f) przełączenie usług na nową infrastrukturę,
- g) dokumentację powykonawczą obejmującą opis podstawowych parametrów dostarczonego rozwiązania,
- h) szkolenie z obsługi i konfiguracji wdrożonych urządzeń,
- i) prace będą prowadzone w dni robocze w godzinach 7-16 w lokalizacji w Warszawie w siedzibie Zamawiającego,
- j) modernizacje infrastruktury sieciowej oraz wdrożenia etapów 1+2 które powinny być realizowane łącznie (WAN+LAN):
 - Etap 1 WAN + Firewall : projekt, wdrożenie, szkolenie, dokumentacja,
 - Etap 2 LAN: projekt, wdrożenie, szkolenie, dokumentacja.

3. Warunki gwarancji serwisowej

Zamawiający wymaga, aby Wykonawca w ramach gwarancji serwisowej zapewnił:

- a) świadczenie gwarancji serwisowej na okres 60 miesięcy,
- b) świadczenie serwisu gwarancyjnego przez podmiot serwisujący który posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych,
- c) dostarczenie licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów zawierających: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analizy typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy,
- d) naprawę lub wymianę urządzenia w przypadku jego wadliwości oraz dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7,
- e) rozszerzone wsparcie techniczne dla systemu gwarantujące dostawę sprzętu zastępczego do czasu usunięcia awarii 24x7xNBD tj. udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu od momentu potwierdzenia zasadności zgłoszenia, realizowane przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres trwania serwisu gwarancyjnego,
- f) przyjmowanie zgłoszeń serwisowych w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim w trybie 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina, reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym,
- g) przeglądy serwisowe przedmiotu zamówienia jeśli takie są niezbędne dla prawidłowego działania przedmiotu zamówienia i/lub dla utrzymania obsługi gwarancyjnej.