Załącznik nr 1 do SIWZ

Nr postępowania: BAG.261.10.2020.PN

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostarczanie sprzętu sieciowego wraz z niezbędnym oprogramowaniem, akcesoriami i usługami zgodnie z poniższą specyfikacją.

Przedmiot zamówienia składa się z:

1. Przełącznik szkieletowy – 2 sztuki
2. Przełącznik dostępowy – 10 sztuk
3. Oprogramowanie zarządzające
4. Moduły optyczne i kable SFP+
5. Usługa wsparcia technicznego

Wymagania w zakresie dostawy, gwarancji, wsparcia technicznego
Całość przedmiotu zamówienia należy zrealizować w ciągu 45 dni.

Od momentu odbioru dostawy potwierdzonej protokołem należy świadczyć na rzecz Zamawiającego wsparcie techniczne do oferowanych rozwiązań przez okres jednego roku. W tym celu wykonawca musi posiadać co najmniej dwóch inżynierów posiadających aktualny certyfikat techniczny (lub certyfikaty) wystawione przez producenta oferowanych urządzeń sieciowych i systemu zarządzania potwierdzające wiedzę z ich zakresu. Certyfikaty te należy dołączyć do oferty. Jeżeli producent oferowanych rozwiązań stosuje certyfikację serwisową to wykonawca zobowiązany jest do jej posiadania, a fakt ten powinien być możliwy do weryfikacji np. na stronie producenta.

Zaoferowane przełączniki sieciowe muszą posiadać minimum 5-cio letnią gwarancję uprawniającą do naprawy w razie awarii oraz możliwość aktualizacji oprogramowania przez okres co najmniej 5 lat od ich dostawy. Przez minimum pierwszy rok wymagane jest również wsparcie techniczne w pełnym zakresie funkcjonalnym oraz priorytetowa naprawa w razie awarii typu NBD. Musi być zapewniona możliwość przedłużenia tego wsparcia na kolejne lata.

Licencja na zaoferowane oprogramowanie musi być dożywotnia wraz z minimum rocznym wsparciem technicznym i aktualizacjami. Musi być zapewniona możliwość przedłużenia tego wsparcia na kolejne lata.

I. Ogólne wymagania odnośnie urządzeń

1. Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu reburbfished/odnowione (zwróconych do producenta i później odsprzedawanych ponownie przez producenta),
2. Oferowane urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia producenta lub przedstawiciela producenta potwierdzającego ważność i zakres uprawnień licencyjnych oraz gwarancyjnych.
3. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u producenta lub polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.
4. Wszystkie urządzenia i moduły muszą pochodzić od producenta przełączników sieciowych i muszą być objęte kontraktem serwisowym producenta, którym będą objęte dostarczane przełączniki.
5. Przełączniki szkieletowe muszą być identyczne co do modelu i firmware-u.
6. Przełączniki dostępowe muszą być identyczne co do modelu i firmware-u.

II. Wymagania serwisowe

1. Urządzenia muszą być objęte minimum 5-cio letnią gwarancję uprawniającą do naprawy w razie awarii oraz możliwość aktualizacji oprogramowania od ich dostawy.
2. Urządzenia muszą być objęte co najmniej 12 miesięcznym serwisem gwarancyjnym opartym na usługach serwisowych producenta, niezależnych od statusu partnerskiego Wykonawcy.
   a) Naprawa lub wymiana urządzenia musi nastąpić nie później niż w następnym dniu roboczym od daty zgłoszenia.
   b) Wraz z produktami ma zostać dostarczone oświadczenie producenta lub przedstawiciela producenta potwierdzające objecie urządzeń serwisem gwarancyjnym opartym na usługach serwisowych producenta.
   c) Zgłoszenia wad lub usterek Urządzeń będą przesyłane drogą elektroniczną według wyboru Zamawiającego.
3. Okres serwisu gwarancyjnego oraz usług gwarancyjnych producenta określone w ust. 2 będzie liczony od daty podpisania bez zastrzeżeń protokołu odbioru końcowego przedmiotu zamówienia.
4. Oferowany serwis gwarancyjny musi zapewnić Zamawiającemu przez cały okres trwania:
   a) serwis świadczony w dni robocze w godzinach pracy Zamawiającego,
   b) możliwość zgłoszenia awarii urządzenia bezpośrednio producentowi urządzenia (a nie tylko Wykonawcy zamówienia) wraz z możliwością otrzymania „z góry" urządzenia zamiennego wolnego od uszkodzeń, bez dodatkowych opłat, a jedynie pod warunkiem zwrotu wadliwego urządzenia,

c) bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon, e-mail oraz WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją urządzeń,

d) możliwość pobierania bezpośrednio od producenta nowych wydań oprogramowania przez okres co najmniej 5 lat od daty dostawy zgodnie z zapotrzebowaniem Zamawiającego, jednakże w ramach ogólnie dostępnej oferty producenta, a także w ramach wykupionego zestawu funkcjonalności oprogramowania i wykupionej konfiguracji urządzeń wraz z wolnym od dodatkowych opłat prawem (tj. licencją) do korzystania z pobranego oprogramowania na zasadach określonych w warunkach licencyjnych dla użytkownika końcowego.

Specyfikacja techniczna urządzeń i oprogramowania

Zamawiający wymaga, by dostarczone urządzenia były nowe oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem). Całość sprzętu i oprogramowania musi pochodzić od jednego producenta.

1. Przełącznik szkieletowy – 2 sztuki		
Wymagania Podstawowe	1.	Przełącznik posiadający 16 portów 10 Gigabit Ethernet SFP+, mogących pracować z prędkością 100 MB, 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+
	2.	Montaż w szafie RACK - Wysokość urządzenia 1U
	3.	Redundantne zasilacze typu hot swap
	4.	Nieblokująca architektura o wydajności przełączania min. 360 Gb/s
	5.	Szybkość przełączania min. 235 Milionów pakietów na sekundę
	6.	Możliwość łączenia do 8 przełączników w stos za pomocą portów 10G
	7.	Tablica MAC adresów min. 16k
	8.	Pamięć operacyjna: min. 1 GB pamięci DRAM
	9.	Pamięć flash: mln. 4 GB pamięci Flash
	10.	Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
	11.	Obsługa sieci wirtualnych protokołowych IEEE 802.1v
	12.	Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
	13.	Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
	14.	Obsługa Q-in-Q IEEE 802.1ad

	15.	Obsługa Quality of Service
		IEEE 802.1p
		DiffServ
		8 kolejek priorytetów na każdym porcie wyjściowym
	16.	Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
	17.	Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
	18.	Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
	19.	Wbudowany DHCP Serwer i klient
	20.	Możliwość instalacji min. dwóch wersji oprogramowania – firmware
	21.	Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
	22.	Możliwość monitorowania zajętości CPU
	23.	Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
	24.	Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
	25.	Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
	26.	Obsługa CDPv2
Routing IPv4	27.	Sprzętowa obsługa routingu IPv4 – forwarding
	28.	Routing statyczny
	29.	Obsługa routingu dynamicznego IPv4
		RIPv1/v2
		OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
Routing IPv6	30.	Sprzętowa obsługa routingu IPv6 – forwarding
	31.	Routing statyczny
	32.	Obsługa routingu dynamicznego dla IPv6
		RIPng
		OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
	33.	Telnet Serwer/Klient dla IPv6
	34.	SSH2 Serwer/Klient dla IPv6
	35.	Ping dla IPv6
	36.	Tracert dla IPv6
	37.	Obsługa MLDv1 (Multicast Listener Discovery version 1)
Obsługa Multicast	38.	Filtrowanie IGMP
	39.	Obsługa Multicast VLAN Registration – MVR
	40.	Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo	41.	Obsługa Network Login
		IEEE 802.1x - RFC 3580
		Web-based Network Login
		MAC based Network Login
	42.	Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
	43.	Możliwość integracji funkcjonalności Network Login z Microsoft NAP
	44.	Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
	45.	Obsługa Guest VLAN dla IEEE 802.1x
	46.	Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
	47.	Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
	48.	Obsługa Identity Management
	49.	Wbudowana obrona procesora urządzenia przed atakami DoS
	50.	Obsługa TACACS+
	51.	Obsługa RADIUS Authentication (RFC 2138)
	52.	Obsługa RADIUS Accounting (RFC 2139)
	53.	RADIUS and TACACS+ per-command Authentication
	54.	Bezpieczeństwo MAC adresów
		ograniczenie liczby MAC adresów na porcie zatrzaśnięcie MAC adresu na porcie możliwość wpisania statycznych MAC adresów na port/vlan
	55.	Możliwość wyłączenia MAC learning
	56.	Obsługa SNMPv1/v2/v3
	57.	Klient SSH2
	58.	Zabezpieczenie przełącznika przed atakami DoS
		Networks Ingress Filtering RFC 2267
		SYN Attack Protection
		Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
	59.	Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
		Adres MAC źródłowy i docelowy plus maska
		Adres IP źródłowy i docelowy plus maska dla IPv4 oraz 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
		Flagi TCP
		Obsługa fragmentów
	60.	Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
	61.	Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
	62.	Obsługa bezpiecznego transferu plików SCP/SFTP
	63.	Obsługa DHCP Option 82
	64.	Obsługa IP Security - Gratuitous ARP Protection
	65.	Obsługa IP Security – Trusted DHCP Server
	66.	Obsługa IP Security – DHCP Secured ARP/ARP Validation
	67.	Obsługa IP Security – IP Source guard
	68.	Ograniczanie przepustowości (rate limiting) na portach wyjściowych
Bezpieczeństwo sieciowe	69.	Możliwość konfiguracji portu głównego i zapasowego
	70.	Obsługa redundancji routingu VRRP - RFC 2338
	71.	Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
	72.	Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
	73.	Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
	74.	Obsługa PVST+
	75.	Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
	76.	Obsługa G.8032
	77.	Obsługa Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
	78.	Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
Zarządzanie	79.	Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
	80.	Obsługa synchronizacji czasu NTP
	81.	Zarządzanie przez SNMP v1/v2/v3
	82.	Zarządzanie przez przeglądarkę WWW – protokół http i https
	83.	Możliwość zarządzania przez protokół XML
	84.	Możliwość zarządzania przełącznikiem z aplikacji Cloud
	85.	Możliwość zarzadzania przełącznikiem z dedykowanej aplikacji zarządzającej
	86.	Możliwość zarzadzania przełącznikiem z poziomu CLI
	87.	Wsparcie dla Zero-touch provisioning
	88.	Telnet Serwer/Klient dla IPv4 / IPv6
	89.	SSH2 Serwer/Klient dla IPv4 / IPv6

	90.	Ping dla IPv4 / IPv6
	91.	Traceroute dla IPv4 / IPv6
	92.	Obsługa SYSLOG z możliwością definiowania wielu serwerów
	93.	Sprzętowa obsługa sFlow
	94.	Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
	95.	Obsługa RMON2 (RFC 2021)
Inne	96.	Zakres temperatury pracy 0-50 °C
	97.	Obsługa skryptów CLI
	98.	Obsługa skryptów w języku Python
	99.	Obsługa funkcji TCL/Tk w skryptach CLI
	100.	Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
	101.	Obsługa AVB (Audio Video Bridging) - możliwość rozszerzenia przez licencje
	102.	Obsługa OpenFlow – możliwość rozszerzenia przez licencje
	103.	Możliwość uruchamiania skryptów
		Ręcznie O określonym czasie lub co wskazany okres czasu Na podstawie wpisów w logu systemowym

Przełącznik dostępowy – 10 sztuk		
Wymagania Podstawowe	1.	Przełącznik posiadający 48 portów 10/100/1000BASE-T PoE+
	2.	Przełącznik posiadający 8 portów 1GBE SFP
	3.	Dla 6 z 10 dostarczanych przełączników należy zapewnić co najmniej 2 porty 10Gb SFP+ z możliwością ich dowolnej konfiguracji funkcjonalnej.
	4.	Montaż w szafie RACK - Wysokość urządzenia 1U
	5.	Nieblokująca architektura o wydajności przełączania min. 176 Gb/s
	6.	Szybkość przełączania min. 130 Milionów pakietów na sekundę
	7.	Posiada porty umożliwiające łącznie przełączników w stos. Wydajność połączenia w stos min. 40 Gb/s.
	8.	Tablica MAC adresów min. 16k
	9.	Pamięć operacyjna: min. 1 GB pamięci DRAM
	10.	Pamięć flash: min. 4 GB pamięci Flash

	11.	Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
	12.	Obsługa sieci wirtualnych protokołowych IEEE 802.1v
	13.	Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
	14.	Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
	15.	Obsługa Q-in-Q IEEE 802.1ad
	16.	Obsługa Quality of Service
		IEEE 802.1p
		DiffServ
		8 kolejek priorytetów na każdym porcie wyjściowym
	17.	Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
	18.	Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
	19.	Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
	20.	Przełącznik musi posiadać możliwość dołączenia redundantnego systemu zasilania
	21.	Wbudowany DHCP Serwer i klient
	22.	Możliwość instalacji min. dwóch wersji oprogramowania - firmware
	23.	Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
	24.	Możliwość monitorowania zajętości CPU
	25.	Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
	26.	Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.
	27.	Obsługa CDPv2
Routing IPv4	28.	Sprzętowa obsługa routingu IPv4 – forwarding
	29.	Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów
	30.	Routing statyczny
	31.	Obsługa routingu dynamicznego IPv4
		RIPv1/v2
		OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
Routing IPv6	32.	Sprzętowa obsługa routingu IPv6 – forwarding
	33.	Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów
	34.	Routing statyczny
	35.	Obsługa routingu dynamicznego dla IPv6
		RIPng
		OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
	36.	Telnet Serwer/Klient dla IPv6
	37.	SSH2 Serwer/Klient dla IPv6

	38.	Ping dla IPv6
	39.	Tracert dla IPv6
	40.	Obsługa MLDv1 (Multicast Listener Discovery version 1)
Obsługa Multicast	41.	Filtrowanie IGMP
	42.	Obsługa Multicast VLAN Registration - MVR
	43.	Obsługa IGMP v1/v2/v3 snooping
Bezpieczeństwo	44.	Obsługa Network Login
		IEEE 802.1x - RFC 3580
		Web-based Network Login
		MAC based Network Login
	45.	Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
	46.	Możliwość integracji funkcjonalności Network Login z Microsoft NAP
	47.	Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
	48.	Obsługa Guest VLAN dla IEEE 802.1x
	49.	Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
	50.	Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
	51.	Obsługa Identity Management
	52.	Wbudowana obrona procesora urządzenia przed atakami DoS
	53.	Obsługa TACACS+ (RFC 1492)
	54.	Obsługa RADIUS Authentication (RFC 2138)
	55.	Obsługa RADIUS Accounting (RFC 2139)
	56.	RADIUS and TACACS+ per-command Authentication
	57.	Bezpieczeństwo MAC adresów
		ograniczenie liczby MAC adresów na porcie
		zatrzaśnięcie MAC adresu na porcie
		możliwość wpisania statycznych MAC adresów na port/vlan
	58.	Możliwość wyłączenia MAC learning
	59.	Obsługa SNMPv1/v2/v3
	60.	Klient SSH2
	61.	Zabezpieczenie przełącznika przed atakami DoS
		Networks Ingress Filtering RFC 2267
		SYN Attack Protection
		Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
	62.	Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4

		Adres MAC źródłowy i docelowy plus maska
		Adres IP źródłowy i docelowy plus maska dla IPv4 oraz 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
		Flagi TCP
		Obsługa fragmentów
	63.	Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
	64.	Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania
	65.	Obsługa bezpiecznego transferu plików SCP/SFTP
	66.	Obsługa DHCP Option 82
	67.	Obsługa IP Security - Gratuitous ARP Protection
	68.	Obsługa IP Security - Trusted DHCP Server
	69.	Obsługa IP Security - DHCP Snooping
	70.	Obsługa IP Security - DHCP Secured ARP/ARP Validation
	71.	Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 64 kb/s
Bezpieczeństwo sieciowe	72.	Możliwość konfiguracji portu głównego i zapasowego
	73.	Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
	74.	Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
	75.	Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
	76.	Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
	77.	Obsługa PVST+
	78.	Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
	79.	Obsługa G.8032 v1/v2
	80.	Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.
	81.	Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.
Zarządzanie	82.	Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
	83.	Obsługa synchronizacji czasu NTP
	84.	Zarządzanie przez SNMP v1/v2/v3
	85.	Zarządzanie przez przeglądarkę WWW – protokół http i https

	86.	Możliwość zarządzania poprzez protokół XML
	87.	Telnet Serwer/Klient dla IPv4 / IPv6
	88.	SSH2 Serwer/Klient dla IPv4 / IPv6
	89.	Ping dla IPv4 / IPv6
	90.	Traceroute dla IPv4 / IPv6
	91.	Obsługa SYSLOG z możliwością definiowania wielu serwerów
	92.	Sprzętowa obsługa sFlow
	93.	Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
	94.	Obsługa RMON2 (RFC 2021)
Inne	95.	Zakres temperatury pracy 0-50 °C
	96.	Obsługa skryptów CLI
	97.	Obsługa funkcji TCL/Tk w skryptach CLI
	98.	Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
	99.	Obsługa OpenFlow – możliwość rozszerzenia przez licencje
	100.	Obsługa AVB (Audio Video Bridging)- możliwość rozszerzenia przez licencję oprogramowania
	101.	Możliwość uruchamiania skryptów
		Ręcznie
		O określonym czasie lub co wskazany okres czasu
		Na podstawie wpisów w logu systemowym

2. Oprogramowanie do zarządzania

1. Aplikacja musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera
    a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
    b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.
2. Aplikacja musi zarządzać siecią przewodową i bezprzewodową
3. Aplikacja zarządzająca musi obsługiwać minimum 10 urządzeń (adresów IP)
4. Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników.
5. Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego
6. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
7. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
8. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
9. Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
10. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
12. Aplikacja musi posiadać wbudowaną przeglądarkę SNMP MIB
13. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
14. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
15. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla danych urządzeń sieciowych.
16. 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.
17. Aplikacja musi posiadać wbudowany Syslog serwer
18. Aplikacja musi posiadać wbudowany BootP serwer
19. Aplikacja musi wspierać protokół IPv4 oraz IPv6
20. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
21. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
22. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
23. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
    a. połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości

b. stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów
c. konfiguracji sieci VLAN
d. konfiguracji protokołu routingu OSPF

24. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https
25. 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
26. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
    b. możliwość odtworzenia wskazanej konfiguracji urządzenia
    c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych
    d. możliwość obsługi urządzeń sieciowych różnych producentów
27. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
28. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
29. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp.
31. Tworzona polityka musi zawierać możliwość:
    a. blokowania lub zezwalania ruchu na podstawie
        i. źródłowy i docelowy adres MAC
        ii. źródłowy i docelowy adres IP
        iii. źródłowy i docelowy adres IP podsieci
        iv. źródłowy i docelowy port TCP/UDP
        v. źródłowy i docelowy zakres portów TCP/UDP
        vi. typ protokołu
        vii. pole IP TOS
    b. przydziału parametrów QoS
        i. priorytety
        ii. ograniczenia przepustowości

iii. przydziału użytkownika do wskazanej sieci VLAN
iv. przekierowania ruchu do zewnętrznego systemu analizującego pakiety

32. Aplikacja musi mieć możliwość wdrażania polityk bezpieczeństwa w całej sieci, dla urządzeń przewodowych i bezprzewodowych za pomocą jednego kliknięcia.
33. Aplikacja musi pozwalać na łatwą modyfikację i ponowne wdrożenie na wszystkich urządzeniach przewodowych i bezprzewodowych
34. 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
35. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
    a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
    b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac
    c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
        i. adres IP kontrolera
        ii. liczba obsługiwanych klientów
        iii. szczytowe wartości zajmowanego pasma
        iv. wersja oprogramowania
    d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
        i. adres IP punktu dostępowego
        ii. MAC adres punktu dostępowego
        iii. wersja oprogramowania
        iv. typ punktu dostępowego
        v. kanały pracy poszczególnych interfejsów radiowych
        vi. szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
    e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
        i. adres IP klienta
        ii. MAC adres klienta
        iii. nazwa użytkownika
        iv. nazwa punktu dostępowego, do którego dołączony jest użytkownik
        v. BSSID, do którego dołączony jest użytkownik
        vi. SSID, do którego dołączony jest użytkownik

f. Musi być zapewniona możliwość tworzenia map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
    i. zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
    ii. zaznaczenie kanałów pracy urządzeń
    iii. lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych

36. Aplikacja zarządzająca musi być zintegrowana z systemem zapewniającym widoczność zautoryzowanych klientów w sieci 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.
37. System zapewniający widoczność zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
38. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
39. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List
40. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
41. System zapewniający widoczność 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.
42. System zapewniający widoczność zautoryzowanych klientów jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 500 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 100 punktów

dostępowych oraz min. 10 przełączników sieciowych. System musi umożliwiać w przyszłości rozbudowę do minimum 250 urządzeń sieciowych. System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7.

43. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.

3. Osprzęt: moduły optyczne i kable SFP+

W ramach zamówienia należy dostarczyć również:

1. Moduły optyczne 10Gb SFP+ wielomodowe szt. 12
2. Kable typu DAC 10Gb SFP+ 1m szt. 11
3. Kable typu DAC 10Gb SFP+ 3m szt. 8

Wszystkie moduły i kable muszą być tego samego producenta co zaoferowane urządzenia sieciowe. Zamawiający nie dopuszcza zaoferowania zamienników.