**Wykaz parametrów urządzeń sieciowych oraz oprogramowania wymienionego w zapytaniu**

1. **Przełącznik dostępowy 48-portowy**
2. Minimum 48 portów gigabitowych w standardzie 100/1000BaseT;
3. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP);

Każdy przełącznik wyposażony w minimum dwie wkładki SFP+ 10GbBaseLR;

1. Przepustowość: minimum 176 Gb/s;
2. Wydajność: minimum 100 Mp/s;
3. Tablica adresów MAC o wielkości minimum 32000 pozycji;
4. Obsługa ramek Jumbo;
5. Routing IPv4 – minimum: statyczny, RIPv2, OSPF;
6. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3;
7. Mechanizmy redundancji bramy domyślnej – VRRP;
8. Wielkość tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6;
9. Wsparcie dla funkcji Policy-based routing;
10. Obsługa ruchu Multicast: IGMP Snooping, MLD Snooping;
11. Obsługa VxLAN: minimum 64 tunele VXLAN, obsługa minimum 64 VTEP/VSI;
12. Obsługa IEEE 802.1s Multiple SpanningTree z nie mniej niż 16 instancji MSTP;
13. Obsługa IEEE 802.1w Rapid Spanning Tree Protocol;
14. Obłsuga RPVST+ z nie mniej niż 128 instancji PVST;
15. Obsługa 2000 tagów IEEE 802.1Q oraz minimum 500 jednoczesnych sieci VLAN;
16. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT;
17. Obsługa standardu IEEE 802.1v protocol VLANs;
18. Funkcja Root Guard oraz BPDU protection;
19. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 4 urządzeń;
20. Zarządzanie stosem musi odbywać się z jednego adresu IP;
21. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster);
22. Dopuszcza się łączenie w stos za pomocą portów uplink 10Gb SFP+ pod warunkiem, że na potrzeby uplink pozostaną nie mniej niż 2 porty 10GbEthernet SFP+;
23. Z przełącznikiem należy dostarczyć wszystkie niezbędne elementy do podłączenia w stos wraz z kablem o długości 1m.;
24. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP);
25. Realizacja łączy agregowanych (LACP) do różnych przełączników będących w stosie;
26. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping (wszystkie dla IPv4 i IPv6);
27. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI;
28. Obsługa minimum 500 Access list (ACL) dla IPv4. Możliwość utworzenia minimum 2000 wpisów Access List entry (ACE);
29. Obsługa minimum 500 Access list dla MAC. Możliwość utworzenia minimum 2000 wpisów Access List entry (ACE);
30. Obsługa standardu 802.1p – min. 8 kolejek na porcie;
31. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres IP, źródłowy/docelowy port TCP;
32. Priorytetyzacja zgodna z 802.1p. Wbudowane mechanizmy rate limiting;
33. Funkcja mirroringu portów na porty lokalne i zdalne (Remote i Local Mirroring);
34. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED);
35. Funkcja autoryzacji użytkowników na porcie w trybie web-based authentication i MAC-based authentication;
36. Funkcja autoryzacji użytkowników zgodna z 802.1x - jednoczesna autentykacja na jednym porcie dla minimum 8 stacji końcowych;
37. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+;
38. RADIUS Accounting;
39. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3;
40. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic;
41. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP);
42. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow;
43. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az;
44. Pełne zarządzanie poprzez port konsoli;
45. Wbudowane porty konsoli RJ45 i USB;
46. Zarządzanie przez protokół SNMP wersje:1, 2c i 3;
47. Zarządzanie przy pomocy następujących protokołów: Telnet, SSH v.2, http i https;
48. Raportowanie zdarzeń przy pomocy mechanizmów Syslog i SNMP Trap;
49. Wsparcie dla protokołu dystrybucji czasu: SNTPv4;
50. Przełącznik musi mieć możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku;
51. Przełącznik musi mieć możliwość przechowywania co najmniej dwóch wersji plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej;
52. Wsparcie dla funkcji Private VLAN lub równoważnego;
53. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego;
54. Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9);
55. Obsługa Secure FTP;
56. Obsługa ochrony procesora;
57. Minimalny zakres pracy od 0°C do 40°C;
58. Wysokość w szafie 19” – 1U;
59. Głębokość do 25 cm.;
60. Wewnętrzny zasilacz 230VAC;
61. Maksymalny pobór mocy nie większy niż 50W;
62. Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD);
63. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego;
64. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji;
65. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu;
66. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta;

Wymagane wkładki optyczne i wymagane kable muszą pochodzić od producenta urządzenia i być objęte jego gwarancją.

1. **Przełącznik dostępowy 24-portowy**
2. Minimum 24 porty gigabitowych w standardzie 100/1000BaseT;
3. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych(SFP);

Każdy przełącznik wyposażony w minimum dwie wkładki SFP+ 10GbBaseLR;

1. Przepustowość: minimum 128 Gb/s;
2. Wydajność: minimum 90 Mp/s;
3. Tablica adresów MAC o wielkości minimum 32000 pozycji;
4. Obsługa ramek Jumbo;
5. Routing IPv4 – minimum: statyczny, RIPv2, OSPF;
6. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3
7. Mechanizmy redundancji bramy domyślnej – VRRP;
8. Wielkość tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6;
9. Wsparcie dla funkcji Policy-based routing;
10. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping;
11. Obsługa VxLAN: minimum 64 tunele VXLAN, obsługa minimum 64 VTEP/VSI;
12. Obsługa IEEE 802.1s Multiple SpanningTree z nie mniej niż 16 instancji MSTP;
13. Obsługa IEEE 802.1w Rapid Spanning Tree Protocol;
14. Obłsuga RPVST+ z nie mniej niż 128 instancji PVST;
15. Obsługa 2000 tagów IEEE 802.1Q oraz minimum 500 jednoczesnych sieci VLAN;
16. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT;
17. Obsługa standardu IEEE 802.1v protocol VLANs;
18. Funkcja Root Guard oraz BPDU protection;
19. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 4 urządzeń;
20. Zarządzanie stosem musi odbywać się z jednego adresu IP;
21. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster);
22. Dopuszcza się łączenie w stos za pomocą portów uplink 10Gb SFP+ pod warunkiem, że na potrzeby uplink pozostaną nie mniej niż 2 porty 10GbEthernet SFP+;
23. Z przełącznikiem należy dostarczyć wszystkie niezbędne elementy do podłączenia w stos wraz z kablem o długości 1m.;
24. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP);
25. Realizacja łączy agregowanych (LACP) do różnych przełączników będących w stosie;
26. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping (wszystkie dla IPv4 i IPv6);
27. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI;
28. Obsługa minimum 500 Access list (ACL) dla IPv4. Możliwość utworzenia minimum 2000 wpisów Access List entry (ACE);
29. Obsługa minimum 500 Access list dla MAC. Możliwość utworzenia minimum 2000 wpisów Access List entry (ACE);
30. Obsługa standardu 802.1p – min. 8 kolejek na porcie;
31. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres IP, źródłowy/docelowy port TCP. Priorytetyzacja zgodna z 802.1p. Wbudowane mechanizmy rate limiting;
32. Funkcja mirroringu portów na porty lokalne i zdalne (Remote i Local Mirroring);
33. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED);
34. Funkcja autoryzacji użytkowników na porcie w trybie web-based authentication i MAC-based authentication;
35. Funkcja autoryzacji użytkowników zgodna z 802.1x - jednoczesna autentykacja na jednym porcie dla minimum 8 stacji końcowych;
36. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+;
37. RADIUS Accounting;
38. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3;
39. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic;
40. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP);
41. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow;
42. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az;
43. Pełne zarządzanie poprzez port konsoli;
44. Wbudowane porty konsoli RJ45 i USB;
45. Zarządzanie przez protokół SNMP wersje:1, 2c i 3;
46. Zarządzanie przy pomocy następujących protokołów: Telnet, SSH v.2, http i https;
47. Raportowanie zdarzeń przy pomocy mechanizmów Syslog i SNMP Trap;
48. Wsparcie dla protokołu dystrybucji czasu: SNTPv4;
49. Przełącznik musi mieć możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku;
50. Przełącznik musi mieć możliwość przechowywania co najmniej dwóch wersji plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej;
51. Wsparcie dla funkcji Private VLAN lub równoważnego;
52. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego;
53. Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9);
54. Obsługa Secure FTP;
55. Obsługa ochrony procesora;
56. Minimalny zakres pracy od 0°C do 40°C;
57. Wysokość w szafie 19” – 1U;
58. Głębokość do 25 cm;
59. Wewnętrzny zasilacz 230VAC;
60. Maksymalny pobór mocy nie większy niż 30W;
61. Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD);
62. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego;
63. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji;
64. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu;
65. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta;

Wymagane wkładki optyczne i wymagane kable muszą pochodzić od producenta urządzenia i być objęte jego gwarancją.

1. **Licencje na zarządzanie infrastrukturą**
2. Budowa w architekturze klient – serwer.
3. System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych w celu uzyskania redundancji i wysokiej wydajności.
4. Uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników z wymuszeniem reguł złożoności haseł dla administratorów.
5. System musi pozwalać na hierarchizację zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów i zewnętrznego serwera uwierzytelniającego. Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń
6. Licencja na system powinna umożliwiać zarządzanie minimum 50 urządzeniami sieciowymi różnych producentów, w tym oferowanymi urządzeniami LAN).
7. System musi mieć możliwość rozbudowy do przynajmniej 300 urządzeń sieciowych.
8. Instalacja na platformach Windows Server 2008 SP2, Windows Server 2012 R2 oraz Red Hat Enterprise Linux 5.x/6.x.
9. System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność.
10. System zarządzania musi spełniać podstawowe funkcje:
11. automatyczna identyfikacja i wyszukiwanie urządzeń instalowanych w sieci
12. możliwość ręcznego i automatycznego dodawania urządzeń
13. automatyczne wykrywanie topologii sieci z użyciem minimum protokołów SNMP, Telnet
14. monitorowanie stanu urządzeń za pomocą mechanizmów SNMP
15. konfiguracja urządzeń
16. konfiguracja list dostępu (ACL) na zarządzanych urządzeniach
17. konfiguracja VLANów na zarządzanych urządzeniach
18. zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania
19. funkcje przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń
20. narzędzie do zarządzania obrazami oprogramowania urządzeń
21. zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń
22. możliwość wysyłania alarmów np. mailem
23. generowanie raportów w oparciu o szablony
24. prezentację urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu każdego urządzenia
25. obrazowanie sieci w postaci hierarchicznych map (urządzania wraz z połączeniami fizycznymi i logicznymi) wraz z wizualizacją alarmów oraz wizualizacją poszczególnych szaf telekomunikacyjnych
26. podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy
27. wbudowane narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych
28. lokalizowanie użytkowników po adresie IP i MAC
29. tworzenie mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym
30. tworzenie wzorców i szablonów konfiguracji na urządzenia
31. dostęp do sytemu zarządzania musi być realizowany przez przeglądarkę internetową.
32. możliwość zarządzania siecią wirtualną poprzez integracje SOAP z VMWare VirtualCenter Server oraz Microsoft Hyper-V vManage oraz WMI/Power shell
33. Muszą być dostępne moduły umożliwiające rozbudowę i integrację systemu o następujące funkcjonalności:
34. Audyt ruchu użytkowników z wykorzystaniem informacji z przepływów sieciowych sFlow, netFlow

Funkcja monitorowania wydajności aplikacji

1. **Licencje na oprogramowanie dostępowe do sieci**
2. Centralny system autentykacji musi umożliwiać logowanie użytkowników do sieci z wykorzystaniem standardu 802.1x oraz sieci dla gości (tzw. hot-spot) z wykorzystaniem portalu www (tzw. captive portal)
3. Musi być systemem multi vendorowym
4. Musi posiadać wbudowany serwer Radius oraz TACACS +
5. Obsługa co najmniej 300 równoczesnych użytkowników/urządzeń autoryzowanych do sieci. Możliwość rozbudowy systemu do 1000 autoryzowanych użytkowników/urządzeń.
6. System dostarczany w formie umożliwiającej instalację na maszynie wirtualnej (zgodnej z HyperV oraz Vmware ESX)
7. Wsparcie dla mechanizmów wysokiej dostępności. System musi być dostarczony i zainstalowany w trybie HA jako klaster złożony z dwóch maszyn wirtualnych w celu zapewnienia odpowiedniego poziomu dostępności.
8. Integracja z różnymi źródłami danych do autentykacji, w szczególności Microsoft Active Directory, RADIUS, LDAP
9. Współpraca z przełącznikami dostępowymi LAN w zakresie określenia i nadania roli dla logującego się użytkownika, dynamiczne przydzielenie reguł kontroli dostępu do zasobów np. sieci VLAN.
10. Obsługa protokołów RADIUS, RADIUS CoA (RFC3756) oraz TACACS+
11. Wbudowane otwarte API do integracji z innymi systemami
12. Możliwość integracji z innymi systemami bezpieczeństwa, w tym oprogramowaniem typu SIEM (Security Information and Event Management), MDM (Mobile Device Management) oraz systemami NGFW (Next Generation Firewall) wiodących na rynku producentów
13. System musi zapewniać mechanizmy do uwierzytelniania wszystkich typów użytkowników (hot-spot, sieć wewnętrzna) różnymi metodami (minimum: EAP-TLS, PEAP, EAP-FAST, autentykacja MAC oraz poprzez portal)
14. Wbudowana funkcja zbierania danych o sesjach zalogowanych użytkowników
15. Rozbudowany mechanizm raportujący, tworzenie standardowych oraz dostosowanych raportów.
16. Funkcja symulowania wdrażanej polityki dostępu zanim zostanie uruchomiona w sieci
17. Funkcja tworzenia skórek dla strony logowania do sieci WLAN (tzw. captive portal), zgodnych z wyglądem marki. Skórki automatycznie muszą dopasować się do typu urządzenia mobilnego (inna wersja dla telefonu, inna dla komputera)
18. Funkcja uwierzytelniania administratorów na urządzeniach sieciowych poprzez protokół TACACS+
19. Możliwość rozbudowy o moduł Network Access Control – odpowiadający za sprawdzanie (skanowanie) stanu oprogramowania urządzenia końcowego (minimum Windows, MacOS, Linux) przy pomocy dedykowanego agenta oraz kreowanie polityk dostępu do sieci w zależność od wyników skanowania.
20. Wymagane jest zapewnienie wsparcia technicznego oraz aktualizacji oprogramowania na wszystkie funkcje systemu zarządzania na okres minimum 3 lat. Całość świadczeń serwisowych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
21. **UPS**
	* + 1. Typ obudowy – Rack 2U
			2. Moc wyjściowa czynna – 420 W
			3. Przyłącze wyjściowe – 3 szt
			4. Wymiary (wys. x szer. x gł.) – 88x485x200 mm