Załącznik Nr 4 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu sieciowego oraz rozbudowa lokalnych sieci komputerowych w siedzibie Starostwa Powiatowego w Słubicach i pięciu lokalizacjach zdalnych w ramach projektu pn.: Rozwój e-usług w Powiecie Słubickim realizowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach Osi Priorytetowej 2 „Rozwój cyfrowy", działanie 2.1 „Rozwój społeczeństwa informacyjnego",

Przedmiotem zamówienia jest rozbudowa lokalnych sieci komputerowych w siedzibie Starostwa Powiatowego w Słubicach, ul. Józefa Piłsudskiego 20, 69-100 Słubice oraz w każdej z pięciu wymienionych poniżej powiatowych jednostek organizacyjnych zwaną dalej lokalizacją zdalną:

1) Zespół Szkół Licealnych (ZSL) ul. Boh. Warszawy 3, 69-100 Słubice,
2) Zespół Szkół Technicznych (ZST) Al. Niepodległości 13, 69-100 Słubice,
3) Centrum Kształcenia Zawodowego i Ustawicznego (CKZU) Al. Niepodległości 23, 69-100 Słubice,
4) Specjalny Ośrodek Szkolno – Wychowawczy (SOSW) Al. Niepodległości 23A, 69-100 Słubice,
5) Centrum Usług Wspólnych (CUW)/Poradnia Psychologiczno – Pedagogiczna (PPP) ul. Sienkiewicza 28, 69-100 Słubice,

dla potrzeb transmisji danych wewnątrz oraz pomiędzy sieciami lokalnymi LAN znajdującymi się w ww. lokalizacjach.

Wymagania techniczne dla Starostwa Powiatowego:

1) W ramach realizacji przedmiotu zamówienia należy w szafie 19" znajdującej się w Centralnym Punkcie Dystrybucyjnym (CPD) Starostwa zainstalować, podłączyć i skonfigurować następujące urządzenia sieciowe:
   1. **Wielofunkcyjna zapora sieciowa z 5. letnią subskrypcją spełniające następujące wymagania minimalne (1 szt.):**

1.1. Architektura urządzenia

1.1.1. Urządzenie o konstrukcji modularnej pełniące funkcje bramy VPN i ściany ogniowej (firewall) typu Statefull Inspection. Urządzenie musi mieć możliwość dalszej rozbudowy sprzętowej.

1.1.2. Urządzenie wyposażone w:

1.1.2.1. min. sześć interfejsów Gigabit Ethernet 10/100/1000 (RJ45) lub min. cztery interfejsy 10 Gigabit Ethernet

1.1.2.2. dedykowany interfejs do zarządzania

1.1.3. Urządzenie obsługuje interfejsy VLAN-IEEE 802.1q na interfejsach fizycznych (min. 50 sumarycznie).

1.1.4. Urządzenie wyposażone w moduł sprzętowego wsparcia szyfrowania 3DES i AES oraz licencje na szyfrowanie 3DES/AES.

1.1.5. Urządzenie posiada dedykowany dla zarządzania port konsoli.

1.1.6. Urządzenie posiada pamięć Flash o pojemności umożliwiającej przechowanie co najmniej 3 obrazów systemu operacyjnego i 3 plików konfiguracyjnych.

1.1.7. Urządzenie posiada pamięć DRAM o pojemności min, 4GB, umożliwiającej uruchomienie wszystkich dostępnych dla urządzenia funkcjonalności.

1.1.8. Urządzenie zapewnia możliwość klastrowania. Wspierane są min. dwa urządzenia w klastrze.

1.2. Zasilanie urządzenia

Urządzenie posiada zasilacz umożliwiający zasilanie prądem przemiennym 230V.

1.3. Wydajność urządzenia

1.3.1. Przepustowość teoretyczna stanowego firewall'a wynosi 1 Gbps, a dla ruchu rzeczywistego (tzw. ruch multiprotocol) 500 Mbps.
1.3.2. Urządzenie posiada wydajność 200 Mbps dla ruchu szyfrowanego protokołami 3DES, AES.
1.3.3. Urządzenie umożliwia terminowanie 250 jednoczesnych sesji VPN (IPSec VPN, SSL VPN).
1.3.4. Urządzenie zapewnia zestawianie do 250 tuneli SSL VPN w trybie client-based i clientless VPN.
1.3.5. Urządzenie obsługuje 100000 jednoczesnych sesji/połączeń z prędkością zestawiania min.9000 połączeń na sekundę.
1.3.6. Urządzenie posiada możliwość agregacji interfejsów fizycznych (IEEE 802.3ad) – 4 łączy zagregowanych. Pojedyncze łącze zagregowane może składać się z 2 interfejsów.
1.3.7. Urządzenie obsługuje funkcjonalność Access Control List (ACL) – zarówno dla ruchu wchodzącego, jak i wychodzącego.
1.3.8. Obsługa min. 50 VLAN'ów.

1.4. Funkcjonalność urządzenia

1.4.1. Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. Stateful Inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.
1.4.2. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (tzw. Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory.
1.4.3. Urządzenie posiada możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos.
1.4.4. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
1.4.5. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access).
1.4.6. Urządzenie zapewnia w zakresie SSL VPN weryfikację uprawnień stacji do zestawiania sesji, poprzez weryfikację następujących cech:
  1.4.6.1. OS Check - system operacyjny
  1.4.6.2. IP Address Check - adres z jakiego następuje połączenie
  1.4.6.3. File Check - pliki w systemie
  1.4.6.4. Registry Check - wpisy w rejestrze systemu Windows
  1.4.6.5. Certificate Check - zainstalowane certyfikaty
1.4.7. Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN.
1.4.8. Oprogramowanie klienta VPN (IPSec oraz SSL) ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows (7, XP – wersje 32 i 64-bitowe) i Linux i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.
1.4.9. Oprogramowanie klienta VPN obsługuje protokoły szyfrowania 3DES/AES.
1.4.10. Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połączenia klientem VPN (wyłączanie tzw. split-tunnelingu).
1.4.11. Urządzenie ma możliwość pracy jako transparentna ściana ogniowa warstwy drugiej modelu ISO OSI.
1.4.12. Urządzenie obsługuje protokół NTP.
1.4.13. Urządzenie współpracuje z serwerami CA.
1.4.14. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego. Urządzenie wspiera translację adresów (NAT) dla ruchu multicastowego.
1.4.15. Urządzenie zapewnia mechanizmy redundancji, w tym:
  1.4.15.1. możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby, active/active dla kontekstów
  1.4.15.2. umożliwia pracę w klastrze
1.4.16. Urządzenie realizuje synchronizację tablicy połączeń pomiędzy węzłami pracującymi w trybie wysokiej dostępności HA.
1.4.17. Urządzenie zapewnia możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia.
1.4.18. Urządzenie zapewnia funkcjonalność stateful failover dla ruchu VPN.
1.4.19. Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
  1.4.19.1. Hypertext Transfer Protocol (HTTP),
  1.4.19.2. File Transfer Protocol (FTP),
  1.4.19.3. Extended Simple Mail Transfer Protocol (ESMTP),
  1.4.19.4. Domain Name System (DNS),
  1.4.19.5. Simple Network Management Protocol v 1/2/3 (SNMP),
  1.4.19.6. Internet Control Message Protocol (ICMP),
  1.4.19.7. SQL*Net,
  1.4.19.8. inspekcji protokołów dla ruchu voice/video – H.323 (włącznie z H.239), SIP, MGCP, RTSP
1.4.20. Urządzenie umożliwia zaawansowaną normalizację ruchu TCP:
  1.4.20.1. poprawność pola TCP ACK
  1.4.20.2. poprawność sekwencjonowania segmentów TCP

1.4.20.3. poprawność ustanawiania sesji TCP z danymi
1.4.20.4. limitowanie czasu oczekiwania na segmenty nie w kolejności
1.4.20.5. poprawność pola MSS
1.4.20.6. poprawność pola długości TCP
1.4.20.7. poprawność skali okna segmentów TCP non-SYN
1.4.20.8. poprawność wielkości okna TCP

1.4.21. Urządzenie ma możliwość blokowania aplikacji (np. peer-to-peer, czy „internetowy komunikator") wykorzystujących port 80.
1.4.22. Urządzenie zapewnia obsługę i kontrolę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP.
1.4.23. Urządzenie ma możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe.
1.4.24. Urządzenie zapewnia wsparcie stosu protokołów IPv6, w tym:
1.4.24.1. listy kontroli dostępu dla IPv6
1.4.24.2. możliwości filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload
1.4.24.3. inspekcję protokołu IPv6, pracując w trybie transparentnym
1.4.24.4. adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover)
1.4.24.5. realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6
1.4.25. Urządzenie obsługuje mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu.
1.4.26. Urządzenie umożliwia współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik.
1.4.27. Urządzenie obsługuje routing statyczny i dynamiczny (min. dla protokołów RIP, OSPF i BGP).
1.4.28. Urządzenie pozwala na osiągnięcie wysokiej dostępności dla protokołów routingu dynamicznego, tzn. trasy dynamiczne zawarte w tablicy routingu są synchronizowane z urządzenia active na urządzenie standby.
1.4.29. Urządzenie umożliwia zbieranie informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL).
1.4.30. Urządzenie umożliwia konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie.
1.4.31. Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu.
1.4.32. Urządzenie umożliwia pominięcie stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu.
1.4.33. Urządzenie wspiera Proxy dla protokołu SCEP i umożliwia zautomatyzowany proces pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN.
1.4.34. Urządzenie wspiera użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie Microsoft AD, bezpośrednio lub poprzez ACS, dla obsługi sytuacji wygaśnięcia terminu ważności hasła w systemie Microsoft AD, umożliwiając zmianę przeterminowanego hasła.
1.4.35. Urządzenie obsługuje IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode. Ponadto urządzenie wspiera protokół IKEv2 (Internet Key Exchange w wersji 2) dla połączeń zdalnego dostępu VPN oraz site-to-site VPN opartych o protokół IPSec.

1.5. Funkcjonalność urządzenia - NGFW

1.5.1. Urządzenie zapewnia funkcjonalności tzw. Next-Generation Firewall w następującym zakresie:
1.5.1.1. system automatycznego wykrywania i klasyfikacji aplikacji (tzw. Application Visibility and Control)
1.5.1.2. system IPS
1.5.1.3. system filtrowania ruchu w oparciu o URL
1.5.1.4. system ochrony przed malware
1.5.2. System posiada otwarte API dla współpracy z systemami zewnętrznymi, takimi jak SIEM.
1.5.3. System automatycznego wykrywania i klasyfikacji aplikacji (AVC):
1.5.3.1. posiada możliwość klasyfikacji ruchu i wykrywania aplikacji sieciowych
1.5.3.2. zapewnia wydajność min. 100Mbps
1.5.3.3. pozwala na tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług
1.5.3.4. pozwala na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
1.5.3.5. umożliwia współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach
1.5.4. System IPS:
1.5.4.1. zapewnia skuteczność wykrywania zagrożeń i ataków na poziomie 95%, udokumentowaną przez niezależnie testy
1.5.4.2. posiada możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)

1.5.4.3. posiada możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu)
1.5.4.4. posiada możliwość wykrywania i eliminowania szerokiej gamy zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługę VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, itp.)
1.5.4.5. posiada możliwość wykrywania modyfikacji znanych ataków, jak i tych nowo powstałych, które nie zostały jeszcze dogłębnie opisane
1.5.4.6. zapewnia następujące sposoby wykrywania zagrożeń:
1.5.4.6.1. sygnatury ataków opartych na exploitach,
1.5.4.6.2. reguły oparte na zagrożeniach,
1.5.4.6.3. mechanizm wykrywania anomalii w protokołach
1.5.4.6.4. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
1.5.4.7. posiada możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego, włącznie z możliwością sprawdzania zawartości pakietu
1.5.4.8. posiada mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives)
1.5.4.9. posiada możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
1.5.4.10. posiada wiele możliwości reakcji na zdarzenia, takich jak monitorowanie, blokowanie ruchu zawierającego zagrożenia, zastępowanie zawartość pakietów oraz zapisywanie pakietów
1.5.4.11. posiada możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
1.5.4.12. posiada możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności (systemy operacyjne, serwisy, otwarte porty, aplikacje oraz zagrożenia) w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności
1.5.4.13. posiada możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych
1.5.4.14. zapewnia możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
1.5.4.15. posiada możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
1.5.4.16. zapewnia możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS - w tym celu stosuje odpowiedni mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
1.5.4.17. zapewnia mechanizm bezpiecznej aktualizacji sygnatur - zestawy sygnatur/reguł pobierane są z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
1.5.4.18. zapewnia możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
1.5.4.19. jest zarządzany poprzez system centralnego zarzadzania za pomocą szyfrowanego połączenia
1.5.4.20. zapewnia obsługę reguł Snort
1.5.4.21. zapewnia możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
1.5.4.22. zapewnia mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (tzw. Indication of Compromise)
1.5.4.23. zapewnia mechanizmy automatyzacji w zakresie dostrojenia polityk bezpieczeństwa
1.5.4.24. posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewall'a dla uzyskania pełnej widoczności ruchu – w szczególności posiada możliwość pracy w trybie HA firewalla oraz w trybie klastrowania
1.5.4.25. pozwala na pracę z przepustowością 75 Mbps przy jednoczesnym działaniu AVC
1.5.5. System filtrowania ruchu w oparciu o URL:
1.5.5.1. pozwala na kategoryzację stron w min. 70 kategoriach
1.5.5.2. zapewnia bazę URL o wielkości min. 250 mln URL
1.5.6. System ochrony przed malware:
1.5.6.1. zapewnia sprawdzenie reputacji plików w systemie globalnym
1.5.6.2. zapewnia sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze)
1.5.6.3. zapewnia narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych później jako oprogramowanie złośliwe (analiza retrospektywna)
1.5.6.4. zapewnia wykrywanie ataków typu Zero-Day
1.5.7. System zapewnia centralną konsolę zarządzania zapewniającą informacje ogólne i szczegółowe o:
1.5.7.1. wykrytych hostach
1.5.7.2. aplikacjach
1.5.7.3. zagrożeniach i atakach
1.5.7.4. wskazaniach kompromitacji (tzw. Indication of Compromise) na podstawie:
1.5.7.4.1. zdarzeń z IPS
1.5.7.4.1.1. malare backdoors

1.5.7.4.1.2. exploit kits
1.5.7.4.1.3. ataków na aplikacje webowe
1.5.7.4.1.4. połączeń do serwerów Command'n'Control
1.5.7.4.1.5. wskazań eskalacji uprawnień
1.5.7.4.2. zdarzeń sieciowych
1.5.7.4.2.1. połączeń do znanych adresów IP Command'n'Control
1.5.7.4.3. zdarzeń związanych z malware
1.5.7.4.3.1. wykrytego malware
1.5.7.4.3.2. wykrytej infekcji dropperów

1.6. Zarządzanie i konfiguracja

1.6.1. Urządzenie posiada możliwość eksportu informacji przez syslog.
1.6.2. Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogicznego.
1.6.3. Urządzenie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+ oraz obsługuje mechanizmy AAA (Authentication, Authorization, Accounting).
1.6.4. Urządzenie jest konfigurowalne przez CLI oraz interfejs graficzny.
1.6.5. Dostęp do urządzenia jest możliwy przez SSH.
1.6.6. Urządzenie obsługuje protokół SNMP v 1/2/3.
1.6.7. Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.
1.6.8. Urządzenie posiada wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łącznością w sieciach IP.

1.7. Obudowa i licencjonowanie

1.7.1. Urządzenie ma możliwość instalacji w szafie typu rack 19".
1.7.2. Wysokość urządzenia wynosi maksimum 2RU.
1.7.3. Urządzenie jest wyposażone w 5-letnią subskrypcję na IPS, filtrowanie URL, oraz ochronę przed malware.

2. Zarządzalny przełącznik 24 porty Ethernet, 4 porty SFP z funkcją zasilania PoE, spełniający następujące wymagania minimalne (2 szt.):

1. Typ i liczba portów:
   1.1. Minimum 24 porty 10/100/1000 PoE+ zgodne z IEEE 802.3at
   1.2. Minimum 4 dodatkowe porty uplink Gigabit Ethernet SFP
   1.3. Porty SFP muszą umożliwiać ich obsadzanie wkładkami Gigabit Ethernet – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U oraz modułami CWDM zależnie od potrzeb Zamawiającego
2. Wymagane jest, aby wszystkie porty dostępowe 10/100/1000 obsługiwały standard zasilania poprzez sieć LAN (Power over Ethernet) zgodnie z IEEE 802.3at. Zasilacz urządzenia musi być tak dobrany, aby zapewnić minimum 370W dla portów PoE/PoE+
3. Urządzenie musi obsługiwać minimum 1000 sieci VLAN
4. Urządzenie musi obsługiwać minimum 16000 adresów MAC
5. Urządzenie musi posiadać min. 512MB pamięci DRAM i 128MB pamięci flash
6. Parametry fizyczne – wysokość maksimum 1RU, możliwość montażu w szafie 19"
7. Wydajność przełączania minimum 60 Mpps dla pakietów 64-bajtowych.
8. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
   8.1. Do min. 8 jednostek w stosie
   8.2. Możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel)
   8.3. Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania nie jest wymagane
9. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów
10. Wbudowane funkcje zarządzania energią:
    10.1. Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
11. Obsługa protokołu NTP
12. Musi zapewniać obsługę min. 16 statycznych tras dla routingu IPv4 i IPv6
13. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping
14. 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
15. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server

16. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad.
17. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
    17.1. Minimum 3 poziomy dostępu administracyjnego poprzez konsolę
    17.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
    17.3. Obsługa funkcji Guest VLAN
    17.4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    17.5. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    17.6. Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www
    17.7. Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
    17.8. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
    17.9. Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6
    17.10. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
    17.11. Funkcjonalność Protected Port
    17.12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) oraz ochronę przed fałszowaniem źródłowych adresów IPv6 (IPv6 Source Guard)
    17.13. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
    17.14. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne)
18. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    18.1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    18.2. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek
    18.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    18.4. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. Wymagana jest możliwość skonfigurowania minimum 256 różnych ograniczeń
19. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienia.
20. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)
21. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
22. Przełącznik musi 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)
23. 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
24. Zasilanie 230V AC, możliwość zastosowania redundantnego zasilacza (dopuszczalne rozwiązania zewnętrzne)
25. Wyposażenie urządzenia:
    25.1. wkładki optyczne w standardzie SFP WDM (1 port x 1,25 Gbps SC SM, zasięg 20km) x 4szt
    25.2. Moduły SFP muszą być kompatybilne z oferowanym przełącznikiem
    25.3. Redundantny zasilacz o mocy identycznej jak zasilacz podstawowy.

3. Zarządzalny przełącznik 48 portów Ethernet, 4 porty SFP spełniający następujące wymagania minimalne (1 szt.):

1. Typ i liczba portów:
   1.1. Minimum 48 portów 10/100/1000
   1.2. Minimum 4 dodatkowe porty uplink Gigabit Ethernet SFP
   1.3. Porty SFP muszą umożliwiać ich obsadzanie wkładkami Gigabit Ethernet – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U oraz modułami CWDM zależnie od potrzeb Zamawiającego
2. Urządzenie musi obsługiwać minimum 1000 sieci VLAN
3. Urządzenie musi obsługiwać minimum 16000 adresów MAC
4. Urządzenie musi posiadać min. 512MB pamięci DRAM i 128MB pamięci flash
5. Parametry fizyczne – wysokość maksimum 1RU, możliwość montażu w szafie 19”
6. Wydajność przełączania minimum 100 Mpps dla pakietów 64-bajtowych.
7. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
   7.1. Do min. 8 jednostek w stosie
   7.2. Możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel)
   7.3. Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania nie jest wymagane
8. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów
9. Wbudowane funkcje zarządzania energią:
   9.1. Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
10. Obsługa protokołu NTP
11. Musi zapewniać obsługę min. 10 statycznych tras dla routingu IPv4 i IPv6
12. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping
13. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu STP
14. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server
15. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad.
16. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
   16.1. Minimum 3 poziomy dostępu administracyjnego poprzez konsolę
   16.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
   16.3. Obsługa funkcji Guest VLAN
   16.4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
   16.5. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
   16.6. Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www
   16.7. Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
   16.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
   16.9. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
   16.10. Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6
   16.11. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
   16.12. Funkcjonalność Protected Port
   16.13. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
   16.14. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
   16.15. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne)
17. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   17.1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
   17.2. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek
   17.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

17.4. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. Wymagana jest możliwość skonfigurowania minimum 256 różnych ograniczeń
18. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienia.
19. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)
20. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
21. Przełącznik musi 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)
22. 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
23. Zasilanie 230V AC, możliwość zastosowania redundantnego zasilacza (dopuszczalne rozwiązania zewnętrzne)
24. Wyposażenie urządzenia:
    24.1. wkładki optyczne w standardzie SFP WDM (1 port x 1,25 Gbps SC SM, zasięg 20km) x 4szt.
    24.2. Moduły SFP muszą być kompatybilne z oferowanym przełącznikiem
    24.3. Redundantny zasilacz o mocy identycznej jak zasilacz podstawowy.

2) W uzgodnionych z Zamawiającym lokalizacjach Starostwa zainstalować, podłączyć i skonfigurować 5 punktów dostępowych z zasilaniem PoE spełniające następujące wymagania minimalne:

Punkt dostępu bezprzewodowego (5 szt.):

1. obsługa standardów 802.11a/b/g/n/ac (Wave 2)
    1.1. obsługa SU-MIMO – min. 3x3:2
    1.2. obsługa MU-MIMO – min. 3x3:2
    1.3. obsługa kanałów 20 i 40 MHz dla 802.11n
    1.4. obsługa kanałów 20, 40 i 80 MHz dla 802.11ac
    1.5. obsługa prędkości PHY do 867 Mbps
    1.6. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
    1.7. obsługa TxBF (transmitbeamforming) dla klientów 802.11ac
    1.8. obsługa MRC
2. obsługa szerokiego zakresu kanałów radiowych:
    2.1. dla zakresu 2.4 GHz: 13 kanałów
    2.2. dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów
    2.3. dla zakresu 5GHz (extended UNII-2): min. 8 kanałów
3. konfigurowalna moc nadajnika
    3.1. dla zakresu 2.4 GHz: do 100 mW
    3.2. dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW
    3.3. dla zakresu 5GHz (extended UNII-2): do 200 mW
4. zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
    4.1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
    4.2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
    4.3. obsługa min. 16 BSSID
    4.4. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
    4.5. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN
    4.6. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IDS)
    4.7. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
    4.8. obsługa IPv6
    4.9. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
    4.10. obsługa mechanizmów QoS:
        4.10.1. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik
        4.10.2. obsługa WMM, TSPEC, U-APSD
    4.11. współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne
    4.12. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM
    4.13. wsparcie IEEE 802.11i, WPA2, WPA

5. możliwość pracy jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach: (zmiana trybu pracy (przez wgranie oprogramowania) musi być bezkosztowa w okresie trwania kontraktu serwisowego):
   5.1. obsługa do 50 punktów dostępowych bez dodatkowych licencji
   5.2. obsługa do 1000 klientów
   5.3. możliwość konfiguracji do 16 sieci bezprzewodowych
   5.4. centralna optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
   5.5. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
   5.6. obsługa mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v
   5.7. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)
   5.8. wykrywanie obcych klientów oraz obcych AP
   5.9. konfiguracja polityk bezpieczeństwa per SSID
   5.10. obsługa WPA2 Personal oraz Enterprise
   5.11. współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)
   5.12. tworzenie list kontroli dostępu
   5.13. filtrowanie MAC adresów (Whitelist)
   5.14. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)
   5.15. profilowanie urządzeń podłączających się do sieci bezprzewodowej
   5.16. obsługa mechanizmów QoS
   5.17. obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym
   5.18. obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; obsługa wydrukowania lub wysłania mailem danych logowania użytkowników
   5.19. zarządzanie przez HTTPS
   5.20. wsparcie SSH, SNMP, NTP, SYSLOG
   5.21. wbudowany serwer DHCP
   5.22. wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera
6. interfejs Gigabit Ethernet (10/100/1000)
7. interfejs konsoli RJ45
8. 1 GB RAM, 256 MB Flash
9. zróżnicowane możliwości zasilania:
   9.1. zasilacz sieciowy 230V AC
   9.2. zasilanie PoE+ (802.3at) w sposób zapewniający pełną wydajność
   9.3. zasilanie PoE (802.3af) wyłącza port USB
10. anteny zintegrowane dookólne o zysku min. 3dBi dla pasma 2,4 GHz oraz zysku min. 5 dBi dla pasma 5 GHz
11. obudowa przystosowana do warunków pracy w pomieszczeniach biurowych (0 – 40^{o}C)
12. diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji
13. zgodność z dyrektywą 1999/5/EC i 93/42/ECC

Wymagania techniczne dla każdej lokalizacji zdalnej:

1) W ramach realizacji przedmiotu zamówienia należy w szafie 19” znajdującej się w Centralnym Punkcie Dystrybucyjnym (CPD) lokalizacji zdalnej zainstalować, podłączyć i skonfigurować następujące urządzenie sieciowe:
   1. **Zarządzalny przełącznik 48 porty Ethernet, 4 porty SFP z funkcją zasilania PoE, spełniający następujące wymagania minimalne (1 szt.):**

1. Typ i liczba portów:

1.1. Minimum 48 portów 10/100/1000 PoE+ zgodne z IEEE 802.3at
1.2. Minimum 4 dodatkowe porty uplink Gigabit Ethernet SFP
1.3. Porty SFP muszą umożliwiać ich obsadzanie wkładkami Gigabit Ethernet – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U oraz modułami CWDM zależnie od potrzeb Zamawiającego
2. Wymagane jest, aby wszystkie porty dostępowe 10/100/1000 obsługiwały standard zasilania poprzez sieć LAN (Power over Ethernet) zgodnie z IEEE 802.3at. Zasilacz urządzenia musi być tak dobrany, aby zapewnić minimum 370W dla portów PoE/PoE+
3. Urządzenie musi obsługiwać minimum 1000 sieci VLAN
4. Urządzenie musi obsługiwać minimum 16000 adresów MAC
5. Urządzenie musi posiadać min. 512MB pamięci DRAM i 128MB pamięci flash
6. Parametry fizyczne – wysokość maksimum 1RU, możliwość montażu w szafie 19”
7. Wydajność przełączania minimum 100 Mpps dla pakietów 64-bajtowych.
8. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
8.1. Do min. 8 jednostek w stosie
8.2. Możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel)
8.3. Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania nie jest wymagane
9. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów
10. Wbudowane funkcje zarządzania energią:
10.1. Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
11. Obsługa protokołu NTP
12. Musi zapewniać obsługę min. 10 statycznych tras dla routingu IPv4 i IPv6
13. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping
14. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu STP
15. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server
16. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad.
17. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
17.1. Minimum 3 poziomy dostępu administracyjnego poprzez konsolę
17.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
17.3. Obsługa funkcji Guest VLAN
17.4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
17.5. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
17.6. Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www
17.7. Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
17.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
17.9. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
17.10. Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6
17.11. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
17.12. Funkcjonalność Protected Port
17.13. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
17.14. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
17.15. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne)
18. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
18.1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP

18.2. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek
18.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
18.4. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. Wymagana jest możliwość skonfigurowania minimum 256 różnych ograniczeń
19. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienia.
20. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)
21. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
22. Przełącznik musi 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)
23. 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
24. Zasilanie 230V AC, możliwość zastosowania redundantnego zasilacza (dopuszczalne rozwiązania zewnętrzne)
25. Wyposażenie urządzenia:
25.1. wkładki optyczne w standardzie SFP WDM (1 port x 1,25 Gbps SC SM, zasięg 20km) x 1szt
25.2. Moduły SFP muszą być kompatybilne z oferowanym przełącznikiem
25.3. Redundantny zasilacz o mocy identycznej jak zasilacz podstawowy

2) W uzgodnionych z Zamawiającym punktach lokalizacji zdalnej, podłączyć i skonfigurować 5 punktów dostępowych z zasilaniem PoE spełniające następujące wymagania minimalne:

Punkt dostępu bezprzewodowego (5 szt.):

1. obsługa standardów 802.11a/b/g/n/ac (Wave 2)
1.1. obsługa SU-MIMO – min. 3x3:2
1.2. obsługa MU-MIMO – min. 3x3:2
1.3. obsługa kanałów 20 i 40 MHz dla 802.11n
1.4. obsługa kanałów 20, 40 i 80 MHz dla 802.11ac
1.5. obsługa prędkości PHY do 867 Mbps
1.6. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
1.7. obsługa TxBF (transmitbeamforming) dla klientów 802.11ac
1.8. obsługa MRC
2. obsługa szerokiego zakresu kanałów radiowych:
2.1. dla zakresu 2.4 GHz: 13 kanałów
2.2. dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów
2.3. dla zakresu 5GHz (extended UNII-2): min. 8 kanałów
3. konfigurowalna moc nadajnika
3.1. dla zakresu 2.4 GHz: do 100 mW
3.2. dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW
3.3. dla zakresu 5GHz (extended UNII-2): do 200 mW
4. zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
4.1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
4.2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
4.3. obsługa min. 16 BSSID
4.4. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
4.5. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN
4.6. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IDS)
4.7. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
4.8. obsługa IPv6
4.9. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
4.10. obsługa mechanizmów QoS:

4.10.1. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik
4.10.2. obsługa WMM, TSPEC, U-APSD
4.11. współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne
4.12. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM
4.13. wsparcie IEEE 802.11i, WPA2, WPA

5. możliwość pracy jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach: (zmiana trybu pracy (przez wgranie oprogramowania) musi być bezkosztowa w okresie trwania kontraktu serwisowego):
   5.1. obsługa do 50 punktów dostępowych bez dodatkowych licencji
   5.2. obsługa do 1000 klientów
   5.3. możliwość konfiguracji do 16 sieci bezprzewodowych
   5.4. centralna optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
   5.5. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
   5.6. obsługa mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v
   5.7. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)
   5.8. wykrywanie obcych klientów oraz obcych AP
   5.9. konfiguracja polityk bezpieczeństwa per SSID
   5.10. obsługa WPA2 Personal oraz Enterprise
   5.11. współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)
   5.12. tworzenie list kontroli dostępu
   5.13. filtrowanie MAC adresów (Whitelist)
   5.14. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)
   5.15. profilowanie urządzeń podłączających się do sieci bezprzewodowej
   5.16. obsługa mechanizmów QoS
   5.17. obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym
   5.18. obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; obsługa wydrukowania lub wysłania mailem danych logowania użytkowników
   5.19. zarządzanie przez HTTPS
   5.20. wsparcie SSH, SNMP, NTP, SYSLOG
   5.21. wbudowany serwer DHCP
   5.22. wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera
6. interfejs Gigabit Ethernet (10/100/1000)
7. interfejs konsoli RJ45
8. 1 GB RAM, 256 MB Flash
9. zróżnicowane możliwości zasilania:
   9.1. zasilacz sieciowy 230V AC
   9.2. zasilanie PoE+ (802.3at) w sposób zapewniający pełną wydajność
   9.3. zasilanie PoE (802.3af) wyłącza port USB
10. anteny zintegrowane dookólne o zysku min. 3dBi dla pasma 2,4 GHz oraz zysku min. 5 dBi dla pasma 5 GHz
11. obudowa przystosowana do warunków pracy w pomieszczeniach biurowych (0 – 40^{o}C)
12. diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji
13. zgodność z dyrektywą 1999/5/EC i 93/42/ECC

Wymagania techniczne dla kompleksowego wdrożenia:

1. Wykonawca jest zobowiązany opracować projekt realizacyjny, który będzie zawierał harmonogram działań oraz pełen zakres prac wdrożeniowych dla dostarczanych produktów.
2. Wykonawca w oparciu o uzgodniony z Zamawiającym projekt realizacyjny wykona wdrożenie sieci LAN w siedzibie Starostwie i lokalizacjach zdalnych.

3. W ramach wdrożenia muszą zostać wykonane minimum następujące prace:
   a) konfiguracja adresacji IP;
   b) konfiguracja wielofunkcyjnej zapory sieciowej, przełączników oraz punktów dostępowych;
   c) konfiguracja mechanizmów bezpieczeństwa w dostępie do urządzeń;
   d) zdefiniowanie i skonfigurowanie połączeń między urządzeniami;
   e) zdefiniowanie sieci wirtualnych VLAN;
   f) konfiguracja routingu między sieciami VLAN;
   g) konfiguracja mechanizmów zabezpieczających ruch między sieciami VLAN;
   h) konfiguracja mechanizmów Quality of Service;
   i) konfiguracja mechanizmów bezpieczeństwa w sieci LAN (m.in. blokowanie portów w oparciu o adresy MAC, Access - listy na poziomie portu i VLANu, zabezpieczenie protokołów Spanning Tree oraz DHCP, zabezpieczenie dostępu administracyjnego);
   j) instalacja i konfiguracja oprogramowania zarządzającego;
   k) podłączenie i rekonfiguracja posiadanych przez Zamawiającego urządzeń sieciowych, które nie będą podlegać wymianie;
   m) testy działania sieci zgodnie ze scenariuszami z projektu realizacyjnego.

4. Po wykonaniu wdrożenia, a przed datą odbioru przedmiotu zamówienia Zamawiający otrzyma dokumentację powdrożeniową zawierającą następujące dane:
   a) architekturę logiczną sieci;
   b) architekturę fizyczną sieci;
   c) adresację IP;
   d) konfigurację wszystkich dostarczonych produktów tworzących sieć;
   f) dobre praktyki w zakresie administracji siecią, w szczególności:
   • wykonywania kopii zapasowych konfiguracji poszczególnych produktów;
   • instalacji oprogramowania na poszczególnych produktach;
   • przeglądu podstawowych parametrów sieci i produktów celem badania poprawności działania oraz wczesnego wykrywania problemów;
5. Wszystkie zastosowane rozwiązania techniczne wymagane do zestawienia i uruchomienia sieci muszą być dobrane przez Wykonawcę na podstawie jego wiedzy i doświadczenia oraz powinny być zgodne a obowiązującymi normami.
6. Udostępnienie przedmiotu zamówienia do eksploatacji odbędzie się na podstawie podpisanego obustronnie i bez zastrzeżeń protokołu odbioru końcowego.

Bezpieczeństwo systemu, gwarancja i serwis:

1. Dostarczony sprzęt sieciowy musi być fabrycznie nowy objęty 60 miesięczną gwarancją producenta świadczoną na miejscu u Zamawiającego (diagnoza i naprawa), możliwość zgłaszania awarii w trybie 24/7. Czas reakcji serwisu – do końca następnego dnia roboczego. Firma serwisująca musi posiadać autoryzację producenta.
2. W okresie udzielonej gwarancji Wykonawca zobowiązany będzie do świadczenia serwisu gwarancyjnego na swój koszt (obejmującego również dojazd i transport),

polegającego na wymianie przedmiotu zamówienia na wolny od wad lub usunięcia wad w drodze naprawy,

3. Serwis gwarancyjny świadczony będzie w miarę możliwości w miejscu użytkowania przedmiotu zamówienia (miejscu instalacji), a w przypadku braku takiej możliwości w siedzibie Wykonawcy, z tym że dostarczenie do siedziby Wykonawcy i z powrotem do miejsca instalacji następuje na koszt wykonawcy.
4. W przypadku, gdy naprawa sprzętu jest dłuższa niż 5 dni roboczych lub istnieje konieczność oddania sprzętu lub jego części do serwisu, Wykonawca jest zobowiązany do podstawienia zapasowego sprzętu o parametrach, co najmniej równorzędnych na okres naprawy gwarancyjnej. Sprzęt zapasowy powinien być dostarczony następnego dnia roboczego po dniu, w którym nastąpiło zgłoszenie, czas realizacji naprawy od momentu zgłoszenia nie może potrwać dłużej niż 14 dni od dnia powiadomienia serwisu.
5. W przypadku, gdy naprawa uszkodzonego sprzętu potrwa dłużej niż 14 dni lub sprzęt był naprawiany 2 razy i wystąpi kolejna wada, Zamawiającemu przysługuje wymiana sprzętu na nowy, taki sam lub uzgodniony, o co najmniej takich samych parametrach. Okres gwarancji zostanie automatycznie wydłużony o czas trwania naprawy.
6. Zamawiający wymaga zapewnienie na dedykowanej stronie internetowej producenta dostępu do najnowszego oprogramowania i uaktualnień, realizowanego poprzez podanie numeru seryjnego/modelu.
7. Wszystkie prace instalacyjne w budynkach wskazanych przez Zamawiającego mogą odbywać się tylko w czasie uzgodnionym z Zamawiającym i powinny być wykonane z należytą starannością, z zachowaniem ostrożności i czystości. Wykonawca po zakończeniu wszystkich prac instalacyjnych doprowadzi pomieszczenia w miejscach instalacji do stanu sprzed rozpoczęcia prac.
8. Wizje lokalne w budynku Starostwa i lokalizacjach zdalnych są możliwe w każdy dzień roboczy w godz. od 12:00 do 15:00 po uprzednim telefonicznym ustaleniu daty spotkania.