Załącznik nr 1.3 do SIWZ
Sprawa numer: 10/SISP-2/PN/2014

Opis Przedmiotu Zamówienia – część 3 – zmieniony dnia 06 – 06 – 2014 r.

Przedmiotem zamówienia jest budowa sieci WiFi w Urzędach Statystycznych oraz w Głównym Urzędzie Statystycznym.

A. Dostawę oraz wdrożenie infrastruktury sieci bezprzewodowej w Urzędach Statystycznych oraz w Głównym Urzędzie Statystycznym …… str. 2
B1. Dostawę i wdrożenie Systemu Zarządzania Siecią LAN/WLAN …….. str. 31
B2. Dostawę Systemu Zarządzania Bezpieczeństwem Dostępu do Sieci LAN/WLAN …… str. 38
C. Dostawę przełącznika modularnego, rdzeniowego w Głównym Urzędzie Statystycznym …… str. 50

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

A. Dostawa oraz wdrożenie infrastruktury sieci bezprzewodowej w Urzędach Statystycznych oraz w Głównym Urzędzie Statystycznym

I. Opis Środowiska Zamawiającego

Sieć LAN w Głównym Urzędzie Statystycznym zbudowania jest z przełączników warstwy 3 oraz warstwy 2. Podzielona jest na następujące segmenty:

1. Dostępu do Internetu.

   Strefa ta składa się z dwóch łączy do niezależnych operatorów, dwóch routerów, dwóch przełączników warstwy drugiej i systemu IPS.

2. Sieci WAN.

   W skład tej strefy wchodzą dwa łącza do sieci WAN, dwa routery i system IPS.

3. Sieci LAN GUS.

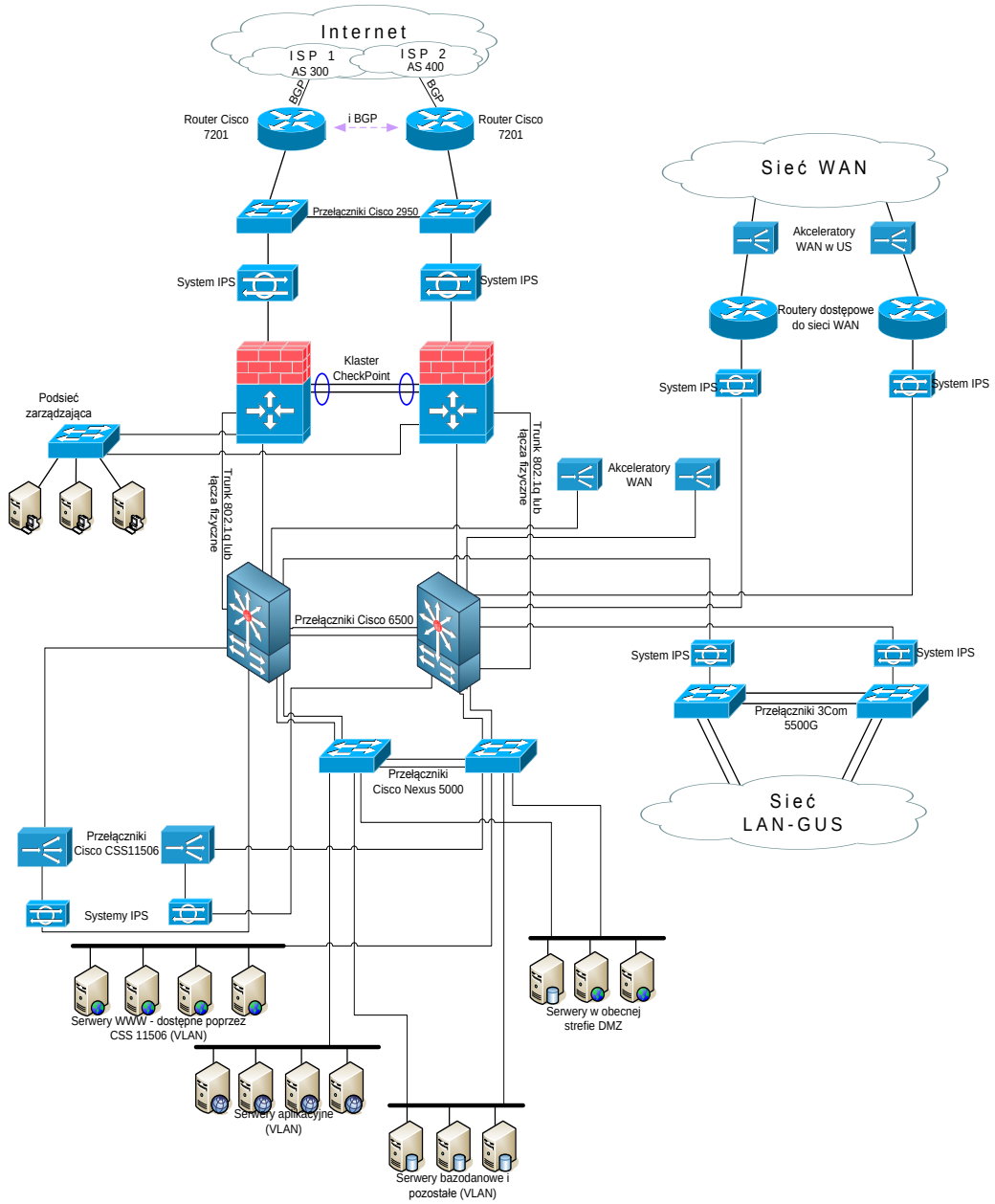
   Do strefy należą wszystkie zasoby znajdujące się w sieci LAN GUS: 50 przełączników dostępowych, 2 przełączniki agregacyjne oraz komputery, laptopy, drukarki, urządzenia wielofunkcyjne.

4. Data Center.

   W skład strefy wchodzą cztery DMZ-y, serwery aplikacyjne, serwery bazodanowe, serwery BackOffice, przełączniki CSS, sondy IPS. Logicznie strefa ta jest podzielona na kilka podsieci, a ruch ze strefami DMZ jest kontrolowany przez system Check Point. Przełącznikami szkieletowymi są dwa urządzenia Cisco Catalyst 6500. Przełącznikami agregującymi są urządzenia Cisco Nexus 5148 oraz Nexus 5548, warstwę dostępową dla serwerów stanowią przełączniki Cisco Catalyst 2960G. Poniżej schemat sieci w GUS, w której zostanie zbudowana sieć WiFi .

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji



Sieci LAN w Urzędach Statystycznych są w większości zbudowane z przełączników warstwy 2. Dominującą topologią są topologie gwiazdy z najszybszym przełącznikiem umieszczonym centralnie i podłączonymi do niego pozostałymi urządzeniami. Do przełącznika podłączone są routery, serwery oraz urządzenia współdzielone. W przeważającej części urządzenia sieciowe nie wpierają technologii PoE, w wielu z nich nie ma możliwości wdrożenia jakichkolwiek mechanizmów bezpieczeństwa czy tez zarządzania jakością usług QoS, sieci nie są podzielone na VLAN-y.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

W poniższej tabeli znajduje się wykaz lokalizacji (Urzędów Statystycznych i Głównego Urzędu Statystycznego), w których zostanie wdrożona sieć WiFi.

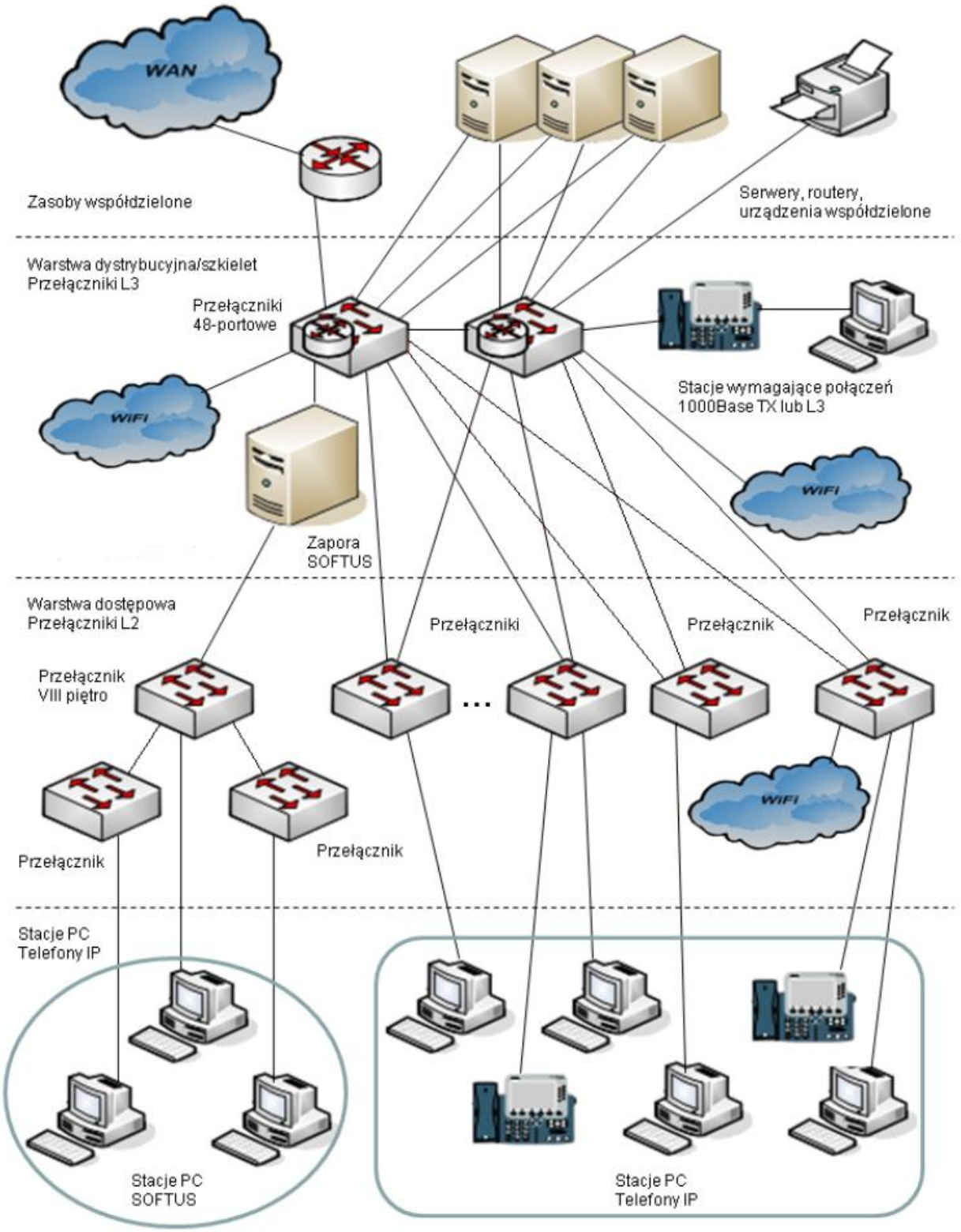
Tabela 1 Lokalizacje dla budowy sieci WiFi

Lokalizacja	Kod	Adres
Białystok	15-959	Krakowska 13
Bydgoszcz	85-066	Konarskiego 1/3
Gdańsk	80-434	Danusi 4
Katowice	40-158	Owocowa 3
Kielce	25-369	Wróblewskiego 2
Kraków	31-223	Wyki 3
Lublin	20-068	Leszczyńskiego 48
Łódź	93-176	Suwalska 29
Olsztyn	10-959	Kościuszki 78/82
Opole	45-064	ks. Kołłątaja 5B
Poznań	60-959	Wojska Polskiego 27/29
Rzeszów	35-002	Jana III Sobieskiego 10
Szczecin	70-530	Jana Matejki 22
Warszawa	02-134	1 Sierpnia 21
Wrocław	50-950	Oławska 31
Zielona Góra	65-954	Spokojna 1
Warszawa GUS	00-925	Niepodległości al. 208
Radom	26-600	Planty 39/45

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

Schemat docelowej struktury sieci LAN w US



BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

II. Wymagania ogólne

1. Sprzęt dostarczony w ramach realizacji Umowy będzie sprzętem fabrycznie nowym , wyprodukowanym nie wcześniej niż na 6 miesięcy od daty dostarczenia urządzeń.
2. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu potwierdzający, że oprogramowanie zawarte w dostarczonym sprzęcie jest licencjonowane na Zamawiającego.
3. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu potwierdzający zarejestrowanie kontraktu serwisowego na dostarczone urządzenia.
4. Wymagane jest dostarczenie wraz z dostawę urządzeń , szczegółowej dokumentacji technicznej producenta oferowanych produktów potwierdzającej spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia.

III. Wymagania w zakresie budowy sieci bezprzewodowej w Urzędach Statystycznych oraz Głównym Urzędzie Statystycznym

1. Zapewnienie wydajnej obsługi wielu klientów jednocześnie.
2. Podział na dwie sieci: produkcyjną i gościnną.
3. Zapewnienie bezpieczeństwa użytkowników oraz własnej infrastruktury IT – np. wykrywanie obcych i/lub wrogich punktów dostępowych.
4. Zapewnienie autoryzacji i rozliczania użytkowników – zaimplementowanie protokołu 802.1x. Autoryzacja użytkowników może następować przy pomocy bazy danych wprowadzonej przez administratora do kontrolera lub też poprzez protokół LDAP, RADIUS – dzięki czemu możliwa będzie integracja np. z Microsoft Activ Directory lub usługami 802.1X. Uwierzytelnienie w sieci gości powinno odbywać się poprzez tzw. „captive portal” – użytkownik łączący się z siecią będzie low serowani do strony WWW, na której musi się zautoryzować. Autoryzacja nastąpi przy pomocy nazwy użytkownika i hasła, hasło powinno być jednorazowe o limitowanym czasie ważności. Na podstawie przeprowadzonej autoryzacji użytkownik zostanie przypisany do określonego VLAN-u oraz uzyska określone uprawienia w sieci.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

5. Zapewnienie kontroli dostępu w wydzielonych wirtualnych strefach: np. dostęp dla gości powinien być ograniczony do dostępu internetowego, pracownicy tymczasowi powinni dodatkowo posiadać dostęp do poczty elektronicznej i wybranych serwisów intranetowych, uprawnienia pracowników powinny pokrywać się z uprawnieniami, jakie posiadają w tradycyjnej sieci, a autoryzacja powinnam odbywać się przy użyciu hasła Active Directory.
6. Centralizacja zarządzania i diagnostyki punktów dostępowych.

IV. Wymagania dla Punktów Dostępowych sieci bezprzewodowej

Architektura średnich i dużych sieci WiFi bazuje na dwu elementach: punktach dostępowych (AP) oraz kontrolerach. Pojedynczy punkt dostępowy zapewnia łączność WiFi w swoim otoczeniu, może też realizować wybrane funkcje administracyjne, kontroler służy do zarządzania Access Point-ami i realizacji funkcji bezpieczeństwa, autoryzacji użytkowników, realizacji roamingu, itp.

1. Obsługa standardów 802.11a/b/g/n/ l
   a. Obsługa MIMO – min. 3x3:3
   b. Obsługa kanałów 20 i 40 MHz dla 802.11n
   c. Obsługa kanałów 20, 40 i 80 MHz dla 802.11ac
   d. Obsługa prędkości PHY do 1,3 Gbps
   e. Obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
   f. Obsługa TxBF (transmitbeamforming) dla klientów 802.11a/g/n/ l
2. Obsługa szerokiego zakresu kanałów radiowych:
   a. Dla zakresu 2.4 GHz: min. 13 kanałów
   b. Dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów
   c. Dla zakresu 5GHz (low ser UNII-2): min. 8 kanałów
3. Konfigurowalna moc nadajnika
   a. Dla zakresu 2.4 GHz:do 100 mW
   b. Dla zakresu 5GHz (UNII-1 i UNII-2): do 150 mW
   c. Dla zakresu 5GHz (low ser UNII-2): do 150 mW

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

4. Zgodność z protokołem CAPWAP (RFC 5415) lub równoważnym, zarządzanie przez kontroler WLAN z funkcjonalnościami:
   a. Automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
   b. Optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
   c. Obsługa min. 16 BSSID
   d. Definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
   e. Współpraca z systemami IDS/IPS
   f. Uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – funkcjonalność 802.11w lub równoważna
   g. Obsługa trybu pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN)
   h. Jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IPS)
   i. Obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
   j. Obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – funkcjonalność 802.11r lub równoważna
   k. Obsługa mechanizmów QoS:
      i) shaping/ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik
      ii) obsługa WMM, TSPEC, U-APSD
   l. Współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne
   m. Wbudowany suplikant 802.1x – możliwość uwierzytelnienia AP do infrastruktury sieciowej

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

5. Możliwość pracy autonomicznej po wymianie oprogramowania – zmiana trybu pracy musi być bezkosztowa w okresie trwania gwarancji
   a. Zarządzanie przez HTTPS, SSH, dedykowany port szeregowy, SNMP
   b. Obsługa min. 16 SSID
   c. Współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)
   d. Obsługa WPA/WPA2, 802.1x (z możliwością tworzenia lokalnej bazy użytkowników)
   e. Obsługa mechanizmów QoS (WMM, priorytetyzacja) i wsparcie dla VoWLAN
   f. Obsługa trybów AP, low se, bridge
   g. Konfiguracja polityk bezpieczeństwa per SSID
   h. Możliwość filtrowania ruchu (w oparciu o MAC, adresy i protokoły IP, porty TCP/UDP)
   i. Uwierzytelnianie ruchu kontrolnego 802.11
   j. Obsługa szybkiego roamingu pomiędzy punktami dostępowymi
   k. Możliwość eksportu logów z wykorzystaniem SYSLOG
6. Zintegrowany moduł analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz) lub dedykowany punkt dostępowy realizujący taką funkcjonalność
   a. Dokładność analizy (kwant próbkowania) max. 200 kHz
   b. Zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych
   c. Automatyczne wykrywanie i klasyfikacja źródeł interferencji (bluetooth, DECT, urządzenia Mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.)
   d. Możliwość wizualizacji wyników analizy na stacji roboczej klasy PC (FFT, gęstość widma, spektrogram, zajętość kanałów, poziom mocy sygnałów) w czasie rzeczywistym
   e. Współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego
7. Interfejs Gigabit Ethernet (100/1000)
8. Zróżnicowane możliwości zasilania:

a. Zasilacz sieciowy 230V AC

b. Zasilanie przez skrętkę Ethernet w sposób zapewniający pełną wydajność (802.3af lub 802.3at)

9. Anteny zintegrowane o zysku przynajmniej 2 dBi dla pasma 2,4 GHz oraz 4,5 dBi dla pasma 5 GHz

10. Obudowa przystosowana do warunków pracy w pomieszczeniach biurowych (5 – 35oC), o niskim profilu (nie więcej niż 6 cm)

11. Diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji

12. Wraz z punktem dostępowym do sieci bezprzewodowej należy dostarczyć: licencję do specjalizowanych przełączników sieci LAN/WAN lub równoważnie kontrolerów sieci bezprzewodowej.

V. Wymagania dla przełącznika sieci LAN/WLAN (pełniącego rolę urządzenia szkieletowego w Urzędach Statystycznych)

1. Przełącznik stakowalny wyposażony w 48 portów 10/100/1000BaseT zgodnych ze standardem IEEE 802.3at (POE+)

2. Minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco” (ang. Hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:

   a. Minimum 4-portowy moduł Gigabit Ethernet z gniazdami SFP

   b. Minimum 2-portowy moduł 10Gigabit Ethernet SFP+,

   c. Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-SX oraz 1000Base-LX zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10Gbase-SR, 10Gbase-LR, 10Gbase-LRM, 10Gbase-ER oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX)

3. Możliwość stakowania z zapewnieniem następujących parametrów:

   a. Przepustowość w ramach stosu min. 320Gb/s

   b. Minimum 8 urządzeń w stosie

   c. Zarządzanie poprzez jeden adres IP

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

d. Możliwość tworzenia połączeń Cross-Stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad

4. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów
5. Urządzenie musi wyposażone w redundantne i wymienne zasilacze prądu przemiennego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania
6. Zainstalowane zasilacze muszą zapewniać min. 800W dla PoE przy pracy w trybie redundantnym
7. Obsługa low ser IEEE 802.3az Energy Efficient Ethernet
8. Szybkość przełączania minimum 130Mpps dla pakietów 64-bajtowych
9. Minimum 2GB pamięci DRAM i 2GB pamięci flash
10. Obsługa minimum:
    a. 1.000 sieci VLAN
    b. 32.000 adresów MAC
    c. 24.000 tras Ipv4
11. Usługi bezprzewodowe
    a. Przełącznik musi posiadać wbudowaną funkcjonalność kontrolera sieci bezprzewodowej WiFi o poniższych wymaganiach:
        i) Centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415) lub równoważnym, w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym, mobilnością i jakością transmisji
        ii) Przepustowość dla sieci WiFi nie mniejsza niż 20Gb/s
        iii) Skalowalność do obsługi minimum 50 punktów dostępowych – licencje na odpowiednią ilość punktów dostępowych będą dostarczone w ramach niniejszego przetargu
    b. Zarządzanie pasmem radiowym punktów dostępowych:
        i) automatyczna adaptacja do zmian w czasie rzeczywistym

ii) optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
iii) dynamiczne przydzielanie kanałów radiowych
iv) wykrywanie, eliminacja i unikanie interferencji
v) równoważenie obciążenia punktów dostępowych
vi) automatyczna dystrybucja klientów pomiędzy punkty dostępowe
vii) mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych

c. Mapowanie SSID do segmentów VLAN w sieci przewodowej

i) 1:1
ii) 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
iii) tunelowanie ruchu klientów do kontrolera

d. Obsługa mechanizmów bezpieczeństwa:

i) 802.11i, WPA2, WPA
ii) 802.1X z EAP (PEAP, EAP-TLS, EAP-FAST)
iii) obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, LDAP, wbudowana lokalna baza użytkowników
iv) możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID
v) możliwość profilowania użytkowników:
   (1) przydział sieci VLAN
   (2) przydział list kontroli dostępu (ACL)
vi) uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509
vii) obsługa list kontroli dostępu (ACL)
viii) wykrywanie i dezaktywacja obcych punktów dostępowych
ix) wbudowany system IDS wykrywający typowe ataki na sieci bezprzewodowe (fake AP, netstumbler, deathentication)
x) współpraca z systemami IDS/IPS
xi) ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego i ruchu użytkowników

e. Obsługa ruchu unicast i multicast

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

i) optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
ii) obsługa konwersji ruchu multicast do unicast

f. Obsługa mobilności (roaming-u) użytkowników (L2 i L3)

g. Obsługa mechanizmów QoS

i) 802.1p,
ii) WMM, Tspec,
iii) ograniczanie pasma per użytkownik

h. Obsługa dostępu gościnnego:

i) przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony)
ii) możliwość kreowania użytkowników z określeniem czasu ważności konta

i. Praca w trybie HA w oparciu o stos opisywanych urządzeń, jeśli do poprawnej pracy w trybie HA wymagane są dodatkowe licencje, to należy je dostarczyć

j. Analiza ruchu pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji w warstwie 7

k. Mechanizmy pozwalające na dezaktywację modułów radiowych w określonych godzinach w celu redukcji poboru energii przez system

l. Zarządzanie przez CLI, HTTPS, SNMPv3, SSH, port konsoli szeregowej

12. Oprogramowanie/funkcjonalność

a. Obsługa protokołu NTP

b. Obsługa IGMPv1/2/3

c. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 128 instancji protokołu STP

d. Obsługa protokołu LLDP i LLDP-MED

e. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

f. Możliwość uruchomienia funkcji serwera DHCP

13. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Minimum 4 poziomy dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    g. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
    h. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    i. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
14. Wsparcie następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:
    a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    b. Implementacja co najmniej 4 kolejek dla ruchu wyjściowego dla sieci WLAN dla obsługi ruchu o różnej klasie obsługi
    c. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek

d. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

e. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP

f. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi

g. Kontrola sztormów dla ruchu broadcast/multicast/unicast

h. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

15. Wbudowane reflektometry (TDR) dla portów 10/100/1000
16. Możliwość routingu statycznego i dynamicznego dla Ipv4 i Ipv6 (minimum protokół RIP)
17. Możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu Ipv4 (OSPF, BGP) i Ipv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych
18. Wsparcie dla protokołu redundancji bramy VRRP/HSRP/GLBP lub innego równoważnego
19. Zarządzanie i konfiguracja:

    a. Umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)

    b. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu low, NetFlow, Net-Flow Lite, J-Flow lub równoważne)

c. Posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)

d. Dedykowany port Ethernet do zarządzania out-of-band

e. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB

f. Posiadać port konsoli

g. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych

h. Obsługa protokołów SNMPv3, SSHv2, https, syslog – z wykorzystaniem protokołów Ipv4 i Ipv6

20. Możliwość montażu w szafie rack 19”. Wysokość urządzenia nie może przekraczać 1 RU

21. Wyposażenie urządzenia:

    a. Moduł sieciowy min. 4x1GE SFP

    b. 4 x Transceivery SFP

    c. Zasilacze redundantne

    d. Wymagane jest, aby moduły SFP, SFP+ oferowane wraz z urządzeniem pochodziły od tego samego producenta co przełącznik celem uniknięcia problemów z serwisowaniem urządzeń

22. Zamawiający dopuszcza realizację funkcji kontrolera sieci WiFi na dedykowanych urządzeniach – pod warunkiem, że zostaną dostarczone minimum dwa kontrolery dla każdego z punktów IDF pracujące w układzie H/A o parametrach nie gorszych niż opisane poniżej. Kontrolery muszą być dołączone do stosu przełączników łączem zagregowanym o przepustowości minimum 2x10Gb/s. Łącze musi być

terminowane na minimum dwóch jednostkach stosu przełączników w celu zapewnienia niezawodności rozwiązania.

VI. Wymagania dla przełącznika sieci LAN/WLAN (pełniącego rolę urządzenia dostępowego w Głównym Urzędzie Statystycznym)

1. Przełącznik stakowalny wyposażony w 24 porty 100/1000BaseT zgodne ze standardem IEEE 802.3at (POE+)
2. Minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco” (ang. Hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:
   a. Minimum 4-portowy moduł Gigabit Ethernet z gniazdami SFP
   b. Minimum 2-portowy moduł 10Gigabit Ethernet SFP+, przy czym wymagane jest, aby w przypadku wykorzystanie pojedynczego łącza 10GE istniała możliwość instalacji dodatkowych 2 portów Gigabit Ethernet SFP
   c. Minimum 4-portowy moduł 10Gigabit Ethernet SFP+
3. Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-SX oraz 1000Base-LX zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10Gbase-SR, 10Gbase-LR, 10Gbase- LRM, 10Gbase-ER oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX)
4. Możliwość stakowania z zapewnieniem następujących parametrów:
   a. Przepustowość w ramach stosu min. 320Gb/s
   b. Minimum 8 urządzeń w stosie
   c. Zarządzanie poprzez jeden adres IP
   d. Możliwość tworzenia połączeń Cross-Stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad
5. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów
6. Urządzenie musi wyposażone w redundantne i wymienne zasilacze prądu przemiennego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania

7. Zainstalowane zasilacze muszą zapewniać min. 800W dla PoE przy pracy w trybie redundantnym
8. Obsługa low ser IEEE 802.3az Energy Efficient Ethernet
9. Szybkość przełączania minimum 130Mpps dla pakietów 64-bajtowych
10. Minimum 2GB pamięci DRAM i 2GB pamięci flash
11. Obsługa minimum:
    a. 1.000 sieci VLAN
    b. 32.000 adresów MAC
    c. 24.000 tras Ipv4
12. Usługi bezprzewodowe
    a. Przełącznik musi posiadać wbudowaną funkcjonalność kontrolera sieci bezprzewodowej WiFi o poniższych wymaganiach:
        i) Zapewniać centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415) lub równoważnym, w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym, mobilnością i jakością transmisji
        ii) Przepustowość dla sieci WiFi nie mniejsza niż 20Gb/s
        iii) Skalowalność do obsługi minimum 50 punktów dostępowych – licencje na odpowiednią ilość punktów dostępowych będą dostarczone w ramach niniejszego przetargu
    b. Zarządzanie pasmem radiowym punktów dostępowych
        i) automatyczna adaptacja do zmian w czasie rzeczywistym
        ii) optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
        iii) dynamiczne przydzielanie kanałów radiowych
        iv) wykrywanie, eliminacja i unikanie interferencji
        v) równoważenie obciążenia punktów dostępowych
        vi) automatyczna dystrybucja klientów pomiędzy punkty dostępowe
        vii) mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych

c. Mapowanie SSID do segmentów VLAN w sieci przewodowej

   i) 1:1
   ii) 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
   iii) tunelowanie ruchu klientów do kontrolera

d. Obsługa mechanizmów bezpieczeństwa:

   i) 802.11i, WPA2, WPA
   ii) 802.1X z EAP (PEAP, EAP-TLS, EAP-FAST)
   iii) obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, LDAP, wbudowana lokalna baza użytkowników
   iv) możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID
   v) możliwość profilowania użytkowników:
      (1) przydział sieci VLAN
      (2) przydział list kontroli dostępu (ACL)
   vi) uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509
   vii) obsługa list kontroli dostępu (ACL)
   viii) wykrywanie i dezaktywacja obcych punktów dostępowych
   ix) wbudowany system IDS wykrywający typowe ataki na sieci bezprzewodowe (fake AP, netstumbler, deathentication)
   x) współpraca z systemami IDS/IPS
   xi) ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego i ruchu użytkowników

e. Obsługa ruchu unicast i multicast

   i) optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
   ii) obsługa konwersji ruchu multicast do unicast

f. Obsługa mobilności (roaming-u) użytkowników (L2 i L3)

g. Obsługa mechanizmów QoS

   i) 802.1p,
   ii) WMM, Tspec,
   iii) ograniczanie pasma per użytkownik

h. Obsługa dostępu gościnnego:

i) przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony)

ii) możliwość kreowania użytkowników z określeniem czasu ważności konta

i. Praca w trybie HA w oparciu o stos opisywanych urządzeń, jeśli do poprawnej pracy w trybie HA wymagane są dodatkowe licencje, to należy je dostarczyć

j. Analiza ruchu pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji w warstwie 7

k. Mechanizmy pozwalające na dezaktywację modułów radiowych w określonych godzinach w celu redukcji poboru energii przez system

l. Zarządzanie przez CLI, HTTPS, SNMPv3, SSH, port konsoli szeregowej

13. Oprogramowanie/funkcjonalność

a. Obsługa protokołu NTP

b. Obsługa IGMPv1/2/3

c. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 128 instancji protokołu STP

d. Obsługa protokołu LLDP i LLDP-MED

e. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

f. Możliwość uruchomienia funkcji serwera DHCP

g. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

i) Minimum 4 poziomy dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)

ii) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN

iii) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL

iv) Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X

v) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

vi) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X

vii) wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem

viii) Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard

ix) Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+

14. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi

b. Implementacja co najmniej 4 kolejek dla ruchu wyjściowego dla sieci WLAN dla obsługi ruchu o różnej klasie obsługi

c. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek

d. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

e. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP

f. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi

g. Kontrola sztormów dla ruchu broadcast/multicast/unicast

h. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

15. Wbudowane reflektometry (TDR) dla portów 10/100/1000
16. Możliwość routingu statycznego i dynamicznego dla Ipv4 i Ipv6 (minimum protokół RIP).
17. Możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu Ipv4 (OSPF, BGP) i Ipv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych
18. Wsparcie dla protokołu redundancji bramy VRRP/HSRP/GLBP lub innego
19. równoważnego
20. Zarządzanie i konfiguracja:

a. zdalna obserwacja ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)

b. możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu low, NetFlow, Net-Flow Lite, J-Flow lub równoważne)

c. dedykowany port Ethernet do zarządzania out-of-band

d. minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB

e. posiadać port konsoli

f. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci

nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych

g. obsługa protokołów SNMPv3, SSHv2, https, syslog – z wykorzystaniem protokołów Ipv4 i Ipv6

21. Możliwość montażu w szafie rack 19”. Wysokość urządzenia nie może przekraczać 1 RU
22. Wyposażenie urządzenia
    a. Moduł sieciowy min. 2x10GE SFP+
    b. 2 x Transceivery 10GE SFP+
    c. Zasilacze redundantne
    d. Wymagane jest, aby moduły SFP, SFP+ oferowane wraz z urządzeniem pochodziły od tego samego producenta co przełącznik celem uniknięcia problemów z serwisowaniem urządzeń
23. Zamawiający dopuszcza realizację funkcji kontrolera sieci WiFi na dedykowanych urządzeniach – pod warunkiem, że zostaną dostarczone minimum dwa kontrolery dla każdego z punktów IDF pracujące w układzie H/A o parametrach nie gorszych niż opisane poniżej. Kontrolery muszą być dołączone do stosu przełączników łączem zagregowanym o przepustowości minimum 2x10Gb/s. Łącze musi być terminowane na minimum dwóch jednostkach stosu przełączników w celu zapewnienia niezawodności rozwiązania.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

Tabela nr 2 Rozdzielnik przełączników szkieletowych, kontrolerów i punktów dostępowych do Urzędów Statystycznych

Lokalizacja	Ilość przełączników z 4-portowym modułem 1Gigabit Ethernet	Ilość Transceiverów światłowodowych 1000Base-SX SFP	Instalacja okablowania światłowodowego	Ilość punktów dostępowych	Ilość kontrolerów
US Białystok	2	0	nie	3	2
US Bydgoszcz	2	2	1x120m 1x170m	3	2
US Gdańsk	2	2	2x70m	3	2
US Katowice	2	0	nie	3	2
US Kielce	2	0	nie	3	2
US Kraków	2	6	2X200m 4x5m	3	2
US Lublin	2	6	3x20m 2x10m	3	2
US Łódź	2	2	już są światłowody	3	2
US Olsztyn	2	8	1x50m reszta jest	3	2
US Opole	2	8	już są światłowody	3	2
US Poznań	2	2	2x150m	3	2
CIS Radom	2	4	4x100m	12	2
US Rzeszów	2	1	1x20m	3	2
US Szczecin	2	8	nie	3	2
US Warszawa	2	2	2x110m	3	2
US Wrocław	2	7	7x40m	3	2
US Zielona Góra	2	0	nie	3	2
Razem	**34**	**58**		**60**	**34**

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

Tabela nr 3 Rozdzielnik przełączników dostępowych, kontrolerów i punktów dostępowych do Głównego Urzędu Statystycznego

Miejsce dostawy	Ilość przełączników z 2-portowym modułem 10Gigabit Ethernet SFP+,	Ilość Transceiverów światłowodowych 10 Gb	Instalacja połączeń światłowodowych	Ilość punktów dostępowych	Ilość kontrolerów
GUS	10	20	tak	60	10

Instalacja połączeń światłowodowych w Głównym Urzędzie Statystycznym:

Pomiędzy LPD6-Serwerownia 1 piętro – 98m

Pomiędzy LPD5-Serwerownia 1 piętro – 94m

Pomiędzy LPD4-Serwerownia 1 piętro – 91m

Pomiędzy LPD3-Serwerownia 1 piętro – 88m

Pomiędzy LPD2-Serwerownia 1 piętro – 84m

Pomiędzy LPD1-Serwerownia 1 piętro – 80m

Pomiędzy LPD0-Serwerownia 1 piętro – 175m

VII. Wymagania dotyczące zakresu wdrożenia sieci bezprzewodowej w GUS oraz w Urzędach Statystycznych

Wdrożenie będzie polegało na instalacji, konfiguracji, zabezpieczeniu oraz uruchomieniu sieci bezprzewodowej oraz integracji z następującymi Systemami:

1. Systemem Zarządzania Siecią LAN/WLAN
2. Systemem do Realizacji Usług Lokalizacji oraz Bezpieczeństwa w Sieci Bezprzewodowej
3. Systemem Zarządzania Bezpieczeństwem Dostępu do Sieci LAN/WLAN

Podczas wdrożenia wykonane zostaną następujące prace:

4. Analiza przedwdrożeniowa obejmująca weryfikację konfiguracji sieci Zamawiającego niezbędna do przygotowania projektu technicznego; analiza będzie

obejmować spotkania robocze na których Zamawiający przedstawi budowę sieci wraz z konfiguracją poszczególnych urządzeń w zakresie niezbędnym do realizacji przedmiotu zamówienia,

5. Opracowanie projektu technicznego opisującego szczegółową konfigurację urządzeń i oprogramowania niezbędnego do realizacji wdrożenia,
6. Instalację sprzętu wraz z okablowaniem w lokalizacjach zdefiniowanych w zaakceptowanym przez Zamawiającego projekcie technicznym, Wykonawca jest zobowiązany do posprzątania miejsc instalacji urządzeń każdorazowo po wykonaniu prac instalacyjnych przed następnym dniem roboczym w siedzibie Zamawiającego oraz pozostawienia tych miejsc w stanie nie gorszym od zastanego przed przystąpieniem do prac
   a. Punkty dostępowe powinny być montowane wewnątrz budynków, urządzenia powinny zostać dobrane w taki sposób, aby pokryć zasięgiem planowane obszary prac. Zamontowane punkty dostępowe należy podłączyć do instalacji okablowania strukturalnego kablem kategorii 6+ .
   b. Instalacja okablowania strukturalnego dla potrzeb sieci bezprzewodowej obejmować może: przebijanie otworów w stropach, ścianach nośnych, działowych, betonowych i nie betonowych, montaż listew instalacyjnych PVC, kanałów kablowych lub rur kablowych, wciąganie kabli w kanały kablowe, montaż paneli, punktów dostępowych , innych urządzeń w punktach dystrybucyjnych LPD, rozszywanie na panelach, pomiary.
7. Konfigurację urządzeń zgodnie z 802.1x (uwzględniając podział na sieć produkcyjną i sieć gościnną, autoryzację gościa poprzez logowanie się do portalu) oraz instalację oprogramowania zgodnie z zaakceptowanym przez Zamawiającego projektem technicznym,
8. Testy akceptacyjne potwierdzające zgodność instalacji z wymaganiami opisanymi w Opisie Przedmiotu Zamówienia – część 3
9. Wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.

VIII. Warunki gwarancji

1. Wykonawca udzieli Zamawiającemu 36-miesięcznej gwarancji na dostarczony sprzęt. Gwarancja obejmuje zobowiązanie Wykonawcy do terminowego usuwania

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

wad i usterek urządzeń sieciowych oraz innych elementów dostarczonych wraz ze sprzętem.

2. Wykonawca zobowiązuje się, iż w okresie gwarancji, czas reakcji na zgłoszoną przez Zamawiającego wadę lub usterkę nastąpi nie później niż w ciągu 4 godzin od momentu zgłoszenia wady lub usterki.
3. Wykonawca zobowiązuje się do przywrócenia pełnej funkcjonalności sprzętu w ciągu 24 godzin od zgłoszenia.
4. Naprawa zostanie dokonana w miejscu instalacji sprzętu.
5. W przypadku niewykonania naprawy gwarancyjnej w miejscu i w terminie, o którym mowa w ust. 3 i 4, Wykonawca zobowiązuje się dostarczyć na czas naprawy takie samo urządzenie wolne od wad i zapewni jego prawidłowe działanie. Ostateczny termin usunięcia wady lub usterki sprzętu nie może być dłuższy niż 30 dni od dnia zgłoszenia jego wady lub usterki.
6. Wykonawca zobowiązuje się do wymiany sprzętu na nowe w przypadku, gdy po wykonaniu dwóch napraw gwarancyjnych dostarczonego urządzenia będzie ono wykazywało nadal wady w działaniu.
7. W przypadku nie wywiązania się Wykonawcy z zobowiązań gwarancyjnych, Zamawiający może dokonać tych czynności we własnym zakresie i kosztami obciążyć Wykonawcę.
8. Wykonawca pokrywa wszelkie koszty związane z naprawami gwarancyjnymi.
9. Zamawiający zobowiązany jest do udzielenia szczegółowych informacji o zewnętrznych objawach wady lub usterki oraz czasie jej wystąpienia.
10. W przypadku naprawy gwarancja ulega przedłużeniu o czas naprawy.
11. Zamawiający ma prawo dokonywania rozbudowy sprzętu, zgodnie z dokumentacją techniczną, przez wykwalifikowanych pracowników, a także prawo do przemieszczenia zainstalowanego sprzętu bez utraty gwarancji. Wykonawca nie ponosi odpowiedzialności za uszkodzenia mechaniczne przedmiotu Umowy powstałe z winy pracowników Zamawiającego.

IX. Szkolenia

1. Wykonawca przeprowadzi szkolenie dla Administratorów zgodnie z następującymi wymaganiami:
   a. ilość uczestników – 5 osób,
   b. czas trwania szkolenia: 5 dni roboczych (40 godzin lekcyjnych).
   c. program szkolenia musi obejmować całość zagadnień z zakresu administrowania urządzeniem (systemem):
      i) Podstawy działania sieci bezprzewodowych
      ii) Podstawowe topologie sieci WLAN
      iii) Standardy 802.11
      iv) Zunifikowana sieć WLAN
      v) Podstawy implementacji punktów dostępowych
      vi) Konfigurowanie dostarczonych przełączników, kontrolerów i punktów dostępowych
      vii) Karty sieciowe i oprogramowanie klienckie dla sieci 802.11
      viii) Bezpieczeństwo w sieciach WLAN
      ix) Administrowanie sieciami bezprzewodowymi i rozwiązywanie problemów
   d. wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim, w formie papierowej lub elektronicznej w formacie PDF.
   e. wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia i posiadania kompetencji Administratora.
   f. szkolenia dla Administratorów musza być prowadzone przez wykładowców certyfikowanych przez producenta oferowanego oprogramowania.
   g. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.
   h. Wykonawca przeprowadzi szkolenia w Warszawie w ośrodku szkoleniowym.
   i. Wykonawca każdego dnia trwania szkolenia zapewni: dwie przerwy kawowe, każda trwająca ok. 10 minut oraz jedną przerwę obiadową trwającą ok. 40 minut.
   j. Wykonawca zapewni każdego dnia szkolenia wyżywienie dla wszystkich uczestników:

i. dostępne przez cały czas trwania szkolenia: kawa, herbata, butelkowana woda mineralna gazowana i niegazowana, naturalne soki owocowe (butelkowane lub w kartonach) oraz ciastka.

ii. obiad – zupa, danie główne, surówki, owoce, herbata, kawa, butelkowana woda mineralna, naturalne soki owocowe (butelkowane lub w kartonach); czyste sztućce i zastawa (nie mogą być jednokrotnego użytku) – podany w oddzielnym pomieszczeniu (strefie przeznaczonej do podawania posiłków), które:

1) spełnia wymagania sanitarne wynikające z obowiązujących przepisów,
2) jest wyposażone w sprawną i wydajną wentylację oraz klimatyzację,
3) jest posprzątane i uporządkowane bez zbędnych przedmiotów lub mebli,

iii. wykonawca zapewni każdemu uczestnikowi odpowiednio danie mięsne, wegetariańskie lub bezglutenowe zgodnie ze zgłoszonym zapotrzebowaniem w harmonogramie szkoleń.

2. Na co najmniej 14 dni przed rozpoczęciem szkolenia Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkolenia przygotowany w porozumieniu z Zamawiającym obejmujący:

a. program szkolenia zawierający szczegółowe informacje o zakresie tematycznym i rozkładzie zajęć dla ww. szkolenia,

b. metodę i formę prowadzenia szkolenia,

c. informacje o wykładowcy, który poprowadzi szkolenia.

3. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkolenia.

4. Zamawiający zastrzega sobie prawo do modyfikacji harmonogramu szkolenia, z wytypowaniem mniejszej lub większej liczby uczestników.

5. Wykonawca w ramach prowadzonego szkolenia zobowiązany jest przekazać Zamawiającemu:

a. materiały szkoleniowe,

b. listy obecności,

c. listę wydanych Zaświadczeń i komplet imiennych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenie, pod warunkiem uczestnictwa w pełnym wymiarze zajęć.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

B1. Dostawa i wdrożenie Systemu Zarządzania Siecią LAN/WLAN

I. Wymagania dla Systemu Zarządzania Siecią LAN/WLAN

System musi posiadać następujące funkcjonalności:

1. W zakresie zarządzania siecią przewodową:
   a. Zarządzanie i zbieranie statystyk z wykorzystaniem co najmniej SNMP
   b. Narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci: możliwość manualnego dodawania urządzeń oraz automatycznie za pośrednictwem protokołów takich jak: LLDP, ARP, BGP, OSPF lub innych
   c. Narzędzia prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu urządzenia
   d. Narzędzie umożliwiające zbieranie i zapisywanie informacji o parametrach pracy zainstalowanego sprzętu
   e. Wbudowane przykładowe wzorce konfiguracji urządzeń, takie jak: konfiguracja usług bezpieczeństwa, agregacji linków, konfiguracji NTP, SNMP, itp.
   f. Narzędzie do tworzenia wzorców konfiguracji na urządzenia
   g. Wbudowane narzędzia do konfiguracji urządzeń w zakresie przynajmniej interfejsów, list kontroli dostępu, wybranych protokołów routingu na routerach
   h. Wbudowane narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych
   i. Narzędzie do zarządzania obrazami oprogramowania urządzeń
   j. Funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń
   k. Wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

l. Możliwość zbierania statystyk za pomocą Netflow lub protokołu równoważnego (funkcjonalność może być realizowana przez zakup dodatkowej licencji) lub dodatkowego urządzenia/systemu

m. Wbudowane narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, przynajmniej takich jak: zajętość CPU, zajętość pamięci, dostępność, itp.

n. Narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku

o. Narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów

p. Możliwość informowania o alarmach/incydentach przez notyfikację email

2. W zakresie zarządzania siecią bezprzewodową:

a. Graficzne planowanie i zarządzanie siecią bezprzewodową (hierarchiczne mapy lokalizacji, mapy zasięgu) z wykorzystaniem własnych planów budynków

b. Zarządzenie punktami dostępowymi i kontrolerami

c. Możliwość monitorowania autonomicznych punktów dostępowych

d. Monitorowanie informacji takich jak: poziom szumu, poziom sygnału, interferencje sygnału pochodzących z punktów dostępowych

e. Raportowanie i statystyka min: wydajności urządzeń, obciążenia sieci, alarmy pochodzące z urządzeń

f. System musi zawierać gotowe, przykładowe formularze wdrożenia dla polityki bezpieczeństwa, polityki QoS dla wielu punktów dostępu radiowego, a także udostępniać możliwość tworzenia własnych

g. Automatyczne wykrywanie nowych punktów dostępowych w sieci radiowej

h. Współpraca z systemami do autentykacji i autoryzacji użytkowników przynajmniej w zakresie zbierania informacji o parametrach podłączenia użytkownika do sieci oraz generowania raportów

i. Możliwość wykrywania nie autoryzowanych punktów dostępowych i klientów sieci z określeniem ich lokalizacji

j. Zarządzanie wersjami oprogramowania urządzeń

k. Współpraca z analizatorami widma częstotliwościowego

l. Mechanizmy tworzenia kopii zapasowych

m. Lokalizacja urządzeń radiowych (punktów dostępowych, klientów, tagów) na żądanie z prezentacją graficzną

n. Możliwość integracji z systemami analitycznymi do analizy aktywności użytkowników w sieciach bezprzewodowych

3. W ogólnym zakresie funkcjonalności:

a. Praca w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci

b. Musi pozwalać na budowanie widoków przez użytkownika

c. Hierarchizacja zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów lub zewnętrznego serwera uwierzytelniającego

d. Współpraca z serwerami czasu (NTP)

e. Narzędzie do generowania raportów, które może być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku

f. Tworzenie raportów dotyczących urządzeń sieciowych, urządzeń klienckich oraz wydajności sieci

g. Narzędzie pozwalające na analizę połączenia urządzeń klienckich i użytkowników podłączonych do infrastruktury

h. Musi umożliwiać zarządzanie 500 urządzeniami z możliwością rozbudowy do przynajmniej 1500

i. Musi umożliwiać rozbudowę (poprzez zakup odpowiednich licencji) o funkcjonalności pozwalające na:

j. zbieranie statystyk za pomocą Netflow/JFlow lub protokołu równoważnego z przynajmniej 500 urządzeń (z możliwością rozbudowy do 1500)

k. System powinien zostać dostarczony wraz z platformą sprzętową rekomendowaną przez producenta dla osiągnięcia docelowej skalowalności 1500 urządzeń oraz zachowaniem redundancji zasilania i interfejsów sieciowych.

l. Dopuszcza się zrealizowanie powyższych wymagań w postaci zintegrowanej w jednej aplikacji lub w postaci zespołu aplikacji – jednej dla LAN i drugiej dla WLAN. Wszystkie użyte komponenty muszą stanowić rozwiązania komercyjne z gwarantowanym wsparciem technicznym producenta.

II. Wymagania dotyczące zakresu wdrożenia Systemu Zarządzania Siecią LAN/WLAN w Głównym Urzędzie Statystycznym

Wdrożenie systemu przeprowadzą osoby legitymujące się certyfikatem producenta oferowanego rozwiązania.

Podczas wdrożenia wykonane zostaną następujące prace:

1. Przeprowadzenie analizy przedwdrożeniowej obejmującej weryfikację konfiguracji sieci Zamawiającego niezbędną do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze na których Zamawiający szczegółowo przedstawi budowę sieci wraz z konfiguracją poszczególnych urządzeń w zakresie niezbędnym do realizacji przedmiotu zamówienia,
2. Przygotowanie projektu technicznego opisującego szczegółową konfigurację urządzeń i oprogramowania niezbędną do realizacji wdrożenia,
3. Instalację sprzętu w segmentach sieci zdefiniowanych w zaakceptowanym przez Zamawiającego projekcie technicznym,.
4. Konfigurację urządzeń i oprogramowania zgodnie z zaakceptowanym przez Zamawiającego projektem technicznym,
5. Testy akceptacyjne potwierdzające zgodność wdrożonego rozwiązania z wymaganiami opisanymi w Opisie Przedmiotu Zamówienia – część 3,
6. Wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.

III. Warunki gwarancji

1. Wykonawca obejmie przedmiot Umowy gwarancją, przez okres 36 miesięcy od daty podpisania Końcowego protokołu odbioru
2. Gwarancja realizowana będzie w siedzibie Zamawiającego.
3. Dopuszcza się połączenie zdalne, kontakt mailowy i telefoniczny, pod warunkiem, że nie wpływa ona na obniżenie jakości świadczenia usług.
4. Świadczenie usług gwarancyjnych odbywać się będzie w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 16:00.
5. Wykonawca gwarantuje maksymalny czas reakcji na zgłoszenie nie dłuższy niż jedna godzina i czas naprawy nie dłuższy niż 48 godzin.
6. Zamawiający nie będzie ponosił żadnych kosztów związanych z pełnieniem gwarancji przez wykonawcę (kosztów dojazdu, kosztów noclegu itp.).
7. W tym okresie w ramach gwarancji Wykonawca zapewni:
   a. przywracanie pełnej funkcjonalności działania oprogramowania,
   b. konsultacje w zakresie konfiguracji i eksploatacji Systemu Zarządzania Siecią
   c. LAN/WLAN.
   d. rozwiązywanie problemów technicznych związanych z funkcjonowaniem Systemu, w szczególności strojenie wydajności Systemu.
   e. rozwiązywanie problemów bieżącej administracji Systemu.

IV. Szkolenia

1. Wykonawca przeprowadzi szkolenie dla Administratorów zgodnie z następującymi wymaganiami:
   a. ilość uczestników – 3 osoby,
   b. czas trwania szkolenia: 3 dni roboczych (24 godziny lekcyjne).
   c. program szkolenia musi obejmować całość zagadnień z zakresu administrowania Systemem oraz zapewnić umiejętności i wiedzę niezbędną do właściwego i samodzielnego rozwoju wdrażanego Systemu, w tym:
      i) niezbędne informacje o budowie, funkcjonowaniu rozwiązań zastosowanych w Systemie,

ii) parametryzacja/konfiguracja Systemu,

iii) narzędzia dostosowawcze (kastomizacyjne) do wprowadzania zmian w Systemie,

d. wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim, w formie papierowej lub elektronicznej w formacie PDF.

e. wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia i posiadania kompetencji Administratora Systemu.

f. szkolenia dla Administratorów musza być prowadzone przez wykładowców certyfikowanych przez producenta oferowanego oprogramowania.

g. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

h. Wykonawca przeprowadzi szkolenie w Warszawie w ośrodku szkoleniowym.

i. Wykonawca każdego dnia trwania szkolenia zapewni: dwie przerwy kawowe, każda trwająca ok. 10 minut oraz jedną przerwę obiadową trwającą ok. 40 minut.

j. Wykonawca zapewni każdego dnia szkolenia wyżywienie dla wszystkich uczestników:

i. dostępne przez cały czas trwania szkolenia: kawa, herbata, butelkowana woda mineralna gazowana i niegazowana, naturalne soki owocowe (butelkowane lub w kartonach) oraz ciastka.

ii. obiad – zupa, danie główne, surówki, owoce, herbata, kawa, butelkowana woda mineralna, naturalne soki owocowe (butelkowane lub w kartonach); czyste sztućce i zastawa (nie mogą być jednokrotnego użytku) – podany w oddzielnym pomieszczeniu (strefie przeznaczonej do podawania posiłków), które:

1) spełnia wymagania sanitarne wynikające z obowiązujących przepisów,
2) jest wyposażone w sprawną i wydajną wentylację oraz klimatyzację,
3) jest posprzątane i uporządkowane bez zbędnych przedmiotów lub mebli,

iii. wykonawca zapewni każdemu uczestnikowi odpowiednio danie mięsne, wegetariańskie lub bezglutenowe zgodnie ze zgłoszonym zapotrzebowaniem w harmonogramie szkoleń.

2. Na co najmniej 14 dni przed rozpoczęciem szkolenia Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkolenia przygotowany w porozumieniu z Zamawiającym obejmujący:
   a. program szkolenia zawierający szczegółowe informacje o zakresie tematycznym i rozkładzie zajęć dla ww. szkolenia,
   b. metodę i formę prowadzenia szkolenia,
   c. informacje o wykładowcy, który poprowadzi szkolenie.
3. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkolenia.
4. Zamawiający zastrzega sobie prawo do modyfikacji harmonogramu szkolenia, z wytypowaniem mniejszej lub większej liczby uczestników.
5. Wykonawca w ramach prowadzonego szkolenia zobowiązany jest przekazać Zamawiającemu:
   a. materiały szkoleniowe,
   b. listy obecności,
   c. listę wydanych Zaświadczeń i komplet imiennych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenie, pod warunkiem uczestnictwa w pełnym wymiarze zajęć.

B2. Dostawa i wdrożenie Systemu Zarządzania Bezpieczeństwem Dostępu do Sieci LAN/WLAN

I. Wymagania dla Systemu Zarządzania Bezpieczeństwem Dostępu do Sieci LAN/WLAN

System Zarządzania Bezpieczeństwem Dostępu do Sieci ma zapewnić metody uwierzytelnienia i autoryzacji użytkowników i urządzeń sieci LAN oraz sieci bezprzewodowej, dostępu gościnnego oraz umożliwiać rozbudowę o funkcjonalności wykrywania urządzeń końcowych oraz oceny stanu bezpieczeństwa urządzeń końcowych. System musi spełniać co najmniej poniższe wymagania:

1. Wspierać następujące protokoły uwierzytelnienia i standardy:
   a. RADIUS, zgodnie z dokumentami:
      i) RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
      ii) RFC 2139 — RADIUS Accounting
      iii) RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
      iv) RFC 2866 — RADIUS Accounting
      v) RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
      vi) RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
      vii) RFC 2869 — RADIUS Extensions
   b. Radius Change of Atuthorisation
   c. RADIUS Proxy dla zewnętrznego serwera RADIUS
2. Wspierać urządzenia firm trzecich przynajmniej na poziomie uwierzytelnienia przez adres MAC
3. Umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych i w ten sposób umożliwiać skalowanie rozwiązania.

4. Umożliwiać realizację wysokiej dostępności wszystkich elementów funkcjonalnych, co najmniej 1:1
5. Wspierać integrację z Windows Active Directory, w tym co najmniej Microsoft Windows Active Directory 2003 32/64bit, Microsoft Windows Active Directory 2008 32/64-bit, Microsoft Windows 2012 32/64-bit
6. Wspierać protokół Lightweight Directory Access Protocol (LDAP).
7. Umożliwiać zarządzanie za pomocą interfejsu graficznego przez przeglądarkę internetową, w tym co najmniej: Google Chrome, Microsoft IE, Mozilla Firefox
8. Wspierać następujące protokoły uwierzytelniania:
   a. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
   b. Protected Extensible Authentication Protocol (PEAP)
   c. umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym, serwerze TFTP/FTP/SFTP, udziale NFS, dysku CDROM
9. Umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
10. Umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
11. Umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
12. Umożliwiać wymuszenie reguł złożoności haseł dla administratorów.
13. Umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora.
14. Umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.
15. Umożliwiać generowanie przynajmniej następujących raportów:
   a. zbiorczego podsumowania uwierzytelnień 802.1X
   b. accountingu RADIUS
   c. uwierzytelniania RADIUS

d. błędów RADIUS

e. aktywnych sesji RADIUS

f. historii sesji RADIUS

g. Top N uwierzytelnień per maszyna

h. Top N uwierzytelnień per użytkownik

i. aktywności użytkowników gościnnych

j. zarejestrowane urządzenia

16. Umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:

    a. Wiadomości e-mail

    b. Syslog

17. Posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

    a. Wyszukiwanie zdarzeń RADIUS z uwzględnieniem: nazwy użytkownika, adresu MAC, ID sesji, statusu uwierzytelnienia , zakresu czasowego itp.

    b. Ewaluację zgodności konfiguracji urządzenia sieciowego

18. Umożliwiać równoczesną obsługę co najmniej 5000 urządzeń końcowych (endpoints) przewodowych i bezprzewodowych dla funkcjonalności uwierzytelnienia, autoryzacji oraz dostępu gościnnego

19. Umożliwiać elastyczne dodawanie licencji w ramach wzrostu liczby obsługiwanych stacji końcowych.

20. Umożliwiać uwierzytelnienie i kontrolę dostępu:

    a. Kablowego w sieci LAN

    b. Bezprzewodowego w sieci WLAN

    c. Zdalnego VPN

21. Umożliwiać inkrementalną skalowalność do przynajmniej 10,000 równocześnie obsługiwanych urządzeń końcowych (endpoints) poprzez dodawanie kolejnych serwerów/wirtualnych instancji do istniejącego wdrożenia.

22. Umożliwiać instalację na maszynie wirtualnej (VM) lub maszynie fizycznej, w tym:
    a. Na hypervisorze VMWare ESXi 4.x, 5.x lub nowszym
    b. Na serwerach fizycznych wspieranych przez producenta
23. Wspierać implementację 802.1X z przynajmniej następującymi suplikantami:
    a. Wbudowanym klientem 802.1X dla Windows XP, 7, 8
    b. Apple Mac OS X Supplicant
24. Umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).
25. Umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
26. Umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych złożone o reguły.
27. Posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV.
28. Posiadać lokalną bazę stacji końcowych. Lokalną bazę stacji końcowych można tworzyć per stacja końcowa na podstawie unikalnego adresu MAC.
29. Wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC za pomocą mechanizmu MAB (MAC Authentication Bypass) lub równoważnego.
30. Umożliwiać integrację z rozwiązaniami MDM (Mobile Device Management).
31. Umożliwiać automatyzację procesu wystawienia certyfikatu i konfiguracji ustawień sieciowych na prywatnych urządzeniach pracowników.
32. Umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym co najmniej:
    a. Microsoft Windows 7, 8, XP (Microsoft IE, Mozilla Firefox, Google Chrome)
    b. Apple Mac OS X (Mozilla Firefox, Safari, Google Chrome)
33. Umożliwiać dodawanie kont gościnnych przez wybrane osoby
34. Uwierzytelnienie takiej osoby musi się odbywać sekwencyjnie w oparciu o:
    a. Wewnętrzną bazę użytkowników

b. Zewnętrzne repozytorium użytkowników

35. Umożliwiać konfigurację uprawnień takiej osoby, w tym uprawnienia do:
    a. Tworzenia pojedynczego konta gościnnego
    b. Tworzenia wielu kont gościnnych
    c. Tworzenia kont losowych
    d. Importowania kont gościnnych z pliku CSV
    e. Wysyłania wiadomości e-mail po utworzeniu konta gościnnego
    f. Wysyłania wiadomości SMS po utworzeniu konta gościnnego
    g. Wydrukowania danych konta gościnnego
    h. Wyświetlenia danych stworzonych kont gościnnych
    i. Zawieszenia (suspend) i reinicjacji kont gościnnych
36. Umożliwiać automatyczne kasowanie wygasłych kont gościnnych:
37. Posiadać wzorce językowe lub umożliwiać ich dodanie dla stron sponsora i gościa, w tym w językach:
    a. Polskim
    b. Angielskim
38. Umożliwiać specyfikację opcjonalną lub obowiązkową następujących danych gościa w trakcie kreacji konta przez sponsora:
    a. Imienia
    b. Nazwiska
    c. Firmy
    d. Adresu e-mail
    e. Numeru telefonu
    f. Danych opcjonalnych takich jak PESEL i inne
39. Umożliwiać konfigurację dla użytkowników gościnnych:
    a. Wyświetlenia im informacji o polityce akceptowalnego użycia sieci
    b. Zezwolenia gościom na zmianę hasła

c. Wymogu zmiany hasła gościa przed wygaszeniem

d. Samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora

e. Samorejestracji urządzenia końcowego dla dostępu gościnnego

40. Umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego
41. Umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne
42. Umożliwiać konfigurację czasu ważności hasła w zadanym przedziale w dniach.
43. Umożliwiać kreację profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego.
44. Umożliwiać konfigurację polityki złożoności haseł i nazw (loginów) użytkowników gościnnych.
45. Umożliwiać rozbudowę licencyjną o funkcjonalność profilowania (profiling) stacji końcowej i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
46. Umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:

    a. DHCP

    b. HTTP

    c. RADIUS

    d. Network Scan (NMAP)

    e. SNMP

47. Umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176 po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.
48. Umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
49. Posiadać dostarczony przez producenta zestaw profili urządzeń, w tym dla:

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

a. Urządzeń Android

b. Urządzeń Apple

c. Urządzeń BlackBerry

d. Stacji roboczych z systemami operacyjnymi (FreeBSD, Linux, OS-X, Windows 8, Windows 7, Windows XP, OpenBSD,)

50. Możliwość regularnych aktualizacji przez producenta o nowe profile urządzeń.
51. Umożliwiać rozbudowę licencyjną o głęboką analizę stacji końcowej.
52. Umożliwiać analizę stacji końcowej Windows pod kątem plików w tym:
    a. Istnienia pliku na stacji końcowej
    b. Wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)
    c. Daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)
53. Umożliwiać analizę stacji końcowej z systemem Windows XP, Windows 8, Windows 7 pod kątem wpisów w rejestrze pod kątem:
    a. Istnienia lub nieistnienia klucza
    b. Wartości klucza rejestru
    c. Istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version
54. Umożliwiać analizę stacji końcowej z systemem Windows XP, Windows 8, Windows 7 pod kątem uruchomionych aplikacji (nazwa uruchomionego lub nieuruchomionego procesu)
55. Umożliwiać analizę stacji końcowej z systemem Windows XP, Windows 8, Windows 7 pod kątem uruchomionych usług ((nazwa uruchomionego lub nieuruchomionego procesu)
56. Umożliwiać analizę stacji końcowej z systemem Windows XP, Windows 8, Windows 7, Mac OS-X pod kątem zainstalowanych aplikacji Antywirusowych w tym:
    a. stwierdzenia czy system AV jest obecny na stacji
    b. stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

57. Umożliwiać analizę stacji końcowej z systemem Windows XP, Windows 8, Windows 7, Mac OS-X pod kątem zainstalowanych aplikacji AntiSpyware w tym:
    a. stwierdzenia czy system AS jest obecny na stacji
    b. stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni
58. System powinien zostać dostarczony wraz z redundantną platformą sprzętową (min. 2 serwery) rekomendowaną przez producenta dla osiągnięcia docelowej skalowalności 10 000 użytkowników i urządzeń i zachowania warunku redundancji.
59. Dopuszcza się zrealizowanie powyższych wymagań w postaci zintegrowanej w jednej aplikacji lub w postaci zespołu aplikacji. W przypadku zespołu aplikacji należy zintegrować poszczególne elementy ze sobą, tak by umożliwiały tworzenie spójnych polityk bezpieczeństwa, zarządzanych centralnie, należy szczegółowo opisać architekturę rozwiązania i udokumentować w jaki sposób realizowane są poszczególne funkcje i jakie informacje i w jaki sposób są wymieniana poprzez poszczególne aplikacje. Wszystkie użyte komponenty muszą stanowić rozwiązania komercyjne z gwarantowanym wsparciem technicznym producenta.

II. Wymagania dotyczące zakresu wdrożenia Systemu Zarządzania Bezpieczeństwem Dostępu do Sieci LAN/WLAN w Głównym Urzędzie Statystycznym

Wdrożenie systemu przeprowadzą osoby legitymujące się certyfikatem producenta oferowanego rozwiązania.

Podczas wdrożenia wykonane zostaną następujące prace:

1. przeprowadzenie analizy przedwdrożeniowej obejmującej weryfikację konfiguracji sieci Zamawiającego niezbędną do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze na których Zamawiający szczegółowo przedstawi budowę sieci wraz z konfiguracją poszczególnych urządzeń w zakresie niezbędnym do realizacji przedmiotu zamówienia,
2. przygotowanie projektu technicznego opisującego szczegółową konfigurację urządzeń i oprogramowania niezbędną do realizacji wdrożenia,
3. instalację sprzętu w segmentach sieci zdefiniowanych w zaakceptowanym przez Zamawiającego projekcie technicznym,

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

4. konfigurację urządzeń i oprogramowania zgodnie z zaakceptowanym przez Zamawiającego projektem technicznym,
5. testy akceptacyjne potwierdzające zgodność wdrożonego rozwiązania z wymaganiami opisanymi w Opisie Przedmiotu Zamówienia – część 2,
6. wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.

III. Warunki gwarancji

1. Wykonawca obejmie przedmiot Umowy gwarancją, przez okres 36 miesięcy od daty podpisania Końcowego protokołu odbioru.
2. Gwarancja realizowana będzie w siedzibie Zamawiającego.
3. Dopuszcza się połączenie zdalne, kontakt mailowy i telefoniczny, pod warunkiem, że nie wpływa ona na obniżenie jakości świadczenia usług.
4. Świadczenie usług gwarancyjnych odbywać się będzie w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 16:00.
5. Wykonawca gwarantuje maksymalny czas reakcji na zgłoszenie nie dłuższy niż jedna godzina i czas naprawy nie dłuższy niż 48 godzin.
6. Zamawiający nie będzie ponosił żadnych kosztów związanych z pełnieniem gwarancji przez wykonawcę (kosztów dojazdu, kosztów noclegu itp.).
7. W tym okresie w ramach gwarancji Wykonawca zapewni:
   a. przywracanie pełnej funkcjonalności działania oprogramowania,
   b. konsultacje w zakresie konfiguracji i eksploatacji Systemu
   c. rozwiązywanie problemów technicznych związanych z funkcjonowaniem Systemu, w szczególności strojenie wydajności Systemu.
   d. rozwiązywanie problemów bieżącej administracji Systemu.

IV. Szkolenia

1. Wykonawca przeprowadzi szkolenie dla Administratorów zgodnie z następującymi wymaganiami:
   a. ilość uczestników – 4 osoby,

b. czas trwania szkolenia: 3 dni (24 godziny lekcyjne).

c. program szkolenia musi obejmować całość zagadnień z zakresu administrowania Systemem oraz zapewnić umiejętności i wiedzę niezbędną do właściwego i samodzielnego rozwoju wdrażanego Systemu, w tym:

   i. niezbędne informacje o budowie, funkcjonowaniu i filozofii rozwiązań zastosowanych w Systemie,
   ii. parametryzacja/konfiguracja Systemu,
   iii. narzędzia dostosowawcze (kastomizacyjne) do wprowadzania zmian w Systemie,

d. wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim, w formie papierowej lub elektronicznej w formacie PDF.

e. wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia i posiadania kompetencji Administratora Systemu.

f. szkolenie dla Administratorów musza być prowadzone przez wykładowców certyfikowanych przez producenta oferowanego oprogramowania.

g. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

h. Wykonawca przeprowadzi szkolenie w Warszawie w ośrodku szkoleniowym.

i. Wykonawca każdego dnia trwania szkolenia zapewni: dwie przerwy kawowe, każda trwająca ok. 10 minut oraz jedną przerwę obiadową trwającą ok. 40 minut.

j. Wykonawca zapewni każdego dnia szkolenia wyżywienie dla wszystkich uczestników:

   i. dostępne przez cały czas trwania szkolenia: kawa, herbata, butelkowana woda mineralna gazowana i niegazowana, naturalne soki owocowe (butelkowane lub w kartonach) oraz ciastka.
   ii. obiad – zupa, danie główne, surówki, owoce, herbata, kawa, butelkowana woda mineralna, naturalne soki owocowe (butelkowane lub w kartonach); czyste sztućce i zastawa (nie mogą być jednokrotnego użytku) – podany

w oddzielnym pomieszczeniu (strefie przeznaczonej do podawania posiłków), które:

1) spełnia wymagania sanitarne wynikające z obowiązujących przepisów,
2) jest wyposażone w sprawną i wydajną wentylację oraz klimatyzację,
3) jest posprzątane i uporządkowane bez zbędnych przedmiotów lub mebli,

iii. wykonawca zapewni każdemu uczestnikowi odpowiednio danie mięsne, wegetariańskie lub bezglutenowe zgodnie ze zgłoszonym zapotrzebowaniem w harmonogramie szkoleń.

2. Na co najmniej 14 dni przed rozpoczęciem szkolenia Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkolenia przygotowany w porozumieniu z Zamawiającym obejmujący:
   a. program szkolenia zawierające szczegółowe informacje o zakresie tematycznym i rozkładzie zajęć dla ww. szkolenia,
   b. metodę i formę prowadzenia szkolenia,
   c. informacje o wykładowcy, który poprowadzi szkolenie.
3. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkolenia.
4. Zamawiający zastrzega sobie prawo do modyfikacji harmonogramu szkolenia, z wytypowaniem mniejszej lub większej liczby uczestników.
5. Wykonawca w ramach prowadzonego szkolenia zobowiązany jest przekazać Zamawiającemu:
   a. Podręcznik: Administratora,
   b. materiały szkoleniowe,
   c. listy obecności,
   d. listę wydanych Zaświadczeń i komplet imiennych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenie, pod warunkiem uczestnictwa w pełnym wymiarze zajęć.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

C. Dostawa i wdrożenie przełącznika modularnego, rdzeniowego w Głównym Urzędzie Statystycznym – 2 sztuki

I. Wymagania dla przełącznika modularnego pełniącego rolę przełącznika rdzeniowego dla sieci LAN oraz Data Center w budynku GUS

Obecnie szkielet sieci LAN w Głównym Urzędzie Statystycznym tworzą dwa przełączniki Cisco Catalyst 6509-E. Zamawiający wymaga aby wszystkie karty liniowe oraz moduły zarządzająco-przełączające zachowały kompatybilność pomiędzy posiadanymi obecnie przełącznikami Cisco Catalyst 6509-E i przełącznikami oferowanymi w ramach niniejszego zamówienia.

1. Urządzenie o architekturze modularnej – minimum 7-slotowe (w tym minimum 5 slotów przeznaczonych na karty liniowe), pozwalającą na instalację 48 portowych kart liniowych i redundantnych modułów zarządzająco-przełączających
2. Wymagane niezbędne wyposażenie urządzenia:
   a. Moduł zarządzająco-przełączający. Urządzenie musi mieć możliwość rozbudowy i wyposażenia w redundantny moduł zarządzająco-przełączający (pracujący w trybie active-hot standby). W przypadku urządzenia wyposażonego w redundantne moduły awaria jednego z modułów zarządzająco-przełączających nie może spowodować spadku wydajności urządzenia poniżej określonego niżej poziomu wydajności
   b. Redundantne zasilacze AC (zapewniające redundancję zasilania w trybie co najmniej N:1)
   c. 2 moduły 48-portowe 100/1000 Gigabit Ethernet (dopuszczalna nadsubskrypcja względem matrycy przełączającej nie większa niż 1.2:1). Jeśli gęstość portów na karcie liniowej jest mniejsza dopuszcza się dostarczenie większej liczby kart tak, aby sumaryczna liczba portów była nie mniejsza niż 96x100/1000
   d. Minimum 24-porty 1 Gigabit Ethernet SFP (dopuszczalna nadsubskrypcja względem matrycy przełączającej nie większa niż 1.2:1). obsadzonych wkładkami

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

e. Minimum 16 portów 10GigabitEthernet przeznaczone dla wkładek typu X2, SFP+ lub równoważnych (dopuszczalna nadsubskrypcja względem matrycy przełączającej nie większa niż 2:1) obsadzonych wkładkami

f. Wkładki optyczne (SFP, SFP+, X2 itp.) przeznaczone do instalacji w przełączniku muszą pochodzić od tego samego producenta co oferowany przełącznik

g. Minimum 1 slot na moduły liniowe w urządzeniu musi pozostać wolny – celem jego przyszłej rozbudowy

h. Możliwość rozbudowy o karty z interfejsami 40GE

3. Dostępne pasmo min. 80 Gb/s (możliwość zapewnienia obsługi kart minimum 8-portowych 10GE bez nadsubskrypcji względem matrycy przełączającej) na każdy z dostępnych slotów
4. Wydajność przełączania na poziomie min. 60 mln p/s per moduł liniowy dla przełączania L2 oraz routingu IPv4 i 30 mln p/s per moduł liniowy dla routingu IPv6, tunelowania GRE
5. Obsługa przetwarzania rozproszonego – wszystkie oferowane karty liniowe muszą mieć możliwość samodzielnego przełączania ruchu (bez pośrednictwa karty zarządzającej), jeśli wymagane są dodatkowe moduły zapewniające tą funkcjonalność muszą być dołączone
6. Wymagane parametry wydajnościowe:
   a. min. 100 000 wpisów w tablicy adresów MAC
   b. min. 250 000 wpisów w tablicy routingowej IPv4
   c. min. 125 000 wpisów w tablicy routingowej IPv6
   d. min. 125 000 tras multicast
   e. min. 64 000 wpisów na potrzeby realizacji polityk QoS i bezpieczeństwa (listy kontroli dostępu)
7. Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4
8. Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), MP-BGP
9. Mechanizm Non-Stop-Forwarding lub równoważny

10. Obsługuje sprzętowo ruch multicastowy w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD
11. Urządzenie musi umożliwiać rozszerzenie funkcjonalności o wsparcie dla MPLS, LDP, L2 i L3 VPN, VPLS, MPLS TE, MPLS traceruote poprzez zakup odpowiedniej licencji lub wymianę oprogramowana bez konieczności modernizacji sprzętowej urządzenia
12. Sprzętowa obsługa tunelowania GRE
13. Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. mechanizm BFD (Bidirectional Forwarding Detection) co najmniej dla protokołu OSPFv2 i OSPFv3
    b. IEEE 802.1w Rapid Spanning Tree
    c. IEEE 802.1s Multiple Spanning Tree
    d. IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów z wykorzystaniem portów znajdujących się na różnych kartach liniowych
    e. pozwala na wymianę kart liniowych i modułów bez wyłączania zasilania (tzw. Hot-Swap)
14. Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS):
    a. Obsługa min. 8 kolejek sprzętowych dla portów 10GE i min. 4 kolejek sprzętowych dla portów GE
    b. Obsługa co najmniej jednej kolejki ze statusem strict priority
    c. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    d. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP

e. Definiowanie polityk QoS per port i per VLAN

f. Mechanizm AutoQoS lub równoważny

15. Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem:

a. Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend

b. Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Gurad

c. Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – sprzętowo zarówno dla IPv4 i IPv6

d. Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP

e. Listy kontroli dostępu także dla IPv6

f. Mechanizmy ochrony warstwy kontrolnej

16. Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem:

a. możliwość zarządzania przez SNMPv3 oraz SSH v2

b. Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Gigabit Ethernet

c. Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+

d. Obsługa kart pamięci Compact Flash (lub równoważnych)

e. Umożliwia stworzenie wirtualnego systemu złożonego z min. 2 urządzeń będącego przedmiotem opisu, zarządzanego jako całość. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10GE Ethernet oraz modułów optycznych

f. Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia

monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN

g. Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow lub odpowiednik)

h. Definiowanie skryptów określających polityki przekazywania zdarzeń do systemów zarządzających (korelacja, zależności parametrów, diagnostyka, definicja alarmów)

i. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych

17. Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)
18. Przystosowane do montażu w szafie 19”, wysokość nie większa niż 10RU
19. Dostarczenie szafy typu Rack „19” 42U
20. Dostarczenie 32x 10GE Transceiver
21. Dostarczenie 24 x 1GE Transceiver
22. Transceivery przeznaczone do instalacji w przełączniku muszą pochodzić od tego samego producenta co oferowany przełącznik
23. spełniać wszystkie wymagania ogólne określone powyżej dla nowych urządzeń

II. Wymagania dotyczące zakresu wdrożenia przełącznika modularnego, rdzeniowego w Głównym Urzędzie Statystycznym

Podczas wdrożenia wykonane zostaną następujące prace:

1. Analiza przedwdrożeniowa obejmująca weryfikację konfiguracji sieci Zamawiającego niezbędną do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze na których Zamawiający szczegółowo przedstawi konfiguracją urządzeń w zakresie niezbędnym do realizacji przedmiotu umowy,
2. Opracowanie projektu technicznego opisującego szczegółową konfigurację urządzeń niezbędną do realizacji wdrożenia,

3. Instalację modułowego przełącznika centralnego w szafie RACK 19” w serwerowni na I piętrze. Dokładne miejsce instalacji wyznaczy Zamawiający,
4. Konfigurację urządzenia zgodnie z zaakceptowanym przez Zamawiającego projektem technicznym, zakładająca przebudowę istniejącej sieci szkieletowej znajdującej się w serwerowni na I piętrze, W ramach modernizacji mają zostać przeniesione interfejsy VLAN-ów oraz połączenia poszczególnych segmentów sieci oraz krytycznych serwerów w taki sposób, by zapewnić ciągłość działania usług i aplikacji.
5. Testy akceptacyjne potwierdzające zgodność wdrożonego rozwiązania z wymaganiami opisanymi w Opisie Przedmiotu Zamówienia – część 3,
6. Wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.

III. Warunki gwarancji

1. Wykonawca udzieli Zamawiającemu 36-miesięcznej gwarancji na dostarczony sprzęt. Gwarancja obejmuje zobowiązanie Wykonawcy do terminowego usuwania wad i usterek urządzeń sieciowych oraz innych elementów dostarczonych wraz ze sprzętem
2. Wykonawca zobowiązuje się, iż w okresie gwarancji, czas reakcji na zgłoszoną przez Zamawiającego wadę lub usterkę nastąpi nie później niż w ciągu 4 godzin od momentu zgłoszenia wady lub usterki.
3. Wykonawca zobowiązuje się do przywrócenia pełnej funkcjonalności urządzeń w ciągu 24 godzin od zgłoszenia
4. Naprawa zostanie dokonana w miejscu instalacji urządzenia lub sprzetu.
5. W przypadku niewykonania naprawy gwarancyjnej w miejscu i w terminie, o którym mowa w ust. 3 i 4, Wykonawca zobowiązuje się dostarczyć na czas naprawy takie samo urządzenie wolne od wad i zapewni jego prawidłowe działanie. Ostateczny termin usunięcia wady lub usterki uszkodzonego urządzenia nie może być dłuższy niż 30 dni od dnia zgłoszenia jego wady lub usterki.
6. Wykonawca zobowiązuje się do wymiany urządzenia na nowe w przypadku, gdy po wykonaniu dwóch napraw gwarancyjnych dostarczonego urządzenia będzie ono wykazywało nadal wady w działaniu.

7. W przypadku nie wywiązania się Wykonawcy ze zobowiązań gwarancyjnych, Zamawiający może dokonać tych czynności we własnym zakresie i kosztami obciążyć Wykonawcę.
8. Wykonawca pokrywa wszelkie koszty związane z naprawami gwarancyjnymi.
9. Zamawiający zobowiązany jest do udzielenia szczegółowych informacji o zewnętrznych objawach wady lub usterki oraz czasie jej wystąpienia.
10. W przypadku naprawy gwarancja ulega przedłużeniu o czas naprawy.
11. Zamawiający ma prawo dokonywania rozbudowy sprzętu, zgodnie z dokumentacją techniczną, przez wykwalifikowanych pracowników, a także prawo do przemieszczenia zainstalowanego sprzętu bez utraty gwarancji. Wykonawca nie ponosi odpowiedzialności za uszkodzenia mechaniczne przedmiotu Umowy powstałe z winy pracowników Zamawiającego.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji