

## OPIS PRZEDMIOTU ZAMÓWIENIA

Niniejszy dokument określa minimalne wymagania dla zamówienia z zakresu cyberbezpieczeństwa w ramach realizacji projektu „Cyberbezpieczny Samorząd” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

### 1. UTM – Typ 1 - 1 sztuka.

#### OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

#### ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interfejs (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

#### INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

#### KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

#### OCHRONA ANTYWIRUSOWA

27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
30. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
31. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym.

#### OCHRONA ANTYSZPAM

31. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
32. Ochrona antyspam ma działać w oparciu o:
  - a. białe/czarne listy,
  - b. DNS RBL,
  - c. Skaner heurystyczny.
33. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
35. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym oraz umożliwiać skanowanie plików w oparciu o Sandboxing zlokalizowany w Internecie na serwerach producenta. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu lub wymagała instalacji

dotatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie.

#### WIRTUALNE SIECI PRYWATNE (VPN)

35. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
36. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
  - a. PPTP VPN,
  - b. IPSec VPN,
  - c. SSL VPN.
37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
38. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
39. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

#### FILTR DOSTĘPU DO STRON WWW

43. Urządzenie ma posiadać wbudowany filtr URL.
44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
45. Administrator ma mieć możliwość dodawania własnych kategorii URL.
46. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
  - a. blokowanie dostępu do adresu URL,
  - b. zezwolenie na dostęp do adresu URL,
  - c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
47. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
48. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
49. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
50. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
51. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
52. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
53. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych.
54. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
55. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.

#### UWIERZYTELNIANIE

53. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
  - a. lokalną bazę użytkowników (wewnętrzny LDAP),
  - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
  - c. usługę katalogową Microsoft Active Directory.
54. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
55. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:

- a. SSL,
- b. Radius,
- c. Kerberos.

56. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

57. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.

58. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

59. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).

60. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

61. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

#### ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

62. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

63. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:

- a. równoważenie względem adresu źródłowego,
- b. równoważenie względem połączenia.

64. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

65. Urządzenie ma umożliwiać przełączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).

66. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.

67. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).

68. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.

66. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.

67. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.

#### ROUTING (TRASOWANIE)

69. Urządzenie ma umożliwiać statyczne trasowanie pakietów.

70. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.

71. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

72. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

#### ADMINISTRACJA URZĄDZENIEM

73. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

74. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

75. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

76. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
77. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
78. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH)
79. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
80. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
81. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
83. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).
85. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
86. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
87. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
88. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
- a. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
  - b. manualnego eksportu do pliku w dowolnym momencie czasu,
89. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
90. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
91. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
92. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

## RAPORTOWANIE

93. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
94. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
95. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
96. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
97. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
98. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
99. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
100. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
101. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

## POZOSTAŁE USŁUGI I FUNKCJE



102. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
103. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
105. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
106. Urządzenie ma posiadać usługę DNS Proxy.
107. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
108. Urządzenie musi mieć zaimplementowane Open API
109. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
110. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

#### GWARANCJA I SERWIS

111. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
112. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

#### PARAMETRY SPRZĘTOWE

113. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
114. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
115. Liczba portów Ethernet 2,5Gbps – min. 8.
116. Liczba portów światłowodowych 1Gbps – min. 1.
117. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
118. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.
119. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps.
120. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.
121. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps.
122. Maksymalna liczba tuneli VPN IPSec – minimum 100.
123. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100.
124. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 100.
125. Obsługa interfejsów 802.11q (VLAN) – minimum 128
126. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę.
127. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
128. Urządzenie nie ma limitu na liczbę użytkowników.
129. Liczba reguł filtrowania – minimum 8 192.
130. Liczba tras statycznego routingu – minimum 512.
131. Liczba tras dynamicznego routingu – minimum 10 000.
132. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
133. Urządzenie musi być wyposażone w moduł TPM.

## 2. UTM – Typ 2 - 4 sztuki.

**OBSŁUGA SIECI**

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

**ZAPORA KORPORACYJNA (Firewall)**

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interfejs (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

**INTRUSION PREVENTION SYSTEM (IPS)**

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

**KSZTAŁTOWANIE PASMA (Traffic Shapping)**

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

#### OCHRONA ANTYWIRUSOWA

27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
30. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
31. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym.
32. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym oraz umożliwiać skanowanie plików w oparciu o Sandboxing zlokalizowany w Internecie na serwerach producenta. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie.

#### OCHRONA ANTYSKAM

31. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
32. Ochrona antyspam ma działać w oparciu o:
  - a. białe/czarne listy,
  - b. DNS RBL,
  - c. Skaner heurystyczny.
33. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

#### WIRTUALNE SIECI PRYWATNE (VPN)

35. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
36. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
  - a. PPTP VPN,
  - b. IPSec VPN,
  - c. SSL VPN.
37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
38. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
39. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

#### FILTR DOSTĘPU DO STRON WWW

43. Urządzenie ma posiadać wbudowany filtr URL.



44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
45. Administrator ma mieć możliwość dodawania własnych kategorii URL.
46. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
  - a. blokowanie dostępu do adresu URL,
  - b. zezwolenie na dostęp do adresu URL,
  - c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
47. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
48. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
49. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
50. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
51. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
52. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
53. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych.
54. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
55. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.

#### UWIERZYTELNIANIE

53. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
  - a. lokalną bazę użytkowników (wewnętrzny LDAP),
  - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
  - c. usługę katalogową Microsoft Active Directory.
54. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
55. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
  - a. SSL,
  - b. Radius,
  - c. Kerberos.
56. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
57. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
58. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
59. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
60. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
61. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

#### ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

62. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
63. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:

- a. równoważenie względem adresu źródłowego,
  - b. równoważenie względem połączenia.
64. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
65. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).
66. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.
68. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).
69. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.
70. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.
71. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.

## ROUTING (TRASOWANIE)

69. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
70. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łączy podstawowego.
71. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
72. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

## ADMINISTRACJA URZĄDZENIEM

73. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
74. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
75. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
76. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
77. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
78. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH).
79. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
80. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
81. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
83. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
85. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
86. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
87. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
88. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

89. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
- manualnego eksportu do pliku w dowolnym momencie czasu,
  - automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
90. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
91. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
92. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

## RAPORTOWANIE

93. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
94. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
95. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
96. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
97. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
98. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
99. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
100. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
101. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

## POZOSTAŁE USŁUGI I FUNKCJE

102. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
103. Urządzenie ma pozwalać na przysyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
105. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
106. Urządzenie ma posiadać usługę DNS Proxy.
107. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
108. Urządzenie musi mieć zaimplementowane Open API
109. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
110. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
111. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowość firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

## GWARANCJA I SERWIS

112. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
113. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

**PARAMETRY SPRZĘTOWE**

114. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
115. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
116. Liczba portów Ethernet 2,5Gbps – min. 8.
117. Liczba portów światłowodowych 1Gbps – min. 1.
118. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
119. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
120. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
121. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
122. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
123. Maksymalna liczba tuneli VPN IPSec – minimum 100.
124. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
125. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
126. Obsługa interfejsów 802.11q (VLAN) – minimum 128
127. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
128. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
129. Urządzenie nie ma limitu na liczbę użytkowników.
130. Liczba reguł filtrowania – minimum 8 192.
131. Liczba tras statycznego routingu – minimum 512.
132. Liczba tras dynamicznego routingu – minimum 10 000.
133. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
134. Urządzenie musi być wyposażone w moduł TPM.

**3. UPS – 3 sztuki.**

L.p.	Nazwa komponentu	Wymagane parametry techniczne
1	2	3
1.	Technologia	online, VFI-SS-111,
2.	Moc wyjściowa	3kVA/3kW; PF=1
3.	Obudowa	Rack Zestaw do montażu w szafie rack na wyposażeniu
4.	Napięcie wejściowe	110 ÷ 300 V AC ± 2 %
5.	Napięcie znamionowe (wartość skuteczna)	230V AC
6.	Prąd znamionowy (wejście)	15,6A
7.	Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz
8.	Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
9.	Zniekształcenia prądu wejściowego THDi	< 5%
10.	Zakres napięcia wyjściowego	200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC )

11.	Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
12.	Gniazda wyjściowe	4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A)
13.	Akumulatory wewnętrzne UPS	Minimum 6szt akumulatorów 12V9Ah
14.	Moduły bateryjne	Opcja – możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah)
15.	Czas podtrzymania UPS dla obciążenia 3kW/2,4kW/1,5kW	3,5 / 5 / 10 min
16.	Czas podtrzymania UPS + MODUŁ dla obciążenia 3kW/2,4kW/1,5kW	17 / 23 / 40 min
17.	Przebieżalność	105-125% - 5min / 125-150% - 30s / >150% - 500ms
18.	EPO	Wymagane – standard NC
19.	Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę baterijną, pracę w trybie online, obejście bypass
20.	Język oprogramowania	polski i angielski do wyboru z poziomu interfejsu użytkownika
21.	Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu)	Wymagane, konfigurowalne z poziomu oprogramowania (przez USB)
22.	Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument)
23.	Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – wymagana na wyposażeniu
24.	Wymiary UPS (rack) (wys x szer x gł)	Nie więcej niż 86 x 439 x 600 mm
25.	Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)



26.	Oprogramowanie - funkcjonalność	możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu
27.	Oprogramowanie - funkcjonalność	Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapas energii na wypadek kolejnego zaniku.
28.	Oprogramowanie - funkcjonalność	Uruchomienie przez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.
29.	Serwis producenta	wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
30.	Gwarancja	Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych
31.	Dokumentacja	Instrukcja w języku polskim

#### 4. Zarządzane urządzenia sieciowe z obsługą VLAN – Typ 1 - 2 sztuki.

- Typ i liczba portów - 24x 10/100/1000 RJ45, 4x 10Gigabit Ethernet SFP+
- Bez wentylatorów (fanless)
- Zasilanie przez wbudowany zasilacz AC 230V
- Obudowa 1U, rackmount (dostarczone uchwyty montażowe)
- Możliwość stackowania przełączników – do 8 przełączników i do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym: Quality of Service (QoS), sieci VLAN, Link Aggregation (LAG) i port mirroring
- Zarządzanie energią:
- Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)
- Zasilanie PoE można włączać i wyłączać w oparciu o harmonogram zdefiniowany przez użytkownika w celu oszczędzania energii [Uwaga! dotyczy modeli z obsługą POE]
- Zapewnia zasilanie PoE podczas restartu urządzenia [Uwaga! dotyczy modeli z obsługą POE]
- Możliwość wyłączenia diod LED w celu oszczędzania energii
- Parametry wydajnościowe:

- Przepustowość przełącznika (Switching capacity): 128 Gbps
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 95.23 Mpps
- Pamięć DRAM – 1GB
- Pamięć Flash – 512MB
- Obsługa 4000 VLAN
- 16000 adresów MAC
- Wire-speed IPv4 routing – 990 tras statycznych, 128 interfejsów IP
- Obsługa ramek jumbo – do 9000 bajtów
- 2000 IGMP group
- 8 połączeń zagregowanych typu „port channel” per grupa, obsługa 8 grup
- Ilość wpisów w listach kontroli dostępu Security ACL – 1000
- Obsługa protokołu SNMP
- Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
- Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
- IEEE 802.1w Rapid Spanning Tree
- IEEE 802.1s Multi-Instance Spanning Tree - obsługa 8 instancji
- Per-VLAN Rapid Spanning Tree (PVRST+) - obsługa 126 instancji
- Obsługa protokołu LLDP i LLDP-MED
- Obsługa translacji sieci VLAN 1:1 (mapowanie 1 do 1 z translacją identyfikatora sieci klienckiej VLAN (C-VLAN) na interfejsie brzegowym na identyfikator sieci VLAN używanej w sieci operatora (S-VLAN))
- Obsługa Q-in-Q oraz Selective Q-in-Q
- Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)
- Realizacja funkcji UDLD w celu wykrywania jednokierunkowych połączeń spowodowanych uszkodzeniami linków
- Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
- Możliwość uruchomienia funkcji serwera DHCP wraz z obsługą wielu puli adresowych i zakresów adresowych
- Obsługa opcji DHCP: opcje 12, 59, 60, 66, 67, 82, 125, 129 oraz 150
- Realizacja funkcji DHCP Relay wraz z obsługą funkcji DHCP opcja 82
- Możliwość konfiguracji interfejsów Layer 3 dla:

- Portów fizycznych przełącznika
- Interfejsów zagregowanych przy pomocy Link Aggregation (LAG)
- Interfejsów VLAN
- Interfejsów loopback
- Obsługa UDP Relay (User Datagram Protocol Relay)
- Obsługa funkcjonalności umożliwiającej powiadomienie przez przełącznik, z wykorzystaniem notyfikacji SYSLOG lub SNMP, nadrzędnego systemu monitorowania o wykryciu zaniku zasilania. Funkcjonalność umożliwia wysłanie komunikatu o zaniku zasilania przed całkowitą utratą zasilania przez urządzenie.
- Mechanizmy związane z bezpieczeństwem sieci:
- Trzy poziomy dostępu administracyjnego poprzez konsolę (3 poziomy uprawnień)
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
- Obsługa różnych trybów uwierzytelniania 802.1x na porcie:
- Tryb pojedynczego hosta, w którym tylko jeden host może być podłączony do portu;
- Tryb wielu hostów, w którym port jest uwierzytelniony wówczas gdy podłączony jest do niego co najmniej jeden uwierzytelniony klient;
- Tryb wielu sesji, w którym status uwierzytelnienia nie jest przypisany do portu a wyłącznie do każdego z klientów podłączonych do portu;
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- Realizacja funkcji Change of Authorization (CoA) realizującej dynamiczną zmianę uwierzytelnienia dla sesji użytkownika podłączonego do danego portu
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
- Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
- Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community
- Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priority, TCP flag. Obsługa czasowych list ACL

- Obsługa mechanizmów zapewniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]
- Bezpieczny proces bootowania urządzenia
- Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika
- Mechanizmy związane z zapewnieniem jakości usług w sieci:
- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
- Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek
- Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
- Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu
- Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN
- Obsługa funkcji port mirroring polegającej na kopiowaniu ruchu z danego portu i przesłanie go do innego portu. Obsługa do 8 portów źródłowych kopiujących swój ruch do jednego portu docelowego (monitorującego)
- Obsługa funkcji VLAN mirroring polegającej na kopiowaniu ruchu z danej sieci VLAN i przesłanie go do innego portu. Obsługa do 8 źródłowych sieci VLAN kopiujących swój ruch do jednego portu docelowego (monitorującego)
- Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
- Obsługa protokołu sFlow
- Obsługa standardów:
- IEEE 802.3 10BASE-T Ethernet,
- IEEE 802.3u 100BASE-TX Fast Ethernet,

- IEEE 802.3ab 1000BASE-T Gigabit Ethernet,
- IEEE 802.3ad Link Aggregation Control Protocol,
- IEEE 802.3z Gigabit Ethernet,
- IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN,
- IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable,
- IEEE 802.3x Flow Control,
- IEEE 802.1D (STP, GARP, and GVRP),
- IEEE 802.1Q/p VLAN,
- IEEE 802.1w Rapid STP,
- IEEE 802.1s Multiple STP,
- IEEE 802.1X Port Access Authentication,
- IEEE 802.3af,
- IEEE 802.3at,
- IEEE 802.1AB Link Layer Discovery Protocol,
- IEEE 802.3az Energy Efficient Ethernet,
- RFC 768,
- RFC 783,
- RFC 791,
- RFC 792,
- RFC 793,
- RFC 813,
- RFC 826,
- RFC 879,
- RFC 896,
- RFC 854,
- RFC 855,
- RFC 856,
- RFC 858,
- RFC 894,
- RFC 919,



## na Rozwój Cyfrowy

- RFC 920,
- RFC 922,
- RFC 950,
- RFC 951,
- RFC 1042,
- RFC 1071,
- RFC 1123,
- RFC 1141,
- RFC 1155,
- RFC 1157,
- RFC 1213,
- RFC 1215,
- RFC 1286,
- RFC 1350,
- RFC 1442,
- RFC 1451,
- RFC 1493,
- RFC 1533,
- RFC 1541,
- RFC 1542,
- RFC 1573,
- RFC 1624,
- RFC 1643,
- RFC 1700,
- RFC 1757,
- RFC 1867,
- RFC 1907,
- RFC 2011,
- RFC 2012,
- RFC 2013,

**na Rozwój Cyfrowy**

- RFC 2030,
- RFC 2131,
- RFC 2132,
- RFC 2233,
- RFC 2576,
- RFC 2616,
- RFC 2618,
- RFC 2665,
- RFC 2666,
- RFC 2674,
- RFC 2737,
- RFC 2819,
- RFC 2863,
- RFC 3164,
- RFC 3176,
- RFC 3411,
- RFC 3412,
- RFC 3413,
- RFC 3414,
- RFC 3415,
- RFC 3416,
- RFC 4330
- Zarządzanie:
- Port konsoli – USB typu C i RJ45
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia
- Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP
- Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
- Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu

- Praca w szerokim zakresie temperatur: -50°C – +50°C
- Możliwość przechowywania w szerokim zakresie temperatur: -25°C – +70°C
- Głębokość urządzenia nie przekracza 35cm

#### 4. Zarządzane urządzenia sieciowe z obsługą VLAN – Typ 2 - 2 sztuki.

**Dodatkowo wraz z urządzeniami sieciowymi powinny być dostarczone wkładki SPF 10G (4szt.) do każdego urządzenia oraz kable umożliwiające połączenia („stakowanie”) urządzeń razem ze sobą.**

- Typ i liczba portów - 48x 10/100/1000 RJ45, 4x 10Gigabit Ethernet SFP+
- Zasilanie przez wbudowany zasilacz AC 230V
- Obudowa 1U, rackmount (dostarczone uchwyty montażowe)
- Możliwość stackowania przełączników – do 8 przełączników i do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym: Quality of Service (QoS), sieci VLAN, Link Aggregation (LAG) i port mirroring
- Zarządzenie energią:
- Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)
- Zasilanie PoE można włączać i wyłączać w oparciu o harmonogram zdefiniowany przez użytkownika w celu oszczędzania energii [Uwaga! dotyczy modeli z obsługą POE]
- Zapewnia zasilanie PoE podczas restartu urządzenia [Uwaga! dotyczy modeli z obsługą POE]
- Możliwość wyłączenia diod LED w celu oszczędzania energii
- Parametry wydajnościowe:
- Przepustowość przełącznika (Switching capacity): 176 Gbps
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 130.94 Mpps
- Pamięć DRAM – 1GB
- Pamięć Flash – 512MB
- Obsługa 4000 VLAN
- 16000 adresów MAC
- Wire-speed IPv4 routing – 990 tras statycznych, 128 interfejsów IP
- Obsługa ramek jumbo – do 9000 bajtów
- 2000 IGMP group
- 8 połączeń zagregowanych typu „port channel” per grupa, obsługa 8 grup

- Ilość wpisów w listach kontroli dostępu Security ACL – 1000
- Obsługa protokołu SNTP
- Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
- Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
- IEEE 802.1w Rapid Spanning Tree
- IEEE 802.1s Multi-Instance Spanning Tree - obsługa 8 instancji
- Per-VLAN Rapid Spanning Tree (PVRST+) - obsługa 126 instancji
- Obsługa protokołu LLDP i LLDP-MED
- Obsługa translacji sieci VLAN 1:1 (mapowanie 1 do 1 z translacją identyfikatora sieci klienckiej VLAN (C-VLAN) na interfejsie brzegowym na identyfikator sieci VLAN używanej w sieci operatora (S-VLAN))
- Obsługa Q-in-Q oraz Selective Q-in-Q
- Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)
- Realizacja funkcji UDLD w celu wykrywania jednokierunkowych połączeń spowodowanych uszkodzeniami linków
- Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
- Możliwość uruchomienia funkcji serwera DHCP wraz z obsługą wielu puli adresowych i zakresów adresowych
- Obsługa opcji DHCP: opcje 12, 59, 60, 66, 67, 82, 125, 129 oraz 150
- Realizacja funkcji DHCP Relay wraz z obsługą funkcji DHCP opcja 82
- Możliwość konfiguracji interfejsów Layer 3 dla:
- Portów fizycznych przełącznika
- Interfejsów zagregowanych przy pomocy Link Aggregation (LAG)
- Interfejsów VLAN
- Interfejsów loopback
- Obsługa UDP Relay (User Datagram Protocol Relay)
- Obsługa funkcjonalności umożliwiającej powiadomienie przez przełącznik, z wykorzystaniem notyfikacji SYSLOG lub SNMP, nadrzędnego systemu monitorowania o wykryciu zaniku zasilania. Funkcjonalność umożliwia wysłanie komunikatu o zaniku zasilania przed całkowitą utratą zasilania przez urządzenie.
- Mechanizmy związane z bezpieczeństwem sieci:

- Trzy poziomy dostępu administracyjnego poprzez konsolę (3 poziomy uprawnień)
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
- Obsługa różnych trybów uwierzytelniania 802.1x na porcie:
- Tryb pojedynczego hosta, w którym tylko jeden host może być podłączony do portu;
- Tryb wielu hostów, w którym port jest uwierzytelniony wówczas gdy podłączony jest do niego co najmniej jeden uwierzytelniony klient;
- Tryb wielu sesji, w którym status uwierzytelnienia nie jest przypisany do portu a wyłącznie do każdego z klientów podłączonych do portu;
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- Realizacja funkcji Change of Authorization (CoA) realizującej dynamiczną zmianę uwierzytelnienia dla sesji użytkownika podłączonego do danego portu
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
- Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
- Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community
- Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priority, TCP flag. Obsługa czasowych list ACL
- Obsługa mechanizmów zapewniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]
- Bezpieczny proces bootowania urządzenia
- Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika
- Mechanizmy związane z zapewnieniem jakości usług w sieci:
- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi



- Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek
- Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
- Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu
- Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN
- Obsługa funkcji port mirroring polegającej na kopiowaniu ruchu z danego portu i przesłanie go do innego portu. Obsługa do 8 portów źródłowych kopiujących swój ruch do jednego portu docelowego (monitorującego)
- Obsługa funkcji VLAN mirroring polegającej na kopiowaniu ruchu z danej sieci VLAN i przesłanie go do innego portu. Obsługa do 8 źródłowych sieci VLAN kopiujących swój ruch do jednego portu docelowego (monitorującego)
- Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
- Obsługa protokołu sFlow
- Obsługa standardów:
- IEEE 802.3 10BASE-T Ethernet,
- IEEE 802.3u 100BASE-TX Fast Ethernet,
- IEEE 802.3ab 1000BASE-T Gigabit Ethernet,
- IEEE 802.3ad Link Aggregation Control Protocol,
- IEEE 802.3z Gigabit Ethernet,
- IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN,
- IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable,
- IEEE 802.3x Flow Control,

**na Rozwój Cyfrowy**

- IEEE 802.1D (STP, GARP, and GVRP),
- IEEE 802.1Q/p VLAN,
- IEEE 802.1w Rapid STP,
- IEEE 802.1s Multiple STP,
- IEEE 802.1X Port Access Authentication,
- IEEE 802.3af,
- IEEE 802.3at,
- IEEE 802.1AB Link Layer Discovery Protocol,
- IEEE 802.3az Energy Efficient Ethernet,
- RFC 768,
- RFC 783,
- RFC 791,
- RFC 792,
- RFC 793,
- RFC 813,
- RFC 826,
- RFC 879,
- RFC 896,
- RFC 854,
- RFC 855,
- RFC 856,
- RFC 858,
- RFC 894,
- RFC 919,
- RFC 920,
- RFC 922,
- RFC 950,
- RFC 951,
- RFC 1042,

## na Rozwój Cyfrowy

- RFC 1071,
- RFC 1123,
- RFC 1141,
- RFC 1155,
- RFC 1157,
- RFC 1213,
- RFC 1215,
- RFC 1286,
- RFC 1350,
- RFC 1442,
- RFC 1451,
- RFC 1493,
- RFC 1533,
- RFC 1541,
- RFC 1542,
- RFC 1573,
- RFC 1624,
- RFC 1643,
- RFC 1700,
- RFC 1757,
- RFC 1867,
- RFC 1907,
- RFC 2011,
- RFC 2012,
- RFC 2013,
- RFC 2030,
- RFC 2131,
- RFC 2132,
- RFC 2233,

**na Rozwój Cyfrowy**

- RFC 2576,
- RFC 2616,
- RFC 2618,
- RFC 2665,
- RFC 2666,
- RFC 2674,
- RFC 2737,
- RFC 2819,
- RFC 2863,
- RFC 3164,
- RFC 3176,
- RFC 3411,
- RFC 3412,
- RFC 3413,
- RFC 3414,
- RFC 3415,
- RFC 3416,
- RFC 4330
- Zarządzanie:
- Port konsoli – USB typu C i RJ45
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia
- Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP
- Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
- Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu
- Praca w szerokim zakresie temperatur: -50oC – +50oC
- Możliwość przechowywania w szerokim zakresie temperatur: -25oC – +70oC
- Głębokość urządzenia nie przekracza 35cm

## 4. Network Attached Storage (NAS) - 2 sztuki.

Minimalne wymagania Zamawiającego	
Typ urządzenia	Serwer NAS
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz)
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 16 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband
Porty zewnętrzne	Minimum: <ul style="list-style-type: none"> <li>2 porty USB 3.2.1</li> <li>1 gniazdo rozszerzenia</li> </ul>
Porty sieciowe	Minimum: <ul style="list-style-type: none"> <li>2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)</li> <li>1 port 10GbE RJ45</li> <li>Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8</li> </ul>
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 4-liniowe gniazdo x8 Gen. 3
Wentylator obudowy	Min. 3 wentylatory 60 mm x 60 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: <ul style="list-style-type: none"> <li>Wewnętrzny: Btrfs, ext4</li> <li>Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT</li> </ul>
Zarządzanie pamięcią masową	<ul style="list-style-type: none"> <li>Maksymalny rozmiar pojedynczego wolumenu: <ul style="list-style-type: none"> <li>200 TB (wymagana pamięć 32 GB)</li> <li>108 TB</li> </ul> </li> <li>Minimalny liczba wewnętrznych wolumenów: 64</li> <li>Minimalny liczba obiektów iSCSI Target: 128</li> <li>Minimalny liczba jednostek iSCSI LUN: 256</li> <li>Obsługa klonowania/migawek jednostek iSCSI LUN</li> </ul>

Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	<ul style="list-style-type: none"> <li>Minimalna liczba kont użytkowników: 2 048</li> <li>Minimalna liczba grup użytkowników: 256</li> <li>Minimalna liczba folderów współdzielonych: 512</li> <li>Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 2 000</li> </ul>
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Oprogramowanie	<ul style="list-style-type: none"> <li>Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych</li> <li>Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów</li> <li>Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez</li> </ul>



	<p>opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.</p> <ul style="list-style-type: none"> <li>• Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.</li> </ul>
Konserwacja	<ul style="list-style-type: none"> <li>• Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack</li> </ul>
Gwarancja	<p>Wykonawca udzieli gwarancji:</p> <ul style="list-style-type: none"> <li>• 3 lata na urządzenie główne</li> <li>• 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack</li> </ul>
Dodatkowe akcesoria	Komplet przesuwanych szyn rack
Zasilacz / Adapter	2 x 350W

#### 5. Dyski twarde do serwera plików NAS – 8 sztuk.

Minimalne wymagania:	
Pojemność	min. 16000 GB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	SATA III (6.0 Gb/s)
Pamięć cache	min. 512 MB
Prędkość obrotowa	7200 obr./ min.

Prędkość odczytu (maksymalna)	do 259 MB/s
Technologia	CMR
Niezawodność MTBF	do 2 500 000 godzin

