Załącznik nr 2 do Zapytania ofertowego

Specyfikacja przedmiotu zamówienia

dot. Zapytania ofertowego w trybie przetargu nieograniczonego na:

Dostawę, instalację, wdrożenie zintegrowanych urządzeń sieciowych typu UTM (HA), przełączników sieciowych oraz przeprowadzenie szkolenia z zaawansowanej konfiguracji urządzeń w Polskim Związku Łowieckim Zarządzie Głównym w Warszawie przy ulicy Nowy Świat 35.

Przedmiotem zamówienia jest dostawa fabrycznie nowych, nieużywanych, wolnych od wad urządzeń sieciowych z oprogramowaniem i licencjami dla Polskiego Związku Łowieckiego ZG wraz z usługą wdrożenia w infrastrukturze PZŁ ZG .
Urządzenia muszą być fabrycznie nowe, tj. wyprodukowane nie później, niż na 6 miesięcy przed jego dostarczeniem. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji (EoL). Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału dystrybucji znajdującego się na terenie Polski.

1. Przedmiotem postępowania jest zakup:

1.1 Dwóch urządzeń typu UTM (HA).
1.2 Centralnego sytemu logowania.
1.3 Dwóch przełączników szkieletowych.
1.4 Dwóch przełączników brzegowych.
1.5 Aplikacji zarządzającej, systemu kontroli dostępu do sieci i analizy ruchu.
1.6 Modułów optycznych i okablowania.

1. Urządzenia UTM – wymagania szczegółowe, 2 szt.

1. Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji.

	• Protokołów routingu dynamicznego.
2. Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN. 5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3. Interfejsy, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: • 8 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 2 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC z możliwością podłączenia redundantnego zasilacza.
4. Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 7 mln jednoczesnych połączeń oraz 400.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 30 Gbps. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14 Gbps. 4. Wydajność szyfrowania VPN IPSec nie mniej niż 10 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 9 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps.
5. Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

	4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
6. Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: •Translację jeden do jeden oraz jeden do wielu. •Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
7. Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

	• Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 3. W ramach postępowania należy dostarczyć dedykowanego klienta VPN o następujących funkcjonalnościach: • Możliwość centralnego zarządzania klientami za pomocą dedykowanej konsoli instalowanej lokalnie na serwerze • Możliwość sprawdzania stanu klienta (co najmniej w zakresie jego wersji) i przydzielanie dostępu na tej podstawie • Możliwość integracji z bazą AD • Możliwość logowania zdarzeń do centralnego systemu będącego przedmiotem postępowania • W przypadki licencjonowania klienta na liczbę stacji należy dostarczyć licencję na co najmniej 300 stacji.
8. Routing i obsługa WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
9. Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. Kontrola Antywirusowa 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

	2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
10. Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Ochrona przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
11. Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Kontrola WWW 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.

	3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
12. Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
13. Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

14. Logowanie	1. System musi mieć możliwość logowania do systemu logowania i raportowania będącego przedmiotem postępowania. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
15. Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall. • ICSA lub NSS Labs dla funkcji IPS. • ICSA dla funkcji IPSec VPN.
16. Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min.24 miesięcy.
17. Gwarancja i wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

Tabela nr 2 - Centralny system logowania – wymagania szczegółowe, szt. 1

1. Wymagania ogólne	W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej. Interfejsy, Dysk, Zasilanie: 1. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45. 2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB. Parametry wydajnościowe: 1.System musi być w stanie przyjmować minimum 90 GB logów na dzień. 2.System musi być w stanie analizować minimum 3000 logów na sekundę. 3.Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 10 systemów.
W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:	

2. Logowanie	1. Podgląd logowanych zdarzeń w czasie rzeczywistym z możliwością zastosowania filtrów dla prezentowanych informacji. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe - dla urządzeń, które logują informacje - obrazujące stan pracy urządzeń oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
3. Raportowanie	W zakresie raportowania system musi zapewniać: 1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
4. Korelacja logów	W zakresie korelacji zdarzeń system musi zapewniać: 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie VPN, utracone połączenie sieciowe, obciążenie zasobów.
5. Zarządzanie	1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

	2. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. 3. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
6. Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres min.24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach serwisu musi być świadczona również pomoc techniczna oraz aktualizacja firmware urządzenia.

Tabela nr 3 - Przełączniki szkieletowe – architektura systemu i wymagania szczegółowe systemu, szt. 2

1. Architektura systemu	Zamawiający wymaga dostarczenia rozwiązania sieci lokalnej składającego się z urządzeń aktywnych do sieci LAN, oprogramowania zarządzającego siecią LAN i WiFi, systemu kontroli dostępu oraz systemu analizy aplikacji działającego do warstwy 7 modelu OSI. Sieć lokalna będzie zbudowana w topologii podwójnej gwiazdy z dwoma przełącznikami szkieletowymi, które muszą zapewnić odporność sieci na awarie w przypadku uszkodzenia jednego z przełączników szkieletowych, jednego z połączeń przełącznika szkieletowego z przełącznikami brzegowymi oraz jednego z połączeń pomiędzy przełącznikami szkieletowymi. Przełączniki szkieletowe do sieci LAN mają zapewnić przyłączenie wszystkich wymaganych przełączników brzegowych z założeniem, iż każdy przełącznik brzegowy zostanie dołączony do szkieletu za pomocą min. 2 łączy światłowodowych 10G – każde z łączy światłowodowych musi być dołączone do innego przełącznika szkieletowego – pary urządzeń szkieletowych. Para przełączników szkieletowych musi zapewniać możliwość przyłączenia urządzeń obsługujących standardowy protokół Link Aggregation IEEE 802.3ad. Jednocześnie przełączniki szkieletowe muszą działać niezależnie (oddzielny Control Plane) – nie dopuszczamy rozwiązania łączenia przełączników szkieletowych w stos, które poprzez zastosowanie pojedynczego Control Plane znacznie zwiększa możliwość awarii. Przełączniki szkieletowe muszą zapewniać możliwość realizacji routingu pomiędzy sieciami VLAN. Routing musi się odbywać na obydwu przełącznikach z zapewnieniem balansownia obciążenia pomiędzy obydwa przełączniki. Przełączniki brzegowe do sieci LAN muszą być dołączone do szkieletu sieci za pomocą min. 2 portów 10G SFP+ do dwóch różnych przełączników szkieletowych. Obydwa łącza musza być aktywne i musza zapewniać balansowanie ruchu. Proponowane przełączniki brzegowe muszą być dostępne przynajmniej w wersjach 24 i 48 portowych z i bez zasilania przez skrętkę PoE+ IEEE 802.3at. Wymagane jest rozwiązanie przełączników brzegowych bazujące na tzw. Port Extenderach działających w oparciu o standard IEEE 802.1BR, czyli urządzeniach dołączanych do przełączników szkieletowych i całkowicie przez nie zarządzanych jako wyniesione moduły. Kluczowym elementem przebudowy sieci jest wdrożenie systemu kontroli dostępu do sieci LAN oraz WiFi. Dostarczone przełączniki muszą zapewniać możliwość uwierzytelniania i autoryzacji dostępu do sieci z wykorzystaniem IEEE 802.1x, MAC authentication oraz przekierowania urządzeń na Captive Portal zapewniający możliwość zalogowania się do sieci poprzez podanie nazwy użytkownika i hasła dla systemów wewnętrznych bez wsparcia IEEE

	802.1x oraz obsługę rejestracji gości. Wszystkie porty brzegowe przełączników powinny posiadać dokładnie taką samą konfigurację bez konieczności jej ręcznej modyfikacji w przypadku zmiany dołączanych do portów urządzeń. Zamawiający zakłada uwierzytelnianie następujących urządzeń: komputer, telefon, komputer i za nim podłączony telefon, drukarka, punkt dostępowy WiFi, kamera CCTV, różnego rodzaju urządzenia IoT – sterowanie listwami zasilającymi, klimatyzacją, systemem kontroli dostępu fizycznego, sterowanie i monitoring UPS itp. Implementacja systemu kontroli dostępu do sieci zakłada zastosowanie minimum dwóch nadmiarowych systemów kontroli dostępu zainstalowanych na oddzielnych dedykowanych serwerach (appliance) lub na oddzielnych serwerach zapewniających wirtualizację VMWare i/lub HyperV. Przełączniki powinny zapewniać możliwość realizacji następujących scenariuszy uwierzytelniania i autoryzacji: • Komputer bez zalogowanego użytkownika – uwierzytelnienie IEEE 802.1x z wykorzystaniem PEAP i/lub EAP-TLS. Komputer jest dołączany do sieci VLAN dla komputerów wraz z zastosowaniem filtracji dostępu do określonych zasobów i/lub aplikacji oraz możliwością konfiguracji QoS. • Komputer z zalogowanym użytkownikiem – uwierzytelnienie IEEE 802.1x z wykorzystaniem PEAP i/lub EAP-TLS. Komputer jest dołączany do sieci VLAN przeznaczonej dla użytkownika wraz z zastosowaniem filtracji dostępu do określonych zasobów i/lub aplikacji oraz możliwością konfiguracji QoS. • Telefon VoIP – uwierzytelnianie IEEE 802.1x z wykorzystaniem PEAP i/lub EAP-TLS. Telefon jest dołączany do sieci VLAN przeznaczonej dla Telefonów wraz z zastosowanie filtracji dostępu niezbędnego dla systemu telefonicznego oraz konfiguracja QoS niezbędnego dla systemu telefonicznego. • Telefon VoIP – w przypadku braku wsparcia IEEE 802.1x przez telefon możliwość uwierzytelnianie telefonu z wykorzystaniem MAC authentication. Możliwość konfiguracji poszczególnych MAC adresów jak i prefixów MAC adresów przydzielonych do wybranych typów telefonów w systemie kontroli dostępu. Telefon jest dołączany do sieci VLAN przeznaczonej dla Telefonów wraz z zastosowaniem filtracji dostępu niezbędnego dla systemu telefonicznego oraz konfiguracji QoS niezbędnej dla systemu telefonicznego. • Telefon VoIP i do niego dołączony komputer firmowy. Rozwiązanie musi obsługiwać wszystkie powyższe scenariusze – komputer ma trafiać do swojej sieci VLAN i mieć zapewnioną filtrację dostępu do określonych zasobów i/lub aplikacji oraz możliwość konfiguracji QoS. Podobnie telefon ma trafiać do swojej sieci VLAN i mieć zapewnioną filtrację dostępu do niezbędnych zasobów oraz konfigurację QoS niezbędnej dla systemu telefonicznego. Przełączniki muszą tutaj zapewniać tzw. Multi-Authentication – uwierzytelnianie wielu klientów na pojedynczym porcie przełącznika oraz Multi-Authorization – przydział różnych sieci VLAN, filtracji dostępu do określonych zasobów i/lub aplikacji oraz możliwość konfiguracji QoS różnych dla każdego z dołączanych do pojedynczego portu urządzeń. • Punkt dostępowy – uwierzytelnianie IEEE 802.1x z wykorzystaniem PEAP i/lub EAP-TLS. Punkt dostępowy jest dołączany do sieci VLAN dla punktów dostępowych oraz do wszystkich sieci VLAN, do których ma być zapewniony dostęp klientów bezprzewodowych w trybie lokalnego dostępu do sieci LAN – local bridging. • Punkt dostępowy – uwierzytelnienie MAC authentication. Możliwość konfiguracji poszczególnych MAC adresów jak i prefixów MAC adresów, przydzielonych do wybranych typów punktów dostępowych, w systemie kontroli dostępu. Punkt dostępowy jest dołączany do wskazanej sieci VLAN dla punktów dostępowych. Rozwiązanie powinno zapewnić możliwość dostępu Punktu dostępowego do kontrolerów bezprzewodowych w celu zdalnej

	konfiguracji nazwy użytkownika i hasła dla IEEE 802.1x PEAP lub wgrania na punkt dostępowy certyfikatu dla EAP-TLS. • Drukarka – uwierzytelnianie IEEE 802.1x z wykorzystaniem PEAP i/lub EAP-TLS. Drukarka jest dołączana do sieci VLAN dla drukarek wraz z możliwością filtracji ruchu, który nie służy procesowi drukowania i kontroli drukarki. • Drukarka – uwierzytelnianie MAC authentication. W przypadku drukarek nieposiadających wbudowanego klienta IEEE 802.1x konieczne jest zapewnienie kontroli dostępu z wykorzystaniem MAC authentication i możliwość konfiguracji poszczególnych MAC adresów jak i prefixów MAC adresów przydzielonych dla konkretnych typów drukarek. Zamawiający, w przypadku wątpliwości co do spełnienia specyfikacji, może zażądać przeprowadzenia testów funkcjonalnych rozwiązania. Testy muszą być przeprowadzone w siedzibie Zamawiającego.
2. Wymagania szczegółowe	1. Przełącznik posiadający 24 porty 10 Gigabit Ethernet SFP+, mogące pracować z prędkością 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+ 2. Przełącznik posiadający 2 porty 10Gb/25Gb/40Gb/ 50Gb/ 100Gb w standardzie QSFP28 3. Wysokość urządzenia 1U 4. Przełącznik wyposażony w dwa modularne, wewnętrzne zasilacze, które umożliwiają uzyskanie redundancji zasilania. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika 5. Przepływ powietrza w przełączniku: przód-tył 6. Moduł wentylatorów zapewniający ich redundancję oraz możliwość wymiany w czasie działania przełącznika 7. Nieblokująca architektura o wydajności przełączania min. 840 Gb/s 8. Tablica MAC adresów min. 272k 9. Pamięć operacyjna: minimum 4 GB pamięci DRAM 10. Pamięć Flash/SSD minimum 32 GB 11. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora 12. Możliwość stakowania do 8 przełączników, magistrala stakująca o przepustowości 400 Gb/s 13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000 14. Obsługa sieci wirtualnych protokołowych IEEE 802.1v 15. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci 16. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów) 17. Obsługa Q-in-Q IEEE 802.1ad 18. Obsługa Quality of Service a. IEEE 802.1p b. DiffServ c. 8 kolejek priorytetów na każdym porcie wyjściowym 19. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB 20. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) 21. Obsługa CDP 22. Wbudowany DHCP Serwer i klient 23. Możliwość instalacji min. dwóch wersji oprogramowania - firmware 24. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash 25. Możliwość monitorowania zajętości CPU oraz pamięci 26. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)

	27. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach. 28. Wbudowany port konsolowy do zarządzania przełącznikiem 29. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management. 30. Port USB do podpięcia zewnętrznego storage Obsługa Routingu IPv4 31. Sprzętowa obsługa routingu IPv4 - forwarding 32. Pojemność tabeli routingu min. 256 tys. wpisów 33. Routing statyczny 34. Obsługa routingu dynamicznego IPv4 a. RIP v1/v2 b. OSPFv2 c. BGP4 oraz MBGP (BGP4+) - możliwość rozszerzenia przez licencje d. IS-IS - możliwość rozszerzenia przez licencje 35. Policy Based Routing dla IPv4 Obsługa Routingu IPv6 36. Sprzętowa obsługa routingu IPv6 - forwarding 37. Pojemność tabeli routingu min. 128 tys. wpisów 38. Routing statyczny 39. Obsługa routingu dynamicznego dla IPv6 a. RIPng b. OSPF v3 c. BGP4 oraz MBGP (BGP4+) - możliwość rozszerzenia przez licencje d. IS-IS - możliwość rozszerzenia przez licencje 40. Obsługa 6to4 (RFC 3056) 41. Obsługa MLDv1 (Multicast Listener Discovery version 1) 42. Policy Based Routing dla IPv6 Obsługa Multicastów 43. Statyczne przyłączanie do grupy multicast 44. Filtrowanie IGMP 45. Obsługa PIM-SM - możliwość rozszerzenia przez licencje 46. Obsługa PIM-DM - możliwość rozszerzenia przez licencje 47. Obsługa PIM-SSM - możliwość rozszerzenia przez licencje 48. Obsługa Multicast VLAN Registration - MVR 49. Obsługa IGMP v1 - RFC 1112 50. Obsługa IGMP v2 - RFC 2236 51. Obsługa IGMP v3 - RFC 3376 52. Obsługa IGMP v1/v2/v3 snooping 53. Możliwość konfiguracji statycznych tras dla Routingu Multicastów Bezpieczeństwo 54. Obsługa logowania do sieci a. IEEE 802.1x Network Login b. Web-based Network Login c. MAC based Network Login 55. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants) 56. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login 57. Obsługa Guest VLAN dla IEEE 802.1x

	58. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos 59. Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication 60. Możliwość wymuszenia zmiany autoryzacji – Change of Authorization (CoA) RFC 5176 i/lub SNMPv3 61. Wbudowana obrona procesora urządzenia przed atakami DoS 62. Obsługa TACACS+ 63. Obsługa RADIUS Authentication (RFC 2138) 64. Obsługa RADIUS Accounting (RFC 2139) 65. RADIUS and TACACS+ per-command Authentication 66. Bezpieczeństwo MAC adresów a. ograniczenie liczby MAC adresów na porcie b. zatrzaśnięcie MAC adresu na porcie c. możliwość wpisania statycznych MAC adresów na port/vlan 67. Możliwość wyłączenia MAC learning 68. Zabezpieczenie przełącznika przed atakami DoS a. Networks Ingress Filtering RFC 2267 b. SYN Attack Protection c. Zabezpieczenei CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania 69. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 a. Adres MAC źródłowy i docelowy plus maska b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6 c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd. d. Numery portów źródłowych i docelowych TCP, UDP e. Zakresy portów źródłowych i docelowych TCP, UDP f. Identyfikator sieci VLAN - VLAN ID g. Flagi TCP h. Obsługa fragmentów 70. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika 71. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI 72. Obsługa bezpiecznego transferu plików SCP/SFTP 73. Obsługa DHCP Option 82 74. Obsługa IP Security - Gratuitous ARP Protection 75. Obsługa IP Security – Trusted DHCP Server 76. Obsługa IP Security – DHCP Secured ARP/ARP Validation 77. Ograniczanie przepustowości (rate limiting) na portach wyjściowych Bezpieczeństwo sieciowe 78. Możliwość konfiguracji portu głównego i zapasowego 79. Obsługa redundancji routingu VRRP - RFC 2338 80. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D 81. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w 82. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s 83. Obsługa PVST+ 84. Obsługa G.8032 v1/v2 85. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów

	86. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników Zarządzanie 87. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol) 88. Obsługa synchronizacji czasu NTP 89. Zarządzanie przez SNMP v1/v2/v3 90. Zarządzanie przez przeglądarkę WWW – protokół http i https 91. Możliwość zarzadzania przełącznikiem z dedykowanej aplikacji zarządzającej 92. Możliwość zarzadzania przełącznikiem z poziomu CLI 93. Telnet Serwer/Klient dla IPv4 / IPv6 94. SSH2 Serwer/Klient dla IPv4 / IPv6 95. Ping dla IPv4 / IPv6 96. Traceroute dla IPv4 / IPv6 97. Obsługa SYSLOG z możliwością definiowania wielu serwerów 98. Obsługa SNMP Traps 99. Sprzętowa obsługa sFlow 100. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events Inne 101. Przełącznik musi zapewniać współpracę z systemem analizy aplikacji do warstwy 7 wysyłając niezbędne informacje do systemu zarządzającego. 102. Obsługa VXLAN 103. Obsługa do 48 jednostek wyniesionych (Port extenderów) 104. Wsparcie 802.1BR dla port extenderów 105. Centralne zarządzanie wszystkimi port extenderami z poziomu switcha 106. Połączenie port extenderów pojedynczymi portami lub wieloma portami za pomocą protokołu LAG i MLAG 107. Wsparcie dla topologii ring z port extenderami (bez limitu ilości połączeń ring) 108. Zakres temperatury pracy 0-45 °C 109. Obsługa skryptów CLI 110. Obsługa skryptów w języku Python 111. Obsługa funkcji TCL/Tk w skryptach CLI 112. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych) 113. Możliwość uruchamiania skryptów a. Ręcznie b. O określonym czasie lub co wskazany okres czasu c. Na podstawie wpisów w logu systemowym 114. Przełączniki muszą posiadać gwarancję typu NBD na okres min. 24 miesiące w ramach której dostępne jest również wsparcie techniczne dla pełnego zakresu funkcjonalności oferowanego urządzenia oraz możliwość aktualizacji firmware urządzeń.

Tabela nr 4 - Przełączniki brzegowe – wymagania szczegółowe, szt. 2

1.Wymagania szczegółowe	1. Przełącznik posiadający min. 48 portów 10/100/1000BASE-T 2. Przełącznik posiadający min. 4 porty 10Gb SFP+ do przyłączenia przełącznika do dwóch przełączników szkieletowych 3. Wysokość urządzenia 1U 4. Wbudowany zasilacz 230W

	5. Przełącznik zarządzany z przełącznika szkieletowego zgodnie ze standardem IEEE 802.1BR 6. Automatyczna konfiguracja przełącznika po dołączeniu do przełącznika szkieletowego 7. Automatyczna aktualizacja oprogramowania po dołączeniu do przełącznika szkieletowego 8. Wsparcie funkcjonalności obsługiwanych poprzez przełącznik szkieletowy w szczególności: 8.1. Obsługa scenariuszy logowania do sieci opisana w części opisowej 8.2. Obsługa logowania do sieci IEEE 802.1x 8.3. Obsługa logowania do sieci MAC authentication 8.4. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants) 8.5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login 8.6. Obsługa Guest VLAN dla IEEE 802.1x 8.7. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos 8.8. Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication 8.9. Możliwość wymuszenia zmiany autoryzacji – Change of Authorization (CoA) RFC 5176 i/lub SNMPv3 8.10. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP 8.11. Obsługa Link Aggregation z różnych przełączników brzegowych 9. Przełączniki brzegowe muszą posiadać gwarancję umożliwiającą naprawę urządzeń przez okres co najmniej 5 lat oraz aktualizację firmware. Przez min. 24 miesiące wymagane jest również wsparcie techniczne dla pełnego zakresu funkcjonalności oferowanego urządzenia

Tabela nr 5 - Aplikacja zarządzająca, system kontroli dostępu do sieci i analizy ruchu

1. Aplikacja zarządzająca	1. Aplikacja musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku wirtualizacyjnym VMWare i/lub HyperV b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS. 2. Aplikacja musi zarządzać siecią przewodową i bezprzewodową 3. Aplikacja zarządzająca musi obsługiwać wszystkie dostarczone przełączniki brzegowe i szkieletowe. 4. Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników. 5. Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowania, jeśli jest to wymagane przez producenta systemu zarządzającego 6. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników 7. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius. 8. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.

	9. Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3. Muszą być wspierane mechanizmy Authentication (MD5 i SHA) i Privacy (DES i AES) dla SNMPv3 10. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu. 11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów 12. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów 13. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II 14. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla danych urządzeń sieciowych. 15. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu. 16. Aplikacja musi posiadać wbudowany Syslog serwer 17. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera. 18. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji, kontaktu do administratora oraz typu urządzenia 19. Aplikacja musi pozwalać na tworzenie przez administratora własnych grup urządzeń oraz portów na urządzeniach. 20. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem a. połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości b. konfiguracji sieci VLAN 21. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https 22. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane: a. adres IP urządzenia b. adresu MAC urządzenia c. nazwy urządzenia d. wersji oprogramowania e. wersji bootrom f. lokalizacji urządzenia g. danych kontaktowych administratora h. numeru seryjnego i. numeru ewidencyjnego – możliwość konfiguracji własnych numerów ewidencyjnych skojarzonych z konkretnym urządzeniem 23. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest: a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie i częstotliwości – np. codziennie, raz w tygodniu b. możliwość odtworzenia wskazanej konfiguracji urządzenia c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych d. automatyczne porównywanie różnic bieżącej i ostatnio zapamiętanej konfiguracji z możliwością generacji alarmu e. możliwość obsługi konfiguracji urządzeń sieciowych innych producentów

	24. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie 25. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania urządzeń sieciowych innych producentów 26. Aplikacja musi przechowywać historię zmian konfiguracji na urządzeniach 27. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych. 28. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp. 29. Tworzona polityka musi zawierać możliwość: a. blokowania lub zezwalania ruchu na podstawie i) źródłowy i docelowy adres MAC ii) źródłowy i docelowy adres IP iii) źródłowy i docelowy adres IP podsieci iv) źródłowy i docelowy port TCP/UDP v) źródłowy i docelowy zakres portów TCP/UDP vi) typ protokołu b. przydziału parametrów QoS i) priorytety c. przydziału użytkownika do wskazanej sieci VLAN 30. Aplikacja musi mieć możliwość wdrażania polityk bezpieczeństwa w całej sieci, dla urządzeń przewodowych i bezprzewodowych za pomocą jednego kliknięcia. 31. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać: a. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać, gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy). b. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne). c. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp. d. generowanie raportów 32. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową. a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa). b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje: i) adres IP kontrolera ii) liczba obsługiwanych klientów iii) szczytowe wartości zajmowanego pasma iv) wersja oprogramowania d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:

	i) adres IP punktu dostępowego ii) MAC adres punktu dostępowego iii) wersja oprogramowania iv) typ punktu dostępowego v) kanały pracy poszczególnych interfejsów radiowych vi) szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje: i) adres IP klienta ii) MAC adres klienta iii) nazwa użytkownika iv) nazwa punktu dostępowego, do którego dołączony jest użytkownik v) BSSID, do którego dołączony jest użytkownik vi) SSID, do którego dołączony jest użytkownik f. Musi być zapewniona możliwość tworzenia map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności: i) zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate). ii) zaznaczenie kanałów pracy urządzeń iii) lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
2. System kontroli dostępu do sieci LAN	1. Aplikacja zarządzająca musi być zintegrowana z systemem kontroli dostępu do sieci z zapewnieniem widzialności następujących informacji o uwierzytelnionych systemach/użytkownikach: a. adresu MAC b. adresu IP c. nazwy komputera d. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp. e. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika. f. adres IP urządzenia, do którego dołączony jest klient. g. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego. h. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp. i. nazwa przydzielonej polityki bezpieczeństwa. j. Atrybutów RADIUS wysłanych do urządzenia przeprowadzającego autoryzację 2. System zapewniający widoczność zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp. 3. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość wymuszenia ponownej autoryzacji użytkownika na żądanie (wsparcie CoA RFC 5176 lub SNMP) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa

	4. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List 5. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci. 6. System kontroli dostępu do sieci musi zapewniać współpracę z systemami Firewall w zakresie przesyłania aktualnych informacji o zalogowanych użytkownikach lub urządzeniach, ich adresach IP. Musi wspierać systemy firewall firmy Fortinet/CheckPoint. 7. System kontroli dostępu musi zapewniać współpracę z systemami UTM, IDS/IPS, SIEM w zakresie automatycznej kwarantanny użytkownika lub urządzenia (przeniesienia do wyizolowanej sieci VLAN), który zostanie zaraportowany przez jeden z wymienionych systemów jako system użytkownik lub urządzenie zagrażające bezpieczeństwu sieci. Automatyczna kwarantanna musi zapewniać możliwość wygenerowania Alarmu i poinformowania Administratora o zaistniałej sytuacji. Użytkownik przeniesiony do kwarantanny musi zostać poinformowany o zaistniałym zdarzeniu poprzez przekierowanie na Captive Portal gdzie otrzyma odpowiednią informację. 8. System kontroli dostępu musi zapewniać współpracę z systemami MDM. 9. System kontroli dostępu do sieci musi posiadać informacje podsumowujące zawierające: a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp. b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp. c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp. 10. System kontroli dostępu do sieci jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 500 urządzeń klienckich (adresów MAC). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 50 punktów dostępowych oraz min. 5 przełączników sieciowych. System musi umożliwiać w przyszłości rozbudowę do minimum 250 urządzeń sieciowych i 1000 punktów dostępowych.
3. Analiza aplikacji warstwy 7	1. System zarządzania musi wspierać analizę ruchu w sieci do warstwy 7. 2. Analiza aplikacji musi być prowadzona przy współpracy przełączników brzegowych, które muszą wysyłać do systemu analizy ruchu niezbędne informacje. 3. System musi zapewniać możliwość monitorowania czasów odpowiedzi sieci oraz aplikacji krytycznych dla działania sieci serwisów takich jak: a. DHCP b. DNS c. Kerberos d. RADIUS e. LDAP 4. System musi zapewniać możliwość monitorowania innych wskazanych przez użytkownika własnych aplikacji np. SAP, Microsoft SQL, Aplikacje Web, Office 365 itp. 5. Odstępstwa czasów odpowiedzi sieci i aplikacji muszą być raportowane poprzez system Alarmów

	6. System analizy ruchu do warstwy 7 musi posiadać wbudowane sygnatury aplikacji jak i umożliwiać tworzenie nowych sygnatur 7. System analizy aplikacji musi zapewniać raportowanie używanych w sieci aplikacji z informacją o najbardziej obciążających aplikacjach ze względu na: ilość przesyłanych danych, liczbę przepływów (flows), liczbę klientów oraz najgorsze czasy odpowiedzi sieci i aplikacji. Powyższe dane powinny być raportowane dla całej sieci jak i dla poszczególnych klientów sieci LAN oraz WiFi. 8. System musi umożliwiać tworzenie raportów dziennych/tygodniowych/za zdefiniowany czas 9. System analizy aplikacji warstwy 7 musi zapewniać obsługę min. 100 klientów
4. Gwarancja i wsparcie	Oferowane oprogramowanie (zarządzanie, kontrola dostępu, analiza aplikacji) musi umożliwiać aktualizację jego wersji oraz musi być dostępne wsparcie techniczne przez okres min. 24 miesiący.

Tabela nr 6 - Moduły optyczne i okablowanie

W ramach postępowania należy dostarczyć:
1. Moduł typu 10/100/1000BASE-T SFP zgodny z oferowanymi przełącznikami – szt. 20 2. Przewód typu DAC 100Gb QSFP28-QSFP28 o długości min. 0,5m zgodny z oferowanymi przełącznikami – szt. 2 3. Przewód typu DAC 10Gb SFP+ o długości min. 3m zgodny z oferowanymi przełącznikami – szt. 10 4. Przewód typu DAC 10Gb SFP+ o długości min. 5m zgodny z oferowanymi przełącznikami – szt. 10 5. Patchcord miedziany rj45 o długości 1m – szt. 2

1.7 **Usług wdrożeniowych i wsparcia technicznego**.

W ramach realizacji zamówienia należy zapewnić wdrożenie oferowanych urządzeń UTM i centralnego sytemu logowania. W ramach wdrożenia należy wykonać:

1. Montaż urządzeń.
2. Analizę obecnych polityk bezpieczeństwa oraz infrastruktury sieciowej (optymalizacja zgodna z aktualnymi trendami panującymi w sferze zagrożeń sieciowych),
3. Przygotowanie środowiska (rejestracja i instalacja urządzeń, aktualizacja oprogramowania),
4. Konfiguracja urządzeń UTM zgodnie z założeniami polityki bezpieczeństwa (interfejsy sieciowe, routing, polityki firewall, DNS, Web filtering, anti-spam, anti-virus, controla aplikacji, ips, ids, virtual private network, integracja z domeną, zarządzanie pasmem, uwierzytelnianie użytkowników, redundancja dostępu do internetu, logowanie oraz raportowanie, alerty administracyjne, dostosowanie do współpracy z zewnętrznym systemem logowania i raportowania).
5. Weryfikacja poprawności implementacji (testy akceptacyjne).
6. Kopia bezpieczeństwa konfiguracji wdrożonych urządzeń.
7. Instruktarz obsługi urządzenia poprzez GUI.

W ramach realizacji zamówienia należy zapewnić wdrożenie oferowanych urządzeń sieciowych i oprogramowania. W ramach wdrożenia należy wykonać:

1. montaż urządzeń

2. konfigurację połączeń oraz stosów
3. instalację i konfigurację sytemu zarządzania,
4. instalację i konfigurację sytemu systemu kontroli dostępu
5. instalację i konfigurację sytemu analizy aplikacji
6. konfigurację polityk dostępowych
7. integrację z systemami UTM.

Po wykonaniu wdrożenia należy świadczyć na rzecz Zamawiającego wsparcie techniczne do wszystkich oferowanych rozwiązań przez ich okres gwarancji. W tym celu wykonawca musi posiadać dla każdej oferowanej technologii (systemu) co najmniej dwóch inżynierów posiadających aktualny certyfikat techniczny (lub certyfikaty) wystawione przez producentów oferowanych rozwiązań potwierdzające wiedzę z ich zakresu. Wszystkie powyższe certyfikaty należy załączyć do oferty

1.8 Szkolenia z zaawansowanej konfiguracji urządzeń.

Szkolenia:

1. Poziom 1 - bezpieczeństwo sieci komputerowej.
   Cel szkolenia: Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji urządzeniami. Poznanie podstaw tworzenia i zarządzania polityką bezpieczeństwa na styku sieci lokalnej z Internetem. Szkolenie prowadzone będzie w formie warsztatów.

2. Poziom 2 – konfiguracja urządzeń.
   Cel szkolenia: Zdobycie umiejętności praktycznych pozwalających na wykorzystanie zaawansowanych funkcjonalności urządzeń - integracja urządzeń, zaawansowane opcje routingu i redundancji łącz.

2. Wymagania ogólne

2.1 Za sprzęt dostarczony odpowiada Wykonawca do czasu odbioru całego zamówienia przez Zamawiającego potwierdzonego odpowiednim protokołem.

2.2 Po dostawie i sprawdzeniu sprzętu pod względem jego zgodności ze specyfikacją istotnych warunków zamówienia, zostanie sporządzony protokół odbioru (w dwóch jednobrzmiących egzemplarzach, dla każdej ze stron po jednym egzemplarzu), którego data wykonania oznacza odbiór końcowy sprzętu z oprogramowaniem i licencjami.