ZI.272.21.2025
ZAŁĄCZNIK NR 1

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ):

ZAKUP I DOSTAWA SIECIOWYCH PRZEŁĄCZNIKÓW ZARZĄDZALNYCH Z SYSTEMEM NAC DLA SYSTEMÓW BACKUPOWYCH.

W ramach realizacji przedmiotu zamówienia Zamawiający wymaga zachowania pełnej kompatybilności z już posiadaną przez Zamawiającego infrastrukturą informatyczną oraz oprogramowaniem i nie może w żadnym stopniu ograniczać jej funkcjonalności. Elementy, których to dotyczy, pracować będą w środowisku opartym o posiadane przez Zamawiającego kontrolery domeny Active Directory (pracujący na poziomie funkcjonalności Microsoft Windows Server 2016 R2).
Każdorazowo, gdy Zamawiający powołuje się w specyfikacji na konkretną nazwę rozwiązania, należy interpretować, iż jest przykładem spełniającym minimalne wymagania techniczne, zarówno wydajnościowe, jak i jakościowe określone przez Zamawiającego, co nie oznacza, że wskazany przykład ogranicza możliwość składania ofert równoważnych (chyba, że Zamawiający w dokumentacji jawnie wskazuje inaczej, np.: w przypadku rozbudowy elementów już posiadanych). Ofertą równoważną jest element o takich samych lub lepszych parametrach technicznych, jakościowych, funkcjonalnych, spełniający ponadto wszystkie minimalne wymagania określone przez Zamawiającego. Zamawiający zastrzega jednak możliwość niedopuszczenia rozwiązań równoważnych, wszędzie tam, gdzie ze względu na kompatybilność technologii z rozwiązaniami już posiadanymi, mogłoby w jakimkolwiek stopniu ograniczyć funkcjonalność rozwiązań, czy narazić go na jakiekolwiek dodatkowe koszty, np.: koszty modernizacji, integracji czy koszty szkolenia.

Warunki wymagane do spełnienia przez Wykonawcę zamówienia:
1. Cena dotyczy przedmiotu opisanego w Szczegółowym Opisie Przedmiotu Zamówienia.
2. Wykonawca dostarczy wszystkie elementy przedmiotu zamówienia do Urzędu Miejskiego w Wołominie.
3. Wykonawca zobowiązany jest do:
- dostawy elementów wraz niezbędnymi licencjami, oprogramowaniem oraz z pełnym zestawem okablowania i akcesoriów dołączanych przez producenta oraz dodawanych przez Wykonawcę, niezbędnym do w pełni funkcjonalnej pracy;
- dostawy w przypadku elementów powtarzalnych, identycznych modeli w identycznej konfiguracji;

- dostawy sprzętu o nienaruszonych plombach gwarancyjnych podzespołów bazowych;
- pokrycia wszelkich kosztów załadunku, transportu, rozładunku oraz dostarczenia do wskazanego pomieszczenia zlokalizowanego w siedzibie Zamawiającego;

4. Wykonawca oświadcza, że oferowany towar jest nowy (rok produkcji najwcześniej - 2024), nieużywany, nieuszkodzony, nieobciążony prawami osób trzecich oraz spełnia normy bezpieczeństwa. Towar, będący przedmiotem umowy, nie jest również refabrykowany, recertyfikowany, poleasingowy, a każdy oferowany element danej pozycji jest jednakowego producenta, modelu i specyfikacji.
5. Wykonawca oświadcza, że oferowane elementy zamówienia poprawnie ze sobą współpracują i w połączeniu ze sobą tworzą oczekiwane rozwiązanie: stos 4szt. połączonych ze sobą zarządzalnych sieciowych przełączników z systemem NAC.
6. Wykonawca udziela gwarancji oraz zobowiązuje się do prowadzenia bezpłatnego serwisu gwarancyjnego w miejscu użytkowania, w okresie trwania gwarancji nie krótszym niż wskazany przez Zamawiającego w opisie przedmiotu zamówienia. Jednocześnie Wykonawca oświadcza, że sprzęt będzie serwisowany przez producenta lub firmę serwisującą - posiadającą certyfikaty serii ISO 9001:2008, ISO 22301 i ISO 27001 na świadczenie usług serwisowych oraz autoryzację producenta sprzętu.
7. Wykonawca oświadcza, że oferowany sprzęt pochodzi z oficjalnej, polskiej dystrybucji.
8. Wykonawca potwierdza, że oferowany sprzęt jest zgodny ze wskazanymi w OPZ obowiązującymi Polskimi Normami i Standardami, posiada deklarację zgodności CE oraz spełnia kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii europejskiej o eliminacji substancji niebezpiecznych.
9. Wykonawca oświadcza, że po trzech nieskutecznych naprawach (lub w przypadku braku możliwości naprawy) dokona wymiany sprzętu na nowy egzemplarz wolny od wad.
10. W przypadku jakichkolwiek wątpliwości, umożliwienia Zamawiającemu wykonania przed podpisaniem protokołu odbioru (w terminie nie dłuższym niż 3 dni od dostawy), testów zgodności dostarczanego przez Wykonawcę sprzętu z oprogramowaniem użytkowanym przez Zamawiającego oraz wymiany sprzętu w przypadku, gdy nie przejdzie on powyższych testów.

Zamawiający informuje, że:

1. Może żądać od Wykonawcy przedstawienia dodatkowych dokumentów potwierdzających spełnienie wymagań w Szczegółowym Opisie Przedmiotu Zamówienia dla oferowanego sprzętu.
2. Warunkiem złożenia oferty jest zapoznanie się z wymaganiami postępowania wraz z załącznikami i ich akceptacja.
3. W przypadku obiektywnej niemożliwości dostarczenia przez Wykonawcę towaru wskazanego w ofercie z powodu braku jego dostępności na rynku, potwierdzonej przez producenta, dopuszczalne jest dostarczenie przez Wykonawcę towaru o parametrach technicznych nie gorszych i cenie nie wyższej niż wynikającej z oferty. Zamiana zaoferowanego towaru wymaga zgody Zamawiającego.

W ramach zamówienia zostaną zakupione i dostarczone następujące elementy zamówienia w określonych ilościach, zgodne z poniższymi wymaganiami specyfikacji technicznej oferowanego towaru:

1.	**[4 szt.]**	**Sieciowy przełącznik zarządzalny ExtremeSwitching 5320 48x10/100/1000BASET FDX/HDX 8x10G unpopulated SFP+ MACSec capable 1x internal fixed PSU wraz z licencją MACsec - *lub równoważny***
Nazwa elementu, parametru lub cechy		Wymagania
Właściwości podstawowe:		- Przełącznik do sieci LAN w metalowej obudowie; - Wysokość urządzenia 1U - montaż w standardowej szafie 19"; - Głębokość urządzenia nie większa niż 35 cm; - Przełącznik musi posiadać wbudowany zasilacz AC 230V; - Przełącznik wyposażony w min.: 48 portów 10/100/1000BASE-T i 8 portów SFP+ 1/10G; - Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex; - Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet; - Przełącznik musi wspierać obsługę diagnostyki wkładek SFP/SFP+; - Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów; - Przełącznik musi posiadać możliwość łączenia do 8 przełączników w stos; - Przepustowość stosu min. 40 Gb/s; - Możliwość budowy stosu za pomocą portów 10G SFP+; - Stos musi zachowywać się jako jedno urządzenie logiczne, a w szczególności musi mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem; - Nieblokująca architektura o wydajności przełączania min. 256 Gb/s; - Szybkość przełączania: 190.5 Mp/s; - Pamięć operacyjna: min. 1 GB pamięci DRAM; - Pamięć flash: min. 1 GB pamięci Flash; - Dedykowany port konsoli szeregowej RS-232 (RJ45);

	- Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika; - Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora; - Możliwość instalacji min. dwóch wersji oprogramowania – firmware; - Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash; - Możliwość monitorowania zajętości CPU; - Możliwość monitorowania zajętości pamięci; - Zabezpieczenie przełącznika przed atakami DoS, Network Ingress Filtering RFC 2267, SYN Attack Protection, Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania; -Wsparcie mirroringu ruchu: Lokalny mirroring na przełączniku, zdalny mirroring, zdalny mirroring do wskazanego adresu IP poprzez tunel - np. GRE, możliwość mirroringu ruchu wybranego za pomocą listy kontroli dostępu ACL – ingress.
Funkcje L2 przełącznika:	- Tablica MAC adresów min. 32 tys.; - Obsługa sieci wirtualnych IEEE 802.1Q - min. 4 tys.; - Obsługa przypisywania ruchu do VLAN na podstawie typu protokołu lub rodzaju enkapsulacji; - Obsługa sieci wirtualnych bazujących na MAC adresach; - Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieciowych; - Obsługa Q-in-Q IEEE 802.1ad; - Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów); - Obsługa STP (Spanning Tree Protocol) IEEE 802.1D; - Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w; - Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s; - Obsługa PVST+ (Per-VLAN Spanning Tree Protocol); - Obsługa min. 64 instancji MSTP; - Obsługa Link Aggregation IEEE 802.3ad wraz z LACP: obsługa min. 128 grup łączy typu Link Aggregation, obsługa umożliwiająca zgrupowanie min. 8 portów;

	- Obsługa MLAG (Multi Chassis Link Aggregation); - Przełącznik musi posiadać funkcję umożliwiającą statyczne skonfigurowanie portu głównego zapasowego. W stanie normalnym, bez awarii, jest używany port główny, port zapasowy jest nieaktywny. Gdy port wskazany jako główny ulegnie awarii, czyli wykryje brak połączenia (link down), to port zapasowy się automatycznie aktywuje; - Obsługa protokołu EAPS - RFC 3619; - Obsługa protokołu ERPS / G.8032; - Obsługa Quality of Service: Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p, Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym, Obsługa kolejek Strict Priority, Obsługa kolejek Weighted Round Robin, Obsługa WRED (Weighted Random Early Detection); - Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB; - Obsługa LLDP Media Endpoint Discovery (LLDP-MED); - Obsługa CDPv1 oraz CDPv2; - Przełącznik musi posiadać obsługę AVB (Audio Video Bridging); - Przełącznik musi wspierać Voice VLAN: bazujący na LLDP, bazujący na adresie OUI; - Kontrola sztormów: Możliwość ograniczenia liczby pakietów Multicast na porcie, Możliwość ograniczenia liczby pakietów Broadcast na porcie, Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie; - Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami innymi niż STP.
Funkcje L3 przełącznika IPv4	- Obsługa min. 1500 interfejsów IP; - Wsparcie dla IP multinetting - wiele adresów przypisanych do jednej sieci VLAN; - Sprzętowa obsługa routingu IPv4; - Pojemność sprzętowej tabeli routingu min. 12 tys. Wpisów; - Obsługa routingu statycznego IPv4; - Obsługa routingu dynamicznego IPv4: RIP v1/v2, OSPFv2 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję, BGPv4 min. 2 sąsiadów - możliwość rozszerzenia do pełnej funkcjonalności przez licencję, ISIS - możliwość rozszerzenia przez licencję;

	- Obsługa redundancji routingu VRRP dla IPv4; - Policy Based Routing dla IPv4; - Obsługa DHCP Relay ; - Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów; - Obsługa Opcji 82 dla DHCP.
Funkcje L3 przełącznika IPv6	- Sprzętowa obsługa routingu IPv6; - Pojemność tabeli routingu min. 6 tys. wpisów; - Obsługa routingu statycznego IPv6; - Obsługa routingu dynamicznego IPv6: RIPng, OSPFv3 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję, BGPv4 min. 2 sąsiadów - możliwość rozszerzenia do pełnej funkcjonalności przez licencję, ISIS - możliwość rozszerzenia przez licencję; - Obsługa redundancji routingu VRRP dla IPv6; - Policy Based Routing dla IPv6; - Obsługa 6to4 (RFC 3056); - Opcja IPv6 Router Advertisement dla DNS - RFC 6106.
Obsługa ruchu rozgłoszeniowego	- Statyczne przyłączania portu do grupy multicast; - Filtrowanie IGMP; - Obsługa IGMP v1 - RFC 1112; - Obsługa IGMP v2 - RFC 2236; - Obsługa IGMP v3 - RFC 3376; - Obsługa IGMP v1/v2/v3 snooping; - Obsługa PIM-SM; - Obsługa PIM-DM - możliwość rozszerzenia przez licencję; - Obsługa PIM-SSM - możliwość rozszerzenia przez licencję; - Obsługa MLDv1 snooping; - Obsługa MLDv2 snooping; - Obsługa MVR (Multicast VLAN Registration).

Funkcje bezpieczeństwa	- Obsługa logowania do sieci Network Login: IEEE 802.1x based Network Login, MAC address based Network Login, Web based Network Login; - Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants); - Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation; - Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x; - Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication; - Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink; - Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na portach dołączonych do przełączników obsługujących IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging; - Automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA; - Automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA; - Przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów; - Obsługa Guest VLAN dla IEEE 802.1x; - Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci - Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176; - Obsługa wymuszania ponownego periodycznego uwierzytelnienie (Reauthentication);

	- Obsługa RADIUS Authentication (RFC 2865); - Obsługa RADIUS Accounting (RFC 2866); - Obsługa RADIUS Authentication over TLS (RadSec); - Obsługa RADIUS Accounting over TLS (RadSec); - Obsługa TACACS+ (RFC 1492); - Bezpieczeństwo MAC adresów: ograniczenie liczby MAC adresów na porcie, zatrzaśnięcie MAC adresów na porcie, możliwość wpisania statycznych MAC adresów na port/vlan; - Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning); - Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4: Adres MAC źródłowy i docelowy plus maska, Adres IP źródłowy i docelowy plus maska dla IPv4, Adres IP źródłowy i docelowy plus maska dla IPv6, Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.., Numery portów źródłowych i docelowych TCP, UDP, Zakresy portów źródłowych i docelowych TCP, UDP, Identyfikator sieci VLAN - VLAN ID, Quality of Service IEEE 802.1p, Quality of Service DiffServ/DSCP, Flagi TCP , Obsługa fragmentów; - Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika; - Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI; - Wsparcie 8 tys. wpisów ACL na wejściu (Ingress); - Wsparcie 1 tys. wpisów ACL na wyjściu (Egress); - Obsługa IP Security: Trused DHCP Server, DHCP Snooping and Guard, Gratuitous ARP Protection, DHCP Secured ARP/ARP Validation, IP Source Guard; - Ograniczenie przepustowości (rate limiting) na portach wyjściowych; - Ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL; - Obsługa wykrywania periodycznego zaniku linku (Port-Flap): możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu, możliwość automatycznej reakcji polegającej na wyłączeniu portu, możliwość automatycznej reakcji polegającej na wyłączeniu portu na wskazany czas,

	możliwość raportowania zdarzenia poprzez Syslog, możliwość raportowania zdarzenia poprzez Trap SNMP; - Wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-128; - Wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-256; - Minimalna wydajność szyfracji MACSec na przełączniku: 25 Gb/s;
Zarządzanie	- Zarządzenia przez SNMP v1/v2/v3; - Obsługa SNMP Traps; - Obsługa synchronizacji czasu SNTP lub NTP; - Obsługa DNS klienta; - Zarządzanie przez przeglądarkę www - protokół http i https; - Możliwość zarządzania przez protokół XML; - Obsługa serwera SSH dla IPv4; - Obsługa serwera SSH dla IPv6; - Obsługa klienta SSH dla IPv4; - Obsługa klienta SSH dla IPv6; - Obsługa serwera Telnet dla IPv4; - Obsługa serwera Telnet dla IPv6; - Obsługa klienta Telnet dla IPv4; - Obsługa klienta Telnet dla IPv6; - Obsługa transferu plików: TFTP, SFTP, SCP; - Obsługa SYSLOG; - Obsługa Secure SYSLOG (TLS); - Obsługa SYSLOG - konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń; - Obsługa logowania komend CLI do logu systemowego; - Obsługa logowania komend do serwera SYSLOG; - Obsługa ping dla IPv4 i IPv6;

	- Obsługa traceroute dla IPv4 i IPv6; - Obsługa RMON min. 4 grupy: Status, History, Alarms, Events ; - Obsługa RMON2;
Inne	- Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników; - Wbudowany DHCP Server; - DHCP Server z możliwość definicji opcji (np. opcje 43, 60, 78 itp.); - Wbudowany DHCP Client - per VLAN; - Obsługa skryptów CLI; - Obsługa funkcji TCL/Tk w skryptach CLI; - Obsługa skryptów Python 3.x; - Możliwość uruchamiania skryptów: ręcznie z CLI przez administratora, o określonym czasie lub co wskazany czas, na podstawie zdarzeń z logu systemowego; - Możliwość edycji skryptów bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych; - Wsparcie standardu IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging.
Zgodność z normami	- EU RoHS - 2011/65/EU; - EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage; - EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation; - EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational.
Gwarancja	- Dożywotnia gwarancja na sprzęt - min. 5 lat po zakończeniu sprzedaży; - Dożywotnia aktualizacja oprogramowania na przełączniku - min. 2 lata po zakończeniu sprzedaży; - Wsparcie typu NBD na pierwszy rok – wysyłka nowego urządzenia tego samego dnia po potwierdzeniu awarii przez producenta do godz. 14:00 oraz pełne wsparcie techniczne dla wszystkich funkcji oferowanych przez przełącznik (w tym MACSEC).

Koniec tabeli.

2.	**[4 szt.]**	**Przewód DAC 10 Gb SFP+ 1m**
Nazwa elementu, parametru lub cechy		Wymagania
Wymagania techniczne		Wszystkie kable i wkładki dostarczone w ramach postępowania muszą pochodzić od tego samego producenta co zaoferowane przełączniki.

Koniec tabeli.

3.	**[4 szt.]**	**Wkładka optyczna 10 Gb SFP+ 850nm SR**
Nazwa elementu, parametru lub cechy		Wymagania
Wymagania techniczne		Wszystkie kable i wkładki dostarczone w ramach postępowania muszą pochodzić od tego samego producenta co zaoferowane przełączniki.

Koniec tabeli.

4.	**[1 szt.]**	**Oprogramowanie zarządzające - System zarządzania i kontroli dostępu** **ExtremeNAC SW subscription for 1,000 end-systems for 1 Year PartnerWorks Plus** ***- lub równoważne***
Nazwa elementu, parametru lub cechy		Wymagania
Wymagania techniczne		- Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci a) Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare; b) Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS;

	- Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli; - Aplikacja zarządzająca musi zarządzać wszystkimi dostarczonymi przełącznikami; - Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników; - Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius; - Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze; - Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES; - Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu; - Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów; - Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów; - Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II; - Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych; - Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email’a, wysłanie trapu SNMP, wpisu do Syslog’a lub uruchomienie skryptu; - Aplikacja musi posiadać wbudowany Syslog serwer; - Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps; - Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych;

	- Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia; - Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak: a) Wysłanie e-mail do wskazanej grupy adresowej; b) Wysłanie informacji SYSLOG do wskazanego serwera; c) Wysłanie TRAP SNMP do wskazanego adresu IP; d) Uruchomienie skryptu w systemie operacyjnym Linux; e) Uruchomienie skryptu skonfigurowanego w systemie zarządzającym. - Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera; - Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora; - Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach; - Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem: a) połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu; b) konfiguracji sieci VLAN. - Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https; - Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane: a) adres IP urządzenia; b) adresu MAC urządzenia; c) nazwy urządzenia; d) wersji oprogramowania; e) wersji bootrom; f) lokalizacji urządzenia; g) danych kontaktowych administratora;

	h) numeru seryjnego; i) numeru inwentaryzacyjnego – własna numeracja. - Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest: a) możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie; b) możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych; c) możliwość odtworzenia wskazanej konfiguracji urządzenia ; d) możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami; e) możliwość obsługi backup'u urządzeń sieciowych różnych producentów. - Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie; - Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach; - Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych; - Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. : Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.; - Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem: a) przyłączenia do sieci VLAN; b) przyłączenia do serwisu w ramach „Fabric" z wykorzystaniem IEEE 802.1Qcj; c) konfiguracji Quality of Service; d) konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4;

	e) możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej. - Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać: a) szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy); b) wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne); c) wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.; d) generowanie raportów. - Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową. a) Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa); b) Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax; c) Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje: • adres IP kontrolera; • liczba obsługiwanych klientów; • szczytowe wartości zajmowanego pasma; • wersja oprogramowania.

	d) Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje: • adres IP punktu dostępowego; • MAC adres punktu dostępowego; • wersja oprogramowania; • typ punktu dostępowego; • kanały pracy poszczególnych interfejsów radiowych; • szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych. e) Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje: • adres IP klienta; • MAC adres klienta; • nazwa użytkownika; • nazwa punktu dostępowego, do którego dołączony jest użytkownik; • BSSID, do którego dołączony jest użytkownik; • SSID, do którego dołączony jest użytkownik. f) Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności: • zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate); • zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem; • lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych. - System zarządzania musi przy współpracy z dostarczonymi urządzeniami pozwalać na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej; - Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji;

	- Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji; - System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos; - System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji; - Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji; - System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.; - System Analityki musi zapewniać możliwość tworzenia raportów; - System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail; - System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością; - System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora); - System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie; - System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu; - System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki

	- System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów: a) Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall, np. Palo Alto, Fortinet, Checkpoint b) Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny c) Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – np. Microsoft Intune, AirWatch MDM - W momencie dostawy system zarządzania musi obsługiwać min. 5 urządzeń sieciowych; - W przypadku, jeżeli wymienione funkcjonalności ograniczone są subskrypcją czasową, należy dostarczyć taką subskrypcję na okres min. 1 rok; - Wszystkie dostarczone systemy muszą być objęte kontraktem serwisowym producenta na okres min. 1 rok; - Aplikacja zarządzająca musi mieć możliwość integracji z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji: a) adresu MAC; b) adresu IP; c) nazwy komputera; d) typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.; e) nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika; f) adres IP urządzenia, do którego dołączony jest klient; g) identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego;

	h) typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.; i) nazwa przydzielonej polityki bezpieczeństwa. - System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.; - System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa; - System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie: a) Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp. b) Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika; c) Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC; d) Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp. ; e) Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia. - System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.;

	- Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń; - System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci; - System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS; - System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.; - System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy; - System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa. - System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające: a) liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.; b) liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.; c) liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android d) liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa; e) liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.. -System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication;

	- System zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 1 000 urządzeń klienckich (adresów MAC) przez okres minimum 1 roku.

Koniec tabeli.

5.	**[1 szt.]**	**Usługi wdrożenia i wsparcia technicznego** **wraz 8 licencjami ExtremeCloud IQ Pilot SaaS Subscription and PWP SaaS Support** **for one (1) device (1 year)** **dla każdego z przełączników** **oraz każdego z 5 administratorów** ***- lub równoważne***
Nazwa elementu, parametru lub cechy		Wymagania
Wymagania techniczne:		W ramach dostawy należy zapewnić wdrożenie wykonane przez inżyniera posiadającego aktualny certyfikat techniczny wystawiony przez producenta zaoferowanych systemów na poziomie Professional dla przełączników sieciowych oraz systemu zarządzania. W ramach wdrożenia należy skonfigurować połączenia pomiędzy przełącznikami, zainstalować i skonfigurować oprogramowanie zarządzające, utworzyć polityki dostępowe w systemie kontroli dostępu, zintegrować system z urządzeniami firewall Zamawiającego. Zamawiający posiada obecnie urządzenia FortiGate i wymaga, aby inżynier realizujący integracje posiadał certyfikat Fortinet FCX. Po zakończeniu wdrożenia należy przez okres roku świadczyć wsparcie techniczne w języku polskim. W tym celu Zamawiający wymaga, aby Wykonawca posiadał co najmniej dwóch inżynierów na poziomie Professional z zakresu zaoferowanych przełączników sieciowych oraz systemu zarządzania, a całość systemu wsparcia Wykonawcy musi być certyfikowana na zgodność z normami ISO9001, ISO22301, ISO27001.

Koniec tabeli.

4. Dopuszcza się zaoferowanie produktów równoważnych do towaru określonego powyżej. Równoważność dotyczy zakupu wszystkich elementów. Równoważność oznacza, że zaoferowane elementy muszą zapewniać co najmniej pełną oczekiwaną funkcjonalność wskazaną przez Zamawiającego, w stosunku do towaru, dla którego jest wskazywany przez Wykonawcę jako równoważny i posiadać nie gorsze parametry techniczne.

5. W przypadku zaoferowania towaru równoważnego Wykonawca zobowiązany jest w ofercie udowodnić, że funkcjonalność oferowanego towaru jest równoważna w stosunku do towaru wskazanego w OPZ przez Zamawiającego, jak również, że równoważny towar posiada nie gorsze parametry techniczne.

6. Zamawiający informuje, że w przypadku, gdy określił w OPZ wymagania przez wskazanie znaków towarowych, patentów, pochodzenia, norm, aprobat, specyfikacji technicznych lub systemów odniesienia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, to należy traktować takie określenie jako przykładowe. W każdym takim przypadku Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych o parametrach nie gorszych niż posiadane przez wskazane usługi, materiały, urządzenia, oprogramowanie, itp.