Załącznik nr 1c do Formularza oferty

ZSPnr1.271.1.2018

„ZAKUP I DOSTAWA SPRZĘTU KOMPUTEROWEGO DLA ZESPÓŁ SZKÓŁ PONADGIMNAZJALNYCH NR 1 W SIERADZU”

Część III: „Zakup i dostawa sprzętu i osprzętu informatycznego ”

1. **Przełącznik dostępowy sieci LAN warstwy 3**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Przełącznik dostępowy sieci LAN 8 portowy warstwy 3	Nazwa …….
Charakterystyka: **Przełącznik dostępowy sieci LAN 8 portowy warstwy 3, szt.9** urządzenie o stałej konfiguracji min.512 MB pamięci DRAM oraz 128MB pamięci Flash wydajność przełączania (full-duplex) co najmniej 32 Gbps oraz przepustowość co najmniej 17,9 Mpps dla pakietów 64 bajtowych; co najmniej 8 portów 10/100/1000 Gigabit Ethernet; dodatkowo dwa porty 1G miedziane plus dwa porty 1G SFP wyposażone w przewód konsolowy do zarzadzania automatyczne wykrywanie przeplotu (AutoMDIX) na portach miedzianych wbudowane narzędzia do diagnozy okablowania na portach miedzianych (time domain reflector) obsługa co najmniej 1023 sieci VLAN i 4000 VLAN ID obsługa mechanizmów dystrybucji informacji o sieciach VLAN pomiędzy przełącznikami obsługa protokołów sieciowych zgodnie ze standardami: - IEEE 802.1x - IEEE 802.1s	

- IEEE 802.1w - IEEE 802.3x full duplex dla 10BASE-T i 100BASE-TX - IEEE 802.3ad - IEEE 802.1D - IEEE 802.1p - IEEE 802.1Q - IEEE 802.3 10BASE-T - IEEE 802.3u 100BASE-TX - IEEE 802.3z 1000BASE-X - IEEE 802.3ab 100BASE-T mechanizmy związane z zapewnieniem jakości usług w sieci: - obsługa co najmniej ośmiu kolejek sprzętowych, wyjściowych dla różnego rodzaju ruchu - mechanizm automatycznej konfiguracji portów do obsługi VoIP - możliwość ograniczania pasma dostępnego na port (rate limiting) dla ruchu wejściowego i wyjściowego mechanizmy związane z zapewnieniem bezpieczeństwa sieci: - dostęp do urządzenia przez konsolę szeregową, SSHv2 i SNMPv3 - możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS lub TACACS+ -możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports) z pozostawieniem możliwości komunikacji z portem nadrzędnym (designated port) lub funkcjonalność private VLAN (w ramach portu) - monitorowanie zapytań i odpowiedzi DHCP (tzw. DHCP Snooping) - możliwość tworzenia portów monitorujących,	

pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika - obsługa list kontroli dostępu (ACL) z uwzględnieniem adresów MAC i IP, portów TCP/UDP bez spadku wydajności urządzenia - min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend) - współpraca z systemami kontroli dostępu do sieci typu NAC, itp. obsługa ruchu multicast z wykorzystaniem IGMPv3 obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP możliwość uruchomienia funkcji serwera DHCP plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian możliwość zarządzania przy pomocy bezpłatnej aplikacji graficznej dostarczanej przez producenta możliwość montażu w szafie 19” (dostarczenie odpowiednich mocowań jest wymagane w ramach tego postępowania) obudowa wykonana z metalu **Wymogi**: Wszystkie urządzenia dostarczone przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producenta sprzętu na rynek Polski, co oznacza, że będzie on sprzętem nowym (nie będzie on sprzętem odnowionym (refurbished), nie będzie on sprzętem pochodzącym z recyklingu) i będzie posiadał wymagany pakiet usług gwarancyjnych producenta długości min. 1 rok kierowany do	

użytkowników z obszaru Rzeczypospolitej Polskiej. Spełnienie powyższego wymogu będzie potwierdzone oświadczeniem producenta sprzętu, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży z Polski, które Wykonawca dostarczy w języku polskim do Zamawiającego najpóźniej w dniu dostawy oferowanego sprzętu. Oświadczenie musi zawierać numery seryjne dostarczonych urządzeń. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich. W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umowa, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację) oraz zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych. Jeżeli inspekcja, o której mowa powyżej wykaże, ze korzystanie z produktów narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję. Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umowa oraz roszczeń odszkodowawczych.	

2. **Adapter USB-RS-232**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Adapter USB-RS-232	Nazwa ……

Charakterystyka: **Adapter USB-RS-232 - 12szt** Wymagania: Musi być kompatybilny z systemami: Windows 10, Windows 7, Windows Vista, Windows XP, Mac OS i Linux Musi zapewniać minimalną prędkość przesyłu: 1Mbps W zestawie musi znajdować się 80 cm kabel USB A M / USB A F Musi być kompatybilny z standardem USB 2.0 Musi być kompatybilny z standardem RS232 Musi być kompatybilny z urządzeniami typu PDA i modem Adapter musi wspierać funkcję remote wake-up i power management	

3. Serwerowe oprogramowanie typu Firewall (zapora sieciowa)

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Serwerowe oprogramowanie typu Firewall (zapora sieciowa)	Nazwa …….
Charakterystyka: Serwerowe oprogramowanie typu Firewall (zapora sieciowa) szt. 3- 1. **Urządzenie pełniące funkcje ściany ogniowej i bramy VPN** 1.1. **Architektura urządzenia** 1.1.1. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. 1.1.2. Urządzenie o konstrukcji modularnej pełniące funkcje bramy VPN i ściany ogniowej (firewall) typu Statefull inspection. Urządzenie musi mieć	

	możliwość dalszej rozbudowy sprzętowej.	
1.1.3.	Urządzenie musi posiadać wbudowane co najmniej 8 miedzianych portów 1000BASE-T.	
1.1.4.	Urządzenie obsługuje interfejsy VLAN-IEEE 802.1q na interfejsach fizycznych – minimum 30 sieci VLAN	
1.1.5.	Urządzenie wyposażone w moduł sprzętowego wsparcia szyfrowania 3DES i AES oraz licencje na szyfrowanie 3DES/AES	
1.1.6.	Urządzenie musi posiadać dedykowany dla zarządzania port konsoli	
1.1.7.	Urządzenie musi posiadać dedykowany dla zarządzania port Ethernet 10/100/100 (Out-of-Band Management)	
1.1.8.	Urządzenie musi posiadać co najmniej 1 port USB 2.0 i umożliwiać podłączenie do niego zewnętrznej pamięci flash do kopiowania plików z i na wewnętrzną pamięć flash urządzenia.	
1.1.9.	Urządzenie musi być wyposażone w co najmniej 8GB pamięci flash.	
1.1.10.	Urządzenie musi być wyposażone w co najmniej 4GB pamięci RAM.	
1.1.11.	Urządzenie musi być wyposażone w wielordzeniowy procesor.	
1.2.	**Obudowa**	
1.2.1.	Urządzenie musi mieć metalową obudowę bez wentylatora.	
1.2.2.	Urządzenie ma możliwość instalacji w szafie typu rack 19”.	
1.2.3.	Wysokość urządzenia nie większa niż 1U	
1.2.4.	Urządzenie musi być przystosowane do pracy w zakresie temperatur 5-40	

stopni Celsjusza 1.2.5. Urządzenie na panelu czołowym musi posiadać świetlną sygnalizację co najmniej następujących stanów urządzenia: 1.2.5.1. wystąpiła awaria zasilacza, 1.2.5.2. wystąpiła krytyczna awaria urządzenia, 1.2.6. Urządzenie musi umożliwiać monitorowanie temperatury procesorów urządzenia, temperatury zasilacza/zasilaczy. 1.3. **Wydajność urządzenia** 1.3.1. Przepustowość teoretyczna firewall'a dla ruchu IPv4 i ruchu IPv6 musi być na poziomie 750 Mb/s, a dla ruchu rzeczywistego (tzw. ruch multiprotocol) nie mniej niż 300 Mb/s. 1.3.2. Urządzenie musi obsługiwać co najmniej 5.000 nowych połączeń na sekundę. 1.3.3. Urządzenie musi obsługiwać co najmniej 20.000 równoczesnych połączeń. 1.3.4. Urządzenie dla pakietów o rozmiarze 64 bajtów musi oferować wydajność nie mniejszą niż 240.000 pakietów na sekundę. 1.3.5. Urządzenie musi być wyposażone w sprzętowy układ odciążający procesor urządzenia przy wykonywaniu operacji szyfrowania algorytmami DES/3DES/AES i oferować wydajność szyfrowania nie mniejszą niż 100Mbps. 1.3.6. Urządzenie musi umożliwiać równoczesną obsługę co najmniej 10 tuneli VPN wykorzystujących IPsec. 1.4. **Funkcjonalność urządzenia**	

1.4.1.	Urządzenie musi działać pod kontrolą 64-bitowego dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia	
1.4.2.	Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji	
1.4.3.	Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory	
1.4.4.	Urządzenie musi posiadać możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos	
1.4.5.	Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej	
1.4.6.	Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access)	
1.4.7.	Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.	
1.4.8.	Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości 256, 384 i 512 bitów.	
1.4.9.	Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM) i Galois Message Authentication Code (GMAC).	
1.4.10.	Urządzenie musi obsługiwać protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19, 20 i 21.	

1.4.11. Urządzenie musi obsługiwać protokół DSA w przestrzeni krzywych eliptycznych (ECDSA)	
1.4.12. Urządzenie musi zapewniać w zakresie SSL VPN weryfikację uprawnień stacji do zestawiania sesji, poprzez weryfikację jej cech, co najmniej:	
1.4.12.1. OS - System operacyjny	
1.4.12.2. IP Address Check - adres z jakiego następuje połączenie	
1.4.12.3. File Check - pliki w systemie.	
1.4.12.4. Registry Check - wpisy w rejestrze systemu Windows.	
1.4.12.5. Certificate Check - zainstalowane certyfikaty	
1.4.13. Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN	
1.4.14. Oprogramowanie klienta VPN (IPSec oraz SSL) ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows (7, XP – wersje 32 i 64-bitowe) i Linux i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.	
1.4.15. Oprogramowanie klienta VPN obsługuje protokoły szyfrowania 3DES/AES	
1.4.16. Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połączenia klientem VPN (wyłączanie tzw. split-tunnelingu)	
1.4.17. Urządzenie ma możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI	
1.4.18. Urządzenie musi umożliwiać wdrożenia w scenariuszu z	

routingiem asymetrycznym.	
1.4.19. Urządzenie obsługuje protokół NTP	
1.4.20. Urządzenie współpracuje z serwerami CA	
1.4.21. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego. Urządzenie wspiera translację adresów (NAT) dla ruchu multicastowego	
1.4.22. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv6 na IPv6, z IPv4 na IPv4, z IPv4 na IPv6.	
1.4.23. Urządzenie musi umożliwiać więcej niż 65535 dynamicznych translacji PAT do pojedynczego zewnętrznego adresu IP.	
1.4.24. Urządzenie musi umożliwiać konfigurację czasu ważności translacji PAT.	
1.4.25. Urządzenie wykonując dynamiczne translacje PAT do puli zewnętrznych adresów IP, musi równomiernie korzystać ze wszystkich zdefiniowanych w puli adresów.	
1.4.26. Urządzenie zapewnia funkcjonalność stateful failover dla ruchu VPN	
1.4.27. Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli co najmniej następujących usług:	
1.4.27.1. Hypertext Transfer Protocol (HTTP),	
1.4.27.2. File Transfer Protocol (FTP),	
1.4.27.3. Extended Simple Mail Transfer Protocol (ESMTP),	
1.4.27.4. Domain Name System (DNS),	
1.4.27.5. Simple Network Management	

Protocol v 1/2/3 (SNMP), 1.4.27.6. Internet Control Message Protocol (ICMP), 1.4.27.7. SQL*Net, 1.4.27.8. inspekcji protokołów dla ruchu voice/video – H.323 (włącznie z H.239), SIP, MGCP, RTSP 1.4.28. Urządzenie umożliwia zaawansowaną normalizację ruchu TCP: 1.4.28.1. poprawność pola TCP ACK(invalid-ack) 1.4.28.2. poprawność sekwencjonowania segmentów TCP (seq-past-window) 1.4.28.3. poprawność ustanawiania sesji TCP z danymi (synack-data) 1.4.28.4. limitowanie czasu oczekiwania na segmenty nie w kolejności 1.4.28.5. poprawność pola MSS (exceed-mss). 1.4.28.6. poprawność pola długości TCP 1.4.28.7. poprawność skali okna segmentów TCP non-SYN 1.4.28.8. poprawność wielkości okna TCP 1.4.29. Urządzenie musi umożliwiać zaawansowane badanie stanu każdej sesji TCP w zakresie: 1.4.29.1. sprawdzania opcji TCP, usuwania opcji TCP i odrzucania segmentów z opcjami TCP 1.4.29.2. poprawności pola TCP ACK 1.4.29.3. poprawności sekwencjonowania segmentów TCP (seq-past-window) ze wsparciem mechanizmów akceleracji sieci WAN wprowadzających przesunięcie numerów sekwencyjnych TCP	

1.4.29.4. weryfikacji sumy kontrolnej segmentu TCP 1.4.29.5. weryfikacji pola TCP SACK ALLOW 1.4.29.6. weryfikacji wielkości okna TCP 1.4.29.7. usuwania flagi URG 1.4.29.8. usuwania segmentów przekraczających maksymalny rozmiar (MSS) 1.4.29.9. usuwania segmentów z flagą SYN i z flagami SYN/ACK, jeśli zawierają one dane 1.4.30. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów. 1.4.31. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych półotwartych połączeń TCP zestawionych do hosta lub do grupy hostów. 1.4.32. Urządzenie musi umożliwiać zresetowanie otwartego połączenia TCP, jeśli przez określony okres czasu przez połączenie nie przesyłano żadnych danych. 1.4.33. Urządzenie musi umożliwiać inspekcję ruchu HTTP w zakresie: 1.4.33.1. zgodności z formalną definicją protokołu 1.4.33.2. ukrywania nagłówka Server w odpowiedzi HTTP 1.4.33.3. filtrowania dopuszczalnych metod HTTP 1.4.33.4. filtrowania dopuszczalnych typów MIME 1.4.33.5. filtrowania dopuszczalnych adresów URL 1.4.34. Urządzenie musi umożliwiać	

inspekcję ruchu SMTP w zakresie:	
1.4.34.1. zgodności z formalną definicją protokołu ESMTP	
1.4.34.2. ukrywania wiadomości powitalnej serwera	
1.4.34.3. filtrowania długości wydawanych komend	
1.4.34.4. filtrowania listy odbiorców dłuższej niż określona liczba	
1.4.34.5. filtrowania długości adresu nadawcy	
1.4.34.6. filtrowania długości pola MIME	
1.4.34.7. filtrowania dopuszczalnych typów MIME	
1.4.35. Urządzenie musi umożliwiać inspekcję ruchu DNS w zakresie:	
1.4.35.1. zgodności z formalną definicją protokołu DNS	
1.4.35.2. filtrowania długości wiadomości	
1.4.35.3. filtrowania po typie zapytania	
1.4.35.4. randomizowania numeru identyfikacyjnego wiadomości	
1.4.35.5. weryfikacji zgodności numeru indentyfikacyjnego zapytania i odpowiedzi	
1.4.35.6. blokowania innych odpowiedzi niż pierwsza (ochrona przed atakiem dns spoofing i dns poisoning)	
1.4.36. Urządzenie ma możliwość blokowania aplikacji (np. peer-to-peer czy „internetowy komunikator") wykorzystujących port 80	
1.4.37. Urządzenie zapewnia obsługę i kontrolę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP	

1.4.38. Urządzenie ma możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe	
1.4.39. Urządzenie zapewnia wsparcie stosu protokołów IPv6 w tym:	
1.4.39.1. dla list kontroli dostępu dla IPv6	
1.4.39.2. możliwości filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Typ 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload	
1.4.39.3. wspiera inspekcję protokołu IPv6, pracując w trybie transparentnym	
1.4.39.4. wspiera realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6	
1.4.40. Urządzenie umożliwia współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik, o wielkości przekraczającej 4KB	
1.4.41. Urządzenie obsługuje routing statyczny i dynamiczny (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).	
1.4.42. Urządzenie musi obsługiwać ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania list kontroli dostępu dla ruchu multicastowego.	
1.4.43. Urządzenie musi umożliwiać konfigurację w roli serwera DHCP.	
1.4.44. Urządzenie musi umożliwiać funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay) dla IPv4 i IPv6.	
1.4.45. Urządzenie umożliwia zbieranie informacji o czasie (timestamp) i	

ilości trafień pakietów w listy kontroli dostępu (ACL)	
1.4.46. Urządzenie umożliwia konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie	
1.4.47. Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu	
1.4.48. Listy kontroli dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:	
1.4.48.1. źródłowy i docelowy adres IPv4	
1.4.48.2. źródłowy i docelowy adres IPv6	
1.4.48.3. źródłowy i docelowy numer portu UDP	
1.4.48.4. źródłowy i docelowy numer portu TCP	
1.4.48.5. nazwy domenowej hosta źródłowego lub docelowego	
1.4.48.6. nazwa użytkownika w usłudze katalogowej Microsoft Active Directory	
1.4.48.7. nazwa grupy w usłudze katalogowej Microsoft Active Directory	
1.4.48.8. czas	
1.4.49. Urządzenie nie może posiadać żadnych ograniczeń na liczbę reguł dostępu jakie mogą być równocześnie wykorzystywane.	
1.4.50. Urządzenie musi umożliwiać inspekcję ruchu IPv4 z wykorzystaniem nagłówków: End of Options List, No Operation, Router Alarm.	
1.4.51. Urządzenie musi umożliwiać	

inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload.	
1.4.52. Jeśli pakiet IPv4/IPv6 został pofragmentowany, urządzenie musi odtworzyć oryginalny pakiet kontrolując przy tym kolejność fragmentów i ich intergralność .	
1.4.53. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby równocześnie odtwarzanych z fragmentów pakietów IPv4/IPv6 per każdy interfejs urządzenia realizujący usługę firewalla.	
1.4.54. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby fragmentów w ramach jednego odtwarzanego pakietu.	
1.4.55. Urządzenie musi umożliwiać skonfigurowanie maksymalnego dopuszczalnego okresu czasu, w którym musi otrzymać wszystkie fragmenty niezbędne do odtworzenia pakietu.	
1.4.56. Urządzenie umożliwia pominięcie stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu	
1.4.57. Urządzenie wspiera Proxy dla protokołu SCEP i umożliwia zautomatyzowany proces pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN	
1.4.58. Urządzenie wspiera użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie Microsoft AD, bezpośrednio lub poprzez ACS, co najmniej dla obsługi sytuacji	

wygaśnięcia terminu ważności hasła w systemie Microsoft AD, umożliwiając zmianę przeterminowanego hasła.	
1.4.59. Urządzenie obsługuje IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode. Ponadto urządzenie wspiera protokół IKEv2 (Internet Key Exchange w wersji 2) dla połączeń zdalnego dostępu VPN oraz site-to-site VPN opartych o protokół IPSec	
1.4.60. Urządzenie musi obsługiwać ramki Ethernet typu Jumbo (o rozmiarze 9216 bajtów).	
1.4.61. Urządzenie musi obsługiwać ramki XOFF zgodnie z definicją standardu 802.3x.	
1.4.62. Urządzenie musi umożliwiać konfigurację następujących mechanizmów zarządzania jakością przesyłania danych (Quality of Service):	
1.4.62.1. Urządzenie obsługuje mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu - obsługa kolejki priorytetowej o konfigurowalnej długości per każdy interfejs urządzenia realizący usługę firewalla– pakiety umieszczone w tej kolejce zostaną obsłużone przed innymi pakietami umieszczonymi w innych kolejkach	
1.4.62.2. policing – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez odrzucanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps. Policing musi być obsługiwany dla ruchu wchodzącego i wychodzącego na każdym interfejsie urządzenia	

realizującym usługę firewalla.

1.4.62.3. shaping – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez buforowanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps konfigurowalną z granularnością co najmniej 8kbps. Zbuforowane pakiety są wysyłane w późniejszym okresie czasu, gdy sumaryczna przepustowość strumieni danych będzie niższa niż zadana wartość w bps. Shaping musi być obsługiwany co najmniej dla ruchu wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.

1.4.63. Urządzenie musi obsługiwać protokół WCCPv2.

1.5. **Funkcjonalność urządzenia - NGFW**

1.5.1. Urządzenie musi zapewniać funkcjonalności tzw, Next-Generation firewall w zakresie nie mniejszym niż

1.5.1.1. System automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control)

1.5.1.2. System IPS

1.5.2. System musi posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. Wymagane jest by system tworzył kontekst z wykorzystaniem co najmniej poniższych parametrów

1.5.2.1. Wiedza o użytkownikach – uwierzytelenienie

1.5.2.2. Wiedza o urządzeniach – pasywne skanowanie ruchu	
1.5.2.3. Wiedza o urządzeniach mobilnych	
1.5.2.4. Wiedza o aplikacjach wykorzystywanych po stronie klienta	
1.5.2.5. Wiedza o podatnościach	
1.5.2.6. Wiedza o bieżących zagrożeniach	
1.5.3. System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM	
1.5.4. System wykrywania aplikacji AVC musi	
1.5.4.1. posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych	
1.5.4.2. zapewniać wydajność co najmniej 250Mbps	
1.5.4.3. pozwalać na tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego z którego korzysta użytkownik oraz wykorzystywanych usług	
1.5.4.4. pozwalać na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji	
1.5.4.5. umożliwiać współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.	
1.5.5. System IPS musi	

1.5.5.1. Posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system) 1.5.5.2. posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu) 1.5.5.3. posiadać możliwość wykrywania i uniemożliwiać szeroką gamę zagrożeń w tym co najmniej 1.5.5.3.1. złośliwe oprogramowanie, 1.5.5.3.2. skanowanie sieci, 1.5.5.3.3. ataki na usługę VoIP, 1.5.5.3.4. próby przepełnienia bufora, 1.5.5.3.5. ataki na aplikacje P2P, 1.5.5.3.6. zagrożenia dnia zerowego, itp.) 1.5.5.4. posiadać możliwość wykrywania modyfikacji znanych ataków (sygnatury) jak i te nowo powstałe, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna) 1.5.5.5. zapewniać co najmniej poniższe sposoby wykrywania zagrożeń 1.5.5.5.1. sygnatury ataków opartych na exploitach, 1.5.5.5.2. reguły oparte na zagrożeniach, 1.5.5.5.3. mechanizm wykrywania anomalii w protokołach 1.5.5.5.4. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego 1.5.5.6. mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu	

1.5.5.7. posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives).	
1.5.5.8. mieć możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń	
1.5.5.9. posiadać wiele możliwości reakcji na zdarzenia takie jak:	
1.5.5.9.1. tylko monitorowanie,	
1.5.5.9.2. blokowanie ruchu zawierającego zagrożenia,	
1.5.5.9.3. zastąpienie zawartości pakietów	
1.5.5.9.4. zapisywanie pakietów	
1.5.5.10. mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6	
1.5.5.11. posiadać możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - co najmniej powinna być zbierana	
1.5.5.11.1. informacja o systemach operacyjnych,	
1.5.5.11.2. informacja o serwisach,	
1.5.5.11.3. informacja o otwartych portach, aplikacjach	
1.5.5.11.4. informacja o zagrożeniach	
1.5.5.12. posiadać możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty,	

usługi oraz ilość przesłanych danych	
1.5.5.13. zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.	
1.5.5.14. posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji	
1.5.5.15. zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego	
1.5.5.16. zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne	
1.5.5.17. zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie	
1.5.5.18. być zarządzany tylko poprzez system centralnego zarzadzania za pomocą szyfrowanego połączenia	
1.5.5.19. zapewniać obsługę reguł Snort	
1.5.5.20. Zapewniać możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS	
1.5.5.21. Zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)	
1.5.5.22. Zapewniać mechanizmy	

automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa	
1.5.5.23. Posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewalla dla uzyskania pełnej widoczności ruchu – w szczególności musi posiadać możliwość pracy w trybie failover firewalla oraz w trybie klastrowania	
1.5.5.24. System IPS powinien pozwalać na pracę z przepustowością co najmniej 125Mbps przy jednoczesnym działaniu AVC	
1.6. **Zarządzanie i konfiguracja**	
1.6.1. Urządzenie musi umożliwiać zarządzanie:	
1.6.1.1. przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.	
1.6.1.2. przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji	
1.6.1.3. programowo przez interfejs API dostępny przy pomocy protokołu https	
1.6.1.4. przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji	
1.6.2. Zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.	
1.6.3. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.	
1.6.4. Urządzenie musi umożliwiać konfigurację maksymalnej	

	równoczesnej liczby sesji zdalnego zarządzania.	
1.6.5.	Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.	
1.6.6.	Urządzenie musi umożliwiać wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.	
1.6.7.	Urządzenie musi mieć możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG. Wymagane jest wsparcie szyfrowanej transmisji wiadomości SYSLOG przy pomocy SSL/TLS.	
1.6.8.	Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow v9 (RFC 3954)	
1.6.9.	Urządzenie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+ oraz obsługuje mechanizmy AAA (autentykacja, autoryzacja, accounting) przy współpracy z systemem Cisco ACS	
1.6.10.	Dostęp do urządzenia jest możliwy przez SSH	
1.6.11.	Urządzenie obsługuje protokół SNMP v 1/2/3	
1.6.12.	Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.	
1.6.13.	Urządzenie umożliwia zrzucenie obecnego stanu programu (coredump) dla potrzeb	

diagnostycznych 1.6.14. Urządzenie posiada wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łącznością w sieciach IP 1.6.15. Urządzenie musi umożliwiać uwierzytelnienie i konfigurację poziomu dostępu administratora w oparciu o role (ang. Role Bases Access Control) z wykorzystaniem bazy danych użytkowników zdefiniowanej lokalnie na urządzeniu lub na zewnętrznych serwerach dostępnych przy pomocy protokołów RADIUS i TACACS+. 1.6.16. Urządzenie musi posiadać zaawansowaną instrumentację pozwalającą na uzyskanie szczegółowej informacji o obciążeniu CPU przez każdy z procesów oddzielnie, z podziałem na procesy, w interwałach czasowych 5 minut, 1 minuta i 5 sekund.	

4. **Nazwa urządzenia**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Telefon internetowy VoIP	Nazwa …….
Charakterystyka: Telefon internetowy VoIP szt. 9 1. Urządzenie musi posiadać możliwość podłączenia słuchawek nagłownych poprzez dedykowane gniazdo dla słuchawek; 2. Obudowa urządzenia w kolorze ciemnym (czarny lub grafit); 3. Urządzenie musi wspierać kodeki audio co najmniej określone przez standardy G.711u, G.729a; 4. Urządzenie musi posiadać wyświetlacz	

graficzny o rozdzielczości co najmniej 396 x 162 piksele, umożliwiający wyświetlanie w dwóch liniach informacji na temat aktualnego czasu (data i godzina), ustawień urządzenia oraz stanu połączenia; 5. Urządzenie musi posiadać podświetlane przyciski do informowania o stanie telefonu; 6. Urządzenie powinno umożliwiać obsługę oraz wyświetlanie tekstowych aplikacji XML; 7. Urządzenie musi posiadać możliwość konfiguracji co najmniej 2 linii (numeru telefonicznego); 8. Urządzenie musi na bieżąco w czasie trwania rozmowy umożliwiać wyświetlanie poprzez przeglądarkę internetową informacji diagnostycznych o połączeniu (rodzaj kodeka, liczba wysłanych, odebranych i zgubionych pakietów z próbkami głosowymi, zmienność opóźnienia przesyłania tych pakietów – używane dla celów diagnostycznych w przypadku konieczności diagnozowania przez administratorów problemów z jakością transmisji głosu w systemie telekomunikacyjnym; 9. Urządzenie musi posiadać wbudowany system głośnomówiący (tzw. speakerphone), umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki i działający w trybie fulldupleks; 10. Urządzenie musi mieć możliwość montażu na ścianie; 11. Urządzenie musi posiadać poniższe dedykowane przyciski funkcyjne: a. przycisk dostępu do ustawień urządzenia; b. przycisk ponownego wybierania; c. przycisk przekierowania rozmowy; d. przycisk zawieszenia połączenia; e. przycisk sterujący głośnością; f. przycisk wyłączenia mikrofonu; g. przycisk trybu rozmowy przez system głośnomówiący; 12. Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 100 Mbps, jeden w kierunku przełącznika sieciowego, drugi dedykowany do dołączenia PC; 13. Port przełącznika urządzenia w kierunku przełącznika sieciowego powinien wspierać trunking 802.1Q celem odseparowania ruchu głosu i ruchu danych; 14. Transmisja głosu oraz danych z komputera PC dołączonego do urządzenia muszą	

być przesyłane w dwóch różnych sieciach VLAN; 15. Urządzenie musi umożliwiać zasilanie go z sieci komputerowej LAN zgodnie ze standardem PoE IEEE oraz z wykorzystaniem lokalnych zasilaczy (transformujących napięcie z sieci 230V); 16. Urządzenie musi być energooszczędne i pracować w klasie 1 PoE zgodnie z IEEE 802.3af; 17. Menu urządzenia musi być zrealizowane w języku polskim oraz angielskim, przy czym wymagane jest, aby możliwa była zmiana rodzaju języka menu w zależności od ustawień w profilu zalogowanego na nim użytkownika; 18. Urządzenie musi wspierać funkcjonalność wykrywania ciszy (Voice Activity Detection) i niewysyłaniu pakietów głosowych IP w czasie jej trwania; 19. Urządzenie musi wspierać funkcjonalność generowania szumu (Comfort Noise Generation) podczas rozmowy w czasie trwania ciszy; 20. Urządzenie musi posiadać lampkę sygnalizującą oczekującą wiadomość poczty głosowej (MWI); 21. Urządzenie musi zapewniać wsparcie dla protokołu sterującego SIP; 22. Urządzenie musi zapewniać wsparcie dla protokołów sieciowych TFTP, DHCP, DNS;	

5. **Dysk do NAS**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Dysk do NAS	Nazwa
Charakterystyka: **Dysk do NAS (5szt.)** Wymagania: format szerokości: 3.5 cala typ: magnetyczny pojemność min. 8000 GB interfejs: Serial ATA III prędkość obrotowa min. 7200 obr./min.	

pamięć cache min. 256 MB min. transfer zewnętrzny 600 MB/s Gwarancja min. 3 lata Uwaga: Dysk musi być kompatybilny z urządzeniem serwer plików NAS, opisanym w pozycji 19	

6. **Wi-Fi USB 3.0 Adapter**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Wi-Fi USB 3.0 Adapter	Nazwa
Charakterystyka: **Wi-Fi USB 3.0 Adapter 12 szt.** Wymagania: Musi posiadać 1 port USB 3.0 Typu A Musi posiadać przycisk WPS Musi posiadać diodę LED Musi posiadać 3 anteny nadawcze i odbiorcze Musi pracować w paśmie: 2.4GHz: IEEE 802.11b, 802.11g, 802.11n 5GHz: IEEE 802.11ac, 802.11a, 802.11n Musi zapewnić szyfrowanie 64/128-bit WEP,WPA & WPA2 min. szybkość transmisji danych : 1300 Mbps maksymalne wymiary: szerokość 18 mm wysokość 27 mm głębokość 21 mm	

7. **Zasilacz awaryjny UPS**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Zasilacz awaryjny UPS	Nazwa …….

Charakterystyka:

Zasilacz awaryjny UPS (1 szt.)

Wymagania:

- Moc wyjściowa pozorna min. 3000VA
- Moc wyjściowa czynna min. 1950W
- Musi posiadać 6 złącz wyjściowych typu IEC320 C13
- Liczba faz napięcia (wejście / wyjście) musi wynosić: 1/1
- Obudowa typu Rack
- Musi móc pracować w temperaturze między 0 ÷ +40 °C
- Musi być Chłodzony Naturalnie
- Napięcie znamionowe musi wynosić: 230V AC
- Częstotliwość znamionowa napięcia wejściowego musi wynosić: 50 Hz
- Progi przełączania: sieć – UPS muszą wynosić podstawowo ~ 160 ÷ 264 V (~ 145 ÷ 280 V) ± 2 %
- Progi przełączania się sieci oraz zakres napięcia wyjściowego powinny być możliwe do zmiany
- Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja - praca sieciowa musi wynosić podstawowo ~ 184 ÷ 264 V (~ 167 ÷ 280 V) ± 2 %
- Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja - praca rezerwowa musi wynosić ~230 V ± 5 %
- Kształt napięcia wyjściowego przy pracy rezerwowe musi być Sinusoidalny.
- Częstotliwość znamionowa napięcia wyjściowego musi wynosić: 50 Hz
- Zakres częstotliwości (tolerancja) - praca rezerwowa musi mieścić się w :

50 Hz ± 1Hz

• Napięcie wyjściowe musi być filtrowane przez LC, Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy • Czas przełączenia na pracę rezerwową musi być poniżej 3 ms • Czas powrotu na pracę sieciową musi wynosić 0 ms • W Ups Muszą znajdować się akumulatory: 12 V / 7 Ah VRLA w liczbie 4 • Minimalna całkowita pojemność akumulatorów wewnętrznych: 7 Ah • MInimalny czas podtrzymywania baterii wewnętrznych dla 100%/80%/50% ma wynosić: 3/4/8 min • Napięcie nominalne obwodu DC musi wynosić: 48V DC • Maksymalny czas ładowania baterii wewnętrznych Ups - po 80% wyładowaniu baterii musi wynosić: 7h • Musi zawierać zabezpieczenia wejściowe takie jak :Przeciwzwarciowy - Bezpiecznik automatyczny 16 A / 250 V AC oraz Przeciwprzepięciowe • Musi zawierać zabezpieczenie wyjściowe Elektroniczne – przeciwzwarciowe i przeciążeniowe • UPS musi posiadać przyłącze zasilania typu IEC320 C20 • Musi posiadać interfejs komunikacyjny: USB 2.0 • Musi posiadać filtr teleinformatyczny: LAN 1 Gbit/s • Musi posiadać oprogramowanie monitorująco-zarządzające: PowerSoft Professional • Maksymalna wysokość Ups: 132 mm (3U) • Maksymalna szerokość: 500 mm(19”) • Maksymalną głębokość: 400 mm	

● Maksymalna waga urządzenia: 31 KG	

8. Tester kabli

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Tester kabli	Nazwa
Charakterystyka: **Tester kabli (1 szt.)** Wymagania: ● Musi posiadać funkcję sprawdzania układu żył, długości do usterki, ID kabli oraz urządzeń licznikowych ● Musi posiadać funkcję rozpoznawania przewodów telefonicznych, Ethernet 10/100/1000 oraz PoE ● Musi móc sprawdzać typ i miejsce usterki (nieprawidłowy układ żył, odwrotna polaryzacja, rozdział par, zwarcia, przerwy) ● Musi mieć możliwość pomiaru odległość od połączenia, przerwy lub zwarcia ● Musi posiadać wskaźnik łącza sieciowego dla przełączników 10/100/1000,telefonów analogowych, zwarć, wtyków końcowych ● Musi mieć funkcję cyfrowego testowania tonowego ● Musi posiadać funkcję rozpoznawania PoE w tym potrafi wykluczyć niedostateczne napięcie jako przyczynę problemu ● Musi posiadać interfejs: Skrętka-UTP, FTP, SSTP, 8-stykowe wkładki modułowe typu RJ-45 i RJ-11;kabel koncentryczny wkładki typu F kabli o impedancji 75/50/93 Ohm ● Musi pozwalać na wskazanie prędkości	

transmisji portów Ethernet 802.3 (10/100/1000) ● Musi pozwalać na test kabli o długości do 460m z układem żył zgodną z normą TIA-568A/B oraz kodowany wtyk końcowy ● Zasilanie elektryczne: 2 x LR6/AA ● Maksymalne wymiary dł. x szer. x wys.: 163 x 76 x 36 mm ● Maksymalna waga: 363 g	

10. Gniazdo natynkowe pasywne

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	
Nazwa: Gniazdo natynkowe pasywne	Nazwa ……
Charakterystyka: **Gniazdo natynkowe pasywne (18 szt.)** Wymagania: Modułowe gniazdo ścienne, CAT6 typ ekranowania S/FTP standard RJ-45 (10/100/1000Mb/s) Musi posiadać 2 porty RJ45 wymiary maksymalne 80 x 80 x 50 mm kolor biały	

10. Przełącznik (Switch) 24 porty 10 szt. Przełącznik warstwy 2

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Przełącznik (Switch) 24 porty. Przełącznik warstwy 2	Nazwa
Charakterystyka: **Przełącznik (Switch) 24 porty 10 szt. Przełącznik warstwy 2** Wymagania: ● 24 RJ-45 10/100/1000 ports (IEEE	

802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: pół lub pełny; 1000BASE-T: tylko pełny ● 2 SFP 100/1000 Mbps ports (IEEE 802.3z Type 1000BASE-X, IEEE 802.3u Type 100BASE-FX) ● Częstotliwość procesora min. 400 Mhz ● Pamięć SDRAM min. 128 MB ● Pamięć flash min. 16 MB ● Pamięć bufora pakietów min. 1.5 MB ● Opóźnienie dla 100 Mb < 7 µs dla LIFO 64-bajtowych pakietów. ● Opóźnienie dla 1000 Mb < 2 µs dla LIFO 64-bajtowych pakietów. ● Przekierowanie pakietów min. 38.6 Mpps dla 64-bajtowych pakietów ● Przepustowość przełącznika min. 52 Gig /s ● Minimalna liczba wpisów do tablicy MAC: 8000 ● Musi móc pracować w zakresie temperatur od 0°C do 40°C ● Nie może posiadać wentylatorów ● Musi być zarządzany przez przeglądarkę internetową ● Musi mieścić się w wysokość 1U ● Zawiera funkcje CPU DoS Protection ● Częstotliwość wejściowa AC 50/60 Hz ● Napięcie wejściowe AC 100 - 127 / 200 - 240 VAC ● Maksymalny pobór mocy 22 W Protokoły: ● IEEE 802.1D Spanning Tree Protocol ● IEEE 802.1p Priority	

• IEEE 802.1Q VLANs • IEEE 802.1W Rapid Spanning Tree Protocol • IEEE 802.3ad Link Aggregation Control Protocol (LACP) • IEEE 802.3x Flow Control • IEEE 802.1AB Link Layer Discovery Protocol (LLDP) • RFC 1534 DHCP/BOOTP Interoperation • RFC 2030 Simple Network Time Protocol (SNTP) v4	

11. Router sprzętowy z funkcjami bezpieczeństwa i centrali VoIP

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Router sprzętowy z funkcjami bezpieczeństwa i centrali VoIP	Nazwa …….
Charakterystyka: Router sprzętowy z funkcjami bezpieczeństwa i centrali VoIP szt. 3 Rodzaj urządzenia 1. Musi być urządzeniem pełniącym rolę wielousługowego routera modularnego. Architektura 2. Musi pozwalać na instalację co najmniej: a. co najmniej 2 kart sieciowych z interfejsami, b. 1 wewnętrznego modułu DSP 3. Musi posiadać zainstalowany wewnętrzny sprzętowy moduł akceleracji szyfrowania. 4. Musi posiadać wszystkie interfejsy „aktywne”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i	

konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów. 5. Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową muszą mieć możliwość obsadzenia kartami: a. z portami szeregowymi o gęstości co najmniej 2 porty na moduł, b. z interfejsem ISDN PRI o gęstości 1 portu per moduł, 2 portów per moduł, 4 portów per moduł , c. umożliwiającymi instalację dysków SSD (ten wymóg dotyczy jednego slotu) 6. Slot urządzenia przewidziany pod rozbudowę o moduł z układami DSP musi mieć możliwość obsadzenia modułem: a. o gęstości nie mniejszej niż 256 kanałów, b. pozwalającym na dynamiczne alokowanie DSP do różnych zadań c. posiadającym wsparcie dla usług wideo. 7. Urządzenie musi oferować wydajność min. 50Mbps 8. Urządzenie musi oferować możliwość licencyjnego podwojenia wydajności. Oprogramowanie/funkcjonalności 9. Funkcjonalność procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia) dla co najmniej 3 abonentów, 10. Oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji. 11. Musi posiadać obsługę protokołów routingu IPv4 takich, jak RIPv2, OSPF, BGPv4, OSPF, ISIS, a także routingu statycznego. 12. Musi posiadać obsługę protokołów	

routingu IPv6 takich, jak RIPng, OSPFv3, BGPv4, ISIS, a także routingu statycznego. 13. Musi posiadać obsługę protokołów routingu multicastowego PIM Sparse oraz PIM SSM, a także oraz routingu statycznego. 14. Protokół BGP musi posiadać obsługę 4 bajtowych ASN. 15. Musi posiadać wsparcie dla funkcjonalności Policy Based Routing. 16. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF). 17. Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q. 18. Musi obsługiwać IPv6 w tym ICMP dla IPv6 oraz protokoły routingu IPv6 takie jak RIP, OSPFv3, IS-IS, 19. Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL. 20. Musi umożliwiać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast. 21. Musi posiadać wsparcie dla protokołów WCCP. 22. Musi posiadać obsługę mechanizmu DiffServ. 23. Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu. 24. Musi zapewniać obsługę mechanizmów kolejkowania ruchu: a. z obsługą kolejki absolutnego priorytetu, b. ze statyczną alokacją pasma dla typu ruchu, c. WFQ. 25. Musi obsługiwać mechanizm WRED. 26. Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP	

Precendence dla ruchu tunelowanego. 27. Musi obsługiwać protokół NTP. 28. Musi obsługiwać DHCP w zakresie Client , Server. 29. Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika). 30. Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+. 31. Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (tzw. Embedded Event Manager – EEM, lub odpowiednik). 32. Funkcjonalność EEM musi pozwalać na generowanie akcji takich jak: a. wykonanie komendy z poziomu linii poleceń urządzenia, b. wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej, c. wykonanie skryptu, d. wygenerowanie SNMP trap, 33. Musi posiadać wsparcie dla Layer-2 Tunneling Protocol Version 3. 34. Musi posiadać funkcjonalności bezpieczeństwa sieciowego: a. funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES/AES, b. algorytmy IPSec następnej generacji oparte o krzywe eliptyczne w szczególności: i. Galois Counter Mode Advanced Encryption Standard (GCM-AES) 128/256 bitów, ii. Galois Message Authentication Code (GMAC-AES) 128/256 bitów, iii. Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2,	

c. możliwość konfiguracji tuneli IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2). Wsparcie dla IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych, dla ruchu IPv4 oraz IPv6, d. funkcjonalność VPN musi wspierać tworzenie niezależnych VPN (w tym różnego typu: site-2-site, dynamicznych) per VRF, e. funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall), f. funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall), g. możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym: i. przesyłu, który jest poddawany inspekcji, ii. przesyłu, który jest odrzucany, iii. przesyłu, który jest przenoszony bez inspekcji, h. ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU, i. możliwość logowania pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU, j. możliwość wymuszenia reguł złożoności haseł tworzonych na urządzeniu, 35. Musi posiadać możliwość następujące funkcjonalności poprzez zakup dodatkowej licencji: a. funkcje pozwalające na automatyzację konfiguracji ustawień QoS (w szczególności dla usług VoIP) w postaci automatycznego tworzenia wzorców konfiguracyjnych na potrzeby implementacji QoS, b. funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia "tam i z powrotem"	

(roundtrip, jitter i utraty pakietów), c. możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych, przy czym brama taka musi mieć możliwość pracy w sposób niezależny lub być sterowana przez system centralny procesowania połączeń. Zarządzanie i konfiguracja 36. Musi być zarządzalne za pomocą SNMPv1, SNMPv2, SNMPv3, Telnet, SSH. 37. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Neftflow/JFlow lub odpowiednika. 38. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI). 39. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. Obudowa 40. Musi być wykonana z metalu. Ze względu na warunki w których pracować będzie urządzenie, nie dopuszcza się stosowania urządzeń w obudowie plastikowej. 41. Musi mieć możliwość montażu w szafie 19”. Zasilanie 42. Urządzenie musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacze AC). 43. Urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet	

(tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia (funkcja wymagana). Wyposażenie 44. Urządzenie musi być wyposażone w minimum 2 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN. 45. Jeden z interfejsów musi mieć możliwość pracy z gigabitowym portem światłowodowym definiowanym przez wkładki GBIC, SFP lub równoważne. 46. Urządzenie musi być wyposażone w minimum 4GB pamięci Flash, z możliwością rozszerzenia do min. 8GB 47. Urządzenie musi być wyposażone w minimum 4GB pamięci RAM, z możliwością rozszerzenia do min. 8GB 48. Urządzenie musi mieć możliwość rozbudowy o dysk SSD o pojemności min. 200GB 49. Urządzenie musi mieć możliwość zastosowania zasilacza o mocy co najmniej 260W zapewniającego budżet mocy do zasilania urządzeń PoE 120W 50. Urządzenie musi być wyposażone w minimum jeden port USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych. 51. Wszystkie karty i moduły muszą być objęte wspólnym serwisem producenta przez okres min. 1 rok.	

12. Router sprzętowy

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: **Router sprzętowy**	Nazwa …….

Charakterystyka: Router sprzętowy szt. 9 Rodzaj urządzenia 1. Musi być urządzeniem pełniącym rolę wielousługowego routera modularnego. Architektura 2. Musi pozwalać na instalację co najmniej: a. co najmniej 2 kart sieciowych z interfejsami, b. 1 wewnętrznego modułu DSP 3. Musi posiadać zainstalowany wewnętrzny sprzętowy moduł akceleracji szyfrowania. 4. Musi posiadać wszystkie interfejsy „aktywne”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów. 5. Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową muszą miećmożliwość obsadzenia kartami: a. z portami szeregowymi o gęstości co najmniej 2 porty na moduł, b. z interfejsem ISDN PRI o gęstości 1 portu per moduł, 2 portów per moduł, 4 portów per moduł , c. umożliwiającymi instalację dysków SSD (ten wymóg dotyczy jednego slotu) 6. Slot urządzenia przewidziany pod rozbudowę o moduł z układami DSP musi mieć możliwość obsadzenia modułem: a. o gęstości nie mniejszej niż 256 kanałów, b. pozwalającym na dynamiczne alokowanie DSP do różnych zadań	

c. posiadającym wsparcie dla usług wideo. 7. Urządzenie musi oferować wydajność min. 50Mbps 8. Urządzenie musi oferować możliwość licencyjnego podwojenia wydajności. Oprogramowanie/funkcjonalności 9. Oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji. 10. Musi posiadać obsługę protokołów routingu IPv4 takich, jak RIPv2, OSPF, BGPv4, OSPF, ISIS, a także routingu statycznego. 11. Musi posiadać obsługę protokołów routingu IPv6 takich, jak RIPng, OSPFv3, BGPv4, ISIS, a także routingu statycznego. 12. Musi posiadać obsługę protokołów routingu multicastowego PIM Sparse oraz PIM SSM, a także oraz routingu statycznego. 13. Protokół BGP musi posiadać obsługę 4 bajtowych ASN. 14. Musi posiadać wsparcie dla funkcjonalności Policy Based Routing. 15. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF). 16. Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q. 17. Musi obsługiwać IPv6 w tym ICMP dla IPv6 oraz protokoły routingu IPv6 takie jak RIP, OSPFv3, IS-IS, 18. Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL. 19. Musi umożliwiać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast. 20. Musi posiadać wsparcie dla protokołów	

WCCP. 21. Musi posiadać obsługę mechanizmu DiffServ. 22. Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu. 23. Musi zapewniać obsługę mechanizmów kolejkowania ruchu: a. z obsługą kolejki absolutnego priorytetu, b. ze statyczną alokacją pasma dla typu ruchu, c. WFQ. 24. Musi obsługiwać mechanizm WRED. 25. Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego. 26. Musi obsługiwać protokół NTP. 27. Musi obsługiwać DHCP w zakresie Client , Server. 28. Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika). 29. Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+. 30. Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (tzw. Embedded Event Manager – EEM, lub odpowiednik). 31. Funkcjonalność EEM musi pozwalać na generowanie akcji takich jak: a. wykonanie komendy z poziomu linii poleceń urządzenia, b. wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej,	

c. wykonanie skryptu, d. wygenerowanie SNMP trap, 32. Musi posiadać wsparcie dla Layer-2 Tunneling Protocol Version 3. 33. Musi posiadać możliwość rozbudowy o funkcjonalności bezpieczeństwa sieciowego: a. funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES/AES, b. algorytmy IPSec następnej generacji oparte o krzywe eliptyczne w szczególności: i. Galois Counter Mode Advanced Encryption Standard (GCM-AES) 128/256 bitów, ii. Galois Message Authentication Code (GMAC-AES) 128/256 bitów, iii. Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2, c. możliwość konfiguracji tuneli IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2). Wsparcie dla IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych, dla ruchu IPv4 oraz IPv6, d. funkcjonalność VPN musi wspierać tworzenie niezależnych VPN (w tym różnego typu: site-2-site, dynamicznych) per VRF, e. funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall), f. funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall), g. możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym: i. przesyłu, który jest poddawany inspekcji, ii. przesyłu, który jest odrzucany, iii. przesyłu, który jest przenoszony bez inspekcji, h. ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania	

ruchu docierającego do CPU, i. możliwość logowania pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU, j. możliwość wymuszenia reguł złożoności haseł tworzonych na urządzeniu, 34. Musi posiadać możliwość następujących funkcjonalności poprzez zakup dodatkowej licencji: a. funkcjonalność procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia) dla co najmniej 50 abonentów, b. funkcje pozwalające na automatyzację konfiguracji ustawień QoS (w szczególności dla usług VoIP) w postaci automatycznego tworzenia wzorców konfiguracyjnych na potrzeby implementacji QoS, c. funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia "tam i z powrotem" (roundtrip, jitter i utraty pakietów), d. możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych, przy czym brama taka musi mieć możliwość pracy w sposób niezależny lub być sterowana przez system centralny procesowania połączeń. Zarządzanie i konfiguracja 35. Musi być zarządzalne za pomocą SNMPv1, SNMPv2, SNMPv3, Telnet, SSH. 36. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Neftflow/JFlow lub odpowiednika. 37. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI). 38. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na	

dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. Obudowa 39. Musi być wykonana z metalu. Ze względu na warunki w których pracować będzie urządzenie, nie dopuszcza się stosowania urządzeń w obudowie plastikowej. 40. Musi mieć możliwość montażu w szafie 19". Zasilanie 41. Urządzenie musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacze AC). 42. Urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia (funkcja wymagana). Wyposażenie 43. Urządzenie musi być wyposażone w minimum 2 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN. 44. Jeden z interfejsów musi mieć możliwość pracy z gigabitowym portem światłowodowym definiowanym przez wkładki GBIC, SFP lub równoważne. 45. Urządzenie musi być wyposażone w minimum 4GB pamięci Flash, z możliwością rozszerzenia do min. 8GB 46. Urządzenie musi być wyposażone w minimum 4GB pamięci RAM, z możliwością rozszerzenia do min. 8GB 47. Urządzenie musi mieć możliwość rozbudowy o dysk SSD o pojemności min. 200GB	

48. Urządzenie musi mieć możliwość zastosowania zasilacza o mocy co najmniej 260W zapewniającego budżet mocy do zasilania urządzeń PoE 120W 49. Urządzenie musi być wyposażone w minimum jeden port USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych. 50. Wszystkie karty i moduły muszą być objęte wspólnym serwisem producenta przez okres min. 1 rok.	

13. **Karty do ruterów**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Karty do ruterów	Nazwa …….
Charakterystyka: **Karty do ruterów** 1. Wyposażenie routerów w karty: a. Jedna dwu portowa karta – serial WAN interface zgodny z V.35 2. Wszystkie elementy maja być nowe (nie starsze niż 6 m-cy), pochodzić od tego samego producenta i być dostarczone z autoryzowanego kanału dystrybucji na rynek Polski Uwaga Karty muszą być kompatybilne z routerami z pozycji 11 i 12	

14. **Kodowany zestaw wtyków końcowych 2-7 do mikro skanera**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Kodowany zestaw wtyków końcowych 2-7 do testera sieci	Nazwa ….....

Charakterystyka: **<u>Kodowany zestaw wtyków końcowych 2-7 do mikro skanera (1 szt.)</u>** Wymagania: ● musi być kompatybilny z urządzeniem, opisanym w pozycji 8	

15. **Listwa zasilająca do Szaf 19"**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Listwa zasilająca do Szaf 19"	Nazwa ….....
Charakterystyka: **<u>Listwa zasilająca do Szaf 19" (12 szt.)</u>** Wymagania: ● Minimalna ilość gniazd:8 schuko ● Musi posiadać przednie uchwyty do montażu w szafie rack ● Musi być zbudowana z aluminium ● Musi posiadać kable standard 3m z wtyczką typu IEC 60884 ● Musi posiadać napięcie znamionowe: 16A,250V AC ● Musi pozwalać na obciążenie 3,5 kW ● Musi posiadać wyłącznik zasilania ● Wtyczka zasilająca: łamana	

16. **Miernik mocy optycznej**

Producent model oferowanego urządzenia **……..**

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Miernik mocy optycznej	Nazwa …...

Charakterystyka: **Miernik mocy optycznej (1 szt.)** Wymagania: ● Musi móc dokonywać Pomiarów 1310 nm upstream, 1490/1550 nm downstream ● Zakres pomiaru musi się mieścić +10..-35 dBm dla 1310 nm, +10..-50 dBm dla 1490 nm, +25..-45 dBm dla 1550 nm ● Maksymalna moc wyjścia musi wynosić 15 dBm dla 1310 nm i 1490 nm oraz 25 dBm dla 1550 nm ● Musi zapewnia Krótki czas ustalania wyniku ● Musi posiada Duży wyświetlacz z podświetleniem ● Musi posiadać Pamięć dla 10 kompletów pomiarów ● Zbudowany jest z Kompaktowej i wytrzymałej obudowy ● Waga musi wynosić maksymalnie 0.54Kg ● 12 miesięcy gwarancji, dwuletni okres kalibracji ● Długi czas pracy na bateriach, automatyczny wyłącznik ● Złącze APC	

17. **24 portowy patch panel**

Producent model oferowanego urządzenia **……..**

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: 24 portowy patch panel	Nazwa ……..

Charakterystyka: **24 portowy patch panel (36 szt.)** Wymagania: ● Musi mieć wysokość 1U ● Musi mieć szerokość 19” ● Musi posiadać 24 porty Rj-45 zgodne z kategorią 5e ● Musi posiadać półkę organizacyjną na kable ● Musi mieć mocowanie doczołowe do szyn rackowych ● Musi być koloru czarnego	

18. **Przewody do ruterów**

Producent model oferowanego urządzenia **……..**

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Przewody do ruterów	Nazwa ……
Charakterystyka: **Przewody do ruterów 1 kpl.** Wyposażenie w przewody: Przewód SmartSerial back to back ok. 1m szt.12 Przewód konsolowy z interfejsami RJ45 oraz DB9F szt. 12 Przewód konsolowy USB USB Type A i mini-B szt. 12 Wszystkie elementy maja być nowe (nie starsze niż 6 m-cy), pochodzić od tego samego producenta i być dostarczone z autoryzowanego kanału dystrybucji na rynek Polski	

19. **Serwer plików NAS 1 szt**

Producent model oferowanego urządzenia **……..**

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu

Nazwa: Serwer plików NAS	Nazwa …….
Charakterystyka: **Serwer plików NAS (1 szt.)** Wymagania: ● min. czterordzeniowy procesor 2,1 GHz ● Pamięć SO-DIMM DDR4 min. 4 GB z możliwością rozbudowy do 32 GB ● Musi posiadać sprzętowy mechanizm szyfrowania AES-NI ● Możliwość obsadzenia sześcioma 3,5” lub 2,5” dyskami SATA SSD /HDD oraz z dwoma M.2 2280/2260/2242 SATA SSD 3 ● Musi posiadać 3 porty USB 3.0 oraz 2 gniazda rozszerzeń ● Maksymalne wymiary: Wysokość: 166 mm , Szerokość: 282 mm , głębokość: 236 mm ● Maksymalna waga 5.05 kg ● Musi posiadać 4 złącza 1Gb (RJ-45) ● Musi posiadać funkcję Wake on LAN/WAN, ● Musi posiadać dwa wbudowane wentylatory ● Musi wspierać karty sieciowe 10 Gb/s i kartę rozszerzeń M.2 SATA SSD ● Częstotliwość wejściowa AC 50/60 Hz ● Napięcie wejściowe AC 100-240V ● Musi móc pracować w zakresie temperatur od 5°C do 40°C ● Musi wspierać protokoły sieciowe takie jak: ○ SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™ , L2TP) ● Musi wspierać systemy plików takie jak: ○ Wewnętrzny: Btrfs, ext4 ○ Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT5 ● Minimalny rozmiar pojedynczego wolumenu: 108 TB ● Minimalna liczba migawek systemu: 65	

5366 ● Minimalna liczba wewnętrznych wolumenów: 512 ● Minimalna liczba iSCSI Target: 32 ● Minimalna liczba jednostek iSCSI LUN: 256 ● Obsługa klonowania/migawek jednostek iSCSI LUN ● Obsługiwane typy macierzy: Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 ● Minimalna ilość kont użytkowników lokalnych: 2048 ● Minimalna liczba lokalnych grup: 256 ● Minimalna ilość udostępnionych folderów: 512 ● Minimalna jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000 ● Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) ● Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP ● Musi posiadać możliwość wizualizacji za pomocą VMware vSphere 6, Microsoft Hyper-V , Citrix, OpenStack ● Musi wspierać funkcje Zabezpieczeń: Zaporę, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS ● Musi wspierać klientów używających Windows 7 i 10, Mac OS X 10.10 i nowszych ● Musi wspierać przeglądarki takie jak:Chrome, Firefox, Internet Explorer 10 i nowsze, Safari 10 i nowsze; Safari (iOS 10 i nowsze), Chrome (Android 6.0 i nowsze) ● Serwer FTP musi pozwalać na Kontrolę pasma w połączeniach TCP, własny zakres pasywnych portów FTP, anonimowe FTP, protokoły FTP SSL/TLS i SFTP, uruchamianie przez	

sieć z obsługą TFTP i PXE, logi transferów ● Musi wspierać: DNS Server, RADIUS Server ● Musi zapewniać funkcję Universal Search ● Musi posiadać funkcję Hyper Backup oraz Active Backup for server ● Musi posiadać narzędzia kopii zapasowej takie jak :OS X Time Machine, DSM, Cloud Station Backup ● Musi zapewniać synchronizację folderów współdzielonych minimalnie 8 zadań ● Musi zapewniać synchronizację danych pomiędzy wieloma platformami przy jednoczesnym zachowaniu min. 32 historycznych wersji pliku ● Minimalna liczba jednoczesnych transferów plików:1 000 ● Musi wspierać Jedno- lub dwukierunkową synchronizację z serwerami pamięci masowej w chmurzę firm Amazon S3,Biadu Cloud Box,Box,Dropbox,Google Cloud Storage,Google Drive,hubiC, MegaDisk,Microsoft OneDrive,OpenStack Swift,WebDAV,Yandex Disk ● Minimalnie musi obsługiwać 40 kamer IP ● Musi umożliwiać Wdrożenie i uruchomienie różnych maszyn wirtualnych takich jak:Windows, Linux, Virtual DSM ● Musi umożliwiać konfiguracji dwóch identycznych systemów NAS jako jednego klastera ● Minimalna wymagana liczba migawek folderów współdzielonych: 1024 ● Minimalna wymagana liczba replikacji: 32 ● Musi wspierać funkcję Packet Active Directory Server ● Server VPN musi minimalnie obsługiwać 20 połączeni jednocześnie oraz wspierać protokoły takie jak: PPTP, OpenVPN, L2TP/IPSec	

• Musi posiadać funkcję MailPlus i MailPlus Server • Musi pozwalać na minimalnie 1500 użytkowników aplikacji CHAT • Musi pozwalać na minimalnie 1800 użytkowników aplikacji Office • Musi pozwalać na korzystanie z CalDAV na urządzeniach mobilnych • Musi wspierać porządkowanie notatek w formacie rich text, obsługi wersji, szyfrowanie, udostępnianie, osadzanie multimediów i załączniki • Musi zawierać w zestawie program antywirusowy umożliwiający pełne skanowanie systemu, zaplanowane skanowanie, modyfikacja białej listy, automatyczna aktualizacja definicji wirusów • Musi obsługiwać protokoły pobierania takie jak: BT, HTTP, FTP, NZB, eMule, Thunder, FlashGet, QQDL • Minimalna liczba zadań pobierania: 80 • Musi pozwalać na utrzymywanie min. 30 witryn z funkcjami PHP/MariaDB i obsługą zewnętrznych aplikacji	

20. **Szafa dystrybucyjna**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Szafa dystrybucyjna	Nazwa
Charakterystyka: **Szafa dystrybucyjna (4 szt.)** • szafa stojąca rack 19" 42U 600x1000mm • Drzwi przednie przeszklone z zamkiem • Drzwi tylne stalowe uchylne z zamkiem • Drzwi boczne demontowane na zatrzaskach	

z możliwością montażu zamka • Wyposażenie: 4 wentylatory, 3 półki, listwa zasilająca, 100 koszyków ze śrubami • Zgodność z normami ANSI/EIA RS-310-D, DIN41491 • Zgodność z normami PART1, IEC297-2, DIN41494 • Zgodność z normami PART7, GB/T3047.2-92 • Kompatybilne ze standardami: metrycznym, ETSI oraz międzynarodowym 19” • Szkielet o obciążalności do 800kg • Stalowa blacha zimnowalcowana • Zabezpieczona przed rdzą, utlenianiem, porysowaniem, korozją • Dwa przepusty kablowe - jeden w suficie, drugi w podłodze • Grubość ramy: 1.2 mm • Grubość szyn montażowych: 2.0 mm • Grubość paneli bocznych: 1.2 mm • Grubość szkła: 5 mm • Regulowane nóżki i kółka o dużej wytrzymałości • Dobry poziom wentylacji i rozpraszania ciepła • Stopień ochrony: IP20 • Kompatybilność ze sprzętem różnych producentów • Pełna gama akcesoriów opcjonalnych	

• Musi być koloru czarnego	

21. **Przełącznik światłowodowy dedykowany**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Przełącznik światłowodowy dedykowany	Nazwa ……
Charakterystyka: **Przełącznik światłowodowy dedykowany (1 szt.)** Musi posiadać Interfejsy: - min 8 x 1000Base-X (SFP) - min 4 x GE dual personality (RJ45/SFP) - min 4 x 10GbE (SFP+) Porty zarządzania - 1 x RJ45 Ethernet Management port - 1x Console port - 1x USB2.0 interface Wymagania: - Przepustowość przełącznika min. 111 Gbps - Szybkość przekierowania pakietów min. 82 Mpps - Rozmiar tablicy MAC min. 16 K - Minimalna wielkość ramek Jumbo: 10 KB - Musi móc pracować w zakresie temperatur 0°C~50°C	

- Częstotliwość wejściowa AC 50/60 Hz - Napięcie wejściowe AC 100-240V - Maksymalny pobór mocy <22W (220V/50Hz) - W zestawie musi znajduje się zestaw montażowy dla szaf 19” Cechy warstwy 2 - obsługiwane protokoły: IEEE802.3z(1000BA IEEE802.3ae(10GBase) - LLDP oraz LLDP-MED - UDLD - 802.3ad LACP, min 4 porty w grupie, min 4 g - N:1 Port Mirroring - RSPAN - ERSPAN - IEEEE802.1d(STP) - IEEEE802.1w(RSTP) - IEEEE802.1s(MSTP) - Root Guard - BPDU Guard - Voice VLAN, PVLAN - Broadcast / Multicast / Unicast Storm Contro - IGMP v1/v2/v3 Snooping - Port Security Cechy warstwy 3 - routing statyczny,RIPv1/v2,OSPFv2	

- OSPFv3, - Policy-based Routing(PBR) dla IPv4 oraz IPv6 - VRRP - IGMP v1/v2/v3, Obsługa QoS - 8 kolejek - Klasyfikacja na podstawie 802.1p, ACL, numerze portu - Traffic Policing Obsługa ACL - IP ACL ,MAC ACL - rozszerzone ACL bazujące na źródłowym i c - czasowe ACL Funkcje bezpieczeństwa - 802.1x AAA - uwierzytelnienie po adresie MAC, MAB - Guest VLAN Zarządzanie oraz wsparcie dla: - CLI, SNMPv1/v2c/v3 - Syslog, logowanie do zewnętrznego Syslog Servera - HTTP SSL - SNMP TRAP - FTP i TFTP - NTP - SSH v1/v2	

22. **Bezprzewodowy punkt dostępowy (access point)**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Bezprzewodowy punkt dostępowy (access point)	Nazwa ….

Charakterystyka:

Bezprzewodowy punkt dostępowy (access point) (3 szt.)

Wymagania:

- Przepustowość dla 2.4 GHz min.450 Mbps
- 2.4 GHz MIMO min. 3x3
- Przepustowość dla 5 GHz min. 867 Mbps
- 5 GHz MIMO min. 2x2
- Musi posiadać certyfikat DFS
- 1 interfejs 10/100/1000 Ethernet Port
- Maksymalne wymiary: 175.7 x 175.7 x 43.2 mm
- Maksymalna waga: 240 g
- Maksymalna waga z zestawem montażowym: 315 g
- Musi posiadać przycisk reset
- Musi dopuszczać metody zasilania takie jak 802.3af/A PoE lub 24V Passive PoE (Pairs 4, 5+; 7, 8 Return)
- Musi być zasilany przez 24V adapter Gigabit PoE 0.5A
- Musi posiadać adapter Gigabit PoE 0.5A
- Wspiera power save
- Maksymalny pobór mocy: 6.5W
- Maksymalna moc TX dla 2.4Ghz: 24 dBm
- Maksymalna moc TX dla 5Ghz: 22 dBm
- Musi posiadać antenę Dual-Band, Tri-Polarity spełniające wymaganie zysku energetycznego dla 2.4 GHz 3dBi oraz 5 Ghz 3 dBi
- Musi spełniać standardy takie jak 802.11

a/b/g/n/ac ● Musi zawierać zabezpieczenia bezprzewodowe takie jak: WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES) ● Minimalna wartość BSSID to 8 na jednę radio ● Musi zawierać montaż ścienny/sufitowy ● Musi móc pracować w zakresie temperatur od -10 do 70° C ● Musi wspierać protokół 802.1Q dla Vlanów ● Musi zawierać funkcje limitowania przesyłu na każdego użytkownika ● Musi wspierać funkcje Guest Traffic isolation ● Musi Zawierać WMM ● Wsparcie dla jednoczesnej liczby min. 250 klientów Wymagana Min. przepustowość danych dla danych standardów: ● 802.11ac 6.5 Mbps to 867 Mbps ● 802.11n 6.5 Mbps to 450 Mbps Uwaga Punkt dostępowy musi być kompatybilny z oprogramowaniem kontrolera sieci WiFi, dostarczonego wraz z urządzeniami.	

23. **Wizualny lokalizator uszkodzeń**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Wizualny lokalizator uszkodzeń	Nazwa ……
Charakterystyka: **Wizualny lokalizator uszkodzeń (1 szt.)** Wymagania: ● Musi zapewniać pracę na długościach fali: 640-665 nm ● Moc wyjściowa urządzenia: od 10mW do	

20 mW ● Musi posiadać złącze uniwersalne dla ferrul 2,5mm (SC; ST; FC) ● Musi posiadać tryby pracy świecenie ciągłe lub pulsacyjne ● Musi być zasilany przez dwie baterie AA ● Musi posiadać maksymalnie długość 170 mm oraz 13 mm średnicy ● Obudowa musi być wykonana z PCV lub aluminium	

24. **Zestaw wkładek (typ A i B) SFP**

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Zestaw wkładek (1 szt. typ A i 1 szt. typ B) SFP 10 kpl.	Nazwa …..
Charakterystyka: **Zestaw wkładek (1 szt. typ A i 1 szt. typ B) SFP (10 szt.)** Wymagania: ● Zasięg min. 20 km 9/125 µm SMF ● prędkość do min. 1.25Gbps ● SFP WDM ● złącze SC ● Typ A: Rx 1310 nm Tx 1550 nm Typ B: Rx 1550 nm Tx 1310 nm ● Zakres pracy w temperaturze: 0℃~+70℃ Uwaga Wkładki muszą być kompatybilne w przełącznikami opisanymi w pozycjach 10 i 21	

25. Zarządzalny przełącznik dostępowy sieci LAN 24 portowy warstwy 2

Producent model oferowanego urządzenia ……..

Minimalne wymagania zamawiającego	Dane techniczne oferowanego sprzętu
Nazwa: Zarządzalny przełącznik dostępowy sieci LAN 24 portowy warstwy 2	Nazwa . .....
Charakterystyka: **Przełącznik dostępowy sieci LAN 24 portowy (9 szt.)** Urządzenie o stałej konfiguracji min. 128 MB pamięci DRAM oraz 64MB pamięci Flash obsługa min. 8000 adresów MAC wydajność przełączania co najmniej 16 Gbps oraz przepustowość co najmniej 6,5 Mpps dla pakietów 64 bajtowych; co najmniej 24 porty FastEthernet w standardzie 10/100BaseTX oraz dwa porty typu combo mogące pracować jako 10/100/1000BASE-T oraz 1000BaseX ze stykiem definiowanym przez SFP, GBIC lub równoważne wyposażone w przewód konsolowy do zarzadzania automatyczne wykrywanie przeplotu (AutoMDIX) na portach miedzianych wbudowane narzędzia do diagnozy okablowania na portach miedzianych (time domain reflector) obsługa co najmniej 255 sieci VLAN i 4000 VLAN ID obsługa mechanizmów dystrybucji informacji o sieciach VLAN pomiędzy przełącznikami obsługa protokołów sieciowych zgodnie ze standardami: - IEEE 802.1x - IEEE 802.1s - IEEE 802.1w - IEEE 802.3x full duplex dla 10BASE-T i 100BASE-TX - IEEE 802.3ad - IEEE 802.1D - IEEE 802.1p - IEEE 802.1Q - IEEE 802.3 10BASE-T	

- IEEE 802.3u 100BASE-TX - IEEE 802.3z 1000BASE-X - IEEE 802.3ab 100BASE-T mechanizmy związane z zapewnieniem jakości usług w sieci: - obsługa co najmniej czterech kolejek sprzętowych, wyjściowych dla różnego rodzaju ruchu - mechanizm automatycznej konfiguracji portów do obsługi VoIP - możliwość ograniczania pasma dostępnego na port (rate limiting) dla ruchu wejściowego i wyjściowego mechanizmy związane z zapewnieniem bezpieczeństwa sieci: - dostęp do urządzenia przez konsolę szeregową, SSHv2 i SNMPv3 - możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS lub TACACS+ - możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports) z pozostawieniem możliwości komunikacji z portem nadrzednym (designated port) lub funkcjonalność private VLAN (w ramach portu) - monitorowanie zapytań i odpowiedzi DHCP (tzw. DHCP Snooping) - możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika - ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe - obsługa list kontroli dostępu (ACL) z uwzględnieniem adresów MAC i IP, portów TCP/UDP bez spadku wydajności urządzenia - min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend) - współpraca z systemami kontroli dostępu do	

sieci typu NAC, itp. obsługa ruchu multicast z wykorzystaniem IGMPv3 obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP możliwość uruchomienia funkcji serwera DHCP plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian możliwość zarządzania przy pomocy bezpłatnej aplikacji graficznej dostarczanej przez producenta możliwość zastosowania zewnętrznego redundantnego zasilacza możliwość montażu w szafie 19” (dostarczenie odpowiednich mocowań jest wymagane w ramach tego postępowania) obudowa wykonana z metalu	

…….
(podpis)