Przedmiot **ZADANIA NR 1** stanowi dostawa 2 szt. przełączników sieciowych szkieletowych wraz z elementami wymaganymi do wdrożenia, 30 szt. przełączników sieciowych dostępowych wraz z elementami wymaganymi do wdrożenia oraz aplikacji/oprogramowania do zarządzania ww. przełącznikami. Wykonawca w terminie określonym ofertą nie krótszym niż 20 dni i nie dłuższym niż 60 dni od dnia zawarcia umowy dostarczy, zainstaluje oraz skonfiguruje wszystkie elementy dostawy zgodnie z zaleceniami zamawiającego w miejscu wskazanym w jego siedzibie.
Przełączniki sieciowe są objęte gwarancją wykonawcy przez minimum 36 miesięcy, polegającą na naprawie lub wymianie urządzenia w przypadku jego wadliwości, na warunkach określonych w umowie. W ramach serwisu gwarancyjnego producent zapewnia również dostęp do aktualizacji oprogramowania, bazy wiedzy, dokumentacji technicznej oraz wsparcie techniczne.
Dodatkowo, przełączniki są objęte serwisem gwarancyjnym producenta w trybie NBD przez 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w NBD od momentu potwierdzenia zasadności zgłoszenia. Zamawiający wymaga, aby wykonawca świadczył pierwszą linię wsparcia w okresie ww. gwarancji na przełączniki oraz 12-miesięcznej licencji na oprogramowanie do zarządzania dostarczonymi przełącznikami sieciowymi. Zamawiający nie wymaga świadczenia przez producenta lub wykonawcę wsparcia technicznego dla przełączników po wygaśnięciu rocznego serwisu NBD, jednak przez pozostały dwuletni okres gwarancji wymagane jest, aby wykonawca nadal pośredniczył w realizacji awarii sprzętowych wymaganych w ramach gwarancji.
Jeżeli producent zaoferowanego sprzętu posiada certyfikację serwisową dla realizacji takiego wymogu to wykonawca musi w pełni dysponować ww. certyfikacją.
Wykonawca zapewnia pierwszą linię wsparcia w języku polskim w godzinach pracy zamawiającego. W tym celu wykonawca dysponuje co najmniej dwoma osobami z aktualnym certyfikatem technicznym oferowanego rozwiązania, które skieruje do realizacji usług. Wykonawca posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.
Najpóźniej przed zawarciem umowy wykonawca przekaże zamawiającemu dokumenty potwierdzające zgodność dostarczonych przełączników sieciowych z opisem przedmiotu zamówienia, certyfikat ISO 9001 dot. świadczenia usług serwisowych, dokumenty licencyjne, a także instrukcje instalacji urządzeń i oprogramowania lub wskaże portal producenta, na którym można pobrać/zweryfikować te informacje.

Przełącznik sieciowy szkieletowy – 2 szt. identyczne

poz.	wymagane funkcje i parametry
1.	Minimum 48 portów SFP28 umożliwiających obsługę prędkości 1/10/25Gb/s
2.	Minimum 8 portów QSFP28 40/100Gb/s
3.	Wysokość urządzenia 1RU
4.	Dedykowany port do zarządzania przełącznikiem „poza pasmem”
5.	Dedykowany port konsoli szeregowej RJ45
6.	Nieblokująca architektura wyposażona w chipset o przepustowości min. 4 Tb/s
7.	Prędkość przełączania pakietów min. 1000 Mpp/s
8.	Przełącznik w chwili dostawy jest wyposażony w dwa zasilacze AC, które umożliwiają realizację redundancji zasilania z możliwością ich wymiany w czasie pracy przełącznika, który również umożliwia ich bezproblemową wymianę na zasilane prądem stałym DC. Urządzenie ma możliwość zastosowania jednocześnie jednego zasilacza AC i jednego DC
9.	Przełącznik jest wyposażony w redundantny system wentylacji z chłodzeniem przód-tył z możliwością adopcji do systemu chłodzenia tył-przód w zależności od potrzeb
10.	Przełącznik ma możliwość pracy w trybie tradycyjnym, czyli przełączanym/routowanym, ale również z wykorzystaniem technologii Fabric (wirtualizacja usług warstwy drugiej i trzeciej wraz z obsługą multicast)
11.	Tablica MAC adresów min. 160 tys. wpisów
12.	Pamięć operacyjna: min. 16 GB pamięci DRAM
13.	Pamięć: min. 128 GB pamięci SSD
14.	Bufor pakietów: minimum 32MB
15.	Obsługa IEEE 802.1Q oraz min. 4 tys. aktywnych sieci VLAN
16.	Wsparcie dla ramek Jumbo Frame 9600 bajtów
17.	Wsparcie protokołów STP, RSTP oraz MSTP
18.	Wsparcie dla min. 12 instancji MSTP – IEEE 802.1s
19.	Wsparcie dla obsługi MLAG (Multi Chassis Link Aggregation) – możliwość dołączenia innych przełączników lub urządzeń z wykorzystaniem standardowego połączenia Link Aggregation IEEE 802.3ad do dwóch różnych przełączników obsługujących MLAG
20.	Możliwość „wirtualizacji” połączenia kontrolnego dla MLAG w ramach rozwiązania Fabric
21.	Obsługa min. 125 grup łączy typu Link Aggregation.
22.	Obsługa Link Aggregation umożliwiająca zgrupowanie min. 8 portów w jednym łączu
23.	Obsługa Link Aggregation wraz z obsługą LACP zgodna z IEEE 802.1AX
24.	Obsługa min. 60 tys. wpisów w tablicy ARP
25.	Możliwość konfiguracji statycznych wpisów ARP

26.	Obsługa protokołów routingu
27.	RIPv2 oraz RIPng
28.	OSPFv2 oraz OSPFv3
29.	Obsługa min. 1000 interfejsów IP dla IPv4 oraz IPv6
30.	Sprzętowa tablica routingu o pojemności min. 24 tys. wpisów dla IPv4 oraz 12 tys. wpisów dla IPv6
31.	Obsługa balansowania ruchu ECMP
32.	Obsługa redundancji routingu VRRPv3 dla IPv4 oraz IPv6 – min. 500 instancji
33.	Obsługa UDP Forwarding / Obsługa DHCP Relay dla IPv4 oraz IPv6
34.	Obsługa IGMPv1, IGMPv2 oraz IGMPv3
35.	Obsługa IGMP Snooping
36.	Obsługa min. 4000 interfejsów IGMP
37.	Wsparcie multicast w rozwiązaniu Fabric
38.	Obsługa DHCP snooping
39.	Obsługa Dynamic ARP Inspection
40.	Obsługa MAC Security
41.	Obsługa uwierzytelniania IEEE 802.1x
42.	Obsługa uwierzytelniania MAC
43.	Wsparcie dla standardu IEEE 802.1aq / RFC 6329 Shortest Path Bridging
44.	Wsparcie dla standardu IEEE 802.1ah Provider Backbone Bridging
45.	Wsparcie dla standardu IEEE 802.1ag Connectivity Fault Management
46.	Obsługa wielu IS-IS Area dla zwiększenia skalowalności
47.	Wsparcie mechanizmu kontroli usług pomiędzy różnymi IS-IS Area – przepuszczania lub blokowanie wskazanych serwisów L2 i L3 pomiędzy różnymi obszarami sieci
48.	Wbudowane mechanizmy automatycznej konfiguracji Fabric – tworzenie nowej konfiguracji jak i dodawanie kolejnych urządzeń do Fabric
49.	Obsługa min. 80 tys. MAC w ramach szkieletu Fabric
50.	Obsługa min. 500 urządzeń w ramach Fabric
51.	Obsługa min. 4000 serwisów L2 w ramach Fabric
52.	Obsługa min. 2000 serwisów L2 z aktywną obsługą multicast
53.	Obsługa min. 256 serwisów L3 z aktywną obsługą multicast
54.	Obsługa 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
55.	Wsparcie Remote Mirroring w ramach Fabric
56.	Wsparcie mechanizmów rozszerzenia sieci Fabric na inne lokalizacje poprzez dostępną sieć IP
57.	Obsługa technologii anycast routing w trybie Fabric
58.	Sprzętowo wspomagana obsługa IPFIX w z prędkością łącza (ang. line-rate)
59.	Obsługa wykrywania aplikacji działających w sieci na warstwie 7 modelu OSI wraz z systemem analizy ruchu
60.	Obsługa sFlow
61.	Wsparcie zarządzania poprzez protokół SNMPv3
62.	Obsługa SSHv2
63.	Obsługa NTPv4
64.	Zarządzanie poprzez przeglądarkę www i protokół HTTPS
65.	Obsługa LLDP oraz LLDP-MED – IEEE 802.1AB
66.	Obsługa RADIUS
67.	Obsługa TACACS+
68.	Obsługa SYSLOG
69.	Możliwość uruchomienia na przełączniku dodatkowych maszyn wirtualnych - jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji zamawiający nie wymaga ich dostarczenia w ramach tego zamówienia

Przełącznik sieciowy dostępowy – 30 szt. identycznych

poz.	wymagane funkcje i parametry
1.	Przełącznik do sieci LAN w metalowej obudowie
2.	Wysokość urządzenia 1U - montaż w standardowej szafie 19”
3.	Przełącznik posiada dwa zasilacze AC 230V
4.	Minimum 48 portów PoE+ 10/100/1000BASE-T
5.	Minimum 4 porty SFP+ 1/10G
6.	Porty 10/100/1000BASE-T pracują w trybie Full/Half Duplex
7.	Przełącznik wspiera IEEE 802.3az Energy Efficient Ethernet
8.	Przełącznik wspiera obsługę diagnostyki wkładek SFP/SFP+
9.	Wszystkie porty są aktywne i zgodne z wymaganiami co do prędkości i liczby portów
10.	PoE+ zgodne ze standardem IEEE 802.3at

11.	Budżet mocy dla zasilania PoE: przy jednym zasilaczu nie mniejszy niż 740 W przy dwóch zasilaczach nie mniejszy niż 1480 W
12.	Możliwość ustawiania priorytetów wyłączenia PoE na portach w przypadku braku mocy
13.	Możliwość ustawienia włączania/wyłączania czasowego PoE
14.	Wsparcie Fast PoE - uruchomienie zasilania PoE bez oczekiwania na pełne uruchomienie oprogramowania przełącznika
15.	Wsparcie Perpetual PoE - brak zaniku PoE podczas restartu przełącznika
16.	Przełącznik posiada możliwość łączenia do 8 przełączników w stos
17.	Przepustowość stosu min. 80 Gb/s
18.	Możliwość budowy stosu za pomocą portów 10G SFP+
19.	Dedykowane 2 porty do budowy stosu przełączników
20.	Stos zachowuje się jak jedno urządzenie logiczne, a w szczególności ma możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiada jeden adres IP w celu zarządzania stosem
21.	Nieblokująca architektura o wydajności przełączania min. 256 Gb/s
22.	Szybkość przełączania: 190.5 Mp/s
23.	Zakres temperatury pracy przełącznika: 0 - 50 stopni C
24.	Pamięć operacyjna: min. 1 GB pamięci DRAM
25.	Pamięć flash: min. 1 GB pamięci Flash
26.	Dedykowany port konsoli szeregowej RS-232 (RJ45)
27.	Przełącznik jest wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
28.	Możliwość instalacji min. dwóch wersji oprogramowania - firmware
29.	Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash
30.	Możliwość monitorowania zajętości CPU
31.	Możliwość monitorowania zajętości pamięci
32.	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
33.	Wsparcie diagnostyki okablowania - wykrywanie przerwy, zwarcia oraz odległości do awarii
34.	Tablica MAC adresów min. 32 tys.
35.	Obsługa sieci wirtualnych IEEE 802.1Q - min. 4 tys.
36.	Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieciowych
37.	Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
38.	Obsługa min. 64 instancji MSTP
39.	Obsługa Link Aggregation IEEE 802.3ad wraz z LACP obsługa min. 128 grup łączy typu Link Aggregation obsługa umożliwiająca zgrupowanie min. 8 portów
40.	Obsługa MLAG (Multi Chassis Link Aggregation)
41.	Obsługa protokołu EAPS - RFC 3619
42.	Obsługa protokołu ERPS / G.8032
43.	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)
44.	Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB
45.	Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
46.	Obsługa CDPv1 oraz CDPv2
47.	Przełącznik posiada obsługę AVB (Audio Video Bridging)
48.	Kontrola sztormów: • Możliwość ograniczenia liczby pakietów Multicast na porcie • Możliwość ograniczenia liczby pakietów Broadcast na porcie • Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie
49.	Przełącznik wspiera mechanizm zabezpieczenia przed pętlami inny niż STP

50.	Wsparcie DCB (Data Center Bridging): • DCBX - Data Center Bridging eXchange • PFC - Priority-based Flow Control • ETS - Enhanced Transmission Selection
51.	Obsługa min. 1500 interfejsów IP
52.	Wsparcie dla IP multinetting - wiele adresów przypisanych do jednej sieci VLAN
53.	Sprzętowa obsługa routingu IPv4
54.	Pojemność sprzętowej tabeli routingu min. 12 tys. wpisów
55.	Obsługa routingu statycznego IPv4
56.	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
57.	Obsługa redundancji routingu VRRP dla IPv4
58.	Policy Based Routing dla IPv4
59.	Obsługa DHCP Relay
60.	Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów
61.	Obsługa Opcji 82 dla DHCP
62.	Sprzętowa obsługa routingu IPv6
63.	Pojemność tabeli routingu min. 6 tys. wpisów
64.	Obsługa routingu statycznego IPv6
65.	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
66.	Obsługa redundancji routingu VRRP dla IPv6
67.	Policy Based Routing dla IPv6
68.	Obsługa 6to4 (RFC 3056)
69.	Opcja IPv6 Router Advertisement dla DNS - RFC 6106
70.	Statyczne przyłączania portu do grupy multicast
71.	Filtrowanie IGMP
72.	Obsługa IGMP v1 - RFC 1112
73.	Obsługa IGMP v2 - RFC 2236
74.	Obsługa IGMP v3 - RFC 3376
75.	Obsługa IGMP v1/v2/v3 snooping
76.	Obsługa PIM-SM
77.	Obsługa PIM-DM - możliwość rozszerzenia przez licencję
78.	Obsługa PIM-SSM - możliwość rozszerzenia przez licencję
79.	Obsługa MLDv1 snooping
80.	Obsługa MLDv2 snooping
81.	Obsługa MVR (Multicast VLAN Registration)
82.	Obsługa logowania do sieci Network Login • IEEE 802.1x based Network Login • MAC address based Network Login • Web based Network Login
83.	Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
84.	Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
85.	Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x
86.	Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication
87.	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
88.	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
89.	Automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA

90.	Automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA
91.	Przełącznik posiada mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który „przejmie" rolę uwierzytelniania klientów
92.	Obsługa Guest VLAN dla IEEE 802.1x
93.	Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci
94.	Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176
95.	Obsługa wymuszania ponownego periodycznego uwierzytelnienie (Reauthentication)
96.	Obsługa RADIUS Authentication (RFC 2865)
97.	Obsługa RADIUS Accounting (RFC 2866)
98.	Obsługa RADIUS Per-Command Authentication - uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS
99.	Obsługa RADIUS Authentication over TLS (RadSec)
100.	Obsługa RADIUS Accounting over TLS (RadSec)
101.	Obsługa TACACS+ (RFC 1492)
102.	Bezpieczeństwo MAC adresów: • ograniczenie liczby MAC adresów na porcie • zatrzaśnięcie MAC adresów na porcie • możliwość wpisania statycznych MAC adresów na port/vlan
103.	Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning)
104.	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
105.	Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
106.	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
107.	Wsparcie 16 tys. wpisów ACL na wejściu (Ingress)
108.	Wsparcie 1 tys. wpisów ACL na wyjściu (Egress)
109.	Obsługa IP Security • Trusted DHCP Server • DHCP Snooping and Guard • Gratuitous ARP Protection • DHCP Secured ARP/ARP Validation • IP Source Guard
110.	Ograniczenie przepustowości (rate limiting) na portach wyjściowych
111.	Ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL
112.	Obsługa wykrywania periodycznego zaniku linku (Port-Flap): • możliwość zdefniowania 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
113.	Wydajność MACSec po rozbudowie przełącznika nie mniejsza niż 50 Gb/s
114.	Zarządzenia przez SNMP v1/v2/v3
115.	Obsługa SNMP Traps
116.	Obsługa synchronizacji czasu SNTP lub NTP
117.	Obsługa DNS klienta
118.	Zarządzanie przez przeglądarkę www - protokół http i https

119.	Możliwość zarządzania przez protokół XML
120.	Obsługa serwera SSH dla IPv4
121.	Obsługa serwera SSH dla IPv6
122.	Obsługa klienta SSH dla IPv4
123.	Obsługa klienta SSH dla IPv6
124.	Obsługa serwera Telnet dla IPv4
125.	Obsługa serwera Telnet dla IPv6
126.	Obsługa klienta Telnet dla IPv4
127.	Obsługa klienta Telnet dla IPv6
128.	Obsługa transferu plików: • TFTP • SFTP • SCP
129.	Obsługa SYSLOG
130.	Obsługa Secure SYSLOG (TLS)
131.	Obsługa SYSLOG - konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń
132.	Obsługa logowania komend CLI do logu systemowego
133.	Obsługa logowania komend do serwera SYSLOG
134.	Obsługa ping dla IPv4 i IPv6
135.	Obsługa traceroute dla IPv4 i IPv6
136.	Obsługa RMON min. 4 grupy: Status, History, Alarms, Events
137.	Obsługa RMON2
138.	Współpraca z systemem kontroli dostępu oferowanym w postępowaniu
139.	Wbudowany DHCP Server
140.	DHCP Server z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
141.	Wbudowany DHCP Client
142.	Obsługa skryptów CLI
143.	Obsługa funkcji TCL/Tk w skryptach CLI
144.	Obsługa skryptów Python 3.x
145.	Możliwość uruchamiania skryptów: • ręcznie z CLI przez administratora • w określonym czasie lub co wskazany czas • na podstawie zdarzeń z logu systemowego
146.	Możliwość edycji skryptów bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych
147.	Wsparcie standardu IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging
148.	Zgodność z EU RoHS - 2011/65/EU Zgodność z EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage Zgodność z EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation Zgodność z EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational

Aplikacja/oprogramowanie do zarządzania przełącznikami sieciowymi

poz.	wymagane funkcje i parametry
1.	Oprogramowanie zarządzające działa w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci. Serwer aplikacji zarządzającej ma możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare; aplikacja wspiera klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
2.	Aplikacja pozwala na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
3.	Licencja na aplikację zarządzającą umożliwia zarządzanie wszystkimi oferowanymi urządzeniami
4.	Aplikacja zarządzająca ma możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
5.	Aplikacja zarządzająca ma możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius
6.	Wszystkie dane aplikacji zarządzającej są przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze
7.	Aplikacja zarządzająca pozwala na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
8.	Aplikacja pozwala 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
9.	Aplikacja ma możliwość przyjmowania trapów SNMP i przekierowywania ich do innych systemów
10.	Aplikacja posiada możliwość kompilowania SNMP MIB innych producentów
11.	Aplikacja zapewnia możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II

12.	Aplikacja zapewnia możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych
13.	Aplikacja posiada 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
14.	Aplikacja posiada wbudowany Syslog serwer
15.	Aplikacja zapewnia możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
16.	Alarmy zapewniają możliwość ograniczenia ich zakresu, np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych
17.	Alarmy mają możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację, np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia
18.	Alarmy mają możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak: • Wysłanie e-mail do wskazanej grupy adresowej • Wysłanie informacji SYSLOG do wskazanego serwera • Wysłanie TRAP SNMP do wskazanego adresu IP • Uruchomienie skryptu w systemie operacyjnym Linux • Uruchomienie skryptu skonfigurowanego w systemie zarządzającym
19.	Aplikacja umożliwia automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera
20.	Aplikacja zapewnia automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
21.	Aplikacja pozwala na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach
22.	Aplikacja zapewnia możliwość wizualizacji sieci z uwzględnieniem połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu oraz konfiguracji sieci VLAN
23.	Aplikacja zapewnia możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
24.	Aplikacja zapewnia możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane: • adres IP urządzenia • adres MAC urządzenia • nazwa urządzenia • wersja oprogramowania • wersja bootrom • lokalizacja urządzenia • dane kontaktowe administratora • numer seryjny • numer inwentaryzacyjny – własna numeracja
25.	Aplikacja zapewnia centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane są: • możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie; • możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych; • możliwość odtworzenia wskazanej konfiguracji urządzenia; • możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami; • możliwość obsługi backup'u urządzeń sieciowych różnych producentów
26.	Aplikacja zapewnia możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
27.	Aplikacja przechowuje historię zmian konfiguracji oraz oprogramowania na urządzeniach
28.	Aplikacja zapewnia możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych
29.	Aplikacja zapewnia możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
30.	Aplikacja zapewnia możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem: • przyłączenia do sieci VLAN, • przyłączenia do serwisu w ramach „Fabric" z wykorzystaniem IEEE 802.1Qcj, • konfiguracji Quality of Service, • konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4, • 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

31.	Aplikacja zarządzająca posiada wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal umożliwia: • 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 wskazuje gdzie użytkownik jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy); • 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); • wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.; • generowanie raportów
32.	Aplikacja zarządzająca zapewnia zarządzanie siecią bezprzewodową w następujący sposób: • Jest zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa); • Jest 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 • Jest zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje: – adres IP kontrolera – liczba obsługiwanych klientów – szczytowe wartości zajmowanego pasma – wersja oprogramowania • Jest 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 • Jest 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 • Jest zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy zapewniają 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
33.	Aplikacja zarządzająca jest zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji: • adres MAC • adres IP • nazwa komputera • typ klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS, itp. • nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika • adres IP urządzenia, do którego dołączony jest klient • 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 • typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping, itp. • nazwa przydzielonej polityki bezpieczeństwa

34.	System zarządzania tożsamością zautoryzowanych klientów w sieci zapewnia przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta, zawierającej zmiany wspomnianych wcześniej parametrów, np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa, itp.
35.	System zarządzania tożsamością klientów zapewnia możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
36.	System zarządzania tożsamością zapewnia możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie: • 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. • przynależności do odpowiedniej grupy użytkowników, np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika • realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC • 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. • realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
37.	System zarządzania tożsamością zautoryzowanych klientów zapewnia 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.
38.	Przydział urządzenia do grupy urządzeń jest 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
39.	System zarządzania tożsamością zautoryzowanych klientów zapewnia możliwość rejestracji urządzeń poprzez portal www; rejestracji podlegają np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci
40.	System zarządzania tożsamością zapewnia możliwość modyfikacji stron służących do rejestracji gości, możliwość zmiany kolorów, wczytania własnego logo, zmiany plików definicji strony CSS
41.	System zarządzania tożsamością w ramach rejestracji gości zapewnia możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. adres email, numer telefonu, adres email osoby zapraszającej, itp.
42.	System zarządzania tożsamością zapewnia możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy
43.	System portalu www służący do rejestracji gości zapewnia obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa
44.	System zarządzania tożsamością zautoryzowanych klientów posiada informacje podsumowujące zawierające: • liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi, itp. • liczbę urządzeń z podziałem typu autoryzacji, np. MAC, 802.1x, itp. • liczbę urządzeń z podziałem na typy systemów operacyjnych, np. Windows, Linux, IOS, Android • liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa • liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2, itp.
45.	System zarządzania tożsamością jest zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python, np. zapewnia możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
46.	System zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników, zapewnia obsługę min. 1 000 urządzeń klienckich (adresów MAC) przez minimum 12 miesięcy
47.	System zarządzania przy współpracy z dostarczonymi urządzeniami pozwala na analizę ruchu w sieci do warstwy 7, co dotyczy przełączników oraz sieci bezprzewodowej
48.	Analiza ruchu w sieci do warstwy 7 zapewnia możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN; prezentacja zapewnia informacje ilościowe ruchu poszczególnych aplikacji
49.	Analiza ruchu zapewnia możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji, z tym że czasy te pozwalają na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji
50.	System Analityki zapewnia bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos
51.	System Analityki zapewnia możliwość monitorowania własnych wybranych aplikacji
52.	Monitorowanie aplikacji zapewnia możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji
53.	System Analityki ma 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.
54.	System Analityki zapewnia możliwość tworzenia raportów

55.	System Analityki zapewnia możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail
56.	System zarządzania posiada 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
57.	System zarządzania posiada możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
58.	System zarządzania posiada możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu, który zapewnia przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie
59.	System zarządzania posiada możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu
60.	System zarządzania posiada możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością, np. pojawienie się nowej niezarejestrowanej w systemie drukarki
61.	System zarządzania posiada wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów, tzn.: • istnieje możliwość integracji systemu kontroli tożsamości z systemami firewall Fortinet posiadanymi przez zamawiającego • istnieje możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM Fortinet zamawiającego, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny • istnieje możliwość integracji systemu kontroli dostępu z systemami MDM

Aplikacja/oprogramowanie do zarządzania jest objęte 12-miesięcznym serwisem (wsparciem technicznym) producenta.
Wraz z przełącznikami wykonawca dostarczy kable stack:

- 2 kable DAC 100Gb o długości 1m dla przełączników szkieletowych,
- 7 kabli stack o długości 1m zapewniających przepustowość stosu przełączników dostępowych min. 80 Gb/s,
- 23 kabli stack o długości 0,5m zapewniających przepustowość stosu przełączników dostępowych min. 80 Gb/s.

Zamawiający dopuszcza dostawę ww. kabli w postaci tzw. zamienników oryginalnych kabli producenta oferowanych przełączników sieciowych pod warunkiem, że w ramach wymaganego rocznego wsparcia dla przełączników producent lub wykonawca będzie również zapewniał wsparcie dla samego połączenia w stos/MLAG zbudowanego w oparciu o dostarczone kable.
Wraz z przełącznikami wykonawca dostarczy także 124 wkładki 10Gb SFP+ SR wielomodowe. Zamawiający dopuszcza dostawę wkładek w postaci tzw. zamienników oryginalnych producenta oferowanych przełączników sieciowych pod warunkiem, że w ramach wymaganego rocznego wsparcia dla przełączników producent lub wykonawca będzie również zapewniał wsparcie dla połączeń zbudowanych w oparciu o dostarczone wkładki. Jeżeli realizacja takiego wymogu wymusza zastosowanie wkładek tego samego producenta co zaoferowane przełączniki, to w takim przypadku wystarczy dostarczyć co najmniej cztery wkładki oryginalne, a pozostałe mogą być zamiennikami.
Realizacja **ZADANIA NR 1** obejmuje wdrożenie dostarczonych przez wykonawcę przełączników sieciowych i aplikacji/oprogramowania do zarządzania przełącznikami, w siedzibie zamawiającego w zakresie: montaż urządzeń, instalacja i konfiguracja aplikacji/oprogramowania do zarządzania, konfiguracja połączeń oraz stosów, konfiguracja polityk dostępowych, integracja z systemami bezpieczeństwa zamawiającego i innych podanych w opisie przedmiotu tej części zamówienia.
Wszystkie czynności podlegają wykonaniu przez skierowane w tym celu przez wykonawcę osoby posiadające certyfikat techniczny wystawiony przez producenta oferowanych przełączników i aplikacji/oprogramowania do zarządzania, a w zakresie integracji z infrastrukturą FortiNet - przez inżyniera z certyfikatem FCX.
Wszystkie wymagane certyfikaty wykonawca przedstawi na wezwanie zamawiającego na dowolnym etapie oceny ofert, najpóźniej przed zawarciem umowy, a także w trakcie realizacji zamówienia.

kwalifikowany podpis elektroniczny wykonawcy
*oferującego wykonanie **ZADANIA NR 1***