Załącznik nr 1
(ODA–2410–31/2020)

OPIS PRZEDMIOTU ZAMÓWIENIA

Specyfikacja techniczna sprzętowo-softwareowa środowiska hiperkonwergentnego dla Laboratorium Sieci Teleinformatycznych i Technologii Internetu Rzeczy

Środowisko hiperkonwergentne, wyposażone, między innymi w klaster pozwalający zbudować pełne środowisko wirtualne, utrzymać zasoby storage, oparte o serwery, każdy co najmniej dwuprocesorowy, pamięć masową oraz dyski mechaniczne, a także infrastrukturę łączącą serwery i zapewniającą zunifikowane zarządzanie, monitoring oraz możliwości elastycznej rozbudowy. Środowisko rozwoju oprogramowania w oparciu o infrastrukturę routingu, switchingu i sieci bezprzewodowych standardu 802.11 oraz Bluetooth; stworzone w oparciu o zestawy kompletów składających się z routerów przygotowanych do hostowania aplikacji, routerów przygotowywanych do zastosowań IoT, przystosowanych do środowisk przemysłowych oraz punktów dostępowych WLAN/Bluetooth, kompletne oprogramowanie, akcesoria, kompletne okablowanie i oprzyrządowanie oraz inny osprzęt teleinformatyczny.
Całość dostarczanego w ramach realizacji przedmiotu zamówienia sprzętu musi być fabrycznie nowa. Dostarczona infrastruktura będzie służyła do testowania nowych rozwiązań teleinformatycznych oraz sprzedaży usług i rozwiązań wdrażanych w oparciu o środowiska testowo-badawcze pozwalające m.in. na:

- symulację obszarów w których funkcjonuje nowy element Internetu Rzeczy (IoT) oraz symulację jego interakcji z otoczeniem,
- analizę świata hiperskomunikowanego LTE wraz z możliwością testowania w przyszłości technologii 5G,
- sprzętową i programową symulację rozwiązań pracujących z wirtualizacją funkcji na masową skalę
- testowanie mechanizmów zabezpieczeń w komunikacji IT.

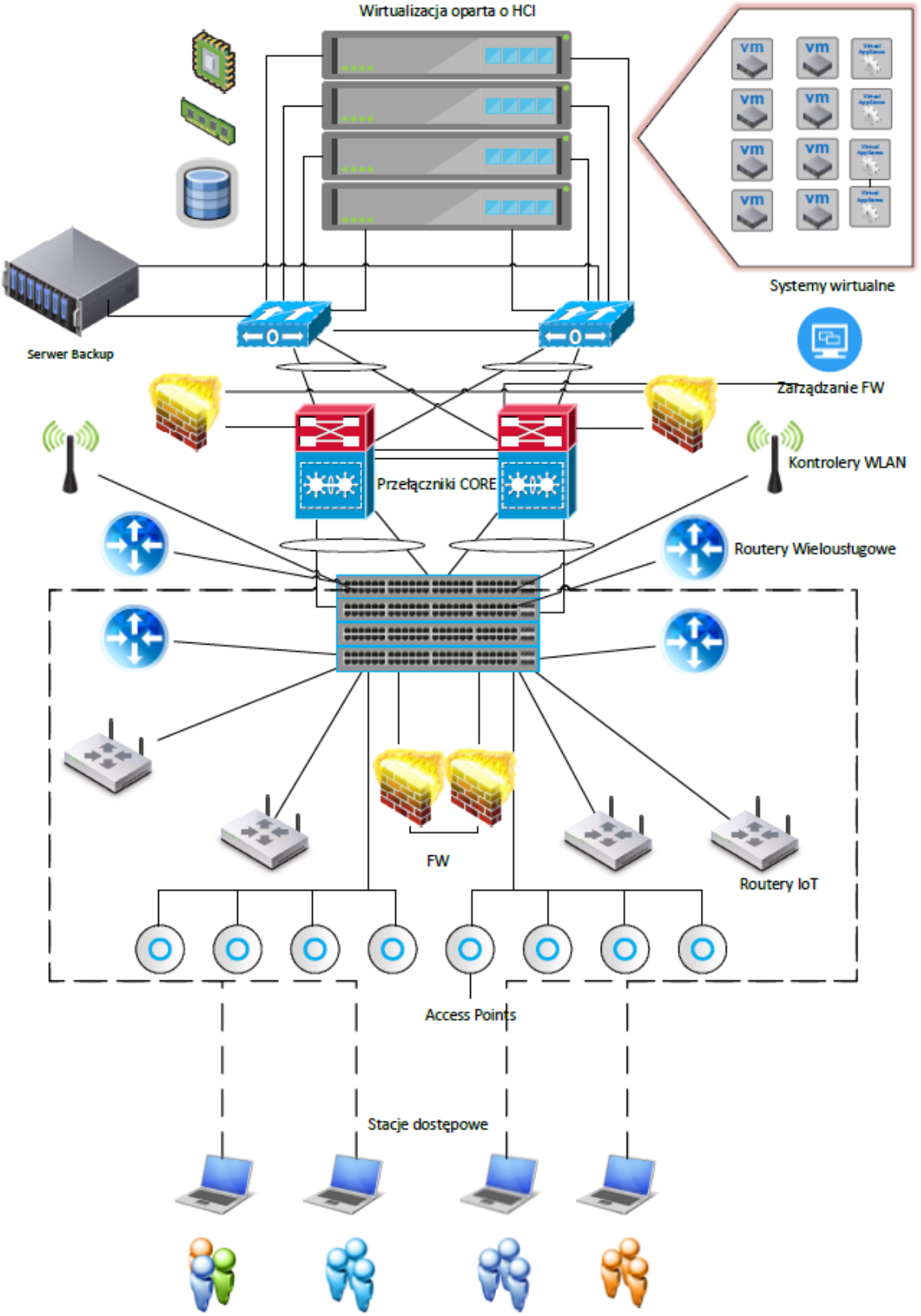
Wszelkie prace muszą być poprzedzone wykonaniem przez Wykonawcę oraz obustronnie zatwierdzonej dokumentacji wdrożeniowej (dotyczy to zarówno części aktywnej, pasywnej oraz zasilającej).

Na rysunku 1 przedstawiono poglądową architekturę systemu zawierającą wszystkie komponenty budowanego rozwiązania. W zakresie prac jest dostawa wyszczególnionych komponentów, ich instalacja oraz uruchomienie, w skład którego wchodzi konfiguracja wszystkich elementów pozwalająca na zarządzanie środowiskiem i realizację jego funkcji. Wdrożenie infrastruktury aktywnej i pasywnej musi obejmować wszystkie prace instalacyjne.

Wszystkie elementy środowiska zostaną dostarczone oraz zainstalowane przez dostawcę w miejscu wskazanym przez Zamawiającego.

W ramach udzielonej gwarancji wykonawca zobowiązany jest do świadczenia serwisu gwarancyjnego z czasem naprawy lub wymiany uszkodzonego urządzenia w terminie nie dłuższym niż 21 dni roboczych.

Rys. 1. Poglądowa architektura systemu



Specyfikacja techniczna

Infrastruktura serwerowa

A) Klaster systemu wirtualizacji typu HCI (Hyperconverged Infrastructure)

Ogólny opis funkcjonalny klastra pamięci masowej HCI

Wymagania funkcjonalne:

1. Rozwiązanie zapewnia architekturę klastrową z możliwością obsługi minimum 32 węzłów pamięci masowej w pojedynczym klastrze.
2. Rozwiązanie oparte jest o węzły serwerowe x86 integrujące procesory, pamięć operacyjną i pamięć masową opartą o dyski HDD/SSD przy czym każdy z serwerów wyprowadza co najmniej dwa interfejsy 40 Gigabit Ethernet QSFP dla łączności w klastrze
3. Węzły pamięci masowej umożliwiają wykorzystanie dysków SSD oraz HDD przy czym jest możliwa implementacja węzła wyposażonego jedynie w zasoby pamięci flash (tzw. All-Flash)
4. Rozwiązanie posiada możliwość implementacji węzłów All-Flash całkowicie opartego o urządzenia z interfejsem NVMe (All-NVMe)
5. Rozwiązanie zapewnia implementację wspólnego zasobu pamięci masowej (datastore) w oparciu o cały klaster, dostępnego w taki sam sposób dla każdego węzła wchodzącego w skład klastra
6. Rozwiązanie zapewnia prezentację wspólnego zasobu pamięci masowej (datastore) również dla węzłów obliczeniowych niezależnych od węzłów pamięci masowej, w tym również serwerów nie wyposażonych w dyski SSD/HDD (bezdyskowych) dołączonych do klastra, w ilości co najmniej odpowiadającej ilości węzłów pamięci masowej
7. Rozwiązanie zapewnia replikację każdego segmentu danych na przynajmniej trzech różnych węzłach (potrójna replikacja)
8. Rozwiązanie jest skalowalne (scale-out) czyli rozbudowa jest zapewniona poprzez bezprzerwowe dołożenie kolejnego węzła do klastra.
9. Rozwiązanie jest oparte na serwerach maksymalnie dwuprocesorowych, tak aby w wyniku awarii jednego z węzłów klastra, spadek wydajności całości był jak najmniejszy.
10. Rozwiązania zapewnia pełną ciągłość i funkcjonalność działania w wypadku awarii lub całkowitej niedostępności pojedynczego węzła.
11. Rozwiązanie zapewnia pełną ciągłość i funkcjonalność działania w wypadku jednoczesnej awarii pojedynczych dysków w dwóch węzłach.
12. Rozwiązanie posiada możliwość kontrolowanego wyłączania pojedynczego węzła z klastra poprzez przełączanie go w tryb utrzymaniowy (maintenance)
13. Rozwiązanie integruje się z infrastrukturą wirtualizacyjną pracującą pod kontrolą oprogramowania opisanego w punkcie C niniejszej specyfikacji.
14. Rozwiązanie posiada wbudowany portal do zarządzania i monitorowania umożlwiający:
    - 14.1. Raportowanie i monitorowanie węzłów pamięci masowej oraz ich zasobów dyskowych
    - 14.2. Tworzenie, modyfikowanie i usuwanie pul pamięci masowej
    - 14.3. Monitorowanie i wizualizowanie wydajności rozwiązania, w tym parametrów: ilość operacji / sekundę, opóźnienie pamięci masowej, przepustowość
    - 14.4. Uruchamianie i zatrzymywanie maszyn wirtualnych VM oraz tworzenie ich klonów oraz kopii migawkowych
    - 14.5. Konfigurowanie replikacji danych między różnymi ośrodkami
    - 14.6. Dziennik czynności, zdarzeń i alarmów
    - 14.7. Aktualizację oprogramowania pamięci masowej oraz innych komponentów
15. Rozwiązanie posiada możliwość zarządzania i monitorowania z poziomu konsoli centralnego zarządzania oprogramowania wirtualizacyjnego.
16. Rozwiązanie posiada możliwość weryfikacji i diagnozowania działania poprzez dedykowany interfejs linii komend (CLI)

17. Rozwiązanie posiada dostępne publicznie potwierdzenie kompatybilności z mechanizmami replikacji i archiwizacji opartymi o rozwiązania Veeam oraz Commvault oraz wykorzystania przez nie wbudowanego mechanizmu wykonywania kopii migawkowych
18. Rozwiązanie zapewnia zwiększenie wydajności operacji wejścia/wyjścia za pomocą architektury Cache implementowanej w oparciu o pamięć Flash (SSD);
19. Rozwiązanie posiada udokumentowaną możliwość implementacji środowisk wirtualnych desktopów (VDI) oraz instalacji modułów GPU
20. Rozwiązanie posiada możliwość sprzętowego szyfrowania zapisanych danych z wykorzystaniem dysków szyfrujących
21. Rozwiązanie zapewnia opartą o oprogramowanie deduplikację i kompresję maszyn wirtualnych. Deduplikacja i kompresja jest implementowana zarówno dla dysków Flash jak i dysków magnetycznych HDD.
22. Rozwiązanie umożliwia zastosowanie dedykowanej karty sprzętowej w celu zwiększenia wydajności algorytmu kompresji danych
23. Rozwiązanie posiada funkcjonalność zoptymalizowanego klonowania maszyn wirtualnych przy czym jest możliwe wygenerowanie co najmniej 200 klonów maszyny w ramach jednoczesnej operacji; klonowanie jest możliwe dla maszyn posiadających kopie migawkowe (snapshot)
24. Architektura rozwiązania umożliwia maszynom wirtualnym na korzystanie również z innych, znajdujących się poza klasterem zasobów pamięci masowej udostępnianych poprzez FC, iSCSCI, NFS
25. Rozwiązanie posiada wbudowany mechanizm dedykowanej asynchronicznej replikacji danych między dwoma ośrodkami przetwarzania danych (OPD) dla wybranych maszyn wirtualnych (VM) z możliwością ich odtwarzania po awarii (distaster recovery)
26. Rozwiązanie posiada możliwość rozbudowy do obsługi funkcjonalności rozciągnięcia pojedynczego klastra na 2 odległe o 100 km ośrodki przetwarzania danych (OPD) z synchroniczną replikacją danych i obsługą środowiska w trybie aktywne-aktywne między OPD (maszyny wirtualne VM aktywne w obu lokalizacjach) przy czym musi być zachowania spójność systemu w przypadku zerwania połączenia między OPD (split-brain).
27. Rozwiązanie posiada ważny certyfikat firmy SAP do działania jako platforma dla produkcyjnych systemów SAP HANA
28. Jeśli jakiekolwiek w/w funkcjonalności rozwiązania są dodatkowo licencjonowane to wymaga się dostarczenia takich licencji jedynie w razie wyraźnego wymienienia danej funkcjonalności przez Zamawiającego.
29. Możliwość implementacji rozwiązania w środowisku opartym, co najmniej o wirtualizację Hyper-V oraz Vmware vSphere
30. Możliwość impementacji rozwiązania w środowisku kontenerowym, co najmniej opartym o orkiestrację Kubernetes ze wsparciem dla permamentnych wolumenów
31. Możliwość aktualizacji firmware i oprogramowania systemowego dla wszystkich warstw, tj infrastruktury sprzętowej, infrastruktury wirtualizacyjnej oraz oprogramowania pamięci masowej z poziomu zarządzania rozwiązaniem pamięci masowej
32. Możliwość uruchomienia automatycznego informowania centrum wsparcia technicznego producenta rozwiązania o błędach i usterkach
33. Możliwość monitorowania klastra poprzez interfejs REST API

Ukompletowanie klastra systemu wirtualizacji typu HCI

1. Wymaga się dostarczenia pojedynczego klastra implementującego na potrzeby środowiska zwirtualizowanego pamięć masową (datastore) o wielkości minimum 21 TB przestrzeni użytecznej wyłącznie w oparciu o urządzenia Flash (tzw All Flash), przy założeniu że dla każdego bloku danych tworzone są co najmniej trzy repliki (kopie) i przy założeniu całkowitego braku oszczędności z tytułu deduplikacji oraz kompresji danych
2. Wymaga się dostarczenia co najmniej czterech węzłów dla zaimplementowania klastra, każdy węzeł wyposażony w:

Lp.	Parametr	Minimalne parametry techniczne
1	CPU	dwa procesory, każdy co najmniej 10 rdzeni, zapewniające dla zaoferowanego serwera osiągnięcie w teście CPU2017 Integer Rate Base publikowanym na stronach spec.org wyniku minimum 92 punkty
2	Pamięć RAM	minimum 384 GB pamięci DRAM DDR4 2666 MHz (32 GB x 12)
3	Dyski pojemnościowe	Odpowiednia ilość dysków SSD (All Flash) konieczna dla zapewnienia opisanej wymaganej surowej przestrzeni 21 TB w ramach całego klastra (przy zakładanej replikacji x3 oraz braku oszczędności na deduplikacji i kompresji danych)
4	Dysk Cache	Urządzenie Cache w oparciu o pamięć flash SSD SAS 12Gb o pojemności min. 1,6 TB
5	Karty sieciowe	Konwergentny adapter sieciowy LAN/SAN, co najmniej 2 x 40GE QSFP wraz z kablami połączeniowymi QSFP o długości co najmniej 3m zapewniającymi dołączenie do dedykowanego systemu przełączania wewnątrz klastra
6	Karta SD	Karta SD o pojemności min. 32 GB
7	Dodatkowe dyski: Boot (OS)	Urządzenie M.2 lub SD do instalacji oprogramowania wirtualizacyjnego w wielkości min. 240 GB
8	Dodatkowe dyski	Dysk systemowy SSD o wielkości min. 240 GB
10	Zasilanie	Dwa redundantne zasilacze o mocy co najmniej 1200 W

3. Wymaga się możliwości rozbudowy pojemności klastra do wielkości minimum 50 TB przestrzeni użytecznej wyłącznie w oparciu o urządzenia Flash (tzw. All Flash), przy założeniu całkowitego braku oszczędności z tytułu deduplikacji oraz kompresji danych, jedynie w oparciu o dostarczoną liczbę węzłów pamięci masowej, bez konieczności ich dodawania
4. Wszystkie licencje dla rozwiązania są zapewnione dla jego maksymalnej możliwej pojemności i rozmiaru klastra;
5. Wszystkie licencje dla rozwiązania są zapewnione tak aby obejmować całkowitą wymaganą dla danego ukompletowania funkcjonalność rozwiązania
6. Wymaga się dostarczenia oprogramowania wirtualizacyjnego, z funkcjonalnością opisaną w punkcie C). Licencje na oprogramowanie wirtualizacyjne muszą obejmować wszystkie cztery węzły w klastrze.
7. Gwarancja dla każdego węzła serwerowego na okres minimum 1 roku oraz bezterminowa licencja na działanie do oprogramowania z nim powiązanego, w tym co najmniej 1 rok dostępne aktualizacje

Dedykowany system zarządzania oraz przełączania LAN dla klastra systemu wirtualizacji typu HCI

Dla zapewnienia zarządzania oraz wewnętrznej łączności klastra systemu wirtualizacji typu HCI wymaga się dostarczenia pary dedykowanych redundantnych przełączników LAN. Każdy przełącznik o następujących parametrach:

Lp.	Parametr	Minimalne parametry techniczne
1	Ilość portów	32 fizyczne porty 40 GbE QSFP dla dołączania węzłów serwerowych klastra pamięci masowej i realizacji połączeń zewnętrznych
2	Wkładki QSFP	4 wkładki 40G SR BiDI
3	Przepustowość	Minimum 2 Tbps
4	Wydajność przełączania	Minimum 720 mln pakietów / sek
5	Opóźnienia	Nie większe niż 1 mikrosekunda dla przełączanych ramek Ethernet
6	Ilość obsługiwanych VLAN	Minimum 3000

7	Ilość obsługiwanych adresów MAC	Minimum 32 000 adresów MAC
8	Porty zarządzające	Zewnętrzny dedykowany port zarządzający Ethernet 100/1000BaseT
9	Obsługa protokołów i standardów	• Obsługa standardu IEEE 802.1Q; • Obsługa standardu IEEE 802.1P; • IEEE Data Center Bridging (obsługa standardów 802.1Qbb PFC, 802.1Qaz Enhanced Transmission Selection • Protokół Link Aggregation Control Protocol (LACP): IEEE 802.3ad; • Obsługa ramek Jumbo dla wszystkich portów (ramki o długości do 9216 bajtów); • Port Security • Protokół IGMP v1, v2, v3 snooping;
10	Zasilanie	2 redundantne zasilacze.
11	Gwarancja	Minimum 12 miesięczna

B) Przełączniki dostępowe 10/25/40/100GE Ethernet – 2 sztuki.

Należy dostarczyć dwa przełączniki stanowiące rdzeń sieci laboratoryjnej. Rolą tych przełączników będzie połączenie urządzeń dedykowanych od każdego środowiska laboratoryjnego do centralnego punktu sieci oraz do klastra systemu wirtualizacji typu HCI.

Wymagania funkcjonalne:

1. Przełącznik posiada:
   1.1. 48 portów 1/10/25GE SFP+ bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego
   1.2. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps
2. Parametry wydajnościowe:
   2.1. Prędkość przełączania „wirespeed" dla każdego portu przełącznika
   2.2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
   2.3. Obsługiwana łączna przepływność (pasmo) min. 3 Tbps
   2.4. Obsługiwana łączna przepustowość pakietowa przełącznika min. 1 bpps
   2.5. Opóźnienie przełączania pakietów nie większe niż 2 µs
3. Przełącznik posiada następującą funkcjonalność warstwy L2:
   3.1. Trunking IEEE 802.1Q VLAN;
   3.2. Wsparcie dla min. 3000 sieci VLAN;
   3.3. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   3.4. Wsparcie sprzętowe dla minimum 250 tysięcy adresów MAC
   3.5. IEEE 802.1w Rapid Spanning Tree (RST)
   3.6. IEEE 802.1s Multiple Spanning Tree (MST)
   3.7. Wsparcie sprzętowe dla tunelowania QinQ
   3.8. Statyczny i dynamiczny NAT
   3.9. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree
   3.10. Internet Group Management Protocol (IGMP) Versions 2, 3;
   3.11. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   3.12. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce
   3.13. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
4. Przełącznik posiada następująca funkcjonalność warstwy L3
   4.1. Sprzętowe przełączanie pakietów w warstwie L3

4.2. Routing w oparciu o trasy statyczne
4.3. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
4.4. Policy Based Routing (PBR) dla IPv4 i IPv6
4.5. Możliwość uruchomienia sprzętowego load balancera dla protokołów IPv4 i IPv6 ze wsparciem dla tworzenia grup serwerów i adresów VIP, próbkowania serwerów, wyboru ruchu na podstawie protokołu/portu L4 i poprzez filtr ACL
4.6. VRRP v3
4.7. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol)
4.8. Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP
4.9. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast)
4.10. Wsparcie dla IGMPv3 oraz MSDP
4.11. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych
4.12. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking)
4.13. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP)
4.14. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - Access Control List
4.15. Jeśli funkcjonalność opisana powyżej w pkt 4. wymaga dostarczenia dodatkowej licencji to jest ona wymagana na tym etapie, licencje nie mogą mieć ograniczeń czasowych

5. Przełącznik posiada możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów lub przełączników nie jest realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3 a jedynie w ramach domeny fizycznej bądź stosu urządzeń. Porty modułu wyniesionego są udostępniane do zarządzania i monitorowania z poziomu przełącznika macierzystego.
6. Przełącznik posiada sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.
7. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   7.1. Obsługa co najmniej 256 sprzętowych VTEP (VXLAN Tunnel Endpoint)
   7.2. Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway)
   7.3. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP
   7.4. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
   7.5. Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol)
   7.6. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).
   7.7. Jeśli funkcjonalność opisana powyżej w pkt 7. wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie
8. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   8.1. Layer 2 IEEE 802.1p (CoS);
   8.2. Klasyfikacja QoS w oparciu o listy (ACL (Access Control List) – w warstwach 2, 3, 4;
   8.3. Kolejkowanie na wyjściu w oparciu o CoS 802.1p;
   8.4. Bezwzględne (strict-priority) kolejkowanie na wyjściu;
   8.5. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający
   8.6. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych
   8.7. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   8.8. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
9. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:

9.1. Wejściowe ACL (standardowe oraz rozszerzone);
9.2. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
9.3. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
9.4. ACL oparte o VLAN-y (VACL);
9.5. ACL oparte o porty (PACL);
9.6. DHCP Snooping
9.7. ARP Inspection
9.8. IP Source Guard
9.9. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast

10. Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
10.1. Port zarządzający 100/1000 Mbps;
10.2. Port konsoli CLI;
10.3. Zarządzanie In-band;
10.4. SSHv2;
10.5. Authentication, authorization, and accounting (AAA);
10.6. RADIUS;
10.7. TACACS+
10.8. Syslog;
10.9. SNMP v1, v2, v3;
10.10. RMON (przynajmniej grupy Events, Alarms)
10.11. sFlow lub netFlow
10.12. IEEE 802.1ab LLDP
10.13. 802.1x i dynamiczny przydział VLAN do portu
10.14. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
10.15. Role-Based Access Control RBAC;
10.16. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
10.17. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror)
10.18. Network Time Protocol (NTP);
10.19. Precision Time Protocol IEEE 1588
10.20. Diagnostyka procesu BOOT;
10.21. Ping
10.22. Traceroute

11. Narzędzia programowania i zarzadzania przełącznikiem:
11.1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
11.2. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika
11.3. Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych, niezależnie od systemu operacyjnego przełącznika. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika.
11.4. Wsparcie dla kontenerów Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych
11.5. Interfejs programistyczny REST API wraz z upublicznionym SDK
11.6. Możliwość zainstalowania klienta Chef
11.7. Możliwosć zainstalowania agenta Puppet
11.8. Wsparcie dls NETCONF i zarządzania poprzez XML
11.9. Wsparcie dla OpenStack Neutron plugin

12. Przełącznik musi być wyposażony w:
12.1. 1 kabel Twinax 100GE QSFP+ o długości co najmniej 1 m

12.2. 8 wkładek 10 Gbps SFP+ typu SR-S

13. Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych.
14. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19", w wypadku zastosowania przełącznika modularnego dopuszcza się większy rozmiar urządzenia

C) Oprogramowanie systemu wirtualizacji

1. Warstwa wirtualizacji powinna być rozwiązaniem systemowym tzn. powinna być zainstalowana bezpośrednio na sprzęcie fizycznym.
2. Rozwiązanie powinno zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min 6TB pamięci operacyjnej.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych do 128 procesorów wirtualnych każda z krokiem co jeden)
5. Rozwiązanie powinno umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
6. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
7. Rozwiązanie powinno wspierać, co najmniej następujące systemy operacyjne:
   7.1. Windows Server 2012 R2,
   7.2. Windows Server 2016
   7.3. Windows Server 2019,
   7.4. RHEL w wersjach 5.x do 8.x,
   7.5. Debian w wersjach 6x –9.x,
   7.6. CentOS w wersjach 5.x –8.x,
   7.7. Oracle Linux w wersjach 4.9 –8.x,
   7.8. FreeBSD w wersjach 7.x –11.x,
8. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i usługami.
9. Rozwiązanie powinno zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
10. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
11. Oprogramowanie do wirtualizacji powinno zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
12. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory.
13. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane.
14. Rozwiązanie powinno mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
15. Powinna zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury. Czas niedostępności innych usług nie powinien przekraczać kilkunastu minut.
16. Rozwiązanie powinno umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.

17. Rozwiązanie powinno zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej tak, aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany

Należy dostarczyć bezterminowe licencje pokrywające wszystkie hosty klastra systemu wirtualizacji typu HCI, w tym co najmniej 1 rok dostępne aktualizacje.

D) Oprogramowanie do zarządzania systemem wirtualizacji

1. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance
2. Konsola graficzna musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum IE i Firefox)
3. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska
4. Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną
5. Rozwiązanie musi zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń fizycznych wykorzystujących technologię ‘Syslog”
6. Rozwiązanie musi integrować się z oprogramowaniem do monitorowania i zarządzania platformą wirtualizacyjną w ten sposób, że z poziomu konsoli użytkownika oprogramowania do monitorowania i zarządzania platformą wirtualizacyjną musi istnieć możliwość uzyskania natychmiastowego dostępu do logów konkretnego urządzenia fizycznego
7. Rozwiązanie musi umożliwiać personalizację i wizualizację logów w postaci wykresów liniowych, kołowych, słupkowych itp.
8. Rozwiązanie musi zapewniać monitorowanie urządzeń typu „Real Time”
9. Rozwiązanie musi posiadać wbudowaną bazę wiedzy dotycząca logów, zdarzeń itp.
10. Rozwiązanie musi umożliwiać łatwą korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację
11. Musi istnieć możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora
12. Rozwiązanie musi umożliwiać łatwe i szybkie przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria
13. Musi istnieć możliwość implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN, itp., tak aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej
14. Rozwiązanie musi posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów, takich jak np. logi aplikacji, logi sieciowe, pliki konfiguracyjne, informacje, dane wydajnościowe, zrzuty awaryjne itp., a także logów ‘nieustrukturyzowanych”
15. Rozwiązanie musi umożliwiać zdefiniowanie struktury dla logów nieustrukturyzowanych
16. Uprawnienia do interfejsu prezentacji i analizy logów muszą dopuszczać rozłączność z uprawnieniami do infrastruktury
17. Rozwiązanie musi umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami

Należy dostarczyć bezterminowe licencje dla systemu centralnego zarządzania systemem wirtualizacji, w tym co najmniej 1 rok dostępne aktualizacje.

E) Serwer kopii zapasowych - 1 sztuka

Należy dostarczyć serwer RACK dedykowany do wykonywania kopii zapasowych o minimalnych parametrach:

Lp.	Parametr	Minimalne parametry techniczne
1	**CPU**	Jeden procesor co najmniej 12 rdzeni, o taktowaniu minimalnym 2.2 GHz zapewniający dla zaoferowanego serwera osiągnięcie w teście CPU2017 Integer Rate Base publikowanym na stronach spec.org wyniku minimum 135 punktów w konfiguracji dwuprocesorowej
2	**Obudowa**	Obudowa wielkości maksymalnie 2U umożliwiająca zamontowanie co najmniej 12 dysków 3,5 oraz 2 dysków 2,5.
2	**Pamięć RAM**	minimum 128 GB pamięci DRAM DDR4 2933 MHz RDIMM (32 GB x 4)
3	**Dyski**	12 dysków 8 TB 12G SAS 7.2 K LFF
5	**Karty sieciowe**	Konwergentny adapter sieciowy LAN/SAN, co najmniej 4 x 10/25 GE SFP28 wraz z dwoma kablami połączeniowymi SFP+ o długości co najmniej 3m
6	**Kontroler RAID**	Wspierający RAID 0, 1,5,10 z 2 GB Cache
7	**OS**	Zainstalowany system operacyjny Windows Server 2019 Standard
8	**Dodatkowe dyski**	2 dyski systemowe SSD o wielkości min. 480 GB 2.5 6G SATA
10	**Zasilanie**	Dwa redundantne zasilacze o mocy co najmniej 1500 W
11	**Gwarancja**	Minimum 12 miesięczna

F) Oprogramowanie do wykonywania kopii zapasowych

Lp.	Minimalne wymagania techniczne
1	Oprogramowanie musi współpracować z infrastrukturą, co najmniej VMware w wersji 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016 oraz 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
2	Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
3	Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
4	Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
5	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
6	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
7	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
8	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
9	Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
10	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty

	możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
11	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
12	Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
13	Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie
14	Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
15	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
16	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
17	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
18	Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować metadane vCD, odtwarzać maszyny wirtualne do vCD. Oprogramowanie musi oferować portal samoobsługowy do backupu i odtwarzania dla użytkowników vCD.
19	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
20	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
21	Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
22	Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
23	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
24	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
25	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
26	Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru
27	Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
28	Oprogramowanie musi integrować się bezpośrednio z HPE StoreServe oraz Nimble Storage. Musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware
29	Takie same funkcjonalności muszą być zapewnione dla macierzy Dell EMC VNX, VNXe oraz Unity.
30	Takie same funkcjonalności muszą być zapewnione dla macierzy IBM Spectrum Virtualize (IBM Storwize, IBM SVC, Lenovo Storage V-series)

31 32	Takie same funkcjonalności muszą być zapewnione dla macierzy Huawei OceanStor
33	Takie same funkcjonalności muszą być zapewnione dla macierzy INFINIDAT InfiniBox
34	Takie same funkcjonalności muszą być zapewnione dla macierzy Pure Storage FlashArray.
35	Takie same funkcjonalności powinny być zapewnione dla macierzy Netapp z oprogramowaniem ONTAP 8.1 i nowsze włączając możliwość wykonania backupów z zmirrorowanych snapshotów SnapVault lub SnapMirror. Rozwiązanie musi wspierać dowolną metodę wdrożenia macierzy (klaster i 7-mode)
36	Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
37	Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
38	Oprogramowanie musi wspierać wykonywanie backupu z wykorzystaniem NDMP bezpośrednio na taśmę
39	Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
40	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
41	Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
42	Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
43	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu.
44	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
45	Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
46	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
47	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
48	Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
49	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
50	Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
51	Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
52	Oprogramowanie musi umożliwiać uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
53	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami

54	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
55	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
56	Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
57	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
58	Oprogramowanie musi wspierać odtwarzanie plików, co najmniej z następujących systemów plików: • Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs • BSD: UFS, UFS2 • Solaris: ZFS, UFS • Mac: HFS, HFS+ • Windows: NTFS, FAT, FAT32, ReFS • Novell OES: NSS
59	Oprogramowanie musi wspierać przywracanie plików z partycji, co najmniej Linux LVM oraz Windows Storage Spaces.
60	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
61	Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
62	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects")
63	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
64	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
65	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
66	Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
67	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
68	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
69	Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
70	Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
71	Oprogramowanie musi pozwalać na odtworzenie maszyn wirtualnych z macierzowych snapshotów ze wspieranych macierzy.
72	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
73	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
74	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym

	środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
75	Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
76	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
77	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
78	Zamawiający wymaga dostarczenia bezterminowych licencji pokrywających wszystkie niezbędne serwery, w tym co najmniej 1 rok dostępne aktualizacje.

Komponenty LAN/WAN dedykowane do środowiska laboratoryjnego

A) Firewall nowej generacji – 4 sztuki

Architektura urządzenia, obudowa, interfejsy

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall)
3. Urządzenie wyposażone w 8 wbudowanych portów GbE RJ45 oraz 4 porty Gigabit Ethernet SFP
4. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 500 sieci VLAN
5. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band
6. Urządzenie wyposażone w port USB 3.0
7. Urządzenie jest zasilanie prądem przemiennym 230V
8. Możliwość montażu w szafie rack 19" (dołączone niezbędne elementy montażowe)
9. Wysokość urządzenia 1RU

Parametry wydajnościowe

1. Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 1.5 Gbps dla pakietów wielkości 1024B
2. Urządzenie osiąga powyższe parametry wydajnościowe również wraz z uruchomionym silnikiem IPS.
3. 200 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 15 000 nowych połączeń na sekundę
4. Możliwość połączenia VPN do 150 urządzeń z maksymalną sumaryczną przepustowością 800 Mbps dla pakietów 1024B TCP
5. Przepustowość dekrypcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi przynajmniej 600 Mbps

Funkcjonalność urządzenia

1. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
2. Możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentnym
3. Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP)
4. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory
5. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT)
6. Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby
7. Urządzanie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN)
8. Urządzenie zapewnia funkcjonalności:
   8.1. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control)
   8.2. systemu IPS
   8.3. systemu ochrony przed malware
   8.4. systemu filtracji ruchu w oparciu o URL
9. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
   9.1. Wiedza o użytkownikach – uwierzytelnienie

9.2. Wiedza o urządzeniach – pasywne skanowanie ruchu
9.3. Wiedza o urządzeniach mobilnych
9.4. Wiedza o aplikacjach wykorzystywanych po stronie klienta
9.5. Wiedza o podatnościach
9.6. Wiedza o bieżących zagrożeniach
9.7. Baza danych URL

10. System posiada otwarte API dla współpracy z systemami zewnętrznymi
11. Rozwiązanie współpracuje z systemami SIEM
12. System wykrywania aplikacji AVC zapewniający:
    12.1. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji
    12.2. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług
    12.3. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
    12.4. 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
13. System IPS zapewniający:
    13.1. możliwość pracy w trybie in-line
    13.2. możliwość pracy w trybie pasywnym (IDS)
    13.3. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        13.3.1. złośliwe oprogramowanie
        13.3.2. skanowanie sieci
        13.3.3. ataki na usługę VoIP
        13.3.4. próby przepełnienia bufora
        13.3.5. ataki na aplikacje P2P
        13.3.6. zagrożenia dnia zerowego, itp.
    13.4. Możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)
    13.5. Wiele sposobów wykrywania zagrożeń w tym:
        13.5.1. sygnatury ataków opartych na exploitach
        13.5.2. reguły oparte na zagrożeniach
        13.5.3. mechanizm wykrywania anomalii w protokołach
        13.5.4. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
    13.6. 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
    13.7. Mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives)
    13.8. Możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
    13.9. Wiele możliwości reakcji na zdarzenia w tym takie, jak:
        13.9.1. tylko monitorowanie
        13.9.2. blokowanie ruchu zawierającego zagrożenia
        13.9.3. zastąpienie zawartości pakietów
        13.9.4. zapisywanie pakietów
    13.10. Możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
    13.11. 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 - zbierane są informacje o:
        13.11.1. systemach operacyjnych
        13.11.2. serwisach
        13.11.3. otwartych portach, aplikacjach
        13.11.4. zagrożeniach
    13.12. 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

13.13. Możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
13.14. Możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
13.15. Możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
13.16. Mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
13.17. Możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
13.18. Obsługę reguł Snort
13.19. Możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
13.20. Mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)
13.21. Mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa
14. System filtracji URL zapewniający:
14.1. Kategoryzację stron – w co najmniej 80 kategoriach
14.2. Bazę URL o wielkości nie mniejszej niż 280 mln URL
14.3. Bazę URL producenta rozwiązania
15. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
15.1. Pliki systemowe
15.2. Pliki graficzne
15.3. Pliki PDF
15.4. Pliki wykonywalne
15.5. Pliki multimedialne
15.6. Pliki pakietu Office
15.7. Pliki skompresowane
16. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download
17. Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez
17.1. Sprawdzenie reputacji plików w systemie globalnym
17.2. Sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze)
17.3. Statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu
18. Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
18.1. Pliki wolne od złośliwego kodu
18.2. Pliki zawierające złośliwy kod
18.3. Pliki podejrzane
18.4. Pliki o własnej, zdefiniowanej przez użytkownika kategorii
19. Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna)
20. Rozwiązanie umożliwia integracje z chmurową konsolą korelacji informacji o zagrożeniach z różnych rozwiązań bezpieczeństwa tego samego producenta.

Urządzenie objęte, co najmniej 12 miesięczną gwarancją. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez cały okres gwarancji.

B) Centralna konsola zarządzająca kompatybilna z urządzeniami Firewall opisanymi w punkcie A)

Wraz z urządzeniem zostanie dostarczona dedykowana platforma zarządzająca oparta na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym. Platforma zarządzająca musi mieć formę maszyny fizycznej i spełnia następujące wymagania:

1. Umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym
2. Jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego
3. Zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria
4. Ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm
5. Ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami
6. Zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany
7. Zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS
8. Zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją
9. Ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci
10. Daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta
11. Ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora
12. Zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS
13. Ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej
14. Zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania
15. Zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu
16. Zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP
17. Zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze
18. Zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika
19. Zapewnia informowanie o zagrożeniach poprzez
    19.1 Wysłanie e-maila,
    19.2 Wysłanie trap SNMP,
    19.3 Przesłanie informacji do serwera Syslog,
    19.4 Uruchomienie skryptu użytkownika
    19.5 Wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze
20. Posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy
    20.1 Aktualnego stanu danego urządzenia,
    20.2 Podglądu historii dostępnych zasobów,

20.3 Możliwość eliminacji powtarzających się alarmów (tzw. Black Listing)

21. Ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym
22. Ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
    22.1 Dozwolone porty i protokoły
    22.2 Dozwolone aplikacje według różnych kategorii
    22.3 Dozwolone kategorie stron internetowych (URL filtering)
    22.4 Dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej
    22.5 Sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne
23. W ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia

Urządzenie objęte, co najmniej 12 miesięczną gwarancją.

C) Kontroler sieci bezprzewodowej – 2 sztuki.

1. Urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
   1.1. Zarządzanie politykami bezpieczeństwa
   1.2. Wykrywanie zagrożeń w sieci bezprzewodowej
   1.3. Zarządzanie pasmem radiowym
   1.4. Zarządzanie mobilnością
   1.5. Zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415)
2. Obsługa do 250 punktów dostępowych (kratowe lub klasyczne)
3. 4 interfejsy 2.5G/1G oraz 2 interfejsy 1/10G (SFP/SFP+)
4. Obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
5. Wydajność urządzenia 5 Gbps
6. Obsługa 5000 klientów sieci bezprzewodowej
7. Zarządzanie pasmem radiowym punktów dostępowych:
   7.1. Automatyczna adaptacja do zmian w czasie rzeczywistym
   7.2. Optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
   7.3. Dynamiczne przydzielanie kanałów radiowych
   7.4. Wykrywanie, eliminacja i unikanie interferencji
   7.5. Równoważenie obciążenia punktów dostępowych
   7.6. Tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
   7.7. Automatyczna dystrybucja klientów pomiędzy punkty dostępowe
   7.8. Mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
   7.9. Dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
8. Mapowanie SSID do segmentów VLAN w sieci przewodowej
   8.1. 1:1
   8.2. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
   8.3. Możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
9. Obsługa sieci kratowych
   9.1. Komunikacja między punktami dostępowymi bez medium kablowego
   9.2. Separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)

9.3. Automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)
9.4. Automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
9.5. Autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC

10. Obsługa mechanizmów bezpieczeństwa:
    10.1. 802.11i, WPA2, WPA, WEP
    10.2. 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
    10.3. Obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
    10.4. Kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
    10.5. Obsługa profilowania użytkowników:
        10.5.1. Przydział sieci VLAN
        10.5.2. Przydział list kontroli dostępu (ACL)
    10.6. Uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w
    10.7. Uwierzytelnianie punktów dostępowych w oparciu o certyfikaty
    10.8. Obsługa list kontroli dostępu (ACL)
    10.9. Obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X
    10.10. Wykrywanie i dezaktywacja obcych punktów dostępowych
    10.11. Ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP
    10.12. DHCP proxy
    10.13. Eksport dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)
    10.14. Zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:
        10.14.1. Kryptograficzne podpisywanie obrazów oprogramowania
        10.14.2. Bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych
        10.14.3. Wbudowany moduł sprzętowy unikalnie identyfikujący urządzenie i jego pochodzenie
11. Obsługa ruchu unicast IPv4 i IPv6
12. Obsługa ruchu multicast IPv4 i IPv6
    12.1. IGMP / MLD snooping
    12.2. Optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
    12.3. Obsługa konwersji ruchu multicast do unicast
13. Obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami)
14. Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k
15. Wsparcie dla IEEE 802.11u
16. Obsługa mechanizmów QoS
    16.1. 802.1p
    16.2. WMM, TSpec, U-APSD
    16.3. Ograniczanie pasma per użytkownik
    16.4. Call Admission Control, SIP CAC, Call Snooping
    16.5. Równomierna obsługa klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego
    16.6. Kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID
17. Obsługa sensorów symulujących pracę klientów bezprzewodowych, które pozwalają na badanie działania wybranych usług w sieci (DNS, DHCP, RADIUS, IMAP, Outlook Web Access, inne) i eksportują wyniki testów do dedykowanego zewnętrznego kolektora
18. Obsługa dostępu gościnnego (IPv4 i IPv6)
    18.1. Przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony)

18.2. Przekierowanie użytkowników do strony logowania na zewnętrznym serwerze
19. Współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych
20. Obsługa NTP wersji 4 (IPv4 oraz IPv6)
21. Obsługa redundancji rozwiązania (N+1)
22. Obsługa redundancji 1:1 (active/standby) zapewniającej:
    22.1. Utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera
    22.2. Synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej
23. Dedykowany interfejs 1GE typu RJ45 służący do połączenia dwóch kontrolerów w redundantną parę 1:1
24. Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie ponad 1000 aplikacji
25. Zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow
26. Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji
27. Zarządzanie przez HTTPS, SNMP, SSH, NETCONF, port konsoli szeregowej
28. Obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020)

Urządzenie objęte, co najmniej 12 miesięczną gwarancją.

D) Punkty dostępu bezprzewodowego – 8 sztuk

Każdy z oferowanych punktów dostępu bezprzewodowego musi spełniać następujące wymagania:

1. Obsługa standardów 802.11a/b/g/n/ac/ax
    1.1. Obsługa OFDMA (downlink), TWT, BSS Coloring (tylko dla 802.11ax)
    1.2. Obsługa MU-MIMO – min. 4x4:4
    1.3. Obsługa kanałów 20, 40 MHz dla 802.11n
    1.4. Obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax
    1.5. Obsługa prędkości PHY do 3,47 Gbps (ac)
    1.6. Obsługa prędkośći PHY do 5,3 Gbps (ax)
    1.7. Obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
    1.8. Obsługa beamforming dla klientów 802.11a/g/n/ac/ax
    1.9. Obsługa MRC (Maximal Ratio Combining)
2. Obsługa szerokiego zakresu kanałów radiowych:
    2.1. Dla zakresu 2.4 GHz: min. 13 kanałów
    2.2. Dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów
    2.3. Dla zakresu 5GHz (extended UNII-2): min. 8 kanałów
3. Konfigurowalna moc nadajnika
    3.1. Dla zakresu 2.4 GHz: do 100 mW
    3.2. Dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW
    3.3. Dla zakresu 5GHz (extended UNII-2): do 200 mW
4. Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
    4.1. Automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
    4.2. Optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
    4.3. Obsługa min. 16 BSSID
    4.4. Definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID

4.5. Uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
4.6. Obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)
4.7. Możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników
4.8. Obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6
4.9. Jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IDS)
4.10. Obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
4.11. Obsługa IPv6
4.12. Obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
4.13. Obsługa mechanizmów QoS:
4.13.1. Ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik
4.13.2. Obsługa WMM, TSPEC, U-APSD
4.14. Współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne
4.15. Wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM
4.16. Wsparcie IEEE 802.11i, WPA2, WPA
4.17. Wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)

5. Możliwość pracy jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach: (zmiana trybu pracy (przez wgranie oprogramowania) musi być bez kosztowa w okresie trwania kontraktu serwisowego):
5.1. Obsługa do 100 punktów dostępowych bez dodatkowych licencji
5.2. Obsługa do 2000 klientów
5.3. Możliwość konfiguracji do 16 sieci bezprzewodowych
5.4. Centralna optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
5.5. Obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
5.6. Obsługa mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v
5.7. Jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)
5.8. Wykrywanie do 1000 obcych klientów oraz do 100 obcych AP
5.9. Konfiguracja polityk bezpieczeństwa per SSID
5.10. Obsługa WPA2 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS)
5.11. Współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)
5.12. Tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe
5.13. Filtrowanie MAC adresów (Whitelist)
5.14. Analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)
5.15. Dwukierunkowe limitowanie transmisji (bidirectional rate-limiting ruchu) per klient, per WLAN, per BSSID
5.16. Profilowanie (rozpoznawanie typów) urządzeń podłączających się do sieci bezprzewodowej z obsługą aktualizacji listy wspieranych sygnatur OUI za pomocą pliku tekstowego
5.17. Obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC)
5.18. Obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym
5.19. Obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; obsługa wydrukowania lub wysłania mailem danych logowania użytkowników

5.20. Zarządzanie przez HTTPS
5.21. Wsparcie SSH, SNMP, NTP, SYSLOG
5.22. Obsługa aktualizacji oprogramowania przez SFTP
5.23. Wbudowany serwer DHCP
5.24. Wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera

6. Interfejs MultiGigabit Ethernet (100/1000/2500) - IEEE 802.3bz
7. Interfejs konsoli RJ45
8. Port USB 2.0 (funkcjonalność dostępna w przyszłych wersjach oprogramowania)
9. 2 GB RAM, 1 GB Flash
10. Zasilanie przez PoE+ (IEEE 802.3at)
11. Anteny zewnętrzne o zysku:
    11.1. Dla modułu 2,4 GHz do 6dBi
    11.2. Da modułu 5 GHz: do 6dBi
12. Obudowa przystosowana do pracy w zakresie temperatur minimum 0 – 50^{o}C
13. Diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji
14. Wbudowane radio Bluetooth Low Energy (BLE) 5.0 IoT ready (Zigbee)
15. Z urządzeniem musi być dostarczone oprogramowanie umożliwiające śledzenie lokalizacji użytkowników oraz urządzeń typu BEACON poprzez protokoły sieć bezprzewodowej oraz Bluetooth. Zamawiający zapewnia zasoby sprzętowe na instalację oprogramowania.
16. Z urządzeniem musi być dostarczonych 10 beacon'ów współpracujących z rozwiązaniem.
17. Punkt dostępowy musi umożliwiać uruchomienie funkcjonalności Wireless IPS. Jeżeli na tą funkcjonalność wymagana jest licencja to należy ją dostarczyć.
18. W przypadku kiedy do obsługi Access Pointa przez kontroler WLAN wymagana jest licencja to należy ją dostarczyć. Zamawiający wymaga dostarczenia licencji bezterminowej, w tym co najmniej 1 rok dostępne aktualizacje.

Urządzenie objęte, co najmniej 12 miesięczną gwarancją.

E) Router wielousługowy – 4 sztuki

Oferowane urządzenie (router) powinno spełniać następujące wymagania funkcjonalne:

1. Urządzenie dedykowane do zastosowań jako wielousługowy router modularny gotowy do obsługi mechanizmów bezpiecznej i niezawodnej sieci WAN w oparciu o Internet.
2. Architektura oferowanego urządzenia powinna umożliwiać:
   2.1. Instalację nie mniej niż 2 karty z interfejsami rozszerzeń z możliwością wyłączenia modułu
   2.2. Instalację wewnętrznego modułu typu DSP z możliwością jego wyłączenia
   2.3. Architektura musi posiadać możliwość bezpośredniej komunikacji pomiędzy modułami z pominięciem głównego procesora jeśli ruch sieciowy nie jest skierowany do routera
3. Oferowane urządzenie musi posiadać wszystkie interfejsy jako „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
4. Oferowane urządzenie musi umożliwiać wsparcie funkcjonalności akceleratora ruchu sieciowego Funkcjonalność ta nie jest wymagana w momencie zamówienia, natomiast uruchomienie funkcjonalności powinno być możliwe po doposażeniu urządzenia w rekomendowane zasoby pamięciowe oraz licencje. Zakres funkcjonalny funkcji akceleratora sieciowego musi obejmować:
   4.1. Kompresji ruchu – np. algorytmem LZ
   4.2. Optymalizacją połączeń TCP
   4.3. Deduplikacją ruchu sieciowego
   4.4. Wsparcie dla obsługi minimum 1300 sesji TCP
5. Oferowane urządzenie musi współpracować z systemem zarządzania optymalizatorami ruchu sieciowego oferującym centralny punkt konfiguracji, monitorowania w czasie rzeczywistym, zarządzania błędami i raportowania.
6. Oferowane urządzenie musi posiadać wsparcie dla akceleracji min. poniższych aplikacji:
   6.1. CIFS (SMBv2)
   6.2. NFSv3
   6.3. Exchange 2003/2007/2010 (MAPI)
   6.4. Encrypted MAPI
   6.5. Microsoft SQL
   6.6. Oracle
   6.7. SSL
   6.8. HTTP
   6.9. Microsoft Office 365
7. Oferowane urządzenie musi posiadać sloty umożliwiające rozbudowę następującymi rodzajami modułów:
   7.1. Moduł z cyfrowymi interfejsem T1/E1 dla ruchu głosowego lub ruchu typu channelized z gęstością interfejsów nie mniejszą niż 4 portów T1/E1
   7.2. Moduł z interfejsami szeregowymi WAN, w liczbie min. 4 porty na moduł
   7.3. Moduł interfejsów głosowych analogowych (FSX/FXO) z gęstością minimum 4 porty FXO lub 4 porty FXS na moduł
   7.4. Moduł z dyskiem twardym SSD
   7.5. Moduł przełącznika Ethernet (funkcje L2 i L3), oczekiwana liczba portów przełącznika nie może być mniejsza niż 8 dla jednego modułu. Porty przełącznika muszą być dostępne również w wersji z zasilaniem PoE
   7.6. Moduł umożliwiający komunikację po sieci komórkowej w technologii 3G/4G (LTE);
   7.7. Moduł z portem VDSL2 / ADSL2+ over POTS
   7.8. Moduł z portem VDSL2 / ADSL2+ over POTS / Annex M
   7.9. Moduł z portem VDSL2 / ADSL2+ over ISDN
   7.10. Moduł z układami DSP
8. Oferowane urządzenie musi umożliwiać rozbudowę o moduł z układami DSP z możliwością obsadzenia modułami:
   8.1. O gęstości nie mniejszej niż 256 kanałów

8.2. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, trancoding, conferencing) z granulacją do 1 DSP.
8.3. Posiadających wsparcie dla usług wideo
8.4. Obsługującymi kodeki:
8.4.1. G.711
8.4.2. ClearChannel
8.4.3. G.729a
8.4.4. G.729ab
8.4.5. G.726
8.4.6. G.722
8.4.7. G.728
8.4.8. G.729
8.4.9. G.729b
8.4.10. Internet Low Bit
8.4.11. Funkcjonalność FaxRelay
8.4.12. Funkcjonalność ModemRelay
8.5. Obsługującymi funkcjonalność transkodowania pomiędzy różnymi typami kodeków
8.6. Obsługującymi funkcjonalność konferencji głosowych (musi być możliwość obsłużenia do co najmniej 6 konferencji po 64 uczestników lub 66 konferencji po 8 uczestników)
8.7. Obsługującymi kompresję, wykrywanie aktywności głosowej, zarządzenie jitterem i funkcje kasowanie echa (co najmniej 128 ms). Funkcja kasowania echa musi być zgodna ze standardem ITU-T G.168
8.8. Obsługującymi szyfrowanie transmisji głosu z wykorzystaniem SRTP

9. Oferowane urządzenie musi posiadać zintegrowaną sprzętową akcelerację szyfrowania DES/3DES/AES oraz musi obsługiwać algorytmy Suite-B dla szyfrowania, w tym:
9.1. SHA-2,
9.2. AES-Galois Counter Mode (AES-GCM),
9.3. Elliptic Curve Diffie-Hellman (ECDH),
9.4. Elliptic Curve Digital Signature Algorithm (ECDSA),
9.5. IKEv2
10. Oferowane urządzenie powinna charakteryzować następująca wydajność:
10.1. Dla pakietów unicast IPv4 o długości 64bajtów przepustowość rzędu 100 Mbps;
10.2. Dla pakietów IMIX przy włączonych usługach szyfrowania z IPSec, szczegółowej analizy aplikacji, kontroli jakości usługi QoS o przepustowości minimum 50 Mbps
11. Oferowane urządzenie musi posiadać następujące funkcjonalności w zakresie oprogramowania
11.1. Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i SSM) oraz routing statyczny;
11.2. Protokół BGP musi posiadać obsługę 4 bajtowych ASN;
11.3. Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv2, Bi-directional PIM;
11.4. Musi posiadać obsługę protokołu IGMPv3
11.5. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)
11.6. Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q
11.7. Musi obsługiwać IPv6 w tym ICMP dla IPv6
11.8. 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
11.9. Musi zapewniać mechanizmy korelacji zdarzeń związanych z filtracją za pomocą list kontroli dostępu dla syslog (np. za pomocą etykiety przypisanej do określonego wpisu na listach kontroli dostępu lub skrót MD5 generowany przez router)
11.10. Musi posiadać obsługę NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast
11.11. Mechanizm NAT musi zapewniać wsparcie dla H.245
11.12. Musi posiadać wsparcie dla protokołów WCCP i WCCPv2
11.13. Musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 300 instancji VRF
11.14. Musi posiadać obsługę mechanizmu DiffServ

11.15. Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
11.16. Musi zapewniać obsługę mechanizmów kolejkowania ruchu:
11.17. z obsługą kolejki absolutnego priorytetu
11.18. ze statyczną alokacją pasma dla typu ruchu
11.19. WFQ
11.20. Musi obsługiwać mechanizm WRED
11.21. Musi obsługiwać mechanizm Traffic Shaping
11.22. Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu
11.23. Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.
11.24. Musi obsługiwać protokół NTP
11.25. Musi obsługiwać DHCP w zakresie Client, Server
11.26. Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub równoważny)
11.27. Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
11.28. Musi obsługiwać protokół MPLS (funkcje LER i LSR)
11.29. Musi obsługiwać MPLS over GRE
11.30. Musi wspierać QoS dla MPLS
11.31. Musi obsługiwać MPLS Traffic Engineering
11.32. Musi obsługiwać MPLS VPN
11.33. Musi obsługiwać funkcjonalność Multicast dla MPLS VPN
11.34. Musi obsługiwać funkcjonalność Any Transport over MPLS Graceful Restart
11.35. Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD) lub równoważny
11.36. Funkcjonalność BFD musi być dostępna dla intefejsów skonfigurowanych do współpracy z VRF
11.37. Musi obsługiwać funkcjonalność BFD Echo Mode lub równoważny
11.38. Funkcjonalność BFD (lubrównoważna) musi posiadać wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego oraz HSRP lub równoważna
11.39. 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 równoważny)
11.40. Funkcjonalność EEM musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych
11.41. Funkcjonalność EEM musi pozwalać na generowanie akcji:
11.42. Wykonanie komendy z poziomu linii poleceń urządzenia
11.43. Wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej
11.44. Wykonanie skryptu
11.45. Wygenerowanie SNMP trap
11.46. Ustawienie lub modyfikacja określonego licznika systemowego
11.47. Musi posiadać funkcjonalność PPPoE
11.48. Musi posiadać funkcjonalność automatycznej optymalizacji routingu (funkcjonalność Optimized Edge Routing lub równoważny
11.49. Funkcjonalność OER (lub równoważna) musi posiadać wsparcie dla:
11.50. Optymalizacji ruchu przychodzącego z wykorzystaniem rozgłaszania informacji BGP do zewnętrznych routerów (BGP external peers)
11.51. Optymalizacji ruchu głosowego
11.52. Optymalizacji w oparciu o informację z protokołów warstw wyższych (protokoły i porty UDP/TCP)

11.53. Musi posiadać wsparcie dla Layer-2 Tunneling Protocol Version 3
11.54. Urządzenie musi posiadać możliwość integracji z centralnym systemem zarządzania, monitorowania, konfiguracji jak również troubleshootingu
11.55. Urządzenie musi umożliwiać obsługę przez zcentralizowany system zarządzania w celu zmiany wersji systemu operacyjnego.
11.56. Musi oferować zaawansowane funkcjonalności bezpieczeństwa takie Zone Based Firewall (ZBF), IPSec VPN, Dynamic Multipoint VPN (DMVPN) oraz FlexVPN
11.57. Musi posiadać funkcjonalność sterowania ruchem i jego rozkładu na łącza różnych operatorów na bazie konfigurowalnych polityk uwzględniających SLA (np. dopuszczalny poziom strat w pakietach, bajtach, dopuszczalne opóźnienia, dopuszczalna zmienność opóźnień - tzw. "jitter").
    11.57.1. Funkcjonalność ta powinna określać klasę ruchu na bazie pól QoS lub analizy wzorca ruchu z uwzględnieniem warstwy aplikacji;
    11.57.2. Funkcjonalność powinna umożliwiać na przełączenie ruchu z klas krytycznych (np. głos, wideo, aplikacje biznesowe) na ścieżkę zapasową w przypadku przekroczenia warunków polityki ruchu dla danej klasy;
    11.57.3. Funkcjonalność musi być kompatybilna z protokołem routingu BGP;
    11.57.4. Funkcjonalność musi mieć możliwość pracy na tunelach IPSec/GRE;
    11.57.5. Funkcjonalność powinna być wspierana razem z włączoną akceleracją ruchu na łączach WAN;
    11.57.6. Mechanizm musi pozwalać na rozkład części ruchu po wszystkich dostępnych łączach operatorskich;

12. Urządzenie musi posiadać zaimplementowanie technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania:
    12.1. Technologia typu Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne, jednoukładowe rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny
    12.2. Technologia typu Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego
    12.3. Technologia typu Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności
13. W zakresie zarządzania i konfiguracji oferowane urządzenie:
    13.1. Musi być zarządzalne za pomocą SNMPv3
    13.2. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JPFlow lub równoważnego
    13.3. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI) jak również interfejsu graficznego (GUI)
    13.4. 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.

Oferowane urządzenie musi spełniać następujące wymagania techniczne:

Lp.	Parametr	Minimalne parametry techniczne
1	**Interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN**	minimum 2 interfejsy Gigabit Ethernet 10/100/1000 minimum jeden interfejs musi mieć możliwość pracy z gigabitowym portem światłowodowym definiowanym przez wkładki GBIC, SFP lub równoważne
2	**Pamięć Flash**	minimum 8GB
3	**Pamięć DRAM**	minimum 8GB
4	**Port USB**	minimum jeden port USB, port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych oraz pełnić funkcję konsoli szeregowej.
5	**Wyposażenie**	urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie zarówno konsoli USB, jak również kablem zasilającym
6	**Obudowa**	Obudowa urządzenia musi być wykonana z metalu, ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej Obudowa musi mieć możliwość montażu w szafie 19" i musi zostać dostarczona z umożliwiającym to zestawem montażowym
8	**Zasilanie**	Oferowane urządzenie musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacze AC)
9	**IPSec VPN**	Urządzenie musi umożliwiać szyfrowanie IPSec z maksymalną wydajnością urządzenia.
10	**Dysk SSD**	minimum SATA 200 GB
11	**Wewnętrzny moduł serwerowy**	CPU 4-Core, 8 GB RAM 1x SSD 200 GB
12	**Gwarancja**	Urządzenie objęte, co najmniej 12 miesięczną gwarancją.

F) Router IOT LTE – 8 sztuk.

Oferowane urządzenie (router) powinno spełniać następujące wymagania funkcjonalne:

1. Posiada obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2, EIGRP oraz routingu multicastowego PIM (Sparse) a także routing statyczny.
2. Posiada wsparcie dla funkcjonalności Policy Based Routing.
3. Posiada wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, PIMv1, PIMv2.
4. Posiada wsparcie dla protokołu DMVPN, GETVPN, IPSec oraz GRE. Router pozwala na zestawienie i obsługę ruchu dla 20 tuneli IPSec.
5. Posiada monitoring parametrów SLA dla protokołów UDP, TCP, HTTP, ICMP, FTP, DNS bezpośrednio z urządzenia
6. Posiada tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.
7. Posiada 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.
8. Posiada wbudowany firewall.
9. Posiada obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast.
10. Posiada obsługę mechanizmu DiffServ.
11. Posiada możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
12. Posiada obsługę mechanizmów kolejkowania ruchu:
13. z obsługą kolejki absolutnego priorytetu
14. ze statyczną alokacją pasma dla typu ruchu
15. WFQ, LLQ, CBWFQ
16. Obsługuje mechanizm WRED.

17. Obsługuje mechanizm ograniczania pasma dla określonego typu ruchu.
18. Obsługuje protokół NTP.
19. Obsługuje DHCP w zakresie Client, Server.
20. Obsługuje obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika).
21. Obsługuje mechanizmy uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+

Oferowane urządzenie (router) powinno spełniać następujące wymagania funkcjonalne w zakresie protokołu SCADA

1. Router zapewnia obsługę protokołów SCADA w zakresie:
2. translacji serial-DNP3 do DNP3/IP
3. translacji EC 60870 T101 do IEC 60870 T104
4. funkcjonowania jako urządzenie dla urządzeń RTU, zapewniające transmisję typu raw-socket.

Oferowane urządzenie (router) powinno spełniać następujące wymagania funkcjonalne w zakresie zarządzania

1. Oferowane urządzenie umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3.
2. Plik konfiguracyjny oferowanego urządzenia (w szczególności plik konfiguracji parametrów routingu) pozwala na edycję w trybie off-line, tzn. Istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej istnieje możliwość przechowywania dowolnej
3. Ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji są widoczne natychmiastowo – bez częściowych restartów urządzenia po dokonaniu zmian.

Oferowane urządzenie (router) powinno spełniać następujące wymagania funkcjonalne w zakresie tworzenia dodatkowych funkcji (programowalność):

1. Możliwość oprogramowania własnych funkcjonalności, których nie ma natywnie w dostarczanym oprogramowaniu. Kod programu lub skryptu ma mieć możliwość wprowadzenia bezpośrednio na urządzenia bez udziału producenta. Kod programu lub skryptu ma być uruchamiany lokalnie na urządzeniu.
2. W ramach tworzenia własnych funkcjonalności kod lub skrypt ma wspierać reakcję na:
    a. Monitorowane obiekty SNMP.
    b. Komunikaty pojawiające się w logu urządzenia.
    c. Liczniki związane z interfejsami oraz systemem.
    d. Komendy wydane w konfiguracji przed użytkownika systemu.
    e. Wskazania próbników i detektorów połączeń.
3. W ramach tworzenia własnych funkcjonalności kod lub skrypt wspiera następujące akcje:
    a. Inicjalizowanie komunikacji email.
    b. Wykonywanie komend typu read, write, execute.
    c. Generowanie trapów SNMP.
    d. Generowanie komunikatów do loga lub zewnętrznego kolektora danych.
    e. Pobieranie danych i informacji środowiskowych systemu.
    f. Sterowanie protokołami routingu, poziomem zabezpieczeń, poziomami dostępu.
    g. Parsowanie tekstu i konfiguracji tak, aby można było odczytać z tekstu lub konfiguracji informację i przekonwertować ją na wybrany format np. numeryczny.
    h. Sortowanie tekstu i konfiguracji.
4. W ramach tworzenia własnych funkcjonalności kod lub skrypt współpracuje z natywnym systemem operacyjnym zainstalowanym na urządzeniu, z zewnętrznymi serwerami FTP, TFTP, plików, DNS, DHCP bez ingerencji producenta.
5. Oprogramowanie lub skrypty mogą być tworzone w pliku tekstowym bez konieczności dodatkowych aplikacji kompilujących kod.
6. Router umożliwia uruchomienie kontenerów docker, co pozwala na pracę urządzenia jako elementu rozproszonej struktury przetwarzania danych (fog computing)

Oferowane urządzenie (router) powinno spełniać następujące wymagania funkcjonalne w zakresie rozproszonego przetwarzania danych (fog computing):

1. Aplikacja z interfejsem web, umożliwiająca następujące działania administracyjne:
    a. Kontrolę działania routera i aplikacji (*kontenerów*) na nim zainstalowanych
    b. Instalację, aktualizację i usuwanie aplikacji z routerów
    c. Uruchamianie i zatrzymywanie, zarządzanie wersjami aplikacji
    d. Monitorowanie zużycia zasobów (chwilowe i czasowe) procesora, pamięci, pamięci i wersji dla aplikacji we wszystkich wdrożonych instancjach
    e. Tagowanie i wyszukiwanie urządzeń
    f. Tworzenie kopii zapasowych i przywracanie aplikacji
    g. Zmianę konfiguracji aplikacji, ustawień sieciowych, portów szeregowych i konfiguracji profilu zasobów w całej docelowej infrastrukturze sieci
    h. Zbieranie logów z zachowania poszczególnych aplikacji w całej infrastrukturze.
2. Aplikacja umożliwia integrację poprzez REST API z innymi systemami zarządzania
3. Aplikacja działa na systemie operacyjnym Ubuntu Server 14.04.1 LTS – 64 bit lub nowszy (Headless)
4. Konfiguracja serwera/maszyny wirtualnej: minimum 4 Core CPU 6 GB RAM 100 GB HDD

Oferowane urządzenie musi spełniać następujące wymagania techniczne:

Lp.	Parametr	Minimalne parametry techniczne
1	**Wymagane interfejsy:**	• 4 porty 1000 BASE T (10/100/1000 Mbps) • 1 port GE SFP (100/1000 Mbps) • 2 porty szeregowe RS-232, z których jeden może działać w trybie RS-485 • modem komunikacji sieci komórkowej, wspierający LTE 800/900/1800/2100/2600 MHz, UMTS/HSPA+ 850/900/1900/2100 MHz • gniazdo anteny GPS, • dwa gniazda na anteny 4G • dwa gniazda do podłączenia anten WiFi
2	**Pamięć Flash**	minimum 4GB
3	**Pamięć RAM**	minimum 2GB
4	**Port USB**	minimum dwa porty USB w tym: 1 port USB pozwalający na podłączenie zewnętrznych pamięci w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych oraz 1 port mini-USB pełniący funkcję konsoli szeregowej
5	**Wyposażenie GPS**	Oferowane urządzenie musi posiadać moduł geolokacji GPS
6	**Punkt dostępowy**	Oferowane urządzenie musi posiadać zintegrowany punkt dostępowy zapewniający komunikację minimum typu 802.11 a/b/g/n z technologią 2x2 (2.4GHz) 802.11n MIMO i 2x2 (5GHz) 802.11n MIMO
7	**Obudowa, warunki środowiskowe**	Oferowane urządzenie musi posiadać obudowę z metalu, umożliwiającą pracę w rozszerzonych warunkach środowiskowych, również w warunkach, w których występują drgania (np. w pojazdach) przy temperaturach –40 do 60°C, zachowaniem szczelności na poziomie IP40 Oferowane urządzenie musi być chłodzone pasywnie, bez ruchomych części Oferowane urządzenie musi umożliwiać na instalację na szynie DIN, musi być również możliwy montaż do powierzchni płaskich czy paneli, w oparciu o otwory w obudowie urządzenia.
8	**Zasilanie**	Oferowane urządzenie musi posiadać możliwość zasilania ze źródeł stałoprądowych w zakresie 12-48V.
9	**Gwarancja**	Minimum 12 miesięcy.

G) Przełączniki Multigigabit – 4 sztuki.

Oferowane urządzenie musi spełniać następujące wymagania techniczne:

Lp.	Parametr	Minimalne parametry techniczne
1	**Typ i liczba portów**	Minimum 36x 100 Mbps,1G, 2.5G + 12x Multigigabit (100M, 1G, 2.5G, 5G, or 10 Gbps)
2	**Moc dostępna dla portów z PoE**	Minimum 490 W
3	**Moduł rozszerzeń**	Możliwość instalacji/wymiany „na gorąco” – ang. hot swap.) z możliwością obsadzenia następującymi rodzajami modułów zależnie od potrzeb: - 4x1G SFP - 8x1/10G SFP/SFP+ - 2x40G QSFP - 2x25G SFP28 - 4x100M/1G/2.5G/5G/10GBaseT RJ-45
4	**Rodzaje wkładek dla portów SFP**	- Gigabit Ethernet 1000Base-T, - Gigabit Ethernet 1000Base-SX, - Gigabit Ethernet 1000Base-LX/LH, - Gigabit Ethernet 1000Base-EX, - Gigabit Ethernet 1000Base-ZX, - Gigabit Ethernet 1000Base-BX-D/U
5	**Rodzaje wkładek dla portów SFP/SFP+**	- Gigabit Ethernet 1000Base-T, - Gigabit Ethernet 1000Base-SX, - Gigabit Ethernet 1000Base-LX/LH, - Gigabit Ethernet 1000Base-EX, - Gigabit Ethernet 1000Base-ZX, - Gigabit Ethernet 1000Base-BX-D/U, - 10Gigabit Ethernet 10GBase-SR, - 10Gigabit Ethernet 10GBase-LR, - 10Gigabit Ethernet 10GBase-LRM, - 10Gigabit Ethernet 10GBase-ER, - 10Gigabit Ethernet 10GBase-ZR, - 10Gigabit Ethernet 10GBase-BX-D/U, - 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
6	**Rodzaje wkładek dla portów SFP/SFP+/SFP28**	- Gigabit Ethernet 1000Base-T, - Gigabit Ethernet 1000Base-SX, - Gigabit Ethernet 1000Base-LX/LH, - Gigabit Ethernet 1000Base-EX, - Gigabit Ethernet 1000Base-ZX, - Gigabit Ethernet 1000Base-BX-D/U, - 10Gigabit Ethernet 10GBase-SR, - 10Gigabit Ethernet 10GBase-LR, - 10Gigabit Ethernet 10GBase-ER, - 10Gigabit Ethernet 10GBase-ZR, - 10Gigabit Ethernet 10GBase-BX-D/U, - 10Gigabit Ethernet typu twinax (SFP+ - SFP+) - 25Gigabit Ethernet 25GBASE-SR, - 25Gigabit Ethernet typu twinax (SFP28 – SFP28) - 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF) - 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)
7	**Rodzaje wkładek dla portów QSFP**	- 40G-SR4, - 40G-LR4, - 40G-ER4, - 40G-SR-BD, - adapter 40G QSFP->10G SFP+ - kable twinax

8	**Stackowanie przełączników**	- Minimalna przepustowość w ramach stacku/stosu - 480Gb/s, - Minimum 8 urządzeń w stosie, - Możliwość zarządzania poprzez jeden adres IP, - Możliwość tworzenia połączeń typu cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, - Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2), - Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie),
9	**Wydajność**	- Oferowane urządzenie powinno zapewniać szybkość przełączania z pełną wydajnością wszystkich interfejsów również dla pakietów 64-bajtowych (przełącznik line-rate). - Przepustowość przełącznika (switching capacity) nie mniejsza niż: 500 Gbps - Prędkość przesyłania (forwarding rate) nie mniejsza niż: 420 Mpps
10	**Bufor dla pakietów**	16 MB
11	**Pamięć DRAM**	Nie mniej niż 8GB
12	**Pamięć Flash**	Nie mniej niż 16GB
13	**Dodatkowe parametry wydajnościowe:**	Obsługa nie mniej niż: - 1000 aktywnych sieci VLAN - 32000 adresów MAC - 8000 tras IPv4 - 4000 tras IPv6 - Ilość wpisów w listach kontroli dostępu Security ACL – 5000 - Ilość wpisów w listach kontroli dostępu QoS ACL – 5000 - 1000 interfejsów SVI L3 - 128 interfejsów L3 - Jumbo frame 9198B - 128 połączeń zagregowanych typu „port channel" - 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
14	**Wsparcie dla protokołów:**	Obsługa protokołu NTP, obsługa IGMPv1/2/3 i MLDv1/2 Snooping
15	**Wsparcie dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci**	- Per-VLAN Rapid Spanning Tree (PVRST+) - IEEE 802.1s Multi-Instance Spanning Tree - Obsługa 128 instancji protokołu STP - IEEE 802.1w Rapid Spanning Tree - LLDP (IEEE 802.1ab) i LLDP-MED
16	**Funkcja śledzenia**	Funkcjonalność nie gorsza niż Layer 2 Traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
17	**Voice VLAN**	Oferowane urządzenie musi umożliwiać uruchomienie funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
18	**DHCP**	Oferowane urządzenie musi mieć możliwość uruchomienia funkcji serwera DHCP

19	**Bezpieczeństwo**	- Oferowane urządzenie musi posiadać wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik powinien umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), - Autoryzacja użytkowników musi odbywać się w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Autoryzacja użytkowników musi odbywać się w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, - Obsługa funkcji Guest VLAN powinna umożliwiać uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, - Oferowane urządzenie powinno posiadać możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, - Oferowane urządzenie powinno posiadać możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, - Oferowane urządzenie powinno posiadać możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, - Oferowane urządzenie powinna posiadać możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, - Oferowane urządzenie powinno posiadać funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), - Oferowane urządzenie powinno posiadać obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, - Oferowane urządzenie powinno zapewniać podstawowe mechanizmy bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS), w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), - Oferowane urządzenie powinno posiadać możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, - Oferowane urządzenie powinno posiadać obsługę list kontroli dostępu (ACL) następujących typów: - Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, - Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, - Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); - Oferowane urządzenie powinno posiadać możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 256-bitów, - Oferowane urządzenie powinna posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP - Control Plane Policing),

		- Oferowane urządzenie powinna posiadać funkcje Private VLAN;
20	**Mechanizm zapewaniający autentyczność uruchamianego oprogramowania**	Oferowane urządzenie musi umożliwiać - sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, - wykonywanie bezpiecznej sekwencji uruchamiania, - sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
21	**Mechanizmy z zapewnieniem jakości usług w sieci**	Oferowane urządzenie musi umożliwiać - Implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, - Implementację algorytmu Shaped Round Robin dla obsługi kolejek, - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), - Klasyfikację 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 z dokładnością do 8 Kbps (policing, rate limiting), - Kontrolę 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;
22	**Obsługa protokołów i mechanizmów routingu**	Oferowane urządzenie musi umożliwiać - Routing statyczny dla IPv4 i IPv6, - Routing dynamiczny – RIP, OSPF do 1000 routes PIM Stub do 1000 routes - Policy-based routing (PBR), - Obsługę protokołu redundancji bramy (VRRP) z obsługą 256 grup, - Obsługę 10 tuneli GRE (Generic Routing Encapsulation);
23	**Dodatkowe funkcjonalności:**	- Oferowany przełącznik musi umożliwiać 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, RSPAN, - Oferowany przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.), - Oferowany przełącznik musi posiadać funkcjonalność sondy IP SLA Responder, - Oferowany przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,
24	**Zarządzanie:**	Oferowany przełącznik musi być wyposażony w następujące funkcjonalności oraz umożliwiać: - Port konsoli, - Dedykowany port Ethernet do zarządzania out-of-band, - Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

		- Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, - Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, - Wsparcie dla protokoły RESTCONF, - Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, - Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą, - Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
25	**Zarządzanie GUI:**	Oferowany przełączniki musi posiadać: Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: - Monitoring pracy przełącznika w zakresie: · Użycie CPU, · Użycie pamięci, · Temperatura pracy, · Podstawowe informacje systemowe: rodzaj sprzętu, czas pracy, czas systemowy, oprogramowanie, data i czas ostatniej zmiany konfiguracji, · Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, wykorzystanie PoE, · Informacji o urządzeniach sąsiednich podłączonych do przełącznika, · Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, · Statystyki ruchu (Rx/Tx) na poszczególnych portach L3, · Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik, - Konfigurację przełącznika w zakresie: · Konfiguracja interfejsów L2: · Konfiguracja interfejsów L3, · Tworzenie i konfiguracja sieci VLAN, · Konfiguracja protokołu STP, · Tworzenie i konfiguracja wirtualnych instancji routingu (VRF), · Konfiguracja routingu statycznego, · Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, · Tworzenie i przypisanie list kontroli dostępu ACL, · Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, · Konfiguracja i uruchomienie NetFlow, - Administracja przełącznika w zakresie: · Zdalne uruchamianie komend linii poleceń, · Czas systemowy w tym protokół NTP, · Konta administracyjne, · Upgrade oprogramowania, · Backup konfiguracji, · Zdalny restart urządzenia, · Konfiguracja i dostęp przez SNMP,

		· Narzędzie PING i TRACEROUTE, · Przeglądanie logów systemowych,
26	**Zasilanie**	- Oferowane urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów, - Oferowane urządzenie musi mieć możliwość instalacji zasilacza redundantnego AC 230V. Musi być zapewniona możliwość instalacji/wymiany „na gorąco” – ang. hot swap), - Oferowany przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia, - Oferowany przełącznik musi wspierać IEEE 802.3az EEE z funkcjonalnością redukcji zużycia energii dla portów w stanie bezczynności)
27	**Obudowa**	Oferowany przełącznik musi mieć możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU,
28	**Oprogramowanie [1]**	Oferowany przełącznik musi być wyposażony w oprogramowanie umożliwiające: - Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, - Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku, - Zamawiający wymaga dostarczenia licencji bezterminowych, w tym co najmniej 1 rok powinny być dostępne aktualizacje
29	**Oprogramowanie [2]**	Oferowany przełącznik musi być wyposażony w oprogramowanie umożliwiające: - Urządzenie realizuje następujące funkcjonalności z zakresu MPLS: - L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 256 połączeń wirtualnych VC, - L2VPN - Virtual Private LAN Services (VPLS) - obsługa 128 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji, - L3 VPN - MPLS Virtual Private Network (VPN) – obsługa 7000 tras routingowych L3 VPN, - Multicast VPN (MVPN); - Obsługę 256 wirtualnych instancji routingu (VRF), - Obsługę zaawansowanych protokołów routingu - IS-IS i BGP dla IPv4 i IPv6, - EIGRP (rfc7868), - Routing multicastów - PIM-SM, PIM-SSM, - Multicast Source Discovery Protocol (MSDP), - Obsługę protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD, - Realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji, - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256), - Możliwość enkapsulacji ruchu w pakiety VXLAN, - Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników: - Statycznie w oparciu o port do którego podłączona jest stacja, - Statycznie w oparciu o VLAN, w którym pracuje stacja, - Statycznie w oparciu o adres IP stacji, - Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;

		- Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu, - Propagację informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa, - Zapewnienie funkcjonalności sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter, - Wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii, - Zamawiający wymaga dostarczenia licencji bezterminowych, w tym co najmniej 1 rok powinny być dostępne aktualizacje
30	**Oprogramowanie [3]**	Oferowany przełącznik musi być wyposażony w oprogramowanie umożliwiające: - Funkcjonalność bramy dla usług mDNS, - Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN), - Zapewnienie widoczności i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7), - Możliwość eksportu dodatkowych pół w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa), - Wbudowany analizator pakietów, - System operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy, - Zamawiający wymaga dostarczenia licencji bezterminowych, w tym co najmniej 1 rok powinny być dostępne aktualizacje
31	**Wyposażenie**	Oferowany przełącznik musi być wyposażony w następujące ukompletowanie: - Redundantny zasilacz o mocy minimum: 1100 W - Moduł do łączenia w stos data wraz z kablem stakującym o długości minimum: 50 cm - Kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną, - Urządzenie objęte, co najmniej 12 miesięczną gwarancją.

H) System uwierzytelnienia dostępu do sieci

1. Podstawowe cechy systemu

1.1. System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.

1.2. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla bazowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
1.3. System musi posiadać bezterminową licencje umożliwiające równoczesną obsługę co najmniej 120 urządzeń końcowych - przewodowych lub bezprzewodowych
1.4. System musi zapewniać skalowalność do przynajmniej 7500 urządzeń poprzez rozbudowę istniejącego wdrożenia.
1.5. System musi zostać dostarczony w formie dwóch maszyn wirtualnych w celu zapewnienia wysokiej dostępności.
1.6. System powinien umożliwiać instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym, co najmniej:
1.6.1. Na hypervisorze VMWare ESXi 5.x i 6.x
1.6.2. Na hypervisorze VMware vSphere Client 5.x and 6.x
1.6.3. Na hypervisorze KVM na Red Hat Enterprise Linux (RHEL) 7.0
1.6.4. Na serwerach fizycznych wspieranych przez producenta
1.7. System musi umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:
1.7.1. Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie
1.7.2. Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
1.7.2.1. Przełączników dostępowych
1.7.2.2. Sesji uwierzytelniania 802.1X
1.7.2.3. Zdarzeń kontroli dostępu (autoryzacji)
1.7.2.4. Zdarzeń związanych z błędami
1.7.2.5. Zdarzeń związanych z alarmami systemowymi
1.7.3. Wydzielenie serwerów usługowych realizujących funkcje:
1.7.3.1. Serwera RADIUS dla infrastruktury sieciowej
1.7.3.2. Serwera polityk uwierzytelniania i kontroli dostępu 802.1X
1.7.3.3. Serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
1.7.3.4. Serwera profilowania stacji końcowych
1.8. System musi mieć możliwość realizacji wysokiej dostępności elementów funkcjonalnych, w tym:
1.8.1. Zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
1.8.2. Zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
1.9. System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS
1.10. System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
1.11. System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
1.12. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
1.13. System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni
1.14. System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
1.14.1. Dostęp do interfejsu konfiguracji usług tożsamości 802.1X
1.14.2. Dostęp do interfejsu konfiguracji urządzeń sieciowych
1.14.3. Dostęp do interfejsu konfiguracji polityk
1.14.4. Dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
1.14.5. Dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
1.15. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.

2. Mechanizmy uwierzytelniania 802.1x

2.1. System musi wspierać następujące protokoły uwierzytelniania i standardy:

2.1.1. RADIUS, zgodnie z dokumentami:
2.1.1.1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
2.1.1.2. RFC 2139 — RADIUS Accounting
2.1.1.3. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
2.1.1.4. RFC 2866 — RADIUS Accounting
2.1.1.5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
2.1.1.6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
2.1.1.7. RFC 2869 — RADIUS Extensions
2.1.2. RADIUS Proxy dla zewnętrznego serwera RADIUS

2.2. System musi wspierać protokół Windows Active Directory, w tym co najmniej następujące repozytoria AD:
2.2.1.1. Microsoft Windows Active Directory 2003 32bit
2.2.1.2. Microsoft Windows Active Directory 2003 R2 32bit i 64bit
2.2.1.3. Microsoft Windows Active Directory 2008 32bit i 64bit
2.2.1.4. Microsoft Windows Active Directory 2008 R2 64bit
2.2.1.5. Microsoft Windows Active Directory 2012
2.2.1.6. Microsoft Windows Active Directory 2012 R2

2.3. System musi wspierać protokół Lightweight Directory Access Protocol (LDAP)

2.4. System musi wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865

2.5. System musi wspierać następujące protokoły uwierzytelniania:
2.5.1. PAP/ASCII
2.5.2. CHAP
2.5.3. MS-CHAPv1
2.5.4. MS-CHAPv2
2.5.5. EAP-MD5
2.5.6. LEAP
2.5.7. EAP-TLS
2.5.8. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
2.5.8.1. EAP-MS-CHAPv2
2.5.8.2. EAP-GTC
2.5.8.3. EAP-TLS
2.5.9. System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect

2.6. System musi wspierać implementację 802.1X z przynajmniej następującymi suplikantami:
2.6.1. Wbudowanym klientem 802.1X dla Windows 10
2.6.2. Wbudowanym klientem 802.1X dla Windows 7
2.6.3. Wbudowanym klientem 802.1X dla Windows 8 i 8.1
2.6.4. Apple Mac OS X Supplicant
2.6.5. Apple iOS Supplicant
2.6.6. Google Android Supplicant

2.7. System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).

2.8. System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.

2.9. System musi umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.

2.10. System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)

2.11. System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC.

2.12. System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC

2.13. System musi wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
2.13.1. Tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
2.13.2. Tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
2.13.3. Tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden w host w domenie danych (Data VLAN) na jednym porcie fizycznym

2.13.4. Tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym
2.13.5. Mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny
2.13.6. Mechanizm umożliwiający poprawną obsługę sytuacji w której nowy host podłącza się do portu na którym uprzednio było uwierzytelnione urządzenie, w tym w VLANie głosowym
2.13.7. Mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA.
2.13.8. Mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X
2.13.9. Mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X
2.13.10. Obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki
2.13.11. Mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych
2.13.12. Mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny
2.13.13. Przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
2.13.14. Uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego się w VLANie głosowym
2.13.15. Współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
2.13.16. Możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web
2.13.17. Możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika

2.14. System musi wspierać uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)

2.15. System wspiera przynajmniej następujące urządzenia sieciowe, jako klientów RADIUS (NAD - Network Access Device):
2.15.1. Przełączniki Ethernet.
2.15.2. Kontrolery sieci bezprzewodowej.

2.16. System powinien zawierać funkcjonalność serwera TACACS+ do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej

3. Realizacja dostępu gościnnego

3.1. System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, co najmniej dla :
3.1.1. Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7, Apple Mac OS X 10.x
3.1.2. Apple iOS 8.0, 7.x, 6.1, 6,
3.1.3. Google Android dla 2.2 i nowszych
3.1.4. Linux

3.2. System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsor).

3.3. System musi zapewniać uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o:
3.3.1. Wewnętrzną bazę użytkowników
3.3.2. Zewnętrzne repozytorium użytkowników

3.4. System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do:
3.4.1. Logowania się do systemu
3.4.2. Tworzenia pojedynczego konta gościnnego
3.4.3. Tworzenia wielu kont gościnnych
3.4.4. Importowania kont gościnnych z pliku CSV
3.4.5. Wysyłania wiadomości email po utworzeniu konta gościnnego
3.4.6. Wysyłania wiadomości SMS po utworzeniu konta gościnnego
3.4.7. Wyświetlenia hasła konta gościnnego
3.4.8. Wydrukowania danych konta gościnnego

3.4.9. Wyświetlenia danych stworzonych kont gościnnych
3.4.10. Zawieszenia (suspend) i reinicjacji kont gościnnych

3.5. System musi umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:
3.5.1. Zmianę logo strony logowania
3.5.2. Zmianę obrazu tła strony logowania
3.5.3. Zmianę logo bannera
3.5.4. Zmianę obrazu tła bannera
3.5.5. Zmianę koloru tła strony z treścią

3.6. System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS

3.7. System musi umożliwiać zmianę adresu URL i FQDN strony sponsora.

3.8. System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System musi umozliwiać wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych

3.9. System musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim

3.10. System musi umożliwiać stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.

3.11. System musi umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
3.11.1. Imienia
3.11.2. Nazwiska
3.11.3. Firmy
3.11.4. Adresu e-mail
3.11.5. Numeru telefonu
3.11.6. Danych opcjonalnych (nie mniej niż 5 dodatkowych pól)

3.12. System musi umożliwiać konfigurację dla użytkowników gościnnych:
3.12.1. Wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
3.12.2. Zezwolenia gościom na zmianę hasła
3.12.3. Samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora

3.13. System musi umożliwiać honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.

3.14. System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.

3.15. System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługiwać co najmniej 20 urządzeń per konto gościnne.

3.16. System musi umożliwiać konfigurację czasu ważności hasła w dniach w przedziale zadanym przedziale w dniach.

3.17. System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny

3.18. System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych:

3.19. System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika

3.20. System musi umożliwiać tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.

3.21. System musi umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.

3.22. System musi umożliwiać udostepnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,

3.23. System musi wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

4. Profilowanie urządzeń (Jeżeli funkcjonalność ta jest dodatkowo licencjonowana to należy dostarczyć licencje na obsługę 120 aktywnych urządzeń końcowych)

4.1. System musi umożliwiać dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.

4.2. System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.

4.3. System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:

4.3.1. DHCP
4.3.2. DHCP SPAN
4.3.3. HTTP
4.3.4. RADIUS
4.3.5. DNS
4.3.6. SNMP
4.3.7. Network Scan (NMAP lub inne narzędzie profilowania aktywnego)

4.4. System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.

4.5. System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.

4.6. System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:

4.6.1. Stacji roboczych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,
4.6.2. Urządzeń mobilnych: Android, Apple, Blackberry
4.6.3. Telefonów IP
4.6.4. Drukarek sieciowych
4.6.5. Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych
4.6.6. Routerów
4.6.7. Punktów dostępu bezprzedowowego
4.6.8. Konsoli gier

4.7. System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:

4.7.1. Reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci
4.7.2. Reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt

4.8. System musi umożliwiać włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.

4.9. System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

5. Analiza stacji końcowej (Posture Assessment) - Jeżeli funkcjonalność ta jest dodatkowo licencjonowana to nie należy dostarczać na nią licencji.

5.1. System umożliwia pobranie bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.

5.2. System umożliwia kontrolę zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).

5.3. System umożliwia regularne ponawianie głębokiej analizy stacji końcowej (periodic reassessment) w przedziale od 1 do 24 godzin.

5.4. System umożliwia przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP). Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji. Zawartość dokumentu AUP jest konfigurowalna.

5.5. System umożliwia głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym:

- istnienia pliku na stacji końcowej
- wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)
- daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)

5.6. System umożliwia głęboką analizę stacji końcowej z systemem:

- Windows 7
- Windows 8 i 8.1
- Windows 10

pod kątem wpisów w rejestrze (Registry Condition), w tym:

- kluczy rejestru z kluczem root: HKLM, HKCC, HKCU, HKU, HKCR z zadanym podkluczem pod kątem:
  - istnienia lub nieistnienia klucza
  - wartości klucza rejestru
  - istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version

5.7. System umożliwia głęboką analizę stacji końcowej z systemem:
- Windows 7
- Windows 8 i 8.1
- Windows 10

pod kątem uruchomionych aplikacji (Application Condition), w tym:
- nazwy uruchomionego lub nieuruchomionego procesu

5.8. System umożliwia głęboką analizę stacji końcowej z systemem:
- Windows 7
- Windows 8 i 8.1
- Windows 10

pod kątem uruchomionych usług systemowych (Service Condition), w tym:
- nazwy uruchomionej lub nieuruchomionej procesu

5.9. System umożliwia tworzenie słownika prostych i złożonych warunków (Simple i Compound Condition) dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT, w tym z uwzględnieniem:
- parametrów dostępu do sieci, w tym:
- lokalizacji stacji końcowej
- nazwy użytkownika
- adresu IP stacji
- metody uwierzytelnienia
- statusu uwierzytelnienia
- repozytorium użytkowników użytych dla uwierzytelnienia
- atrybutów RADIUS, w tym:
  - Calling-Station-ID
  - Framed-IP-Address
  - NAS-Identifier
  - NAS-IP-Address
  - NAS-Port-Type
  - Service-Type
  - User-Name
- parametrów sesji w tym:
  - typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment)
  - architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit)
  - adresu URL, z którego nastąpiło przekierowanie

5.10. System umożliwia głęboką analizę stacji końcowej z systemem:
- Windows 7
- Windows 8 i 8.1
- Windows 10
- Mac OS-X

pod kątem zainstalowanych aplikacji Antywirusowych (AV Compound Condition), w tym:
- stwierdzenia czy system AV jest obecny na stacji
- stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od:
  - daty ostatniego pliku definicji
  - aktualnego czasu systemowego

5.11. System umożliwia głęboką analizę stacji końcowej z systemem:
- Windows 7
- Windows 8 i 8.1
- Mac OS-X

pod kątem zainstalowanych aplikacji AntiSpyware (AS Compound Condition), w tym:
- stwierdzenia czy system AS jest obecny na stacji
- stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni od:
  - daty ostatniego pliku definicji
  - aktualnego czasu systemowego

6. Obsługa serwerów certyfikatów CA

6.1. System musi posiadać funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.
6.2. Funkcja CA musi umożliwiać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.
6.3. System musi wspierać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów.
6.4. Funkcja CA musi zapewniać przynajmniej następujące funkcjonalności:
6.4.1. Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS
6.4.2. Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym
6.4.3. Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji
6.4.4. Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA

7. Raportowanie

System musi umożliwiać generowanie przynajmniej następujących raportów:
7.1. Raportów dla protokołów AAA:
7.1.1. diagnostyki protokołów AAA
7.1.2. trendów uwierzytelnienia 802.1X
7.1.3. accountingu RADIUS
7.1.4. uwierzytelniania RADIUS
7.2. Raportów dozwolonych protokołów
7.2.1. sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
7.2.1.1. uwierzytelnień pomyślnych
7.2.1.2. uwierzytelnień nieudanych
7.2.2. „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
7.2.2.1. uwierzytelnień pomyślnych
7.2.2.2. uwierzytelnień nieudanych
7.3. Raportów dla poszczególnych instancji serwerów systemu, w tym:
7.3.1. uwierzytelnień RADIUS per serwer
7.3.2. Top „N"uwierzytelnień per serwer
7.3.3. monitorowania Online Certificate Status Protocol (OCSP)
7.3.4. administratorów systemu i ich uprawnień
7.3.5. logowania administratorów do systemu
7.3.6. zmian konfiguracji serwera dokonanych przez administratorów
7.3.7. stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
7.3.8. zmian operacyjnych serwera dokonanych przez administratorów
7.3.9. zmian haseł przez użytkowników
7.4. Raportów dla stacji końcowych, w tym:
7.4.1. uwierzytelnień typu MAC Authentication
7.4.2. Top „N"uwierzytelnień per adres MAC stacji
7.4.3. Top „N" uwierzytelnień per maszyna
7.4.4. Top „N"uwierzytelnień per RADIUS Calling Station ID
7.4.5. działań podsystemu profilera per adres MAC
7.4.6. czasu wymaganego na sprofilowanie stacji per adres MAC
7.5. Rraportów dla błędów, w tym:
7.5.1. błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
7.5.2. sumarycznych przyczyn nieudanych uwierzytelnień
7.5.3. Top „N" uwierzytelnień per rodzaj błędu
7.6. Raportów dla urządzeń sieciowych:
7.6.1. sumarycznych uwierzytelnień dla urządzeń sieciowych
7.6.2. Top „N" uwierzytelnień per urządzenie sieciowe
7.6.3. niedostępności serwera AAA dla urządzenia sieciowego
7.6.4. wiadomości logowanych przez urządzenia sieciowe
7.6.5. stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
7.7. Raportów użytkowników:
7.7.1. sumarycznych uwierzytelnień użytkowników

7.7.2. Top „N”uwierzytelnień per użytkownik
7.7.3. sesji użytkowników gościnnych
7.7.4. aktywności użytkowników gościnnych
7.7.5. sumarycznych uwierzytelnień sponsorów dostępu gościnnego
7.7.6. uwierzytelnień per unikalny użytkownik

7.8. Raportów katalogu sesji
7.8.1. aktywnych sesji RADIUS
7.8.2. historii sesji RADIUS
7.8.3. zaterminowanych sesji RADIUS

8. Alarmy

8.1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą
8.1.1. wiadomości e-mail
8.1.2. syslog

8.2. Alarmy muszą być generowane w następujących sytuacjach:
8.2.1. ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
8.2.2. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
8.2.3. status krytycznych procesów będzie niepożądany, w tym status:
8.2.3.1. procesu wewnętrznej bazy danych systemu
8.2.3.2. serwera aplikacyjnego systemu
8.2.3.3. bazy danych sesji
8.2.3.4. kolektora i procesora wiadomości log
8.2.3.5. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
8.2.3.6. stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
8.2.3.6.1. obciążenie systemu (load)
8.2.3.6.2. zajętość pamięci

8.3. System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
8.3.1. badanie łączności IP za pomocą ping, nslookup, traceroute
8.3.2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
8.3.2.1. nazwy użytkownika
8.3.2.2. adresu MAC
8.3.2.3. statusu uwierzytelnienia (udana lub nieudana)
8.3.2.4. powodu, jeżeli uwierzytelnienie nieudane
8.3.2.5. zakresu czasowego, co do dnia, godziny i minuty
8.3.3. wykonanie zdalnego polecenia na urządzeniu sieciowym
8.3.4. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
8.3.4.1. definicji serwerów AAA
8.3.4.2. protokołu RADIUS
8.3.4.3. odkrywania urządzeń
8.3.4.4. logowania
8.3.4.5. uwierzytelniania Web
8.3.4.6. konfiguracji trybu 802.1X
8.3.5. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

9. Dopuszczalne sposoby realizacji rozwiązania

9.1. Zamawiający wymaga spełnienia następujących warunków realizacji systemu uwierzytelnienia dostępu do sieci
9.1.1. Zamawiający dopuszcza stosowanie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.
9.1.2. W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje, iż system będzie zapewniał pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia)
9.1.2.1. W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje iż system będzie serwisowany przez jeden podmiot tzn. zgłoszenia serwisowe będą kierowane do jednego dostawcy. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia).

9.1.2.2. W przypadku zastosowania serwera CA jako dedykowanego rozwiązania Zamawiający będzie traktował to rozwiązanie jako integralną część systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia).

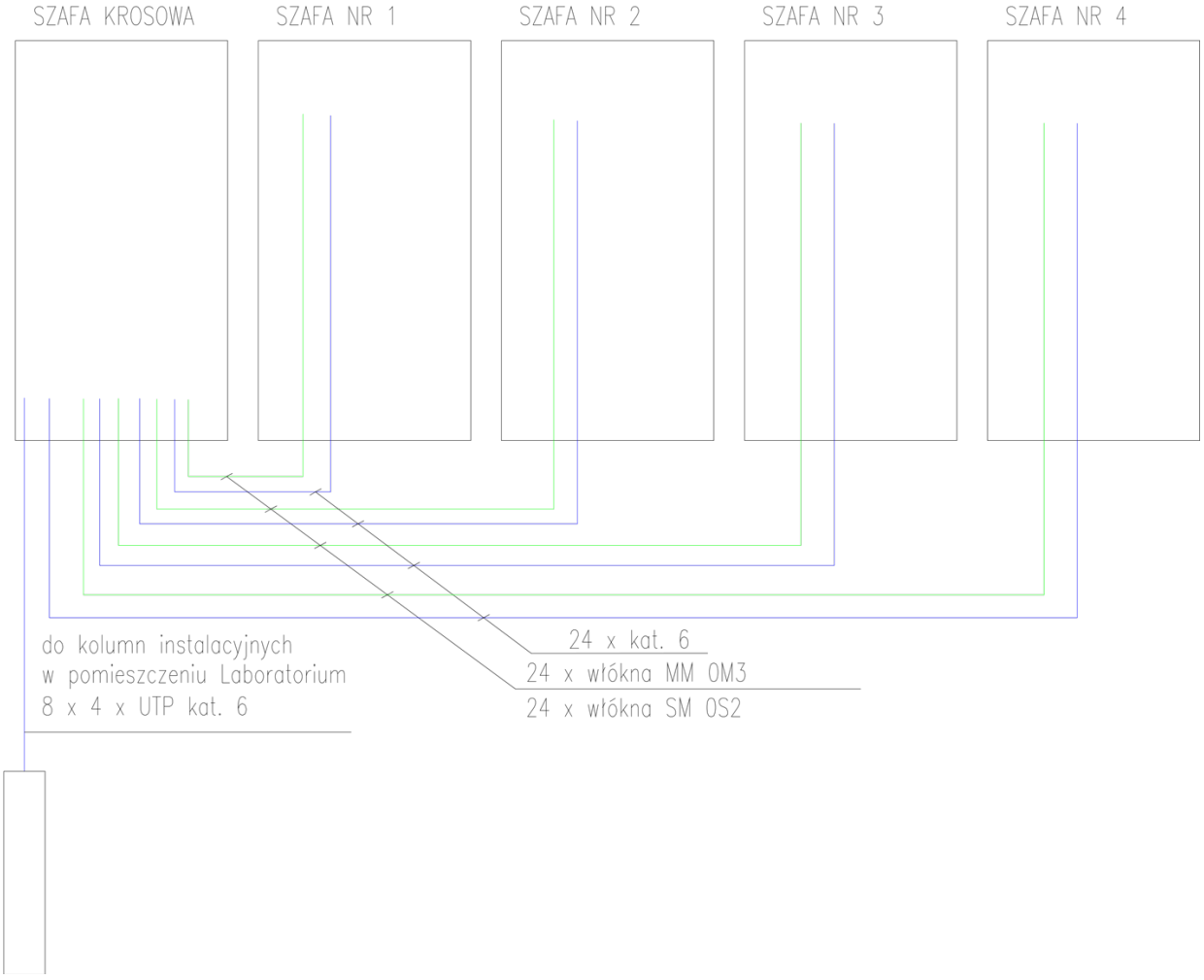
Pozostałe elementy infrastruktury (zasilanie, okablowanie, szafy rack oraz inne elementy)

UPS, szafy oraz listwy zasilające PDU muszą pochodzić od jednego producenta.

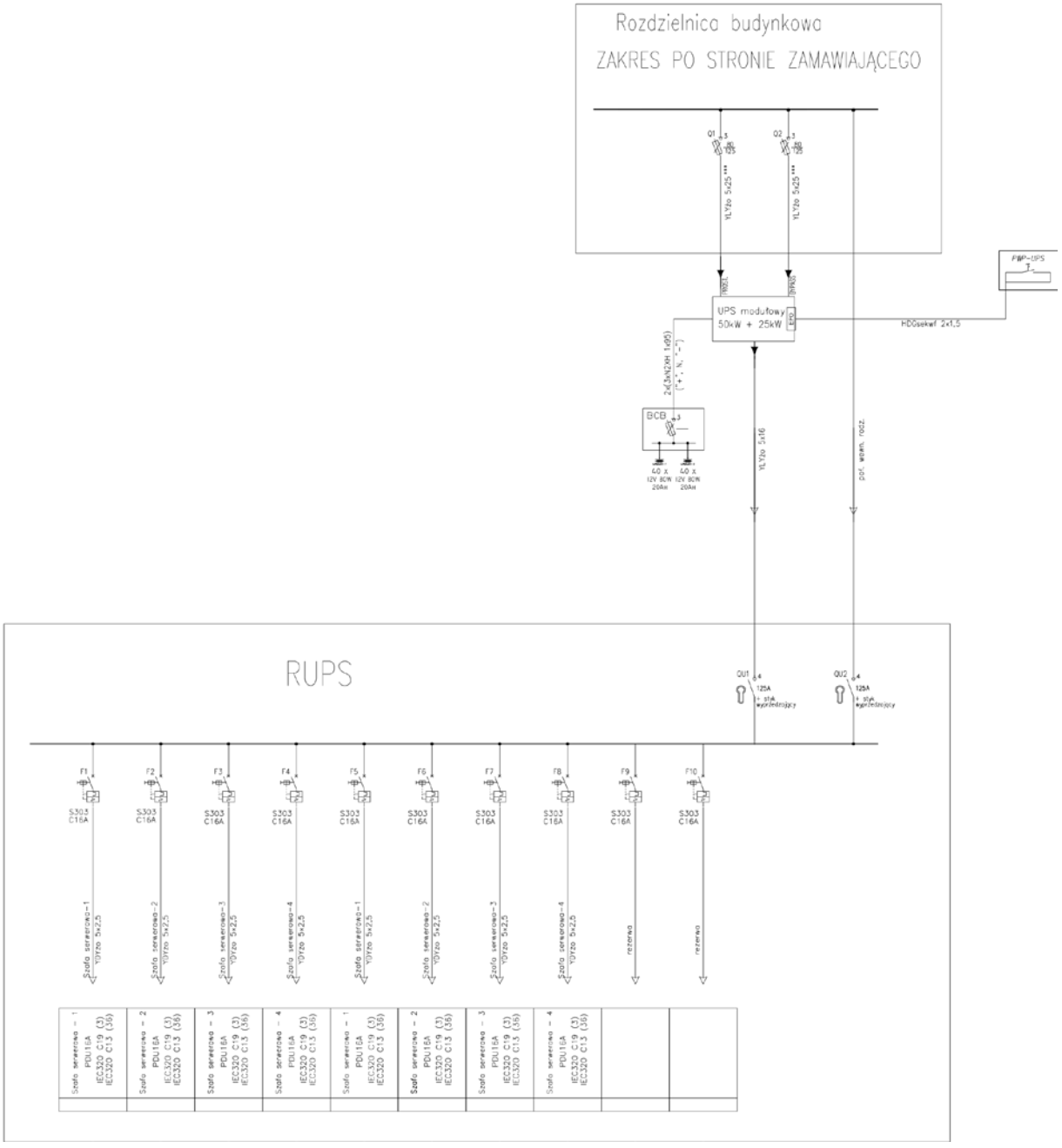
W zakresie realizacji zasilania należy doprowadzić kable zasilające do UPS z rozdzielnicy budynkowej, dostarczyć, zainstalować i uruchomić modułowego UPSa. Dostarczyć i zainstalować rozdzielnicę UPS. Z rozdzielnicy doprowadzić okablowanie zasilające do szaf (po dwa obwody do każdej szafy). Każdy odpływ do szafy należy zakończyć gniazdem IEC309. Rozdzielnica UPS musi posiadać odpowiedni zapas na potrzeby rozbudowy laboratorium o kolejne szafy Rack wymagające zasilania gwarantowanego.

Na poniższych rysunkach przedstawiono ideowe schematy instalacji zasilania oraz LAN.

Rys. 2. Instalacja logiczna



Rys. 3. Instalacja zasilania gwarantowanego laboratorium



A) UPS

Do UPSa należy doprowadzić kable zasilające z rozdzielnicy piętrowej/budynkowej (przekroje należy zweryfikować po ustaleniu długości okablowania). Za UPSem należy wykonać rozdzielnicę RUPS, z której należy rozprowadzić zasilanie gwarantowane do odbiorów (szaf rack). Kable zakończyć nad szafami gniazdami IEC 16A 3f.

Na potrzeby laboratorium zakłada się dostawę i montaż UPS'a modułowego o maksymalnej mocy 75kW. W celu zapewnienia zasilania dla całego Laboratorium. UPS'a należy wyposażyć w 3 moduły mocy każdy o mocy 25kW. UPS będzie pracować na 2 modułach mocy, 1 moduł będzie modułem nadmiarowym.

Wymagania dotyczące konstrukcji;

1. Konstrukcja modułowa, panelowa polegająca na umiejscowieniu modułów mocy, kontroli oraz bypassu elektronicznego UPS w specjalnej szafie. Montaż modułu wykonywany przez wsunięcie modułu UPS do szafy bez wykonywania jakichkolwiek połączeń kablowych,
2. Konstrukcja modułowa, zapewniająca możliwość wyjęcia modułu UPS z szafy, nie wymagająca wyłączania systemu UPS i nie wymagająca przejścia na by-pass. Podczas wymiany modułu, cały czas odbiorniki muszą być zasilane z falownika,
3. System UPS ma się składać z modułów o mocy do 25 kVA/kW, jednak ilość modułów dla systemu nie powinna przekraczać 3 sztuk.

Wymagania parametrów technicznych:

Oferowane urządzenie do bezprzerwowego zasilania musi być fabrycznie nowe i musi pochodzić z seryjnej produkcji. Producent oferowanego urządzenia powinien posiadać własny certyfikat ISO 9001 oraz 14001 jako potwierdzenie wymagań międzynarodowego standardu jakości. Oferowane urządzenie musi posiadać oznakowanie CE (deklarację zgodności CE załączyć do oferty). Oferent ma obowiązek przedstawienia karty katalogowej producenta urządzenia, karta dystrybutora własnej marki nie jest wystarczającym potwierdzeniem parametrów urządzenia. Proponowany UPS musi posiadać budowę modułową w oparciu o moduły mocy 25 kVA / 25 kW i spełniać poniżej opisane wymagania. Zaprojektowano system zasilania awaryjnego złożony z systemu o maksymalnej rozbudowie do 75kW wyposażony w 3 moduły mocy po 25kW.

1. Moc wyjściowa pojedynczej jednostki UPS-a min 75 kVA/75kW.
2. Moc wyjściowa pojedynczego modułu mocy UPS-a min 25 kVA / 25 kW
3. Ilość faz 3/3 - trzy fazy wejściowe i trzy fazy wyjściowe
4. Zakres napięcia wejściowego: 176 ~ 276 / 305 ~ 477 V
5. Zniekształcenia harmoniczne prądu wejściowego: <3%
6. Zakres dopuszczalnej częstotliwości wejściowej: 50Hz ± 5Hz
7. Współczynnik szczytu: 3:1
8. Wyjściowy współczynnik mocy równy: 1
9. Zniekształcenia harmoniczne napięcia wyjściowego: ≤ 2%
10. Regulacja napięcia wyjściowego: ± 1%
11. Dopuszczalne przeciążenie: ≤ 125%: 10min; ≤ 150%: 1min;
12. Parametry pracy równoległej: max 6 modułów mocy każdy po 25 kVA/25 kW,
13. Z uwagi na wysoką niezawodność UPS powinien posiadać budowę modułową kluczowych elementów, których wymiana jest możliwa na zasadzie hot plug („na gorąco") potwierdzone przez producenta. Dotyczy to następujących, krytycznych elementów:
    - Moduły mocy UPS (każdy moduł posiada, falownik, prostownik, zdecentralizowany moduł kontroli w każdym module)
    - Moduł kontroli i sterowania UPS (system posiada centralny moduł kontroli)
    - Moduł bypassu elektronicznego (static switch)
14. Każdy z modułów musi bezwzględnie posiadać zamek mechaniczny umożliwiający blokadę przed omyłkowym wyjęciem modułu.
15. Moduły mocy UPS powinny posiadać własny, dodatkowy układ sterownia i synchronizacji. Awaria głównego modułu kontroli i sterowania nie powoduje awarii UPS-a oraz zapewnia synchronizację układu modułów mocy.
16. Możliwość instalacji modułu dystrybucji zasilania (wewnątrz UPSa) wraz z opomiarowaniem odbiorów dedykowanego rozwiązania tego samego producenta urządzenia, kompatybilnego z UPSem potwierdzony przez producenta.

17. Urządzenie musi posiadać wbudowane w UPS dostępne z przodu:
    - Zabezpieczenie wyjścia
    - Zabezpieczenie Manual Bypass
    - Zabezpieczenie Bypass Input
    - Zabezpieczenie wejścia
18. Urządzenie musi posiadać:
    - Wejście trójfazowe 5-cio przewodowe (TN-S) - oddzielne dla toru prostownika i wewnętrznego toru obejściowego
    - Wyjście trójfazowe 5-cio przewodowe (TN-S)
19. Urządzenie musi zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i wahaniach częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia.
20. Urządzenie powinno być wyposażone w komunikacyjny wyświetlacz LCD z odczytem parametrów elektrycznych wejścia/wyjścia i komunikatów o stanie pracy UPS w języku polskim.
21. Zasilacz UPS musi być wyposażony w adapter Web/SNMP IPv6 z Modbus TCP.
22. Zasilacz UPS powinien być przystosowany do podłączenia zewnętrznego wyświetlacz LCD po Modbus TCP lub RTU, umożlwiający wizualizację parametrów zasilacza, wyświetlacz powinien pochodzić z seryjnej produkcji tej samej marki co UPS co gwarantuje pełną kompatybilność.
23. Z uwagi na ograniczone miejsce całkowite wymiary zasilacza nie powinny przekraczać następujących wymiarów:
    - Szerokość: ≤ 600mm
    - Głębokość: ≤ 1100mm
    - Wysokość: ≤ 2000mm
24. Preferowany kolor obudowy: szary/czarny.
25. Poziom hałasu urządzenia w trybie podwójnego przetwarzania przy obciążeniu znamionowym nie może przekraczać 65 dB w zależności od obciążenia.
26. Stopień ochrony IP20 zgodnie z normą EN60529
27. Rejestr zdarzeń: 3000 rekordów
28. Urządzenie musi mieć możliwość zainstalowania zewnętrznego wyłącznika awaryjnego ppoż. ,który należy dostarczyć wraz z urządzeniem. Miejsce instalacji wyłącznika wskaże Zamawiający.
29. Sprawność w trybie TRUE ONLINE
    - min. 96% w rybie normalnym
    - min. 99% osiągane w ekonomicznym trybie pracy
30. UPS musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:
    - Gniazdo komunikacji RS-232,
    - Wejście bezpotencjałowe
    - Wyjścia bezpotencjałowe
    - REPO
    - Gniazda w ilości minimum 2 sztuk do zabudowy kart sieciowych 10/100 Base-T RJ-45 (Web/SNMP) lub karty modbus RTU lub karty relay
31. Możliwość sygnalizacji stanów pracy UPS stykami bezpotencjałowymi z programowalnymi funkcjami.
32. Urządzenie powinno posiadać BYPASS ręczny(serwisowy) oraz BYPASS elektroniczny.
33. Urządzenie powinno posiadać możliwość podłączenia BYPASSu serwisowego ze stykiem wyprzedzającym
34. Możliwość podejścia kablowego od góry i dołu z tyłu urządzenia.
35. Aby zapewnić oczekiwany czas podtrzymania dobrano poniższe baterie:
36. Aby zapewnić oczekiwany czas podtrzymania 15 min dla 50kW obciążenia (dla napięcia odcięcia 1,75V na celę oraz temperatury 25 stopni) dobrano baterie: 1 łańcuch 40 sztuk baterii o pojemności min 80Ah w technologii TPPL (thin plate pure lead).
34. Projektowana żywotność baterii 12+ lat, produkcja europejska, pojemności UPS powinien być kompatybilny z ruchomym łańcuchem baterii +/- 2 sztuki. Awaria pojedynczego ogniwa baterii powinna umożliwiać poprawną pracę UPS z zestawem 38 - 42 baterie.
35. Baterie dobrano dla temperatury 25 stopni i napięcia odcięcia 1,75V na celę.
36. Baterie należy zainstalować na zewnętrznym stojaku bateryjnym.

B) Szafa teleinformatyczna RACK – 5 sztuk

Materiał:	Blacha stalowa, Aluminium
Powierzchnia:	Stelaż szafy: gruntowany zanurzeniowo Zabudowa wewnętrzna: gruntowana zanurzeniowo Drzwi i dach: gruntowane zanurzeniowo, lakierowane proszkowo
Kolor:	Rama obudowy i części płaskie: RAL 7035 Zabudowa, kratka wentylacyjna przednia: RAL 9005
Materiały podstawowe:	Blacha stalowa
Wymiary minimalne:	Szerokość: 800 mm Wysokość: 2000 mm Głębokość: 1100 mm
Wysokość montażowa dla komponentów:	42 U
Wersja 19":	Szyny profilowe, 482,6 mm (19")
Wykonanie drzwi:	wentylowane

C) PDU: 3 fazowa, 16A, 36 x Gniazdo C13, 3 x Gniazdo C19 – 8 szt,

Wysokiej klasy rozdział prądu w szafach IT, z funkcjami monitorowania PDU. Listwa 0U, montowana pionowo, dzięki czemu nie zajmuje miejsca w szafie. Możliwy montaż beznarzędziowy. Wskaźnik LED poziomu prądu (wartość skuteczna) oraz ostrzeżenie przed przeciążeniem. Zabezpieczenie grupy gniazd. Redundantne zasilanie odbywa się z wszystkich faz. Możliwe jest również monitorowanie otoczenia za pomocą czujników (np. temperatury, wilgotności, dostępu,).

Lp.	Minimalne parametry techniczne	
1	Materiał	Profil aluminiowy, czarny
2	Klasa ochrony IP	IP20
3	Wariant	Funkcje i monitorowania
4	Gniazda wtykowe	36 x Gniazdo C13 - Czarny 3 x Gniazdo C19 - Czarny
6	Wymiary	Szerokość: 48 mm Głębokość: 50 mm
7	Zasilanie	Ilość: 1 Fazy na zasilanie: 3
8	Długość kabla przyłączeniowego	1,8m
11	Prąd znamionowy (maks.):	16A

D) Kolumny elektroinstalacyjne – 8 sztuk

Lp.	Minimalne parametry techniczne	
1	Materiał	Aluminium
2	Głębokość [mm]	110 mm
3	Szerokość [mm]	80 mm
4	Wysokość [mm]	Min. 3000 mm
6	Stopień ochrony (IP)	IP40

7	Kolor	Aluminium
8	Zabezpieczenie powierzchni	Anodowanie
9	Model	Dwustronna
10	Ilość komór	2
11	Ilość przegród	1
12	Kształt produktu	Owalna
13	Sposób montażu	Podłogowy, rozporowy, sufitowy, śrubowy
14	Zakres regulacji	0-0,5 metra
15	Sposób montażu gniazd	Montaż bezpośredni modułów w standardzie K45

Każda kolumna musi być wyposażona w 5 gniazd zasilających 230V doprowadzonych z rozdzielnicy laboratoryjnej oraz 4 gniazda logiczne RJ-45 kat. 6 doprowadzonych z szafy krosowniczej.

E) Okablowanie miedziane i światłowodowe

W zakresie instalacji okablowania miedzianego i światłowodowego jest dostawa elementów zgodnie z poniższą tabelą oraz punktem „Pozostałe elementy infrastruktury" a także wykonanie instalacji wg. opisów przedstawionych w poniższych punktach.

W zakresie dostawy znajdują się 4 szafy Rack, z czego trzy z nich są przeznaczone na urządzenia aktywne (każda z nich musi być wyposażona w dwie listwy PDU zasilane z UPS). Czwarta szafa pełni rolę szafy krosowniczej, która będzie agregować połączenia światłowodowe i miedziane z pozostałych szaf a także ze stanowisk laboratoryjnych. Do szafy tej będą także doprowadzone łącza operatorskie oraz styki z innymi sieciami.

Wykonawca wykona w pełni funkcjonalną sieć logiczną wraz ze wszelkimi wymaganymi połączeniami miedzianymi oraz światłowodowymi (np. spawy). Wykonawca ma dostarczyć wszelkie elementy nie ujęte w poniższym zestawieniu a wymagane do realizacji infrastruktury sieci logicznej.

W poniższej tabeli podano minimalne ilości głównych elementów jakie musi dostarczyć Wykonawca na potrzeby realizacji sieci logicznej pomiędzy szafami Rack, a także do stanowisk laboratoryjnych.

Lp.	Nazwa	Jm.	ilość
1	Panel krosowy 24RxJ45 kat.6 UTP w pełni wyposażony	szt.	8
2	Kompletna przełącznica światłowodowa zawierająca kasetę, pigtaile, adaptery oraz panel światłowody dla 12xLCdx OM3 + 12LCdx OS2	szt.	8
3	Kabel UTP kat. 6	m	2400
4	Kabel światłowodowy jednomodowy OS2 24 włókna	m	120
5	Kabel światłowodowy wielomodowy OM3 24 włókna	m	120
6	Panel z wieszakami poziomy 1U	szt.	16

Opis w zakresie okablowania miedzianego i światłowodowego

Rozwiązanie ma pochodzić od jednego producenta i być objęte jednolitą i spójną gwarancją systemową udzieloną bezpośrednio przez producenta okablowania (nie dostawcę/dystrybutora) na okres minimum 25 lat obejmującą wszystkie elementy pasywne toru transmisyjnego wraz z kablami krosowymi. Wszystkie elementy okablowania (w szczególności: kabel, panele krosowe, gniazda, płyty czołowe gniazd, kable krosowe, prowadnice kablowe i inne) mają być oznaczone logo lub nazwą tego samego producenta i pochodzić z jednolitej oferty rynkowej. Wymagania odnośnie wydajności kanału transmisyjnego muszą spełniać minimum Klasę E a wszystkie komponenty spełniać kryteria kategorii 6. Wszystkie te elementy powinny być w wersji nieekranowanej.

1) Połączenia miedziane

Między szafami należy wykonać połączenia kablem UTP kat. 6. Od szafy krosowej do każdej szafy należy wykonać 24 połączenia i zakończyć na panelu krosowym 24xRJ45 kat 6 UTP.

Panele miedziane muszą mieć wysokość 1U, mieścić min. 24 portów RJ45 oraz posiadać następującą funkcjonalność:

- montaż w szafach 19'', wysokość 1U
- modularną budowę tj. skalowalność (rozbudowę) z dokładnością do jednego złącza RJ45,
- możliwość dokonywania naprawy jednego łącza bez przerywania ciągłości pracy pozostałych.
- kodowanie kolorem gniazd w panelu

W celu zagwarantowania najwyższej jakości połączenia, a przede wszystkim powtarzalnych parametrów, wszystkie złącza, zarówno w gniazdach końcowych, panelach oraz złączach RJ45 w kablach krosowych i przyłączeniowych muszą być zarabiane w oparciu o technologię IDC. Proces montażu modułów gniazd RJ45 ma gwarantować najwyższą powtarzalność. Maksymalny rozplot par transmisyjnych na modułach gniazd RJ45 montowanych zarówno w panelach, jak i w zestawach instalacyjnych naściennych nie może być większy niż 8 mm. Ze względu na wymaganą najwyższą długoterminową trwałość i niezawodność oraz doskonałe parametry kontaktu należy stosować kable przyłączeniowe i krosowe wykonanymi i przetestowanymi przez producenta systemu okablowania. Nie dopuszcza się stosowania modułów wyposażonych w dodatkowe elementy elektroniczne (płytki PCB) do redukowania przesłuchów pochodzących od złącza.

Wydajność komponentów (złącze-wtyk) ma być potwierdzona certyfikatem De-Embedded Testing wystawionym przez niezależne laboratorium badawcze. System ma się składać w nieekranowanych elementów, to wymaganie dotyczy zarówno gniazd w zestawach naściennych, jak i w panelach krosowych. Zgodnie z wymaganiami norm każdy 4-parowy kabel ma być w całości (wszystkie pary) trwale zakończony na 8-pozycyjnym złączu modularnym.

Kable instalacyjne miedziane.

- Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 6,4 mm. Nie dopuszcza się kabli o większej średnicy zewnętrznej. Kabel ten ma spełniać wymagania stawiane komponentom Kategorii 6 przez obowiązujące specyfikacje norm, równocześnie zapewniając pełną zgodność z niższymi kategoriami okablowania. Z uwagi na konieczność odsunięcia par splecionych od siebie spowodowaną przeciwdziałania przesłuchom od par sąsiednich, konstrukcja kabla musi zawierać separator krzyżowy wewnątrz kabla.
- Wymaga się, aby charakterystyka kabla uwzględniała odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min. 450MHz dla nieekranowanego kabla kat.6.

Wymagane parametry kabla teleinformatycznego:

Standaryzacja	ISO/IEC 11801 2nd ed.; IEC 61156-5 2nd ed.; EN 50173-1; EN 50288-3-1;EIA/TIA 568B.2
Kategoria	Kat.6
Pasmo przenoszenia	450 MHz
Rodzaj kabla	Kabel instalacyjny
Rodzaj ekranowania	U/UTP
Liczna przewodników	8
Splot	4P
Średnica całkowita kabla	6.0 mm ± 0.4
Typ przewodu	Ścisła tuba
Średnica żyły	AWG 23
Długość kabla w szpuli	500 m
Materiał powłoki	LSZH
Zbrojenie kabla	Brak
Kolor	szary

Moduł przyłączeniowy

Do wyposażenia zarówno gniazd abonenckich jak i paneli krosowych w punktach dystrybucyjnych dopuszcza się użycie jednego rodzaju modułu przyłączeniowego kat.6 typu RJ45. Moduł musi pozwalać na pewne przytwierdzenie do niego kabla instalacyjnego za pomocą opaski uciskowej oraz pozwalać na zarabiania kabla instalacyjnego metodą beznarzędziową i być wyposażony w złącza IDC gwarantujące uzyskanie najwyższej jakości kontaktu modułu z żyłą kabla. Kable przyłączeniowe również muszą być wyposażone we wtyki RJ45 terminowane w złączu IDC, co ma decydujący wpływ na jakość kontaktu wtyk-moduł. Moduł musi być wyposażony w dedykowany system przeciwdziałania wpływom wibracji występujących w szczególności w punktach dystrybucyjnych. Moduł musi zapewniać możliwość dokonywania co najmniej 20 krotnej terminacji kabli instalacyjnych co umożliwi korektę ewentualnych błędów instalacyjnych bez konieczności wymiany całego modułu oraz pozwoli na przyszłe zmiany w strukturze sieci. Kabel instalacyjny musi być przytwierdzany do modułu za pomocą opaski uciskowej co ma przeciwdziałać wyszarpaniu go z modułu. Kable terminowane w module musza mieć możliwość rozszycia żył zarówno w sekwencji T568A jaki i T568B. Konstrukcja modułu ma eliminować wpływy przesłuchów poprzez kompensację przesłuchów wewnątrz modułów realizowaną poprzez mechaniczne ukształtowanie kontaktów. Nie dopuszcza się stosowania modułów wyposażonych w dodatkowe elementy elektroniczne (płytki PCB) do redukowania przesłuchów pochodzących od złącza.

Standaryzacje	IEC 60603-7: Electrical Characteristics of the Telecommunication Outlets ISO/IEC 11801, Second Edition: September 2002 EN 50173-1: May 2007
Typ złącza (A)	RJ45
Kategoria złącza (A)	Kat.6
Ekranowanie - złącze (A)	Nie
Mocowanie	Płytka montażowa/snap-in
Rozszycie żył	EIA/TIA 568A / EIA/TIA 568B
Ilość kontaktów	8
Materiał	Plastik: PC, UL 94 V-0
Kolor	Szary

Przełącznice miedziane
Przełącznice miedziane powinny charakteryzować się brakiem kategorii. O tym jakiego rodzaju okablowanie można terminować na przełącznicach decydują zainstalowane moduły. Wpływa to na nieograniczoną elastyczność i możliwość łatwej i taniej migracji do okablowania o wyższej kategorii.

24-portowa nieekranowana przełącznica kat.6 o wysokości montażowej 1U powinna być wyposażona w moduły RJ45 montowane metodą zatrzaskową, co zapewnia zwartą konstrukcję oraz łatwy i szybki sposób instalacji niewymagający żadnych specjalistycznych narzędzi zapewniając uniwersalne rozszycie kabla w sekwencji T568A lub T568B. Przełącznica musi zapewniać jednoportową skalowalność portów oraz możliwość migracji/implementacji łączy światłowodowych. Rama przełącznicy musi być przystosowana do montażu zarówno modułów przyłączeniowych ekranowanych jak i nieekranowanych. Musi być zaopatrzona w dedykowane miejsca do przytwierdzania kabli instalacyjnych za pomocą opasek zaciskowych. W celu oszczędności miejsca w szafie dystrybucyjnej powinna posiadać prowadnice boczne do przeprowadzania kabli krosowych. Przełącznica musi mieć możliwość zastosowania systemu zabezpieczeń poprzez kodowanie kolorem.

Kable krosowe miedziane:
- wyposażony w zestyk IDC na styku z żyłą kabla
- kabel linka
- powłoka LSFRZH
- przystosowany do montażu 3 poziomowego systemu zabezpieczeń (kodowanie kolorem, kształtem oraz zabezpieczenie przeciw wpięciowo-wypięciowe)
- materiał: wolny od związków halogenów oraz metali ciężkich zgodny z wytycznymi EU, RoHS i WEEE
- kable krosowe kat 6muszą pochodzić o tego samego producenta i posiadać złącza IDC.

2) Połączenia światłowodowe

Między szafami należy wykonać połącznia światłowodowe jedno i wielomodowe. Od szafy krosowej do każdej szafy należy ułożyć 24 włókna kabla jednomodowego OS2 i wieomodowego OM3. Zakończyć na wspólnym panelu światłowodowym.

Przełącznice światłowodowe muszą umożliwiać instalację do 24 dupleksowych łączników centrujących na wysokości 1U i posiadać następująca funkcjonalność:

- konstrukcja przełącznicy musi umożliwiać w swoim obszarze możliwości zorganizowania zapasu tub(min 2m) z włóknami oraz samych włókien (min.2m)
- obsługujący przełącznice, poprzez podwójny wysuw części centralnej przełącznicy (szuflady) muszą otrzymać dostęp do części połączeniowej (adapter-wtyk) oraz do sekcji spawów w obszarze tacek spawów
- przełącznica musi mieć możliwość regulacji pozycji panela czołowego względem ramy szafy 19”
- włókna kabla FO wchodzącego do szafy 19” muszą być dystrybuowane poprzez rozdzielacz kabla
- przełącznica musi być wyposażona w zintegrowaną półkę do prowadzenia kabli krosowych nie wymagającą dodatkowego miejsca w przestrzeni szafy.

Przełącznice światłowodowe LC
Przełącznice światłowodowe muszą umożliwiać instalację do 24 dupleksowych łączników centrujących na wysokości 1U (Terminacja 48 włókien FO). Konstrukcja przełącznicy musi umożliwiać w swoim obszarze możliwości zorganizowania zapasu tub (min 2m) z włóknami oraz samych włókien (min.2m). Obsługujący przełącznice, poprzez podwójny wysuw części centralnej przełącznicy (szuflady) muszą

otrzymać dostęp do części połączeniowej (adapter-wtyk) oraz do sekcji spawów w obszarze tacek spawów. Tacki spawów muszą umożliwiać ułożenie zapasu pigtaili oraz właściwa separację włókien.

Przełącznica musi mieć możliwość

- regulacji pozycji panela czołowego względem ramy szafy 19". W celu właściwego zabezpieczenia kabla wprowadzanego w obszar szafy 19" tuby z włóknami optycznymi muszą być ochraniane przez peszle aż do wejścia do przełącznicy. Przełącznica w związku z tym musi umożliwiać instalację specjalnych uchwytów pozwalających na pewne przytwierdzenie peszli. Włókna kabla FO wchodzącego do szafy 19" muszą być
- dystrybuowane poprzez rozdzielacz kabla. Przełącznica musi być wyposażona w zintegrowaną półkę do prowadzenia kabli krosowych nie wymagającą dodatkowego miejsca w przestrzeni szafy.

Na jednej przełącznicy 1U należy zakończyć światłowody jedno i wielomodowe.

F) Pozostałe elementu infrastruktury

Lp.	Ilość	Opis
1	5 op	Kabel instalacyjny skrętka UTP kat. 6 linka, 305m szary
2	3 op.	Kabel instalacyjny skrętka UTP kat. 6 drut, 305m
3	50m	Instalacyjne koryto kablowe, umożliwiające doprowadzenie okablowania sieciowego oraz elektrycznego - dzielone. Wymiary np.: 16x16 / 25x16 / 40x16 / 60x40 / 90x40 / 110x40
4	30m	Kanał parapetowy dwuścienny z przegrodą z możliwością bezpośredniego montażu gniazd modułowych w systemie K45. Szerokość max. 120mm, głębokość max. 55mm,
5	16 szt.	Panel krosowy kat. 6; szerokość (cale): 19, wysokość: 1U, liczba portów: 24, rodzaj złącza: RJ-45, rodzaj kabla: U/UTP, kolor: czarny.
6	8 szt.	Panel światłowody 12xLCdx OM3 + 12LCdx OS2
7	16 szt.	Listwa zasilająca RACK 19'' 9 gn z włącznikiem, przewód 5m.
8	20 szt.	Półka do szafy rack 19", 800mm
9	8 szt.	Panel 4 wentylatorów do szaf Rack stojących
10	8 szt.	Termostat do wentylatorów
11	16 szt.	Organizer kabli 1U – do szafy RACK
12	16 szt.	Panel przelotowy 1U do szafy RACK ze sztotkami
13	60 szt.	Gniazdo elektryczne 32A, 250V do stosowania w systemach modułowych 45x45mm
14	120 szt.	moduł Keystone UTP kat.6
15	120 szt.	adapter Keystone podwójny 2M 45x45
16	20 opakowań	wtyk RJ45 8p/8c kat.6 UTP linka opakowanie 100szt.
17	5 op.	wtyk RJ45 8p/8c kat.6 UTP drut opakowanie 100szt
18	40 op.	Zestaw montażowy do szaf rack (śruba,koszyczek,podkładka) 4szt
19	150 szt.	Patch cord RJ45, kat. 6 UTP, 0.5m szary, 100% miedź
20	150 szt.	Patch cord RJ45, kat. 6 UTP, 1.0m szary, 100% miedź
21	100 szt.	Patch cord RJ45, kat. 6 UTP, 2,0m szary, 100% miedź
22	100 szt.	Patch cord RJ45, kat. 6 UTP, 3.0m szary, 100% miedź
23	60 szt.	Patch cord RJ45, kat. 6 UTP, 5.0m szary, 100% miedź
24	60 szt.	Patch cord RJ45, kat. 6 UTP, 10.0m szary, 100% miedź
25	20 szt.	Patchcord światłowodowy OM3 LCdx/LCdx 5m
26	40 szt.	Patchcord światłowodowy OM3 LCdx/LCdx 2m

27	40 szt.	Patchcord światłowodowy OM3 LCdx/LCdx 1m
28	40 szt.	Patchcord światłowodowy OM3 LCdx/LCdx 0,5m
29	20 szt.	Patchcord światłowodowy OS2 LCdx/LCdx 5m
30	40 szt.	Patchcord światłowodowy OS2 LCdx/LCdx 2m
31	40 szt.	Patchcord światłowodowy OS2 LCdx/LCdx 1m
32	40 szt.	Patchcord światłowodowy OS2 LCdx/LCdx 0,5m
33	10 szt.	Patchcord światłowodowy SM 9/125 SC APC FTTH 10m
34	20 szt.	Patchcord światłowodowy SM 9/125 SC APC FTTH 5m
35	10 szt.	Patchcord światłowodowy, 50/125, OM4, LC-LC DUPLEX 3m
36	10 szt.	Gniazdo światłowodowe podwójne FO 2xSC/APC
37	10 szt.	Gniazdo keystone typu LC duplex żeńskie
38	5 szt.	Przewód HDMI 20m 24AWG v1.4
39	5 kpl.	Gniazdo 10xRJ45 kat. 6 UTP montaż w słupkach pionowych
40	25 szt.	Panel z wieszakami poziomy 1U
41	10 szt.	Panel z wentylatorem i termostatem
42	10 szt.	Listwa zasilająca pozioma 1U 9 gniazd

G) Stacje robocze – 4 szt.

Do stacji roboczych o parametrach zawartych poniżej należy zapewnić pełną infrastrukturę sieciową. Wykonane to będzie za pomocą kolumn elektroinstalacyjnych opisanych w podpunkcie D) (każda kolumna musi posiadać co najmniej 4 gniazda RJ-45 oraz 5 gniazd zasilających 230V). Stacje robocze muszą być podłączone do kolumn elektroinstalacyjnych za pomocą dostarczonych przez Wykonawcę przewodów zasilających i logicznych.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Typ	Komputer stacjonarny – wydajna stacja graficzna. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
2.	Zastosowanie	Komputer będzie wykorzystywany jako profesjonalna stacja robocza m.in. dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do Internetu oraz poczty elektronicznej
3.	Procesor	Min. 6-rdzeniowy, min 3.70GHz*,* osiągający w teście PassMark CPU Mark wynik min. 15900 punktów. Do oferty należy dołączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie wymogów SIWZ.
4.	Pamięć operacyjna	*minimum 16GB* (DDR4 SDRAM 2666MHz) z funkcją non-ECC Registered - możliwość rozbudowy do 64GB, min cztery gniazda pamięci.
5.	Parametry pamięci masowej	Min. *z Turbo Drive 512GB PCIe SSD*, możliwość instalacji dysków 3,5”, SSD, M.2 (PCIe Gen 3 x4)
6.	Grafika	128-bitowa z własną pamięcią *4GB GDDR5*, zgodna ze standardem OpenGL 4.4, DIRECTX 11 oraz CUDA, posiadająca co najmniej cztery złącza cyfrowe z obsługą czterech monitorów o rozdzielczościach do 4096x2160 @60Hz pikseli *osiągająca w teście Average G3D Mark wynik na poziomie 4650 punktów.* *Do oferty należy dołączyć wydruk ze strony: http://www.videocardbenchmark.net potwierdzający spełnienie wymogów SIWZ*
7.	Wyposażenie multimedialne	Zintegrowana z płytą główną, zgodna z High Definition (HD) Audio

8.	Obudowa	Obudowa fabrycznie konwertowalna typu Small Form Factor z możliwością pracy w pozycji pionowej i poziomej, o maksymalnej sumie wymiarów 82 cm, posiadająca min.: 1 zewnętrzną półkę 5,25" SLIM, 1 zewnętrzną/wewnętrzną współdzieloną półkę 3,5", 1 wewnętrzną półkę 2,5" dla dysków SSD. Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta, metalowa. Obudowa musi umożliwiać serwisowanie komputera bez użycia narzędzi. *Czytnik kart SD/SDHC/SDXC z przodu obudowy. Port serial (RS232) z tyłu obudowy.* Maksymalna suma wymiarów 82 cm. Obudowa musi posiadać możliwość montażu czujnika otwarcia obudowy. Obudowa musi umożliwiać serwisowanie komputera bez użycia narzędzi. Z przodu obudowy wymagany jest wbudowany fabrycznie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej: – awarie procesora – uszkodzenie kontrolera Video – uszkodzenie pamięci RAM uszkodzenie zasilacza Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko na kłódkę) Zasilacz o mocy: min 310W z aktywnym PFC i sprawności min 90%
9.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać, co najmniej certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows (załączyć wydruk ze strony Microsoft WHCL)
10.	BIOS	Możliwość odczytania z BIOS: 1. Wersji BIOS wraz z datą wydania wersji 2. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3 3. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach 4. Informacji o dysku twardym: model, pojemność, 5. Informacji o napędzie optycznym: model, 6. Informacji o MAC adresie karty sieciowej Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, serial portu, portów USB (przód, tył), funkcjonalności ładowania zewnętrznych urządzeń przez port USB, poszczególnych slotów SATA, czytnika kart SD, wewnętrznego głośnika, funkcji TurboBoost, wirtualizacji, RAID z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie administratora. - BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.

11.	Bezpieczeństwo	1. BIOS musi posiadać możliwość - skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, - możliwość ustawienia hasła na dysku (drive lock) - blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio; - blokady/wyłączenia poszczególnych kart rozszerzeń/slotów PCIe - kontroli sekwencji boot; - startu systemu z urządzenia USB - funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń - włączenia/wyłączenia RAID 2. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0); 3. Możliwość zapięcia linki typu Kensington i kłódki do dedykowanego oczka w obudowie komputera 4. Udostępniona bez dodatkowych opłat, pełna wersja oprogramowania, szyfrującego zawartość twardego dysku zgodnie z certyfikatem X.509 oraz algorytmem szyfrującym AES 256bit, współpracującego z wbudowaną sprzętową platformą bezpieczeństwa 5. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego: - informacje o systemie, min.: 1. Procesor: typ procesora, jego obecna prędkość 2. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta 3. Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku 4. Napęd optyczny: model, wersja firmware, nr seryjny 5. Data wydania i wersja BIOS 6. Nr seryjny komputera - możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera - możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej - rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii
12.	Zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, posiadająca sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiająca: - monitorowanie konfiguracji komponentów komputera - CPU, pamięć, HDD, wersje BIOS płyty głównej; - zdalną konfigurację ustawień BIOS;

		- zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; - zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej; - technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/); - nawiązywanie przez sprzętowy mechanizm zarządzania zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS; - wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego. - *zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie*
13.	Certyfikaty i standardy	– Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) – Deklaracja zgodności CE (załączyć do oferty) – Komputer musi spełniać wymogi normy Energy Star 6.1 Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej
14.	Ergonomia	Maksymalnie 25 dB w pozycji operatora w trybie IDLE, pomiar zgodny z normą ISO 9296 / ISO 7779; wymaga się dostarczenia odpowiedniego certyfikatu lub deklaracji producenta
15.	Warunki gwarancji	minimum 36 miesięcy w miejscu instalacji. Firma serwisująca musi posiadać ISO 9001: 2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
16.	Wsparcie techniczne producenta	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer – w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: - weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć) - czasu obowiązywania i typ udzielonej gwarancji Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera

		Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera
17.	Wymagania dodatkowe	1. Zainstalowany system operacyjny Windows *10 Professional 64bit PL* niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft + *nośnik* lub system równoważny – przez równoważność rozumie się pełną funkcjonalność, jaką oferuje wymagany w SIWZ system operacyjny 2. Wbudowane porty i złącza: - min. 8 x USB w tym minimum 4 porty USB 3.0 z tyłu i min 2 porty USB 3.0 z przodu obudowy - port sieciowy RJ-45, - porty audio: z przodu obudowy gniazdo wejście mikrofonowe/wyjście słuchawek typu COMBO, z tyłu obudowy wejście liniowe i wyjście liniowe - opcjonalny port serial (RS-232) - *opcjonalny LPT* - opcjonalny *czytnik kart multimedialnych SD z przodu obudowy* - *opcjonalny port Thunderbolt 3.0* Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. 3. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL, iAMT, vPro 4. Płyta główna, wyposażona w: - 4 złącza DIMM z obsługą do 64GB pamięci RAM DDR4 2666 MHz - sloty wyłącznie o niskim profilu: 1 x PCIe x16 Gen3 1 x PCIe x4 Gen3 (złącze x16) 1 x PCIe x1 Gen3 (złącze x4) 1 x M.2 (PCIe x4 Gen3) 1 x M.2 Wlan (PCIe Gen3 x1) - 4 złącza SATA - kontroler dysków obsługującym konfiguracje RAID 0, 1 5. Klawiatura *USB* w układzie polski programisty 6. Mysz optyczna *USB* z min dwoma klawiszami oraz rolką (scroll) 7. Nagrywarka SATA DVD +/-RW x8 SuperMulti

H) Monitor – 8 szt.

Lp.	Parametr	Wymagany, minimalny parametr
1	Typ	LCD kolorowy 27” panoramiczny, matryca typu IPS z podświetleniem LED
2	Plamka	0,312 mm
3	Rozdzielczość	min. 1920 x 1080 @ 60Hz
4	Jasność	min. 250 cd/m2
5	Kontrast	min. 1000:1 (dynamiczny 5 000 000:1)
6	Kąty widzenia	Poziom/Pion: 178°/178° (10:1 contrast ratio)
7	Częstotliwość odświeżania	Pozioma: od 30 do 80 kHz Pionowa: od 50 do 60 Hz

8	Pobór mocy	Typowo: max 25W, Max: 42W
9	Czas reakcji matrycy	max 5ms
10	Normy	TCO, Energy Star, EPEAT Gold
11	Złącza	wejście VGA, HDMI 1.4, DisplayPort 1.2, wbudowany hub USB 3.0 min 2 szt, slot dla linki Kensingtona
12	Inne	Regulacja pochylenia ekranu (tilt) -5° to +22°, Regulacja wysokości (min. 15cm), Regulacja obrotu monitora (swivel) -45°/+45°, Możliwość obracania ekranu (pivot), Zasilacz zintegrowany w monitorze Waga samego monitora bez standu max: 4,5 kg System montażowy VESA 100mm Kolor Gamut (typowy) – 94% sRGB, NTSC 72% Możliwość instalacji do monitora dedykowanych głośników
13	Gwarancja	Min. 12 miesięcy.

I) Urządzenie do wykonywania płytek drukowanych PCB – 1 szt.

1. Parametry techniczne:

- Maksymalny obszar roboczy (X x Y x Z) : min. 229 mm x 305 mm x 8 mm
- Maksymalny rozmiar materiału (X x Y x Z) : 250 mm x 330 mm x 26 mm
- Prędkość pozycjonowania osi (X x Y): 150 mm/s
- Maksymalne obroty wrzeciona: 60 000 obr/min, regulowane programowo
- Szybkość wiercenia: 100 otworów/min
- Uchwyt narzędziowy: 3.175 mm (1/8”)
- Zmiana narzędzi: automatyczna
- Regulacja szerokości frezowania: automatyczna ± 1 µm (0,04 mil)
- Powtarzalność: ± 0.001 mm (± 0.04 mil)
- Rozdzielczość mechaniczna (X / Y): ± 0.5 µm (± 0.02 mil)
- Załączony system odsysający
- Załączone oprogramowanie sterujące maszyną

2. Możliwości użytkowe:

- Frezowanie / wiercenie jedno- i dwustronnych płytek drukowanych
- Frezowanie / wiercenie podłoży o wysokiej częstotliwości i mikrofalowych
- Frezowanie / wiercenie wielowarstwowe
- Frezowanie konturowe płytek drukowanych
- Grawerowanie paneli / płyt przednich
- Frezowanie wycięć w panelach przednich
- Frezowanie szablonów past lutowniczych SMD
- Obróbka obudów
- Frezowanie ramek lutowniczych
- Depaneling i postprocessing płytek drukowanych
- Dozowanie pasty lutowniczej

3. Akcesoria w zestawie:

- wiertarko-frezarka - 1 szt.
- system odsysający – 1 szt
- zestaw akcesoriów i narzędzi do uchwytu 1/8” - 1 szt.

4. Gwarancja: minimum 12 miesięcy.