IR.271.3.8.2025 **Załącznik nr 9 do SWZ**

OPIS PRZEDMIOTU ZAMÓWIENIA

Niniejszy załącznik stanowi szczegółowy opis przedmiotu zamówienia. Zaoferowane przez Wykonawcę rozwiązania muszą spełniać minimalne wymagania postawione w niniejszym załączniku w kolumnie „Wymagane minimalne parametry techniczne" oraz zostać dostarczony na warunkach określonych poniżej.

Wykonawca zobowiązany jest podać w formularzu oferty producenta, model/wersję oferowanego rozwiązania, typ dzięki czemu będzie można jednoznacznie określić jaki produkt został zaoferowany. Dodatkowo Zamawiający dopuszcza podanie linków dostępowych dla oferowanego n/w sprzętu dostępnych na stronach internetowych producentów.

Spis treści

1. Urządzenia UTM wraz z licencjami i wsparciem technicznym

a. UTM do Urzędu Miejskiego – 1 szt.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
ZAKRES DOSTAWY	**1.** Przedmiotem zamówienia jest zakup, wdrożenie oraz konfiguracja urządzenia UTM wraz z integracją z istniejącą infrastrukturą IT urzędu.
OBSŁUGA SIECI	**2.** Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (FIREWALL)	**3.** Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. **4.** Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. **5.** Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). **6.** Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. **7.** Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. **8.** Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. **9.** Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. **10.** Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. **11.** Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. **12.** Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	13. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
INTRUSION PREVENTION SYSTEM (IPS)	**14.** System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. **15.** Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. **16.** Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. **17.** Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. **18.** Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. **19.** Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. **20.** Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. **21.** Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. **22.** Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). **23.** Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
KSZTAŁTOWANIE PASMA (TRAFFIC SHAPPING)	**24.** Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. **25.** Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. **26.** Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	27. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA	**28.** Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). **29.** Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. **30.** Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. **31.** Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
OCHRONA ANTYSPAM	**32.** Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). **33.** Ochrona antyspam ma działać w oparciu o: **33.1.** białe/czarne listy, **33.2.** DNS RBL, **33.3.** Skaner heurystyczny. **34.** W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. **35.** Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	**36.** Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). **37.** Urządzenie ma wspierać co najmniej następujące typy sieci VPN: **37.1.** PPTP VPN, **37.2.** IPSec VPN, **37.3.** SSL VPN. **38.** SSL VPN ma działać co najmniej w trybach tunelu i portalu. **39.** Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	40. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) **41.** Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). **42.** Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. **43.** Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
FILTR DOSTĘPU DO STRON WWW	**44.** Urządzenie ma posiadać wbudowany filtr URL. **45.** Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. **46.** Administrator ma mieć możliwość dodawania własnych kategorii URL. **47.** Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: **47.1.** blokowanie dostępu do adresu URL, **47.2.** zezwolenie na dostęp do adresu URL, **47.3.** blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. **48.** Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. **49.** Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. **50.** Filtr URL musi uwzględniać komunikację po protokole HTTPS. **51.** Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. **52.** Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. **53.** Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
UWIERZYTELNIANIE	**54.** Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: **54.1.** lokalną bazę użytkowników (wewnętrzny LDAP), **54.2.** zewnętrzną bazę użytkowników (zewnętrzny LDAP), **54.3.** usługę katalogową Microsoft Active Directory. **55.** Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	56. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: **56.1.** SSL, **56.2.** Radius, **56.3.** Kerberos. **57.** Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. **58.** Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. **59.** Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. **60.** Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). **61.** Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). **62.** Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	**63.** Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). **64.** Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: **64.1.** równoważenie względem adresu źródłowego, **64.2.** równoważenie względem połączenia. **65.** Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. **66.** Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). **67.** Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. **68.** W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	69. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
ROUTING (TRASOWANIE)	**70.** Urządzenie ma umożliwiać statyczne trasowanie pakietów. **71.** Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. **72.** Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). **73.** Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
ADMINISTRACJA URZĄDZENIEM	**74.** Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. **75.** Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. **76.** Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. **77.** Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. **78.** Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. **79.** Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) **80.** Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. **81.** Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. **82.** Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. **83.** Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. **84.** Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. **85.** Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	86. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). **87.** Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. **88.** Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. **89.** Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). **90.** Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. **91.** Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: **91.1.** manualnego eksportu do pliku w dowolnym momencie czasu, **91.2.** automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu **92.** Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. **93.** Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. **94.** Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
RAPORTOWANIE	**95.** Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. **96.** System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. **97.** System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. **98.** System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. **99.** System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. **100.** System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. **101.** Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	102. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. **103.** Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
POZOSTAŁE USŁUGI I FUNKCJE	**104.** Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. **105.** Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. **106.** Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). **107.** Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. **108.** Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). **109.** Urządzenie ma posiadać usługę DNS Proxy. **110.** Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). **111.** Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. **112.** Urządzenie musi mieć zaimplementowane Open API **113.** Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
GWARANCJA I SERWIS	**114.** Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. **115.** W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
PARAMETRY SPRZĘTOWE	**116.** Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. **117.** Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy. **118.** Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16. **119.** Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10. **120.** Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	120.1. Moduł z 8 interfejsami miedzianymi 2,5Gbps **120.2.** Moduł z 4 interfejsami miedzianymi 10Gbps. **120.3.** Moduł z 4 interfejsami światłowodowymi 1Gbps. **120.4.** Moduł z 8 interfejsami światłowodowymi 1Gbps. **120.5.** Moduł z 4 interfejsami światłowodowymi 10Gbps. **121.** Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. **122.** Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45. **123.** Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps. **124.** Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps. **125.** Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps. **126.** Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps. **127.** Maksymalna liczba tuneli VPN IPSec – minimum 1000. **128.** Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150. **129.** Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150. **130.** Obsługa interfejsów 802.11q (VLAN) – minimum 256. **131.** Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę. **132.** Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. **133.** Urządzenie nie ma limitu na liczbę użytkowników. **134.** Liczba reguł filtrowania – minimum 16 384. **135.** Liczba tras statycznego routingu – minimum 5 120. **136.** Liczba tras dynamicznego routingu – minimum 10 000. **137.** Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. **138.** Urządzenie musi być wyposażone w moduł TPM.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
WDROŻENIE	**139.** Instalacja i konfiguracja urządzenia **139.1.** Urządzenie ma zostać zainstalowane w serwerowni urzędu, w pełnej zgodności z infrastrukturą sieciową. **139.2.** Zakres prac obejmuje: **139.2.1.** Konfigurację reguł firewalla w celu zabezpieczenia ruchu sieciowego. **139.2.2.** Ustawienie polityk bezpieczeństwa oraz reguł filtrowania treści (np. blokowanie złośliwych stron, filtrowanie URL, ochrona przed phishingiem). **139.2.3.** Konfigurację IPSec VPN, SSL VPN oraz konfigurację zarządzania zdalnego. **139.2.4.** Integrację urządzenia z istniejącym systemem monitorowania logów (SIEM) i zarządzania incydentami. **139.3.** Zastosowanie polityk QoS dla priorytetyzacji ruchu krytycznego. **140.** Testy akceptacyjne **140.1.** Po zainstalowaniu i skonfigurowaniu urządzenia Wykonawca zobowiązuje się przeprowadzić testy akceptacyjne, które potwierdzą prawidłowe działanie urządzenia zgodnie z wymaganiami. **140.2.** Testy obejmą: **140.2.1.** Testowanie przepustowości firewall'a oraz VPN. **140.2.2.** Symulację ataków oraz testy IPS/IDS w celu zweryfikowania skuteczności ochrony. **140.2.3.** Weryfikację konfiguracji reguł i polityk bezpieczeństwa. **141.** Szkolenie dla administratorów IT **141.1.** Wykonawca zobowiązuje się przeprowadzić szkolenie dla co najmniej 2 administratorów IT z urzędu. **141.2.** Zakres szkolenia obejmuje: **141.2.1.** Wprowadzenie do interfejsu zarządzania urządzeniem **141.2.2.** Konfigurację i zarządzanie regułami firewalla, filtrowaniem treści oraz IPS/IDS. **141.2.3.** Zarządzanie VPN (IPSec, SSL VPN) oraz konfigurację dostępu zdalnego. **141.2.4.** Monitorowanie działania urządzenia, analiza logów oraz zarządzanie zdarzeniami. **141.2.5.** Tworzenie kopii zapasowych i odtwarzanie konfiguracji.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO URZĘDU MIEJSKIEGO
	142. Wykonawca musi posiadać odpowiednie doświadczenie w zakresie wdrożeń urządzeń klasy UTM

b. UTM do jednostek organizacyjnych – 2 szt.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
OBSŁUGA SIECI	**1.** Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)	**2.** Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. **3.** Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. **4.** Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). **5.** Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. **6.** Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. **7.** Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. **8.** Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. **9.** Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. **10.** Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). **12.** System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
INTRUSION PREVENTION SYSTEM (IPS)	**13.** System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. **14.** Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. **15.** Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. **16.** Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. **17.** Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. **18.** Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. **19.** Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. **20.** Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. **21.** Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). **22.** Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
KSZTAŁTOWANIE PASMA (Traffic Shapping)	**23.** Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. **24.** Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). **26.** Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA	**27.** Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). **28.** Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. **29.** Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. **30.** Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
OCHRONA ANTYSPAM	**31.** Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). **32.** Ochrona antyspam ma działać w oparciu o: **32.1.** białe/czarne listy, **32.2.** DNS RBL, **32.3.** Skaner heurystyczny. **33.** W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. **34.** Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	**35.** Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). **36.** Urządzenie ma wspierać co najmniej następujące typy sieci VPN: **36.1.** PPTP VPN, **36.2.** IPSec VPN, **36.3.** SSL VPN.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	37. SSL VPN ma działać co najmniej w trybach tunelu i portalu. **38.** Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. **39.** Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) **40.** Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). **41.** Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. **42.** Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
FILTR DOSTĘPU DO STRON WWW	**43.** Urządzenie ma posiadać wbudowany filtr URL. **44.** Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. **45.** Administrator ma mieć możliwość dodawania własnych kategorii URL. **46.** Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: **46.1.** blokowanie dostępu do adresu URL, **46.2.** zezwolenie na dostęp do adresu URL, **46.3.** blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. **47.** Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. **48.** Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. **49.** Filtr URL musi uwzględniać komunikację po protokole HTTPS. **50.** Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. **51.** Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. **52.** Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
UWIERZYTELNIANIE	**53.** Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: **53.1.** lokalną bazę użytkowników (wewnętrzny LDAP), **53.2.** zewnętrzną bazę użytkowników (zewnętrzny LDAP),

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	53.3. usługę katalogową Microsoft Active Directory. **54.** Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. **55.** Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: **55.1.** SSL, **55.2.** Radius, **55.3.** Kerberos. **56.** Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. **57.** Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. **58.** Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. **59.** Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). **60.** Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). **61.** Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	**62.** Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). **63.** Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: **63.1.** równoważenie względem adresu źródłowego, **63.2.** równoważenie względem połączenia. **64.** Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. **65.** Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). **66.** Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	67. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). **68.** Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
ROUTING (TRASOWANIE)	**69.** Urządzenie ma umożliwiać statyczne trasowanie pakietów. **70.** Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. **71.** Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). **72.** Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
ADMINISTRACJA URZĄDZENIEM	**73.** Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. **74.** Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. **75.** Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. **76.** Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. **77.** Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. **78.** Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) **79.** Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. **80.** Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. **81.** Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. **82.** Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. **83.** Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). **85.** System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). **86.** Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. **87.** Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). **88.** Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. **89.** Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: **89.1.** manualnego eksportu do pliku w dowolnym momencie czasu, **89.2.** automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu **90.** Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. **91.** Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. **92.** Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
RAPORTOWANIE	**93.** Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. **94.** System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. **95.** System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. **96.** System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. **97.** System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. **98.** System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	99. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. **100.** Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. **101.** Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
POZOSTAŁE USŁUGI I FUNKCJE	**102.** Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. **103.** Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). **104.** Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. **105.** Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). **106.** Urządzenie ma posiadać usługę DNS Proxy. **107.** Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. **108.** Urządzenie musi mieć zaimplementowane Open API **109.** Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. **110.** Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. **111.** Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
GWARANCJA I SERWIS	**112.** Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. **113.** W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
	114. PARAMETRY SPRZĘTOWE **115.** Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	116. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. **117.** Liczba portów Ethernet 2,5Gbps – min. 8. **118.** Liczba portów światłowodowych 1Gbps – min. 1. **119.** Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. **120.** Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps. **121.** Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps. **122.** Przepustowość filtrowania Antywirusowego – minimum 500Mbps. **123.** Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps. **124.** Maksymalna liczba tuneli VPN IPSec – minimum 100. **125.** Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50. **126.** Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50. **127.** Obsługa interfejsów 802.11q (VLAN) – minimum 128 **128.** Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę. **129.** Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. **130.** Urządzenie nie ma limitu na liczbę użytkowników. **131.** Liczba reguł filtrowania – minimum 8 192. **132.** Liczba tras statycznego routingu – minimum 512. **133.** Liczba tras dynamicznego routingu – minimum 10 000. **134.** Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. **135.** Urządzenie musi być wyposażone w moduł TPM.
WDROŻENIE	**143.** Instalacja i konfiguracja urządzenia **143.1.** Urządzenie ma zostać zainstalowane w serwerowni urzędu, w pełnej zgodności z infrastrukturą sieciową. **143.2.** Zakres prac obejmuje:

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – UTM DO JEDNOSTEK ORGANIZACYJNYCH
	143.2.1. Konfigurację reguł firewalla w celu zabezpieczenia ruchu sieciowego. **143.2.2.** Ustawienie polityk bezpieczeństwa oraz reguł filtrowania treści (np. blokowanie złośliwych stron, filtrowanie URL, ochrona przed phishingiem). **143.2.3.** Konfigurację IPSec VPN, SSL VPN oraz konfigurację zarządzania zdalnego. **143.2.4.** Integrację urządzenia z istniejącym systemem monitorowania logów (SIEM) i zarządzania incydentami. **143.3.** Zastosowanie polityk QoS dla priorytetyzacji ruchu krytycznego. **144.** Testy akceptacyjne **144.1.** Po zainstalowaniu i skonfigurowaniu urządzenia Wykonawca zobowiązuje się przeprowadzić testy akceptacyjne, które potwierdzą prawidłowe działanie urządzenia zgodnie z wymaganiami. **144.2.** Testy obejmą: **144.2.1.** Testowanie przepustowości firewall'a oraz VPN. **144.2.2.** Symulację ataków oraz testy IPS/IDS w celu zweryfikowania skuteczności ochrony. **144.2.3.** Weryfikację konfiguracji reguł i polityk bezpieczeństwa. **145.** Szkolenie dla administratorów IT **145.1.** Wykonawca zobowiązuje się przeprowadzić szkolenie dla co najmniej 2 administratorów IT z urzędu. **145.2.** Zakres szkolenia obejmuje: **145.2.1.** Wprowadzenie do interfejsu zarządzania urządzeniem **145.2.2.** Konfigurację i zarządzanie regułami firewalla, filtrowaniem treści oraz IPS/IDS. **145.2.3.** Zarządzanie VPN (IPSec, SSL VPN) oraz konfigurację dostępu zdalnego. **145.2.4.** Monitorowanie działania urządzenia, analiza logów oraz zarządzanie zdarzeniami. **145.2.5.** Tworzenie kopii zapasowych i odtwarzanie konfiguracji. **146.** Wykonawca musi posiadać odpowiednie doświadczenie w zakresie wdrożeń urządzeń klasy UTM

2. Serwer aplikacyjno-domenowy – 2 szt.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
Obudowa	**1.** Obudowa Rack o wysokości max 1U **2.** 8 wnęk na dyski 2.5” **3.** Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej **4.** Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	**5.** Płyta główna z możliwością zainstalowania do dwóch procesorów. **6.** Obsługa procesorów 32 rdzeniowych. **7.** Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. **8.** Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. **9.** Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	**10.** Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	**11.** Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	**12.** 128GB DDR5 RDIMM 5600MT/s,
Kontroler RAID	**13.** Sprzętowy kontroler dyskowy, posiadający o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. **14.** Wsparcie dla dysków samoszyfrujących
Dyski twarde	**15.** Zainstalowane **15.1.** 4x dysk SSD SATA o pojemności min. 1.92TB Hot-Plug.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	15.2. 2x dysk SAS o pojemności min. 2.4TB Hot-Plug. **16.** Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.
Gniazda PCI	**17.** Trzy sloty PCIe LP
Interfejsy sieciowe/FC/SAS	**18.** Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Wbudowane porty	**19.** 4 porty USB w tym min: **19.1.** 1 port USB 3.0 z tyłu obudowy, **19.2.** 1 port micro USB z przodu obudowy **20.** 2 port VGA z czego jeden z przodu obudowy **21.** Możliwość rozbudowy o port RS232
Video	**22.** Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	**23.** Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	**24.** Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Bezpieczeństwo	**25.** Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. **26.** Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. **27.** Możliwość wyłączenia w BIOS funkcji przycisku zasilania. **28.** BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła **29.** Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. **30.** Moduł TPM 2.0 **31.** Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	32. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem **33.** Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	**34.** Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: **34.1.** zdalny dostęp do graficznego interfejsu Web karty zarządzającej; **34.2.** zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); **34.3.** szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; **34.4.** możliwość podmontowania zdalnych wirtualnych napędów; **34.5.** wirtualną konsolę z dostępem do myszy, klawiatury; **34.6.** wsparcie dla IPv6; **34.7.** wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; **34.8.** możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; **34.9.** możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; **34.10.** integracja z Active Directory; **34.11.** możliwość obsługi przez dwóch administratorów jednocześnie; **34.12.** wsparcie dla automatycznej rejestracji DNS **34.13.** wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. **34.14.** możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera **34.15.** możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: **35.** Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	36. Przesyłanie danych telemetrycznych w czasie rzeczywistym **37.** Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze **38.** Automatyczna rejestracja certyfikatów (ACE)
System operacyjny	**39.** Zakup licencji Microsoft Windows Server 2022 x64 Standard PL pozwalającej na utworzenie 4 instancji wirtualnych wraz z 35 licencjami dostępowymi dla użytkownika lub produkt równoważny. Za równoważność rozumie się zakup produktu obejmującego licencję systemu operacyjnego który zapewnia: **39.1.** licencję obejmującą minimum 16 rdzeni procesora(ów), **39.2.** Obsługę Windows Server Containers. **39.3.** Możliwość pełnienia funkcji drugiego kontrolera domeny Active Directory w istniejącej infrastrukturze Zamawiającego (zgodność z AD na poziomie Windows Server 2008 R2). **39.4.** interfejsy użytkownika dostępne w wielu językach do wyboru - w tym polskim i angielskim, **39.5.** graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, **39.6.** możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach **39.7.** wersji systemu operacyjnego poprzez wdrożony w jednostce **39.8.** Zamawiającego serwer aktualizacji Microsoft Windows Server Update Services (WSUS), **39.9.** wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), **39.10.** zabezpieczenie hasłem dostępu do systemu, konta i profilu użytkowników, **39.11.** mechanizmy logowania w oparciu o login i hasło, **39.12.** Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi **39.13.** uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości współbieżnej (ang. Simultaneous Multi-Threading, SMT). **39.14.** Wbudowane wsparcie instalacji i pracy na wolumenach, które: **39.14.1.** pozwalają na zmianę rozmiaru w czasie pracy systemu,

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	39.14.2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, **39.14.3.** umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, **39.14.4.** umożliwiają zdefiniowanie list kontroli dostępu (ACL). **39.15.** Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. **39.16.** Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. **39.17.** Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. **39.18.** Wsparcie dla środowisk Java i .NET Framework 6.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. **39.19.** Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: **39.19.1.** Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, **39.19.2.** Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe). **39.19.3.** Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 2 aktywnych środowisk wirtualnych systemów operacyjnych. **39.20.** Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. **39.21.** Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. **40.** Dostarczone oprogramowanie musi być fabrycznie nowe. **41.** Zamawiający dopuszcza zakup licencji typu „Government” (GOV). **42.** Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do dostarczenia testowej wersji oprogramowania równoważnego.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
Oprogramowanie do zarządzania – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	**43.** Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: **44.** Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych **45.** integracja z Active Directory **46.** Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta **47.** Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish **48.** Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram **49.** Szczegółowy opis wykrytych systemów oraz ich komponentów **50.** Możliwość eksportu raportu do CSV, HTML, XLS, PDF **51.** Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. **52.** Grupowanie urządzeń w oparciu o kryteria użytkownika **53.** Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji **54.** Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach **55.** Szybki podgląd stanu środowiska **56.** Podsumowanie stanu dla każdego urządzenia **57.** Szczegółowy status urządzenia/elementu/komponentu **58.** Generowanie alertów przy zmianie stanu urządzenia. **59.** Filtry raportów umożliwiające podgląd najważniejszych zdarzeń **60.** Integracja z service desk producenta dostarczonej platformy sprzętowej **61.** Możliwość przejęcia zdalnego pulpitu **62.** Możliwość podmontowania wirtualnego napędu **63.** Kreator umożliwiający dostosowanie akcji dla wybranych alertów **64.** Możliwość importu plików MIB **65.** Przesyłanie alertów „as-is” do innych konsol firm trzecich

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	66. Możliwość definiowania ról administratorów **67.** Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów **68.** Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) **69.** Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta **70.** Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów **71.** Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. **72.** Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. **73.** Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile **74.** Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. **75.** Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. **76.** Zdalne uruchamianie diagnostyki serwera. **77.** Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. **78.** Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	**79.** Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: **80.** Monitoring: **80.1.** ilość podłączonych oraz rozłączonych systemów **80.2.** stan podłączonych urządzeń **80.3.** informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	80.4. Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia **80.5.** informacje o statusie gwarancji dla poszczególnych urządzeń **80.6.** informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń **80.7.** informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. **80.8.** Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych **80.9.** Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. **80.10.** Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. **80.11.** Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. **80.12.** Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. **80.13.** Monitoring parametrów serwerów z informacją o minimum: **80.13.1.** Obciążeniu procesora **80.13.2.** Zużyciu pamięci RAM **80.13.3.** Temperaturze procesorów **80.13.4.** Temperaturze powietrza wlotowego **80.13.5.** Zużyciu prądu **80.13.6.** Zmianach w fizycznej konfiguracji serwera **80.13.7.** Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. **80.14.** Monitoring parametrów pamięci masowych z informacją o minimum: **80.14.1.** Opóźnieniach **80.14.2.** IOPS

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	80.14.3. Przepustowości **80.14.4.** Utylizacji kontrolerów **80.14.5.** Pojemność całkowita i dostępna **80.14.6.** Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. **80.14.7.** Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. **80.14.8.** Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata **80.14.9.** Informacje o poziomie redukcji danych **80.14.10.** Informacje o statusie replikacji oraz snapshotów **80.15.** Monitoring parametrów przełączników sieciowych z informacją o minimum: **80.15.1.** Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny **80.15.2.** Stanie komponentów: zasilacze, wentylatory **80.15.3.** Podłączonych hostach **80.15.4.** Ilości i statusu portów **80.15.5.** Utylizacji procesora **80.15.6.** Utylizacji poszczególnych portów **80.15.7.** Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. **81.** Aktualizacja firmware **81.1.** możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania **81.2.** możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania **81.3.** możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	81.4. możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania **81.5.** możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania **82.** Raporty **82.1.** Możliwość generowania raportów dla serwerów zawierających informację o: **82.1.1.** Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej **82.1.2.** Średnim obciążeniu: procesorów, pamięci RAM, IO, **82.2.** Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: **82.2.1.** Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji **82.3.** Generowanie raportów do plików CSV i PDF **83.** Cyberbezpieczeństwo **83.1.** Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. **83.2.** Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. **83.3.** Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. **83.4.** Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. **84.** Wspierane urządzenia **84.1.** Urządzenie Producenta dostarczane w ramach postępowania **84.2.** Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) **85.** Wirtualny asystent

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	85.1. Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; **86.** Możliwość rozszerzenia funkcjonalności **86.1.** Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. **87.** Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android **88.** Oferowana platforma musi być zaprojektowana zgodnie ze standardami: **88.1.** ISO 27001 **88.2.** NIST Security and Privacy Controls for Federal Information Systems and Organization **88.3.** CSA Cloud Control Matrix
Certyfikaty	**89.** Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 **90.** Serwer musi posiadać deklaracja CE. **91.** Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** **92.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	**93.** Zamawiający wymaga dokumentacji w języku polskim lub angielskim. **94.** Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
Wsparcie techniczne i oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	**95.** Oprogramowanie połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. **96.** Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. **97.** Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub Linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. **98.** Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu. **99.** Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów oraz wirtualną konsolę z dostępem do myszy, klawiatury. **100.** Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: **100.1.** Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. **100.2.** Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. **100.3.** Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. **100.4.** upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, **100.5.** możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: **100.5.1.** o poprawkach i usprawnieniach dotyczących aktualizacji **100.5.2.** dacie wydania ostatniej aktualizacji **100.5.3.** priorytecie aktualizacji **100.5.4.** zgodność z systemami operacyjnymi **100.5.5.** jakiego komponentu sprzętu dotyczy aktualizacja

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	100.5.6. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. **100.6.** wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne **100.7.** możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. **100.8.** rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) **100.9.** sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) **100.10.** dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml **101.** raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Warunki gwarancji	**102.** Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. **103.** Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. **104.** Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. **105.** Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. **106.** Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. **107.** Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. **108.** Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE – SERWER APLIKACYJNO-DOMENOWY
	109. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. **110.** Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: **110.1.** Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. **110.2.** Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. **110.3.** Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. **110.4.** Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. **110.5.** Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. **111.** Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. **112.** Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

3. DLP System ochrony przed wyciekiem danych - 70 użytkowników

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
Architektura / budowa	**1.** System musi umożliwić bezproblemową i stabilną obsługę co najmniej 100 Klientów jednocześnie. **2.** **Błąd! Nie można odnaleźć źródła odwołania.**: **2.1.** Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. **2.1.1.** Połączenie klient – serwer, Komunikacja odbywa się z wykorzystaniem TLS 1.3. **2.1.2.** Serwer i klient posiadają certyfikaty SSL (4096 bitowe). **2.2.** Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych). **2.3.** Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej. **2.4.** Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami. **2.5.** Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej. **3.** Konfiguracja Architektury: **3.1.** Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. **3.2.** Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją. **3.3.** System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, polityk, pomoc i inne wbudowane bazy wiedzy. **3.4.** Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI. **3.5.** Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi. **3.6.** Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej. **3.7.** System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu. **3.8.** Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa). **3.9.** System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków. **3.10.** Klient musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów. **3.11.** Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta. **3.12.** System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	3.13. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów. **4.** System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem. **4.1.** Automaty powinny realizować co najmniej: Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych. **4.2.** Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie.
Wymagania systemowe	**5.** Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera). **6.** Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. **6.1.** Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2 **7.** Serwer musi działać minimum na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11. **8.** Serwer www musi być oparty o platformę minimum Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9. **9.** Baza danych musi działać na silniku minimum Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition). **10.** System musi mieć możliwość pracy w środowisku wirtualnym minimum Microsoft Hyper-V oraz VMWare.
Interfejsy	**11.** System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. **11.1.** Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	11.2. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS. **11.3.** Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny. **12.** System musi umożliwiać import użytkowników z zewnętrznego pliku CSV. **13.** System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane. **14.** System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS. **15.** System zapewnia integrację z modelem LLM.
Funkcjonalności systemu	**16.** Funkcjonalność Klienta **16.1.** System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego). **16.2.** Klient musi mieć możliwość konfiguracji zakresu skanowania plików. **16.3.** Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił. **17.** Funkcjonalność konsoli administracyjnej. **17.1.** Konsola musi być w pełni polskojęzyczna. **17.2.** Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie). **17.3.** Konsola administracyjna musi posiadać dashboard – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	17.4. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi. **17.5.** Dane na widżetach muszą być aktualizowane automatycznie. **17.6.** System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność). **17.7.** Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. **17.8.** Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego. **17.9.** System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji. **17.10.** Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu. **17.11.** Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko). **17.12.** Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera. **17.13.** Konsola musi zawierać w sobie pełną dokumentację systemu. **18.** Odczytywanie zainstalowanego oprogramowania **18.1.** System powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji. **19.** Wzorce aplikacji i pakietów **19.1.** System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	19.2. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania. **19.3.** Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów. **19.4.** System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu. **20.** Inwentaryzacja sprzętu komputerowego **20.1.** System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem). **20.2.** System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language. **20.3.** System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu). **20.4.** System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania. **20.5.** System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru. **20.6.** System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu). **20.7.** System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART). **20.8.** System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku. **20.9.** System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu. **20.10.** System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	20.11. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne. **20.12.** System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów. **20.13.** System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik) **20.14.** System umożliwia dodawanie notatek do każdej pozycji sprzętu. **20.15.** System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części). **20.15.1.** System musi umożliwiać definiowanie typów serwisów **20.15.2.** System musi umożliwiać definiowanie wartości serwisu **20.15.3.** System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji **20.16.** System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium. **20.17.** System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja). **21.** Inwentaryzacja urządzeń podłączanych do komputera. **21.1.** System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.) **21.2.** System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika. **21.3.** System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika). **22.** Inwentaryzacja urządzeń sieciowych. **22.1.** System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3. **22.2.** Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	22.3. System musi zbierać informacje o jakości połączenia: **22.4.** Czas odpowiedzi serwisów (usług) podawany w milisekundach: **22.4.1.** Średni czas odpowiedzi. **22.4.2.** Minimalny czas odpowiedzi. **22.4.3.** Maksymalny czas odpowiedzi. **22.5.** Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat. **22.6.** System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta. **22.6.1.** Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci **22.6.2.** Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług. **22.6.3.** System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą. **22.7.** System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci. **22.7.1.** System musi umożliwiać generowanie map według dowolnych filtrów użytkownika. **23.** Zdalna administracja komputerami **23.1.** System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika. **23.2.** System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania. **23.3.** Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego. **23.4.** Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status). **23.5.** System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty. **23.6.** Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów **23.7.** System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.). **23.8.** System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako) **23.9.** System musi umożliwiać tworzenie zadań cyklicznych dla komputerów. **23.10.** Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania. **23.11.** System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie. **23.12.** System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	23.12.1. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji. **23.12.2.** System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6). **23.13.** System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch). **23.14.** System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC. **23.15.** System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie. **23.16.** System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu). **23.17.** System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. **23.18.** System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. **24.** Wysyłanie wiadomości **24.1.** Komunikator **24.1.1.** System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu. **24.1.2.** Powinien zapewniać możliwość inicjowania czatu przez administratora. **24.1.3.** Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta. **24.1.4.** System musi przechowywać historię konwersacji. **24.1.5.** Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników. **24.2.** Wiadomość Jednorazowa: **24.2.1.** System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	24.2.2. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu. **24.2.3.** Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML. **24.2.4.** Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów lub użytkowników. **24.2.5.** System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości. **24.3.** Wiadomości Cykliczne: **24.3.1.** Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku. **24.3.2.** Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML. **24.3.3.** System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników. **24.3.4.** Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników. **24.3.5.** Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie. **24.4.** System szkolenia pracowników za pomocą wiadomości. **24.4.1.** System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów. **24.4.2.** System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”. **24.4.3.** Formatowanie treści musi być zgodne z HTML. **24.4.4.** System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych). **24.4.5.** System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców. **24.4.6.** Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości. **24.4.7.** Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	24.4.8. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników. **24.4.9.** System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem). **25.** Repozytorium CMDB **25.1.** System musi posiadać wbudowaną centralną bazę systemu umożliwiająca import i eksport niektórych danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta. **26.** Worktime manager **26.1.** System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników. **26.2.** System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych. **26.3.** System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną. **27.** Zarządzanie politykami bezpieczeństwa. **27.1.** System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących. **27.2.** System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami. **27.3.** System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią). **27.4.** System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu. **27.5.** Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia. **27.6.** Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych. **27.7.** Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	27.8. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status podłączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną **27.9.** Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych. **27.10.** System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu). **27.11.** System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP. **27.12.** System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji. **27.13.** Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę. **27.14.** System musi mieć możliwość określenia ram czasowych działania danej reguły. **27.15.** System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego. **28.** System musi w pełni wspierać następujące polityki ochrony danych: **28.1.** Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione. **28.2.** Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu. **28.3.** Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym. **28.4.** Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera. **29.** Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
Klasyfikacja i ochrona dokumentów (KD)	**30.** Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami. **31.** Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu. **32.** Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
Raportowanie i eksport danych	**33.** System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp. **34.** System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www. **35.** System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf. **36.** System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu). **37.** System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.
Bezpieczeństwo	**38.** System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej. **38.1.** Uwierzytelnianie do systemu musi być realizowane: **38.1.1.** z wykorzystaniem imiennego konta użytkownika i hasła, **38.1.2.** z wykorzystaniem imiennego konta administratorów aplikacji i hasła, **38.1.3.** za pośrednictwem uwierzytelniania poprzez Active Directory, **38.1.4.** za pośrednictwem uwierzytelniania poprzez CAS, **39.** Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej. **40.** Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków). **41.** System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA).

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	41.1. Uwierzytelnianie z wykorzystaniem obrazu wideo. **41.2.** Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika. **41.3.** Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP. **42.** Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256. **42.1.** Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019. **43.** System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować: **43.1.** Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności. **43.2.** Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną. **44.** Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport. **45.** System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID. **46.** Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie. **47.** System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http. **48.** System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera. **49.** System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii. **50.** System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych. **51.** W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy). **52.** System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od Klientów.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	53. System musi zapewniać: **53.1.** Pełne logowanie błędów w celu weryfikowania nieprawidłowości. **53.2.** Przechowywanie logów systemowych. **53.3.** Przechowywanie logów bezpieczeństwa. **53.4.** Przechowywanie logów aktywności użytkowników i administratorów. **53.5.** Pobieranie logów z Klientów z poziomu konsoli administracyjnej. **53.6.** Możliwość eksportu logów. **53.7.** Definiowanie maksymalnego czasu przechowywania plików log. **53.8.** System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji. **53.9.** Definiowanie ścieżki do kopii zapasowej **53.10.** Definiowanie ścieżki do importu danych **53.11.** Definiowanie ścieżki do zapisu raportów **53.12.** Definiowanie serwera do importu danych
Wsparcie i pomoc	**54.** System musi posiadać dokumentację w postaci min. 5 filmów instruktażowych/nagrań z webinariów w języku polskim. **55.** System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim. **56.** Pomoc techniczna **56.1.** Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00. **56.2.** Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania. **57.** Czas trwania usługi SLA wynosi do 30.06.2026 r. od dnia zakupu. **58.** Usługi Utrzymania Oprogramowania obejmują: **58.1.** asystę techniczną, **58.2.** świadczenie usług SLA, w ramach, których realizowana jest obsługa zgłoszeń w zakresie:

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - DLP
	58.2.1. reakcja na zgłoszenia błędów w określonym czasie reakcji; **58.2.2.** dokonywanie analizy przyczyn błędów; **58.2.3.** zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich; **58.2.4.** zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego; **58.2.5.** usuwania błędów w czasie naprawy; **58.2.6.** usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy; **58.3.** zapewnienia dostępności Oprogramowania.

4. Wdrożenie Active Directory w Urzędzie Miejskim, Miejsko-Gminnym Ośrodku Pomocy Społecznej oraz Centrum Sportu i Rekreacji

KOMPONENT	WYMAGANIA MINIMALNE ZAKRESU WDROŻENIA ACTIVE DIRECTORY
Cel wdrożenia	**1.** Celem wdrożenia usługi Active Directory (AD) jest stworzenie centralnego systemu zarządzania tożsamościami, dostępem i zasobami IT. Wdrożenie AD pozwoli na efektywne zarządzanie kontami użytkowników, zwiększenie bezpieczeństwa danych oraz uproszczenie obsługi infrastruktury IT.
Analiza potrzeb i projektowanie środowiska AD	**2.** Analiza istniejącej infrastruktury IT oraz wymagań urzędu. **3.** Zdefiniowanie struktury organizacyjnej w Active Directory, zgodnej z podziałem na wydziały, referaty i stanowiska. **4.** Określenie polityk bezpieczeństwa, zasad haseł i kontroli dostępu. **5.** Przygotowanie szczegółowego projektu wdrożenia, obejmującego hierarchię jednostek organizacyjnych (OU), grup zabezpieczeń, i przypisanych ról.
Przygotowanie infrastruktury serwerowej	**6.** Instalacja i konfiguracja dedykowanego serwera fizycznego lub wirtualnego dla roli kontrolera domeny (DC). **7.** Aktualizacja systemów operacyjnych i sterowników serwerów do najnowszych wersji. **8.** Przygotowanie zapasowego systemu kopii bezpieczeństwa kontrolerów domeny.
Instalacja i konfiguracja Active Directory	**9.** Instalacja usługi AD Domain Services (AD DS) na wyznaczonych serwerach. **10.** Utworzenie domeny o nazwie zgodnej z nazwą urzędu, np. um.warka.local. **11.** Implementacja jednostek organizacyjnych (OU) zgodnie z podziałem strukturalnym urzędu, np. Referaty Finansowe, Administracyjne, Techniczne. **12.** Tworzenie polityk grupowych (GPO) dla wymuszania standardów konfiguracji na komputerach i użytkownikach, w tym: **12.1.** Polityki haseł (długość, złożoność, czas ważności). **12.2.** Ustawienia zabezpieczeń dla komputerów (blokady ekranu, szyfrowanie). **12.3.** Zarządzanie mapowaniem dysków sieciowych i drukarek.

KOMPONENT	WYMAGANIA MINIMALNE ZAKRESU WDROŻENIA ACTIVE DIRECTORY
Migracja użytkowników i zasobów	**13.** Przeniesienie istniejących kont użytkowników, komputerów oraz zasobów do Active Directory. **14.** Automatyzacja migracji za pomocą narzędzi takich jak Active Directory Migration Tool (ADMT). **15.** Testowanie poprawności przeniesienia i eliminowanie potencjalnych konfliktów kont.
Integracja z innymi usługami	**16.** Konfiguracja serwera DNS i DHCP w celu zapewnienia poprawnej komunikacji z Active Directory. **17.** Integracja z systemami pocztowymi i innymi aplikacjami wykorzystywanymi przez urząd, np. systemami ERP, CRM czy ePUAP. **18.** Wdrożenie mechanizmów jednorazowego logowania (Single Sign-On) dla zgodnych aplikacji.
Zabezpieczenia i monitoring	**19.** Wdrożenie polityk bezpieczeństwa AD, w tym ograniczenie praw administracyjnych do niezbędnego minimum. **20.** Konfiguracja inspekcji i logowania zdarzeń związanych z dostępem do zasobów i kont użytkowników. **21.** Implementacja systemu wykrywania naruszeń bezpieczeństwa w infrastrukturze AD.
Testy i optymalizacja	**22.** Testowanie działania Active Directory w środowisku produkcyjnym. **23.** Optymalizacja polityk grupowych i struktury organizacyjnej na podstawie testów. **24.** Eliminacja potencjalnych wąskich gardeł w infrastrukturze.
Szkolenie administratorów i użytkowników	**25.** Przeprowadzenie warsztatów dla administratorów IT z zakresu: **25.1.** Zarządzania użytkownikami i zasobami w Active Directory. **25.2.** Tworzenia i zarządzania politykami grupowymi. **25.3.** Rozwiązywania problemów związanych z AD. **26.** Organizacja szkoleń dla użytkowników z obsługi systemów uwierzytelniania i dostępu.
Wsparcie powdrożeniowe	**27.** Zapewnienie wsparcia technicznego przez okres minimum 30 dni po wdrożeniu. **28.** Dostarczenie dokumentacji technicznej obejmującej konfigurację AD oraz procedury awaryjne.
Efekty wdrożenia	**29.** Centralizacja zarządzania kontami użytkowników i zasobami IT. **30.** Zwiększenie bezpieczeństwa dzięki zaawansowanym mechanizmom kontroli dostępu i politykom haseł. **31.** Uproszczenie procesów administracyjnych dzięki automatyzacji zadań. **32.** Redukcja ryzyka przestojów dzięki redundancji i mechanizmom awaryjnym.

5. Wykonanie segmentacji sieci w Urzędzie Miejskim, Miejsko-Gminnym Ośrodku Pomocy Społecznej oraz Centrum Sportu i Rekreacji

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
Etap analizy i planowania	**1.** Audyt infrastruktury sieciowej **1.1.** Przeprowadzenie szczegółowego audytu istniejącej infrastruktury IT, w tym topologii sieci, urządzeń końcowych, serwerów, drukarek i innych urządzeń sieciowych. **1.2.** Identyfikacja krytycznych zasobów, przepływów danych oraz potencjalnych punktów awarii lub luk w bezpieczeństwie. **2.** Opracowanie projektu segmentacji **2.1.** Stworzenie logicznej struktury segmentacji sieci opartej na potrzebach urzędu, np. podział na VLAN-y dla wydziałów (np. Administracja, Finanse, IT, Obsługa interesantów) oraz usług (np. Internet, drukarki, monitoring). **2.2.** Zdefiniowanie reguł dostępu między segmentami sieci zgodnie z zasadą minimalnych uprawnień (Least Privilege). **2.3.** Uwzględnienie przyszłych potrzeb skalowalności w projekcie.
Etap instalacji i konfiguracji sprzętu	**3.** Przygotowanie urządzeń sieciowych **3.1.** Sprawdzenie kompatybilności nowych przełączników z istniejącą infrastrukturą. **3.2.** Aktualizacja oprogramowania firmware przełączników do najnowszej wersji w celu zapewnienia pełnej funkcjonalności i bezpieczeństwa. **3.3.** Konfiguracja podstawowych parametrów przełączników, takich jak adresy IP, nazwy urządzeń, połączenia uplinkowe i redundancja. **4.** Montowanie sprzętu w szafach rack **4.1.** Instalacja minimum czterech nowych przełączników w szafach rackowych zgodnie z zaleceniami producenta, uwzględniając odpowiednie zarządzanie kablami i ergonomię. **4.2.** Podłączenie urządzeń do istniejącej infrastruktury sieciowej oraz konfiguracja połączeń uplink w celu zapewnienia redundancji.
Wymagania minimalne dla nowych	**5.** Instalacja sprzętu **5.1.** Montaż nowych przełączników w szafach rackowych w pomieszczeniach serwerowych.

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
przełączników sieciowych	**5.2.** Podłączenie urządzeń do infrastruktury zgodnie z projektem segmentacji oraz zarządzanie okablowaniem w celu uniknięcia potencjalnych awarii. **6.** Konfiguracja przełączników **6.1.** Tworzenie VLAN-ów dla wydzielonych segmentów sieciowych. **6.2.** Konfiguracja portów jako porty dostępowe lub trunkowe w zależności od ich funkcji w topologii sieci. **6.3.** Konfiguracja routingu warstwy 3, umożliwiająca komunikację między VLAN-ami zgodnie z zasadami minimalnych uprawnień. **7.** Parametry i minimalne wymagania techniczne: **7.1.** Przełącznik musi posiadać minimum 24 porty RJ45 o minimalnej prędkości 1Gb/s. **7.2.** Dodatkowo przełącznik musi posiadać minimum 4 porty SFP+ o prędkości minimum 10Gb/s . **7.3.** Przełącznik musi posiadać port konsolowy umożliwiający zarządzanie urządzeniem z poziomu linii komend. **7.4.** Przełącznik musi umożliwiać przekonfigurowanie portów przełącznika, aby była możliwa transmisja na odległość do 250 metrów z portu RJ-45. **7.5.** Przełącznik musi być, posiadać ochronę wszystkich portów przed przepięciami do 6000V. **7.6.** Przełącznik musi posiadać ochronę przeciwzwarciową. **7.7.** Zasilacz przełącznika musi posiadać ochronę przeciw przegrzaniem. **7.8.** Zasilacz przełącznika musi posiadać przed nadmiernym napięciem. **7.9.** Przełącznik musi umożliwiać montaż w standardowej szafie rack 19” za pomocą dostarczonych do zestawu uchwytów montażowych. **7.10.** Przepustowość przełącznika nie może być mniejsza niż 128Gb/s. **7.11.** Szybkość przełączania ramek wewnątrz przełącznika nie może być mniejsza niż 95,2Mp/s. **7.12.** Przełącznik musi posiadać wsparcie dla technologii 802.1Q. **7.13.** Przełącznik musi posiadać przynajmniej wsparcie dla takich protokołów jak: **7.13.1.** MAC VLAN **7.13.2.** IP VLAN **7.13.3.** QinQ

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	7.13.4. Voice VLAN **7.14.** Przełącznik musi posiadać możliwość tworzenia tras statycznych dla protokołu IPv4 jak i dla IPv6. **7.15.** Przełącznik musi posiadać obsługę przynajmniej takich protokołów przesyłania grupowego takich jak: **7.15.1.** IGMP v1 **7.15.2.** IGMP v2 **7.15.3.** IGMP v3 **7.15.4.** MLD **7.15.5.** PIM-DM **7.15.6.** PIM-SSM **7.16.** Przełącznik musi posiadać ochronę podszywania w grupach multiemisyjnych za pomocą przynajmniej takich protokołów jak: **7.16.1.** IGMP v1 **7.16.2.** IGMP v2 **7.16.3.** IGMP v3 **7.16.4.** MLD v1 **7.16.5.** MLD v2 **7.17.** Przełącznik musi posiadać możliwość tworzenia dynamicznych tras za pomocą przynajmniej takich protokołów jak: **7.17.1.** RIP **7.17.2.** RIPNG **7.17.3.** OSPF **7.17.4.** OSPF v3 **7.18.** Przełącznik musi przynajmniej umożliwiać agregację portów za pomocą protokołu LACP. **7.19.** Przełącznik musi przynajmniej posiadać agregację portów w trybie: **7.19.1.** Pasywnym **7.19.2.** Aktywnym

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	7.19.3. Statycznym **7.20.** Przełącznik musi obsługiwać technologię drzewa rozpinającego w przynajmniej w wersji: **7.20.1.** STP (IEEE 802.1d) **7.20.2.** RSTP (IEEE 802. 1w) **7.20.3.** MSTP (IEEE 802. 1s) **7.21.** Przełącznik musi obsługiwać technologię ERPS. **7.22.** Przełącznik musi przynajmniej umożliwiać przeciwdziałanie burzom rozgłoszeniowym jak i multiemisyjnym. **7.23.** Przełącznik musi posiadać ochronę przed zapętleniem ruchu poprzez automatyczne zablokowanie portu. **7.24.** Przełącznik musi posiadać możliwość uruchomienia serwera DHCP. **7.25.** Przełącznik musi posiadać możliwość przesyłania na wskazany port lub porty wszystkich pakietów przychodzących i wychodzących z wybranego portu. **7.26.** Przełącznik musi posiadać możliwość automatycznego oszczędzania energii poprzez wyłączenie portów w przypadku, gdy nie są one używane. **7.27.** Przełącznik musi posiadać możliwość ustawienia limitu szybkości przesyłanych pakietów. **7.28.** Serwer DHCP musi przynajmniej posiadać możliwość stworzenia pul adresowych jak i statycznego przypisania adresu MAC do wskazanego adresu IP. **7.29.** Przełącznik musi posiadać ochronę przed podszywaniem się serwer DHCP. **7.30.** Przełącznik musi posiadam możliwość uwierzytelniania przynajmniej za pomocą protokołów takich jak: **7.30.1.** RADIUS **7.30.2.** TACACS+ **7.30.3.** 802.1X **7.31.** Przełącznik musi posiadać ochronę przed odmową usługi. **7.32.** Przełącznik musi posiadać ochronę ARP. **7.33.** Przełącznik musi posiadać ochronę źródłowych adresów IP. **7.34.** Przełącznik musi posiadać obsługę przynajmniej protokołów zarządzających takich jak:

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	7.34.1. IEEE 802.1ag CFM **7.34.2.** IEEE 802.3ah EFM OAM **7.35.** Przełącznik musi przynajmniej posiadać możliwość zarządzania za pomocą protokołów takich jak: **7.35.1.** Telnet **7.35.2.** SSH **7.35.3.** Port konsolowy **7.36.** Przełącznik musi posiadać możliwość badania stanu urządzenia za pomocą przynajmniej takich protokołów jak: **7.36.1.** SNMP v1 **7.36.2.** SNMP v2 **7.36.3.** SNMP v3 **7.36.4.** RMON **7.37.** Przełącznik musi posiadać możliwość pozyskiwania zdarzeń z urządzania przynajmniej za pomocą protokołu syslog. **7.38.** Przełącznik musi posiadać wsparcie dla protokołu LLDP. **7.39.** Przełącznik musi przynajmniej posiadać możliwość wybrania portu, na którym będzie działać protokołu LLDP. **7.40.** Przełącznik musi umożliwiać konfigurację protokołu QoS. **7.41.** Przełącznik musi umożliwiać ustawienie polityk QoS w przynajmniej takich trybach jak: **7.41.1.** SP **7.41.2.** WRR **7.41.3.** WFQ **7.42.** Przełącznik musi przynajmniej posiadać możliwość wskazania czy dany port będzie wykorzystywany do wysyłania, odbierania lub do obustronnej transmisji pakietów LLDP na wskazanym porcie. **7.43.** Przełącznik musi przynajmniej posiadać możliwość pobierania i wysyłania konfiguracji za protokołu TFTP. **7.44.** Przełącznik musi przynajmniej posiadać możliwość konfiguracji listy dostępowej, która umożliwiałaby blokowanie lub zezwalanie dostępu do urządzenia za pomocą takich parametrów jak:

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	7.44.1. Adres MAC źródłowy **7.44.2.** Adres MAC docelowy **7.44.3.** Adres IP źródłowy **7.44.4.** Adres IP docelowy **7.44.5.** Zakres czasowy **7.45.** Przełącznik musi umożliwiać konfiguracje i zarządzanie konfiguracją funkcji Port Security. **7.46.** Przełącznik musi umożliwiać rejestrowanie ilości nadużyć w funkcji Port Security. **7.47.** Przełącznik musi przynajmniej posiadać możliwość zarządzania urządzeniem za pomocą protokołu TR-069. **7.48.** Przełącznik musi posiadać dostarczony przez producenta na urządzeniu panel administracyjny. **7.49.** Panel administracyjny musi być dostępny z poziomu przeglądarki. **7.50.** Panel administracyjny musi posiadać możliwość łączności za pomocą przynajmniej protokołów takich jak: **7.50.1.** HTTP **7.50.2.** HTTPS **7.51.** Panel administracyjny musi posiadać polską wersję językową. **7.52.** Panel administracyjny musi umożliwiać wyłączenie zasilania dla wybranego portu Ethernet. **7.53.** Panel administracyjny musi umożliwia diagnozowanie łączności przynajmniej za pomocą takich technologii jak: **7.53.1.** Ping **7.53.2.** Tracert **7.54.** Panel administracyjny musi umożliwiać diagnozowanie połączenia sieciowego w pierwsze warstwie sieciowej OSI. **7.55.** Panel administracyjny umożliwia wykonanie testu zapętlenia ruchu na portach przełącznika. **7.56.** Panel administracyjny musi umożliwiać wyświetlanie dzienników systemowych. **7.57.** Panel administracyjny musi umożliwiać przekazywanie dzienników systemowych do zewnętrznego serwera syslog. **7.58.** Panel administracyjny musi umożliwiać wyświetlanie w dzienniku systemowym przynajmniej takich informacji jak: **7.58.1.** zdarzeń połączenia sieciowego zarówno dla interfejsów fizycznych jak i wirtualnych

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	7.58.2. zdarzeń połączenia sieciowego do serwera zarządzającego **7.58.3.** zdarzeń zarejestrowanych przez protokół OSPF **7.58.4.** zdarzeń zarejestrowanych przez moduł DDM **7.59.** Panel administracyjny musi umożliwiać skonfigurowanie alarmów dotyczących przynajmniej takich elementów jak: **7.59.1.** moduły zasilające **7.59.2.** połączenie sieciowe w pierwsze warstwie sieciowej OSI **7.59.3.** zapętlenie ruchu sieciowego **7.60.** Panel administracyjny musi umożliwiać eksportowanie i importowanie pliku konfiguracyjnego urządzenia. **7.61.** Panel administracyjny musi umożliwiać przywrócenie poprzedniego oprogramowania bez konieczności przesyłania go do przełącznika. **7.62.** Przełącznik musi posiadać możliwość podłączenia urządzenia do chmury producenta bez ponoszenia żadnych dodatkowych kosztów. **7.63.** Przełącznik musi posiadać możliwość podłączenia urządzenia do lokalnego serwera zarządzającego. **7.64.** Przełącznik musi posiadać możliwość sprawdzenia status nawiązanego połączenia z chmurą producenta. **7.65.** Chmurowy system producenta musi posiadać polską wersję językową. **7.66.** Chmurowy system producenta musi umożliwiać wyświetlenie podstawowych informacji o dodanym urządzeniu takich jak: **7.66.1.** Model **7.66.2.** Wersja oprogramowania **7.66.3.** Adres IP urządzenia **7.66.4.** Adres MAC urządzenia **7.66.5.** Graficzne przedstawienie aktywnych portów wraz z wynegocjowanymi prędkościami **7.67.** Chmurowy system producenta musi umożliwiać zdalne restartowanie portu na przełączniku. **7.68.** Chmurowy system producenta musi umożliwiać edytowanie ustawień portów w tym edytowanie przypisania do określonego VLANu. **7.69.** Chmurowy system producenta musi umożliwiać zmianę trybu działania portu na przynajmniej taki tryb jak:

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	7.69.1. Access **7.69.2.** Trunk **7.69.3.** Hybrid **7.70.** Chmurowy system producenta musi umożliwiać tworzenie widoków. **7.71.** Chmurowy system producenta musi umożliwiać wyświetlenie dzienników systemowych urządzenia. **7.72.** Chmurowy system producenta musi umożliwiać wyświetlenie statystyk portów. **7.73.** Chmurowy system producenta musi umożliwiać konfigurowanie i modyfikowanie mechanizmu przeciwdziałanie burzom rozgłoszeniowym jak i multiemisyjnym. **7.74.** Chmurowy system producenta musi umożliwiać konfigurowanie i modyfikowanie mechanizmu ochrony przed zapętleniem ruchu poprzez automatyczne zablokowanie portu. **7.75.** Chmurowy system producenta musi umożliwiać zdalne uruchomienie diagnostyki urządzenia i konfiguracji, która sprawdza między innymi takie pozycje jak: **7.75.1.** Funkcjonalności portów optycznych **7.75.2.** Napięcia na portach Ethernet **7.75.3.** Aktualnego stanu serwera DHCP **7.75.4.** Wykorzystania wszystkich adresów IP z puli adresów w usłudze DHCP **7.75.5.** Wystąpienia konfliktu adresów IP **7.75.6.** Wystąpienia pętli między podłączonymi urządzeniami **7.76.** Chmurowy system producenta musi umożliwiać wizualizowanie łączności urządzeń sieciowych podłączonych do serwera. **8.** Oferowany produkt musi posiadać przynajmniej certyfikaty takie jak: **8.1.** CE MEC **8.2.** CE LVD **8.3.** FCC-SDOC **8.4.** ROHS **9.** Producent produktu lub Autoryzowany Dystrybutor Producenta musi posiadać certyfikaty jakości:

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	9.1. ISO 9001 **9.2.** ISO 27001 **10.** Rozszerzone wsparcie serwisowe **10.1.** System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 24 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres do 30.06.2026 r. **10.2.** System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: **10.2.1.** Wsparcie telefoniczne zespołu certyfikowanych inżynierów. **10.2.2.** Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. **10.2.3.** Doradztwo w zakresie konfiguracji. **10.2.4.** Zdalne wsparcie techniczne. **10.2.5.** Pomoc w zakładaniu zgłoszeń serwisowych u producenta. **10.2.6.** Przygotowanie do zdalnej konfiguracji. **10.2.7.** Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. **10.2.8.** Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. **10.2.9.** Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. **10.2.10.** Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. **10.3.** Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. **10.4.** Oferent winien przedłożyć dokumenty:

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	10.4.1. Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). **10.4.2.** Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego.
Etap konfiguracji sieci VLAN	**11.** Tworzenie VLAN-ów **11.1.** Wprowadzenie VLAN-ów w celu oddzielenia ruchu między różnymi działami urzędu (np. VLAN dla finansów, administracji, IT, obsługi interesantów). **11.2.** Utworzenie VLAN-ów dla zasobów wspólnych, takich jak drukarki sieciowe, kamery monitoringu oraz Internet. **12.** Przypisywanie portów do VLAN-ów **12.1.** Przypisanie portów przełączników do odpowiednich VLAN-ów w zależności od przynależności urządzeń do danego działu lub funkcji. **12.2.** Konfiguracja trunków VLAN na portach uplink w celu zapewnienia komunikacji między przełącznikami i urządzeniami zarządzającymi siecią. **13.** Zastosowanie routingu między VLAN-ami **13.1.** Skonfigurowanie routingu warstwy 3 na przełącznikach w celu umożliwienia komunikacji między VLAN-ami zgodnie z określonymi zasadami bezpieczeństwa. **13.2.** Wdrożenie polityk trasowania i priorytetów (QoS) w celu optymalizacji ruchu sieciowego.
Etap konfiguracji zabezpieczeń	**14.** Listy kontroli dostępu (ACL) **14.1.** Zdefiniowanie list kontroli dostępu dla każdego VLAN-u w celu ograniczenia ruchu tylko do autoryzowanych urządzeń i użytkowników. **14.2.** Przykłady reguł ACL: **14.3.** Użytkownicy w VLAN administracyjnym mają dostęp do zasobów finansowych tylko przez określone aplikacje. **14.4.** Blokowanie dostępu do Internetu dla urządzeń monitoringu. **15.** Implementacja zabezpieczeń na poziomie warstwy 2 **15.1.** Wdrożenie mechanizmów ochrony, takich jak DHCP Snooping, ARP Inspection i Port Security, aby zapobiegać atakom wewnętrznym, np. spoofingowi.

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	16. Włączenie logowania i monitorowania **16.1.** Skonfigurowanie centralnego systemu logowania dla przełączników w celu rejestrowania zdarzeń, takich jak nieautoryzowane próby dostępu. **16.2.** Wdrożenie narzędzi monitorujących (np. SNMP, Syslog) do bieżącej analizy wydajności i bezpieczeństwa sieci.
Etap testowania	**17.** Testy wydajnościowe i funkcjonalne **17.1.** Sprawdzenie przepustowości sieci oraz poprawności konfiguracji VLAN-ów. **17.2.** Symulacja różnych scenariuszy ruchu, takich jak przesyłanie danych między VLAN-ami czy dostęp do usług wspólnych. **18.** Testy awaryjne **18.1.** Symulacja awarii jednego z przełączników i sprawdzenie poprawności działania mechanizmów redundancji. **18.2.** Testowanie zachowania sieci w przypadku naruszenia polityk bezpieczeństwa.
Szkolenie i dokumentacja	**19.** Szkolenie administratorów IT **19.1.** Szkolenie z zakresu zarządzania nową infrastrukturą, w tym konfiguracji VLAN-ów, routingu oraz mechanizmów bezpieczeństwa. **19.2.** Przekazanie procedur diagnostycznych i rozwiązywania problemów. **20.** Przygotowanie dokumentacji **20.1.** Opracowanie pełnej dokumentacji technicznej, obejmującej topologię sieci, konfiguracje przełączników oraz reguły ACL. **20.2.** Przekazanie procedur awaryjnych i harmonogramu przeglądów.
Dobre praktyki uwzględnione w wdrożeniu	**21.** Zasada minimalnych uprawnień: Dostęp do zasobów przydzielany wyłącznie na podstawie faktycznych potrzeb. **22.** Redundancja: Konfiguracja portów uplink i zastosowanie dwóch przełączników dla kluczowych połączeń w celu zapewnienia ciągłości działania. **23.** Regularne aktualizacje: Utrzymywanie aktualnego oprogramowania przełączników w celu minimalizacji ryzyka podatności. **24.** Monitorowanie i audyt: Stały nadzór nad działaniem sieci i okresowe przeglądy polityk bezpieczeństwa.
Efekty wdrożenia	**25.** Zwiększenie bezpieczeństwa dzięki izolacji segmentów sieci. **26.** Optymalizacja wydajności i przepływów danych.

KOMPONENT	OPIS MINIMALNEGO ZAKRESU WYKONANIA SEGMENTACJI SIECI
	27. Poprawa zarządzania siecią i skalowalność na przyszłość. **28.** Gotowość infrastruktury do obsługi nowych usług i wymagań urzędu.

6. NAC – system kontroli dostępu do sieci – 150 hostów

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
Podstawowa funkcjonalność systemu NAC	**1.** System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych. **2.** System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor) **3.** System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek. **4.** System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji. **5.** System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji. **6.** System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych. **7.** System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. **8.** Licencja ma być zwalniana po rozłączeniu urządzenia końcowego **9.** System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia. **10.** System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym: **10.1.** VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x **10.2.** Maszyny fizyczne - serwery wspierane przez producenta. **10.3.** System musi posiadać funkcjonalność serwerów: **10.4.** serwera RADIUS dla infrastruktury sieciowej, **10.5.** serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	10.6. serwera SYSLOG, **10.7.** serwera TACACS+, **10.8.** serwera Monitoringu, **10.9.** serwera DHCP, **10.10.** serwera polityk uwierzytelniania i kontroli dostępu 802.1X, **10.11.** serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego. **11.** System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP. **12.** System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC. **13.** System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. **14.** System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now. **15.** Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email. **16.** System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci. **17.** System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania. **18.** System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników. **19.** System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	20. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status). **21.** System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania. **22.** Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim). **23.** System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci. **24.** System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP. **25.** System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia. **26.** System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP. **27.** System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP. **28.** Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu. **29.** System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej. **30.** System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP. **31.** System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci. **32.** System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3. **33.** System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+. **34.** System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych. **35.** System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	końcowych (BYOD). **36.** System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn. **37.** System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS. **38.** System musi posiadać funkcję personalizacji strony gościnnej. **39.** Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon. **40.** Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor. **41.** Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS. **42.** Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory. **43.** Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory. **44.** Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu. **45.** Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru. **46.** Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim). **47.** Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP. **48.** Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni. **49.** Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań. **50.** System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. **51.** System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego. **52.** System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. **53.** System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. **54.** System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	55. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF. **56.** System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc). **57.** System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA. **58.** System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej: **58.1.** Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności **58.2.** Czy włączony jest firewall **58.3.** Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur **58.4.** Czy jest włączone szyfrowanie dysku systemowego **58.5.** Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory **58.6.** Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora **58.7.** Czy w systemie są uruchomione procesy wskazane przez administratora **58.8.** Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności **58.9.** Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: **58.9.1.** Wartości klucza rejestru **58.9.2.** Typu wartości: Number, String, Version **59.** System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej: **59.1.** Microsoft Windows **59.2.** Mac OS

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	59.3. iOS **59.4.** Android **60.** System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci). **61.** System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory. **62.** System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. **63.** System musi współpracować z serwerem tokenów.
Mechanizmy uwierzytelniania	**64.** System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. **65.** System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: **65.1.** MAC, **65.2.** PAP/ASCII, **65.3.** CHAP, **65.4.** SNMP, **65.5.** 802.1X. **66.** wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp. **67.** System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości. **68.** System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych. **69.** System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant). **70.** System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: **70.1.** Tożsamość/Urządzenie końcowe, **70.2.** Grupa tożsamości/urządzeń końcowych,

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	70.3. Parametry urządzeń końcowych, min: system operacyjny, wersja, **70.4.** Atrybuty Active Directory, **70.5.** Jednostka organizacyjna tożsamości/urządzeń końcowych, **70.6.** Urządzenia sieciowe sieci przewodowej, bezprzewodowej, **70.7.** Grupy urządzeń sieciowych, **70.8.** Porty urządzeń sieciowych, **70.9.** Grupy portów urządzeń sieciowych, **70.10.** Jednostka organizacyjna portów, **70.11.** Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID), **70.12.** Data, czas ważności polityki, **70.13.** Wewnętrzny Captive Portal, **70.14.** Metoda autoryzacji. **71.** System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks. **72.** System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC. **73.** System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI. **74.** System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli. **75.** System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV. **76.** System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV. **77.** System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach. **78.** System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	79. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC. **80.** System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC. **81.** System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www. **82.** System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników. **83.** System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.
Obsługa serwerów certyfikatów CA	**84.** System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. **85.** Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności: **85.1.** możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych. **85.2.** możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych. **85.3.** Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol). **85.4.** usługę OCSP (Online Certificate Status Protocol).
Obsługa serwerów DHCP	**86.** System musi posiadać funkcję zintegrowanego serwera DHCP. **87.** System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP. **88.** System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP: **88.1.** Uruchamianie usługi dla wybranych podsieci, **88.2.** Przypisanie ustalonego adresu IP dla adresu MAC. **88.3.** Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci, **88.4.** Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	88.5. Możliwość określania braku dostępu dla wybranych adresów MAC, **88.6.** Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC, **88.7.** Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP, **88.8.** Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego, **88.9.** Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi, **88.10.** Dokonywanie zmian bez konieczności wyłączania usług.
Obsługa serwerów TACACS+	**89.** System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych: **89.1.** System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów. **89.2.** System musi umożliwiać tworzenia haseł administratorom. **89.3.** System musi umożliwiać tworzenie listy komend uprawnień dla administratorów **89.4.** System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych. **89.5.** System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu. **89.6.** System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory. **89.7.** System musi wspierać logowanie administratorów za pomocą tokenów OTP. **89.8.** System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.
Raportowanie i monitoring	**90.** System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów: **90.1.** Monitoring autoryzacji. **90.2.** Monitoring dla zdarzeń systemowych. **90.3.** Monitoring dla zdarzeń DHCP. **90.4.** Monitoring dla tożsamości. **90.5.** Monitoring dla urządzeń końcowych. **90.6.** Monitoring dla urządzeń sieciowych.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	90.7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email. **90.8.** Raport ze zdarzeń logowania z informacją o nadam adresie IP. **90.9.** Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług. **90.10.** Raport z logów DHCP z informacją o polityce dostępu logowania do sieci. **90.11.** System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym. **90.12.** System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie. **90.13.** System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku. **90.14.** System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych. **90.15.** System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja. **90.16.** System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi. **90.17.** Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS. **90.18.** Raport zdarzeń Microsoft Active Directory, minimum: **90.18.1.** Logowania, wylogowania z system w tym błędne logowania **90.18.2.** Logowania do sieci 802.1X
Alarmy	**91.** System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: **91.1.** wiadomości e-mail, **91.2.** Syslog, **91.3.** notyfikacji systemowych.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
	92. Alarmy mogą być generowane w sytuacjach, min: **92.1.** Ilości obsługiwanych transakcji RADIUS, **92.2.** Opóźnienie obsługi transkacji RADIUS, **92.3.** Statusu krytycznego modułów. **93.** System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: **93.1.** badanie łączności IP za pomocą ping, traceroute, **93.2.** tcpdump protokołów RADIUS, TACACS+, **93.3.** wyszukiwanie zdarzeń RADIUS z uwzględnieniem: **93.3.1.** nazwy użytkownika, **93.3.2.** adresu MAC, **93.3.3.** statusu uwierzytelnienia (udana lub nieudana), **93.3.4.** powodu, jeżeli uwierzytelnienie nieudane, **93.3.5.** zakresu czasowego, co do dnia, godziny i minuty, **93.4.** wykonanie zdalnego polecenia na urządzeniu sieciowym.
Wymagania dotyczące wdrożenia i harmonogram ramowy:	**94.** Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta. **95.** Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji). **96.** Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.). **97.** Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list). **98.** Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach. **99.** Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy. **100.** Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.

KOMPONENT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE - NAC
Licencja wsparcia technicznego producenta oprogramowania:	**101.** Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – licencję na wsparcie producenta oprogramowania na okres do 30.06.2026. Licencja ta powinna obejmować minimum: **101.1.** Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC **101.2.** Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia. **101.3.** Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów. **101.4.** Dostęp do dokumentacji i instrukcji na stronie internetowej. **101.5.** Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

7. Szkolenia dla dwóch Administratorów z nowych technologii

Szkolenie 1: Urządzenie UTM wraz z licencjami i wsparciem technicznym

1. Cele szkolenia:

1.1. Przygotowanie administratora do konfiguracji, monitorowania i zarządzania urządzeniem UTM w celu ochrony infrastruktury sieciowej urzędu przed zagrożeniami.

1.2. Nabycie umiejętności wdrażania polityk bezpieczeństwa, zarządzania regułami zapory sieciowej oraz konfiguracji VPN.

2. Zakres tematyczny:

2.1. Instalacja i konfiguracja UTM:

2.1.1. Wprowadzenie do funkcji urządzenia UTM.

2.1.2. Podstawowe ustawienia sieciowe: konfiguracja adresów IP, VLAN, routing.

2.1.3. Integracja urządzenia z istniejącą infrastrukturą sieciową.

2.2. Zarządzanie regułami zapory sieciowej (Firewall):

2.2.1. Tworzenie i zarządzanie regułami filtrowania ruchu sieciowego.

2.2.2. Konfiguracja polityk bezpieczeństwa.

2.3. Monitorowanie i raportowanie:

2.3.1. Analiza logów i alertów generowanych przez system UTM.

2.3.2. Generowanie raportów bezpieczeństwa.

2.4. VPN:

2.4.1. Konfiguracja tuneli IPSec VPN i SSL VPN.

2.4.2. Zarządzanie dostępem zdalnym.

2.5. Aktualizacje i wsparcie techniczne:

2.5.1. Zarządzanie aktualizacjami systemu.

2.5.2. Współpraca z dostawcą w zakresie wsparcia technicznego.

3. Forma realizacji:

3.1. Czas trwania: 16 godzin (8 godzin teoretycznych + 8 godzin warsztatowych).

3.2. Forma: Stacjonarne lub zdalne warsztaty z ćwiczeniami praktycznymi.

3.3. Materiały: Dostęp do dokumentacji technicznej oraz ćwiczeń praktycznych.

Szkolenie 2: System ochrony przed wyciekiem danych (DLP)

1. Cele szkolenia:

1.1. Przygotowanie administratora do efektywnej ochrony danych urzędu przed nieautoryzowanym dostępem i wyciekiem.

1.2. Nabycie umiejętności wdrażania i monitorowania polityk ochrony danych.

2. Zakres tematyczny:

2.1. Wprowadzenie do systemu DLP:

2.1.1. Kluczowe funkcje i zastosowanie.

2.1.2. Przegląd dostępnych narzędzi i technologii.

2.2. Konfiguracja polityk ochrony danych:

2.2.1. Tworzenie reguł monitorowania i zapobiegania wyciekom danych.

2.2.2. Definiowanie wyjątków i polityk dla poszczególnych działów urzędu.

2.3. Monitorowanie aktywności:

2.3.1. Analiza zdarzeń i incydentów.

2.3.2. Zarządzanie alertami i raportami.

2.4. Zarządzanie użytkownikami:

2.4.1. Kontrola dostępu do danych wrażliwych.

2.4.2. Uwierzytelnianie i autoryzacja.

2.5. Reagowanie na incydenty:

2.5.1. Procedury postępowania w przypadku wykrycia naruszenia.

2.5.2. Tworzenie kopii zapasowych i odzyskiwanie danych.

3. Forma realizacji:

3.1.1. Czas trwania: 12 godzin (6 godzin teoretycznych + 6 godzin praktycznych).

3.1.2. Forma: Stacjonarne lub zdalne warsztaty z ćwiczeniami praktycznymi.

3.1.3. Materiały: Przewodniki użytkownika oraz scenariusze testowe.

Szkolenie 3: System kontroli dostępu do sieci (NAC)

1. Cele szkolenia:

1.1. Wyposażenie administratora w wiedzę i umiejętności niezbędne do skutecznego zarządzania dostępem użytkowników do sieci.

1.2. Wdrażanie polityk bezpieczeństwa zgodnie z zasadą minimalnego dostępu.

2. Zakres tematyczny:

2.1. Podstawy NAC:

2.1.1. Omówienie funkcji i korzyści.

2.1.2. Architektura systemu kontroli dostępu.

2.2. Konfiguracja polityk dostępu:

2.2.1. Tworzenie reguł kontroli urządzeń i użytkowników.

2.2.2. Definiowanie poziomów dostępu do zasobów sieciowych.

2.3. Integracja z infrastrukturą:

2.3.1. Powiązanie NAC z istniejącymi rozwiązaniami (np. Active Directory).

2.3.2. Zarządzanie urządzeniami w sieci.

2.4. Monitorowanie i analiza:

2.4.1. Śledzenie aktywności użytkowników.

2.4.2. Generowanie raportów zgodności.

2.5. Reagowanie na naruszenia:

2.5.1. Automatyczne izolowanie zagrożeń.

2.5.2. Procedury eskalacji i rozwiązywania incydentów.

3. Forma realizacji:

3.2. Czas trwania: 14 godzin (7 godzin teoretycznych + 7 godzin warsztatowych).

3.3. Forma: Stacjonarne lub zdalne warsztaty z ćwiczeniami praktycznymi.

3.4. Materiały: Dokumentacja techniczna oraz przykładowe scenariusze wdrożeniowe.