Dostawa, wdrożenie i uruchomienie infrastruktury IT dla nowo budowanego budynku Małopolskiego Centrum Nauki Cogiteon

OPIS PRZEDMIOTU ZAMÓWIENIA

1 Spis treści

2 Przedmiot postępowania

Przedmiotem postępowania jest dostawa, wdrożenie i uruchomienie infrastruktury IT dla nowo budowanego budynku Małopolskiego Centrum Nauki Cogiteon. Ilekroć zamawiający opisując daną funkcjonalność wskazuje, że powinna być ona opcjonalna, należy to interpretować, że w danym postępowaniu rozwiązanie powinno posiadać daną funkcjonalność, lecz nie jest wymagane dostarczenie licencji na jej uruchomienie.

3 Zakres przedmiotu zamówienia

Dostawa i instalacja urządzeń i oprogramowania obejmuje swym zakresem:

1. Wykonanie dokumentacji przedwdrożeniowej w oparciu o dokumentację Zamawiającego oraz zakres określony przez Zamawiającego,
2. Dostarczenie urządzeń oraz oprogramowania,
3. Montaż i konfiguracja dostarczony urządzeń oraz oprogramowania zgodnie z opracowaną i zaakceptowaną dokumentacją przedwdrożeniową,
4. Opracowanie scenariuszy testów dla dostarczonego rozwiązania,
5. Przeprowadzenie testów akceptacyjnych dostarczanego urządzeń i oprogramowania zgodnie z zaakceptowanym przez Zamawiającego scenariuszem testów,
6. Opracowanie dokumentacji powykonawczej dostarczonego systemu,
7. Opracowanie procedur utrzymania dostarczonego systemu,
8. Przeprowadzenie szkoleń z dostarczonego rozwiązania.

4 Miejsce realizacji przedmiotu zamówienia

Miejscem realizacji przedmiotu zamówienia jest budynek Małopolskiego Centrum Nauki Cogiteon przy ul. Bora Komorowskiego – obecnie w budowie.

5 Etapy realizacji zamówienia

Wykonawca zobowiązany jest do wykonania przedmiotu zamówienia według następujących etapów:

LP	Nazwa etapu	Opis	Czas trwania
1	Etap I - wykonanie dokumentacji przedwdrożeniowej.	Dokumentacja przedwdrożeniowa powinna uwzględniać m. in.: • Architekturę fizyczną oraz logiczną docelowego rozwiązania. • Harmonogram zawierający niezbędne, szczegółowo opisane działania dot. realizacji wdrożenia. • Konfigurację urządzeń w zakresie sprzętowym. • Opis integracji z elementami środowiska Zamawiającego wraz ze szczegółami dot. konfiguracji tych elementów..	Czas trwania etapu: do 30 dni od dnia podpisania umowy

LP	Nazwa etapu	Opis	Czas trwania
		• Plan testów akceptacyjnych zawierający scenariusze oraz procedury składające się z co najmniej: o czasu trwania testów wraz z iteracjami, o informacje na temat obiektu testu. W przypadku wymagania przez Wykonawcę kolejnych wizji lokalnych, Zamawiający umożliwi ich przeprowadzenie. Etap zakończy się pisemny potwierdzeniem wykonania przez Zamawiającego.	
2	Etap II - dostawa urządzeń objętych zamówieniem oraz wdrożenie rozwiązania	Wykonawca dostarczy sprzęt objęty w terminie określonym w ofercie do wskazanych przez Zamawiającego lokalizacji Wykonawca po zakończeniu dostawy i wdrożenia sporządzi listę dostarczanego sprzętu. Wypełnioną listę sprzętu Wykonawca przekaże Zamawiającemu na koniec dostawy, również w formie elektronicznej. Lista zawierać będzie minimum: • numer seryjny urządzenia, • model dostarczonego sprzętu, • imię i nazwisko osób dokonujących odbioru, • adres i numer pomieszczenia dostarczanego sprzętu, • wartość sprzętu. Zamawiający dopuszcza dostawy i odbiory częściowe. Zamawiający informuje, że nie posiada wolnej przestrzeni na składowanie dostarczonego sprzętu, a zatem dostawy powinny być tak zaplanowane by sprzęt od razu był montowany na obiekcie zgodnie z dokumentacją przedwdrożeniową. Wdrożenie rozwiązania następować będzie wg. poniższego schematu: • Podłączenie fizyczne dostarczonych urządzeń. • Uruchomienie nowo podłączonych urządzeń. • Konfiguracja nowych podłączonych urządzeń zgodnie z dokumentacją przedwdrożeniową. • Weryfikacja poprawności połączeń między poszczególnymi urządzeniami. • Instalacja dostarczonego oprogramowania i/lub licencji. Etap zakończy się pisemny potwierdzeniem wykonania przez Zamawiającego.	Czas trwania etapu: 110 dni od dnia podpisania umowy
3	Etap III - testy powdrożeniowe.	Po zakończeniu etapu wdrożenia, Wykonawca wykona testy poprawności oraz bezpieczeństwa działania nowopowstałej infrastruktury na podstawie szczegółowego opisu testów zawartego w dokumentacji przedwdrożeniowej. Zakres testów obejmować będzie minimum: • Weryfikację możliwości połączeń między przełącznikami. • Test przypadków awarii urządzeń zlokalizowanych w serwerowniach (wyłączenie urządzenia lub urządzeń).	Czas trwania etapu: do 7 dni od zakończenia etapu II

LP	Nazwa etapu	Opis	Czas trwania
		• Test przypadków awarii pojedynczego połączenia pomiędzy urządzeniami. • Test dostępu do i z sieci Internet • Test wykrywający pętlę w warstwie 2 modelu OSI/ISO oraz pętle w sieci pomiędzy VLANami. • Weryfikację możliwości połączeń między serwerami. • Weryfikację połączeń pomiędzy serwerami, a macierzami. • Weryfikację bezpieczeństwa połączenia – sprawdzenie braku dostępu możliwości połączeń z sieci, które nie powinny mieć dostępu – test bezpieczeństwa. • Test przypadku awarii dysku/dysków twardych • Test połączenia między przełącznikami i kontrolerami bezprzewodowymi • Test połączenia między kontrolerami, a punktami bezprzewodowymi • Test połączenia między urządzeniami systemu firewall – test redundancji systemu • Testy systemu zarządzania • Testy systemu kopii zapasowej • Test systemu kontroli dostępu • Test systemu analizy aplikacji • Test oprogramowani do wirtualizacji W przypadku, gdy testy nie zakończą się pozytywnym rezultatem, Wykonawca jest zobowiązany do usunięcia usterki oraz do ponownego przeprowadzenia testów zgodnie z zaproponowaną formułą iteracji przypadku. Etap zakończy się pisemny potwierdzeniem wykonania przez Zamawiającego.	
6	Etap IV - wykonanie dokumentacji powykonawczej	Dokumentacja powykonawcza dostarczona przez Wykonawcę musi zawierać co najmniej: Opisaną końcową konfigurację urządzeń oraz schemat połączeń wraz z oznaczeniem niestandardowych rozwiązań lub obejść . Opis przeprowadzonych testów zawierających wyniki testów wraz z wnioskami . Opis przeszkód napotkanych w trakcie implementacji oraz opis ich rozwiązania. Skrypty, jeżeli zostały użyte, do automatyzacji zadań wraz z ich opisem. Konfigurację urządzeń w postaci elektronicznej. Etap zakończy się podpisaniem protokołu końcowego przez Zamawiającego.	Czas trwania etapu: do 14 dni od zakończenia etapu II

6 Główne założenia

Głównym założeniem przedmiotu zamówienia jest wyposażenie nowo budowanego budynku w niezbędną infrastrukturę IT. W ramach zamówienia zostanie dostarczona i zainstalowana:

- Infrastruktura sieciowa przewodowa i bezprzewodowa wraz z systemem zarządzania;

- Systemy bezpieczeństwa;
- Systemy kopii zapasowej;
- Infrastruktura serwerowo macierzowa;
- Systemy kontroli dostępu.

W rozdziale tym przedstawione zostały założenia projektowe, opis stanu aktualnego oraz proponowana architektura projektowanego rozwiązania.

6.1 Opis stanu projektowanego

6.1.1 Opis ogólny

Serwerownia Zamawiającego znajduje się w nowo budowanym budynku Małopolskiego Centrum Nauki Cogiteon przy ul. Bora Komorowskiego. Pomieszczenia wyposażone są w odpowiednią infrastrukturę teletechniczną. Serwerownia główna (GPD) zlokalizowana jest na jest na parterze. Natomiast 14 serwerowni pełniących rolę pośrednich punktów dystrybucyjnych zlokalizowane na różnych piętrach budynku. W GPD znajduje się 10 szaf RACK, a w PPD 17 szaf rack. Wszystkie szafy wyposażone są w niezbędne patchpanele światłowodowe z portami LC i miedziane, listwy zasilające model 49BM9PM, organizery itp. Wszystkie połączenia między szafami wykonane są na światłowodach wielomodowych. Jeżeli w danym punkcie dystrybucyjnym IDFx znajduje się więcej niż jedna szafa to tylko jedna z nich jest skrosowana światłowodowo z szafami w GPD. W ramach zamówienia Zamawiający wymaga dostawy dodatkowych listw zasilających o parametrach nie gorszych niż wyżej wymieniona listwa. Jednocześnie Zamawiający informuje, że w ramach zamówienia nie przewiduje krosowania przełączników sieciowych z patchpanelami Ethernet do których schodzą się połączenia z poszczególnych pomieszczeń. Wykonawca będzie musiał wykonać niezbędne krosowania, która jest niezbędna do uruchomienia wszystkich dostarczanych urządzeń i wybudowania działającego systemu IT. Dostarczane rozwiązanie musi być zainstalowane w wyżej wymienionych szafach.

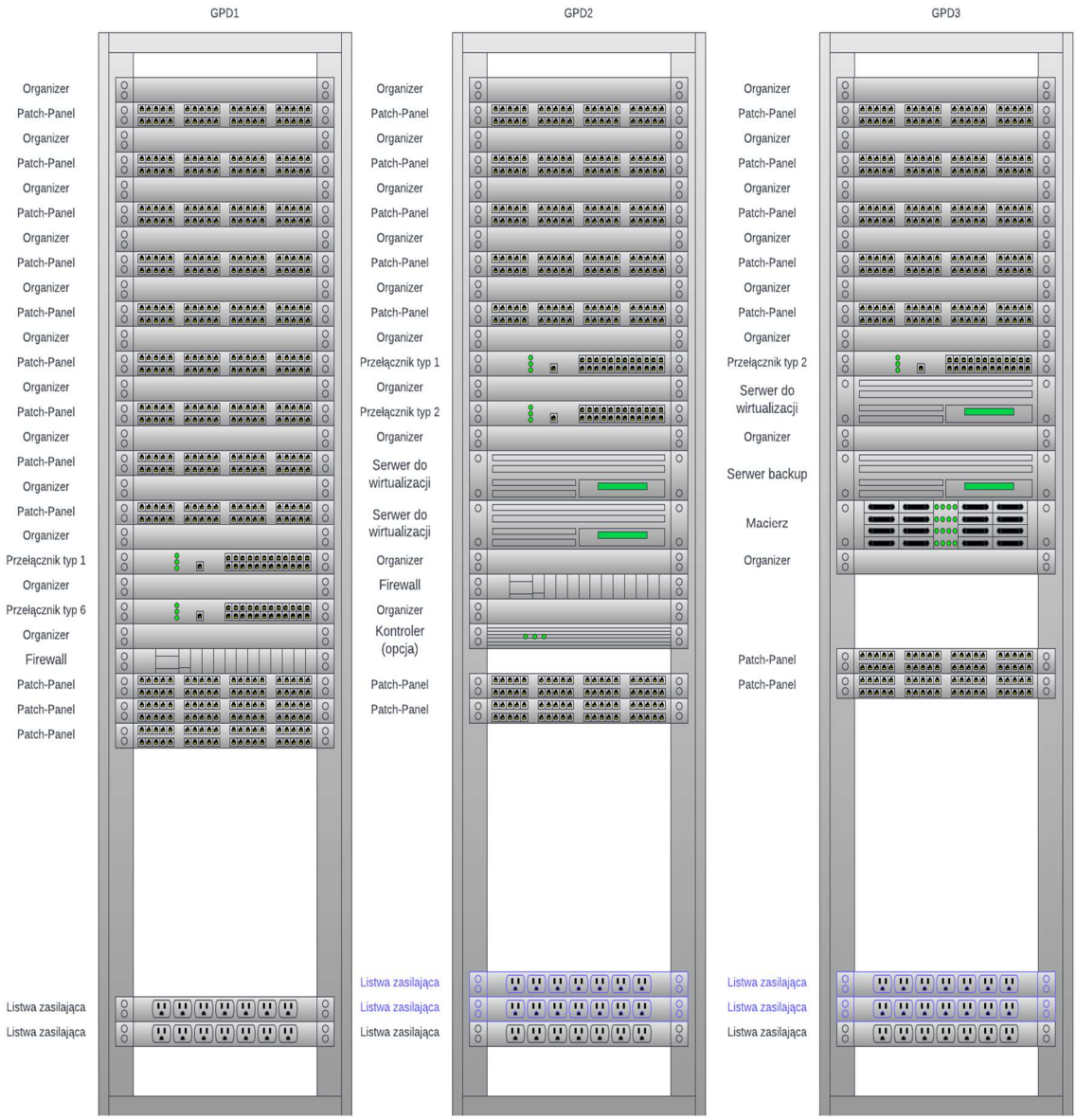
Dodatkowo na całym budynku przygotowane są punkty PEL niezbędne do instalacji podłączenia bezprzewodowych punktów dostępowych. Zamawiający posiada również patchcordy światłowodowe wielomodowe LC w ilościach i długości: 1 m - 100 szt. i 2m 100 szt.

Wszystkie przewody zasilające dla urządzeń powinny umożliwiać podłączenie do listw zasilających posiadanych przez Zamawiającego. Listwy posiadają gniazda typu NFC61-314.

6.1.2 Proponowane rozłożenie infrastruktury w szafach.

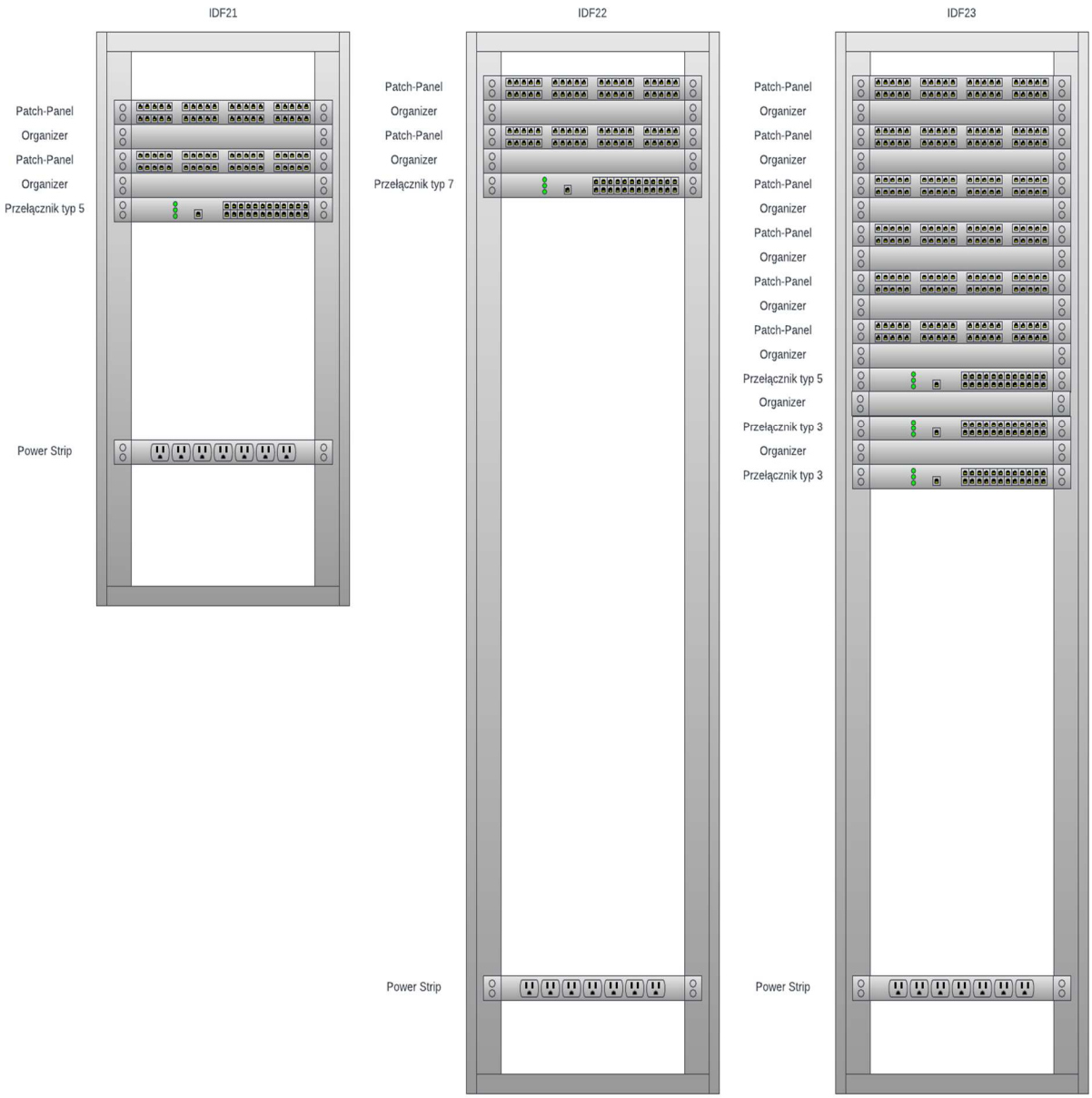
Na poniższych rysunkach przedstawiono proponowane rozłożenie sprzętu w poszczególnych szafach serwerowych. Proponowane rozłożenie może ulec zmianie i zostanie ostatecznie zatwierdzone w dokumentacji przedwdrożeniowej przedstawionej przez Wykonawcę. Listwy zaznaczone kolorem niebieskim należy dostarczyć

6.1.2.1 Serwerownia GPD

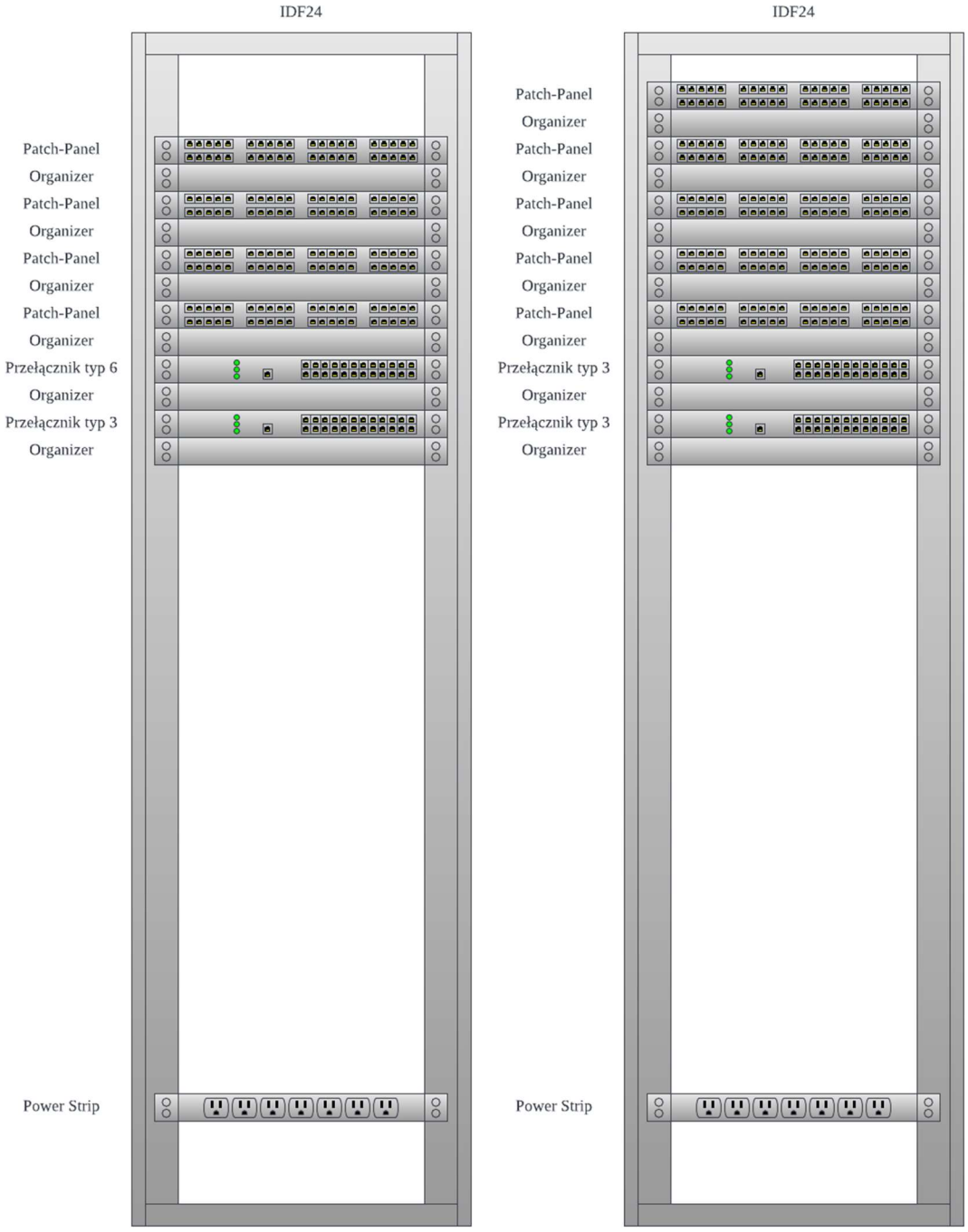


Rysunek 1 Rozmieszczenie sprzętu w szafach

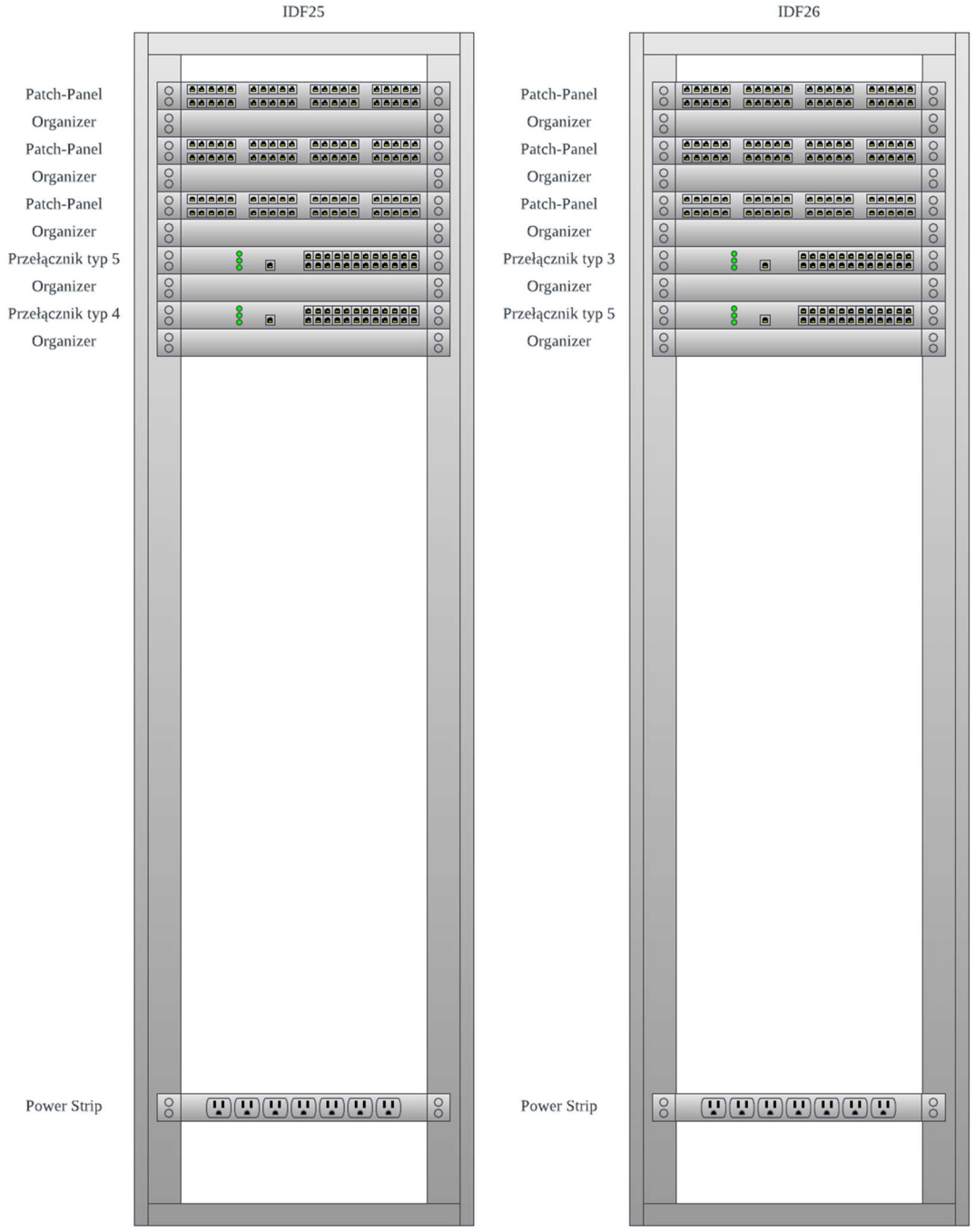
6.1.2.2 Serwerownie PPD



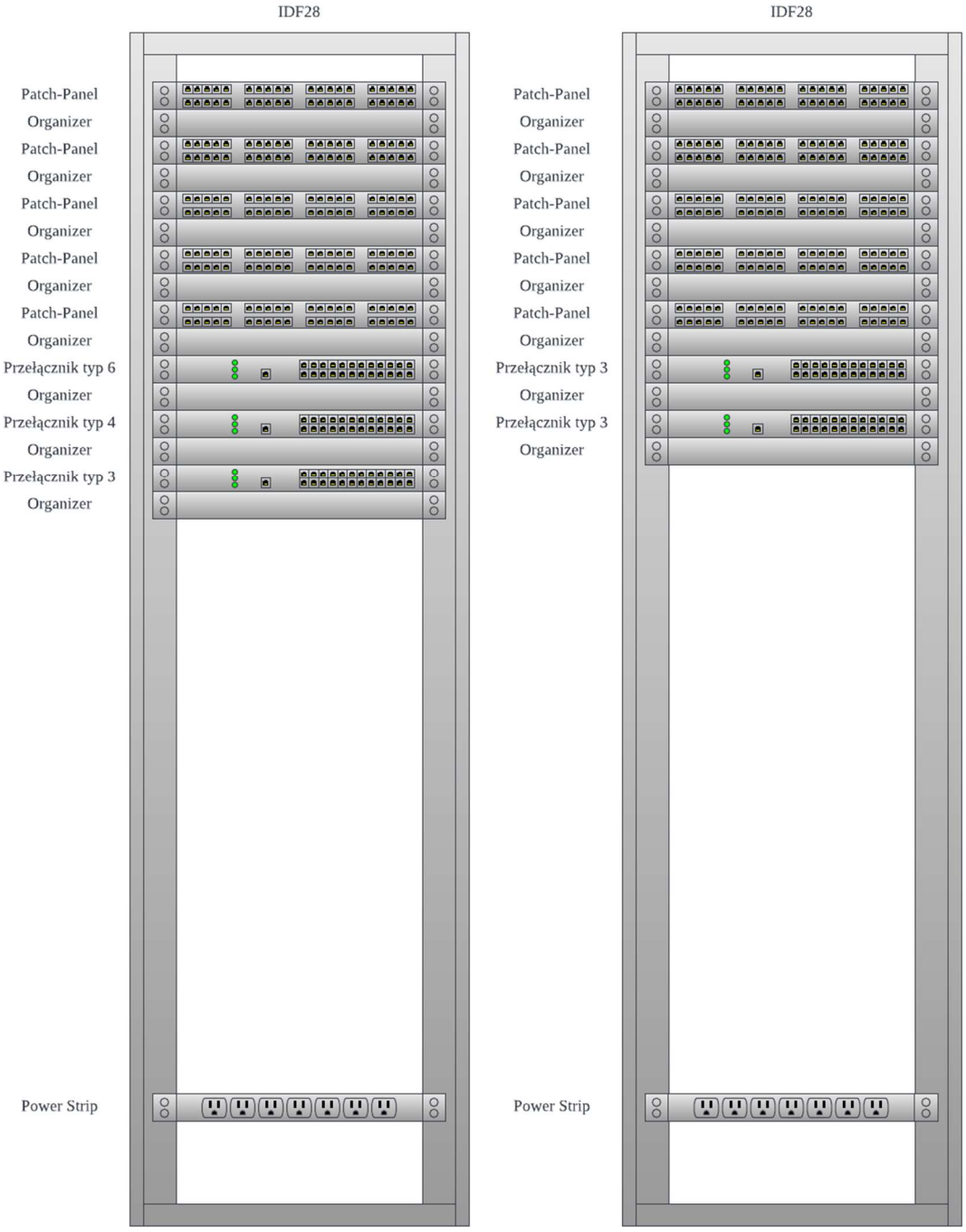
Rysunek 2 Rozmieszczenie sprzętu w szafach



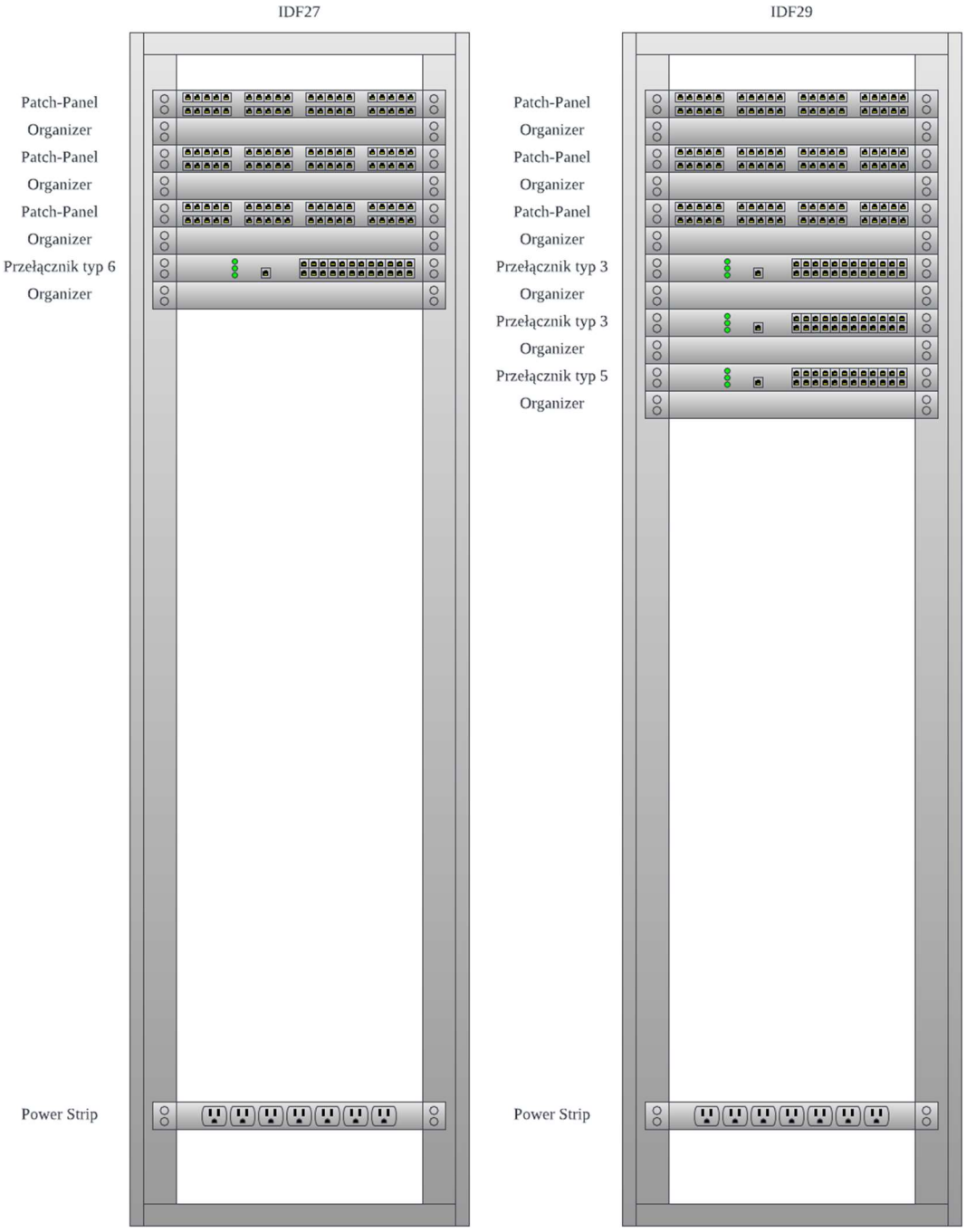
Rysunek 3 Rozmieszczenie sprzętu w szafach



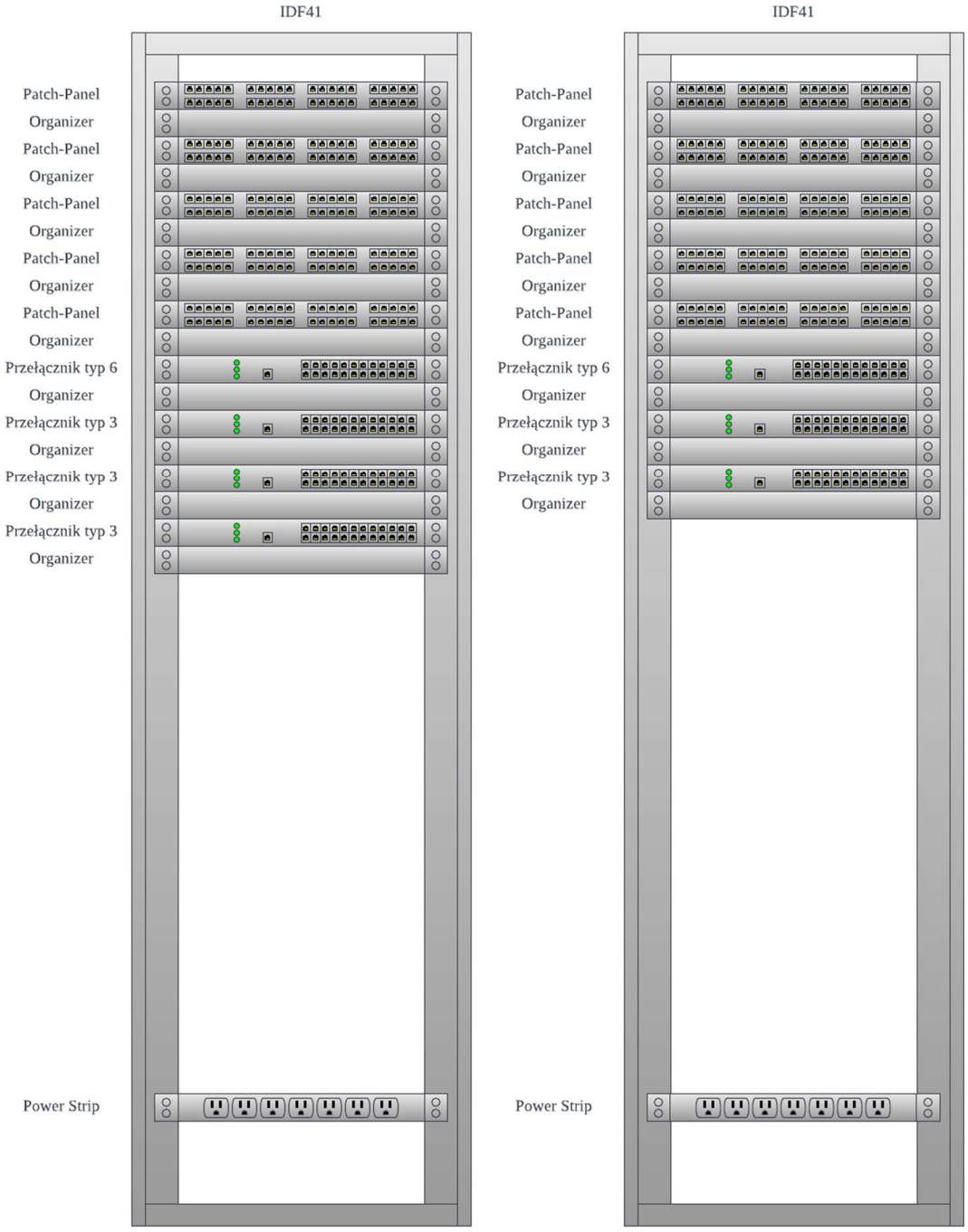
Rysunek 4 Rozmieszczenie sprzętu w szafach



Rysunek 5 Rozmieszczenie sprzętu w szafach



Rysunek 6 Rozmieszczenie sprzętu w szafach



Rysunek 7 Rozmieszczenie sprzętu w szafach

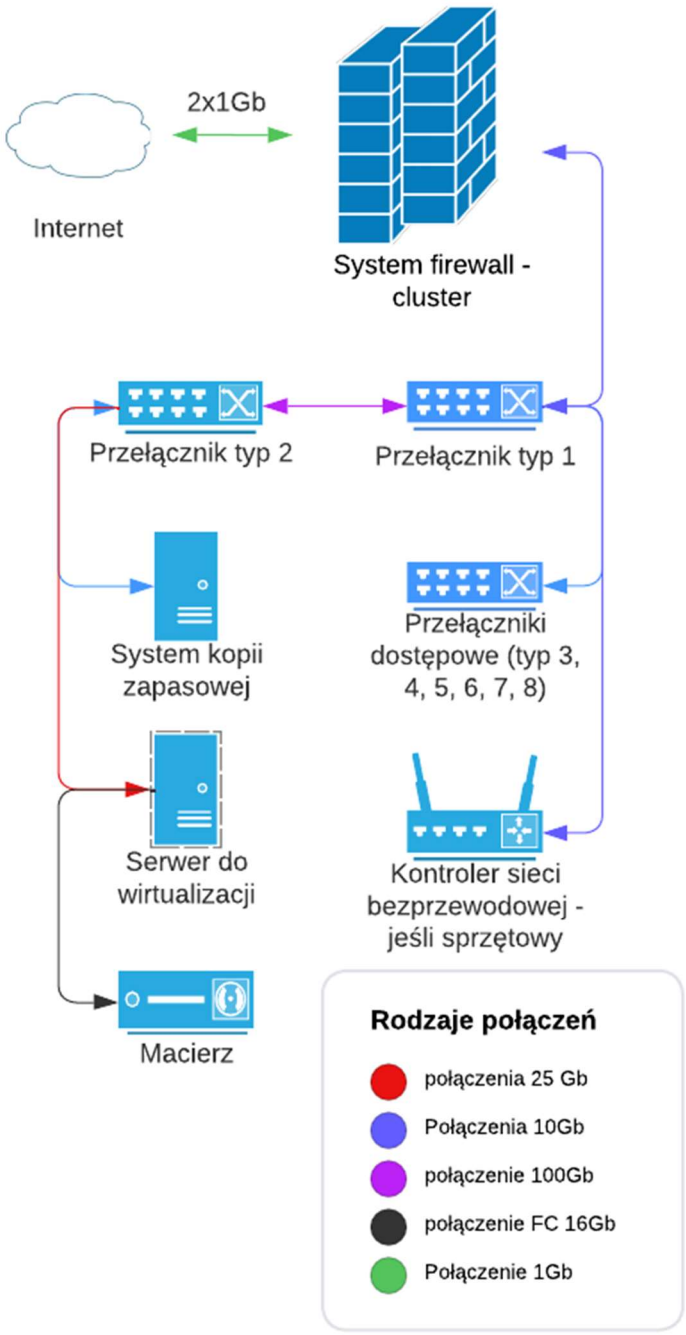
Rysunek 8 Rozmieszczenie sprzętu w szafach

Rysunek 9 Rozmieszczenie sprzętu w szafach

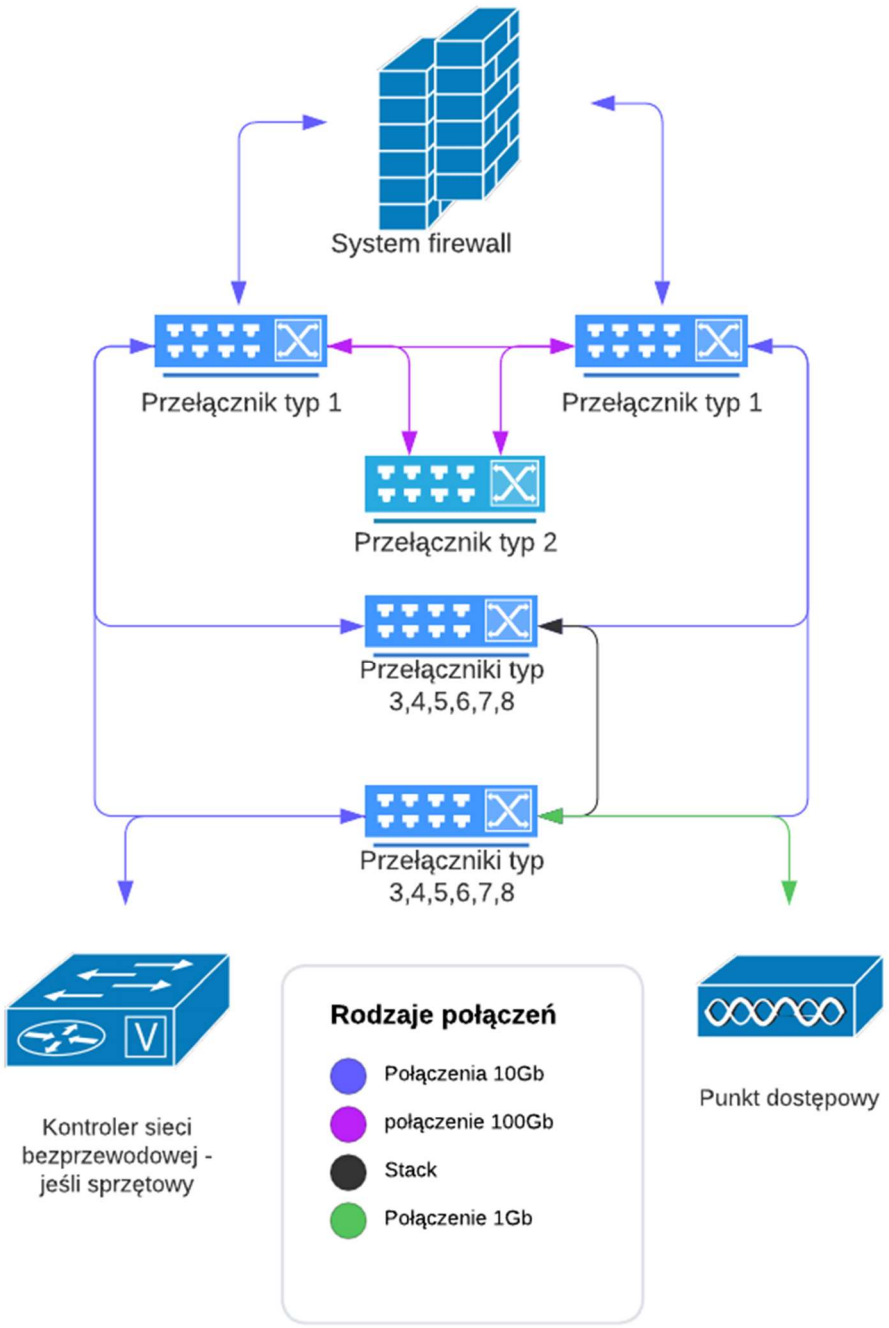
6.1.3 Proponowane schematy połączeń między urządzeniami

Poniżej przedstawiono proponowane schematy połączeń między urządzeniami:

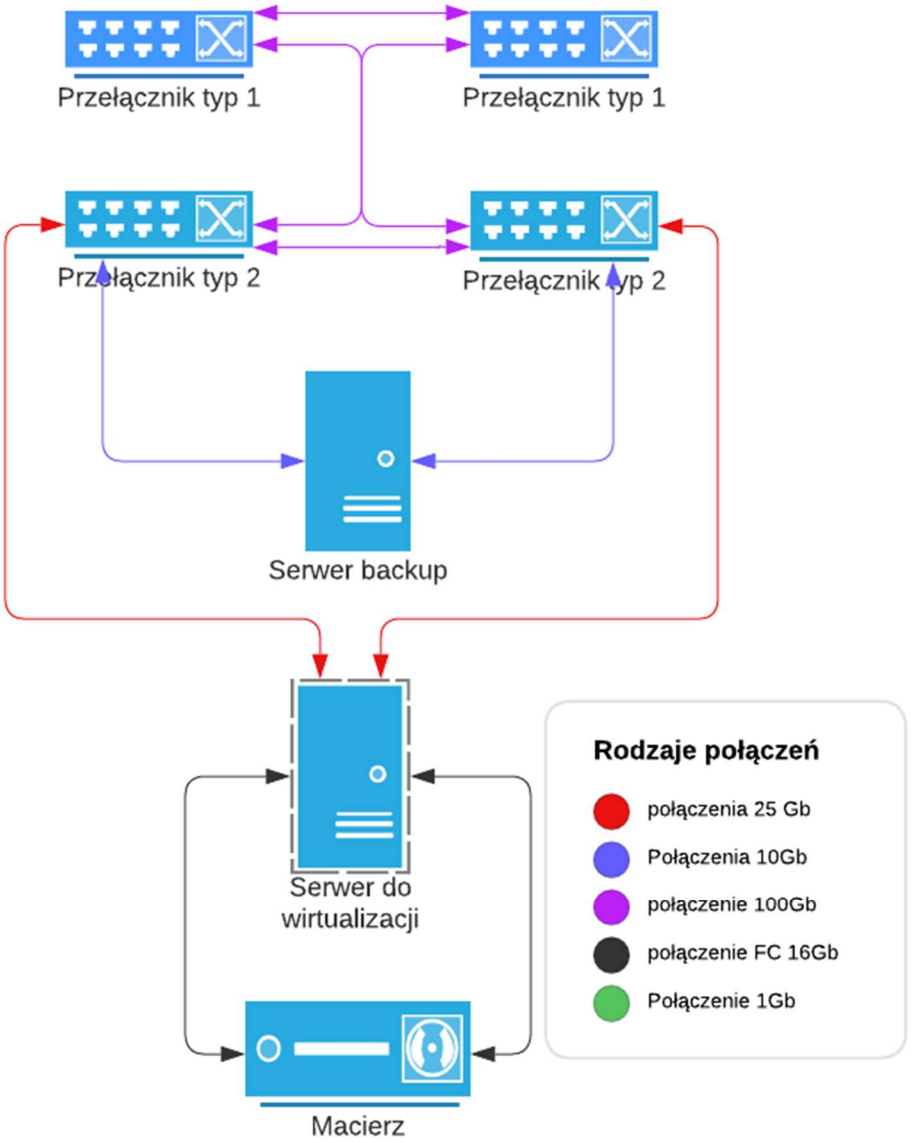
- Połączenie pomiędzy każdym przełącznikiem rdzeniowym (Typ1), a dwoma przełącznikami serwerowymi (Typ 2) realizowane powinno być z prędkością 100Gbit każde.
- Przełączniki rdzeniowe (Typ 1) muszą być połączone między sobą za pomocą portów uplink 2x100Gbit.
- Przełączniki dostępowe (Typ 3, 4, 5, 6, 7, 8) muszą zostać podłączone z każdym przełącznikiem rdzeniowym (Typ 1) linkami o prędkości 10Gbit.
- Przełączniki serwerowe (Typ 2) połączone są w stos.
- Jeśli zajdzie taka konieczność to przełączniki dostępowe (Typ 3, 4, 5, 6, 7, 8) powinny być połączone w stos w ramach jednej szafy i jednego lub wielu typu – zależnie od wymagań producenta
- Każdy serwer do wirtualizacji połączony musi być podłączony po jednym linku 25Gbit do każdego z przełączników serwerowych (Typ2) zapewniając redundancję połączenia.
- System kopii zapasowych musi być podłączony po jednym linku 10Gbit do każdego z przełączników serwerowych (Typ 2) zapewniając redundancję połączenia.
- Każdy z dwóch kontrolerów macierzy dyskowej musi być podłączony bezpośrednio uplinkiem FibreChannel 16Gbit z każdym z serwerów do wirtualizacji tworząc sieć SAN, tak aby każdy z serwerów miał bezpośrednio połączenie z każdym z kontrolerów macierzy.
- System Firewall – Cluster musi być połączony z każdym z przełączników rdzeniowych (Typ 1) uplinkiem o prędkości 10Gbit.



Rysunek 10 Proponowany schemat połączeń



Rysunek 11 Proponowany schemat połączeń siei LAN



Rysunek 12 Proponowany schemat połączeń sieci SAN i LAN

6.2 Szczegółowa specyfikacja techniczna urządzeń i oprogramowania

W poniższej tabeli zamieszono minimalną ilość wymaganego sprzętu i oprogramowania, które należy dostarczyć w ramach niniejszego postępowania:

LP	Nazwa	Ilość
1	Klaster wirtualizacyjny z oprogramowaniem	1
2	Macierz dyskowa	1
3	System kopii zapasowych	1
4	Przełącznik typ 1	2
5	Przełącznik typ 2	2

6	Przełącznik typ 3	16
7	Przełącznik typ 4	2
8	Przełącznik typ 5	8
9	Przełącznik typ 6	7
10	Przełącznik typ 7 lub typ 8	1
11	Bezprzewodowy punkt dostępowy	65
12	Kontroler sieci bezprzewodowej	2
13	System zarządzania	1
14	System kontroli dostępu	1
15	System analizy aplikacji	1
16	System firewall	2
17	Listwy zasilające – o parametrach nie gorszych niż posiadane przez Zamawiającego	4
18	Patchcordy kat 6A – 25 cm	200
19	Dodatkowe moduły SFP+ 10Gb – oprócz wymaganych do uruchomienia całej infrastruktury - kompatybilne z systemem firewal	4
20	Dodatkowe moduły SFP+ 10Gb – oprócz wymaganych do uruchomienia całej infrastruktury – kompatybilne z przełącznikami typ 1	6

W poniższej tabeli zamieszono maksymalną ilość sprzętu i oprogramowania, które należy dostarczyć w ramach opcji:

LP	Nazwa	Ilość
1	Przełącznik typ 3	1
2	Bezprzewodowy punkt dostępowy	10

6.2.1 Klaster wirtualizacyjny

Klaster wirtualizacyjny ma składać się z min. 3 serwerów według poniższej specyfikacji oraz oprogramowania wirtualizacyjnego w ilości niezbędnej do działania całego klastra.

6.2.1.1 Serwer do wirtualizacji 3 szt.

Dostarczony serwer do wirtualizacji musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

Lp.	Parametr lub warunek	Minimalne wymagania
1	Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Możliwość zainstalowania 16 dysków twardych hot plug 2,5”; • Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; • Zainstalowane 2 szt. dyski SSD M.2 SATA lub M.2 NVMe SSD 240GB podpięte do sprzętowego kontrolera RAID-1; • Możliwość zainstalowania dedykowanego napędu optycznego;

2	Płyta główna	• Dwuprocesorowa;
		• Wyprodukowana i zaprojektowana przez producenta serwera
		• Możliwość zainstalowania modułu TPM 2.0;
		• Min 7 złącz PCI Express generacji 4:w tym:
		  ○ 4 fizyczne złącza o prędkości x16;
		  ○ 3 fizyczne złącza o prędkości x8;
		  ○ Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;

		○ Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; Lub ○ 6 fizycznych złącz o prędkości x8 ○ 2 fizyczne złącza o prędkości x16 • 32 gniazda pamięci RAM; • Obsługa minimum 4TB pamięci RAM DDR4; • Obsługa minimum 8TB pamięci RAM DDR4 + pamięć nieulotna; • Wsparcie dla technologii: ○ Memory Scrubbing lub równoważne ○ SDDC lub równoważne ○ ECC lub równoważne ○ Memory Mirroring lub równoważne ○ ADDDC lub równoważne; • Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) • Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;
3	Procesory	• Zainstalowany minimum jeden procesor maksymalnie 16-sto rdzeniowy • Taktowanie 2,9GHz • architektura x86_64 osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 148pkt (wynik osiągnięty dla zainstalowanego jednego procesora). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html
4	Pamięć RAM	• 512 GB pamięci RAM • DDR4 Registered • 3200Mhz • Możliwość rozbudowy do 1024GB pamięci RAM przez dołożenie kolejnych modułów pamięci bez konieczności wymiany zainstalowanych
5	Kontrolery LAN	• Karta LAN wyposażona minimum w interfejsy: 2x 25Gbit SFP28,
6	Kontrolery I/O	• Zainstalowana dwuportowa karta FC 16Gbit
7	Porty	• Zintegrowana karta graficzna ze złączem VGA; • 2 port USB 3.0 wewnętrzne; • 2 porty USB 3.0 dostępne z tyłu serwera; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; • 1 porty USB 3.0 na panelu przednim
8	Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 96% (tzw. Klasa Titanium) o mocy minimalnej 800W; • Redundantne wentylatory hotplug;
9	Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii zainstalowane w dowolnym slocie PCI Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera; ○ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z

		możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ○ Dostęp poprzez przeglądarkę Web, SSH; ○ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ○ Zarządzanie alarmami (zdarzenia poprzez SNMP) ○ Możliwość przejęcia konsoli tekstowej ○ Możliwość zarządzania przez 3 administratorów jednocześnie ○ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) ○ Obsługa serwerów proxy (autentykacja) ○ Obsługa VLAN ○ Obsługa protokołów TLS 1.2, SSL v3 ○ Obsługa protokołu LDAP ○ Integracja z HP SIM ○ Synchronizacja czasu poprzez protokół NTP • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • BIOS UEFI w specyfikacji min 2.7;
10	Wspierane OS	• Microsoft Windows Server 2022, 2019, 2016 • VMWare vSphere 6.7, 7.0 • Suse Linux Enterprise Server 15 • Red Hat Enterprise Linux 7.9, 8.2 • Hyper-V Server 2016, 2019
11	System operacyjny	Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej ilości wirtualnych środowisk serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 12 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading lub równoważne 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:

		a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika na przykład typu certyfikatu użytego do logowania, - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

		- Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 11. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: - Dystrybucję certyfikatów poprzez http - Konsolidację CA dla wielu lasów domeny, - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wsparcie dla algorytmów Suite B (RFC 4869), l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych. - Obsługi 4-KB sektorów dysków - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31. Wykonawca dostarczy 200 licencji dostępowych per USER – jeśli oferowany system operacyjny tego wymaga.
12	Gwarancja	• 60 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną reakcją serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.

		• Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; • Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki;
13	Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; • Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; • Zgodność z normami: RoHS, CE;

6.2.1.2 Oprogramowanie do wirtualizacji

Dostarczone oprogramowanie do wirtualizacji musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

Minimalne parametry wymagane:

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.

7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10/11, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, CoreOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
14. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
16. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
17. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
18. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
19. Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
20. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
21. Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
22. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
23. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
24. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne.
25. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
26. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
27. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
28. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 8 takich procesów przenoszenia jednocześnie.

29. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
30. Wsparcie dla oprogramowania na okres minimum 5 lat z prawem update do najnowszej wersji przez ten okres.
31. Oprogramowanie do wirtualizacji musi być w pełni kompatybilne z zaoferowanym oprogramowaniem do wykonywania kopii zapasowych oraz z zaoferowanymi serwerami.

6.2.2 Macierz dyskowa

Dostarczona macierz dyskowa musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
1.	Obudowa	1. Macierz musi być wyposażona w co najmniej jedną parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe macierzy bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami (nie dopuszcza się żadnych połączeń typu IP/LAN poprzez zewnętrzne switche, główki, itp.). 2. Macierz posiada architekturę modułową dla instalacji kontrolerów, portów komunikacyjnych, oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski. 3. Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w standardowej szafie rack 19”. 4. Zajętość kompletnej macierzy z modułami dyskowymi i modułami kontrolerów w oferowanej konfiguracji -maksymalnie 2U w szafie rack. 5. Każdy skonfigurowany moduł kontrolerów i/lub dyskowy musi posiadać nadmiarowy układ zasilania i chłodzenia zapewniający ciągłą pracę całej konfiguracji macierzy bez ograniczeń czasowych i wydajnościowych w przypadku utraty nadmiarowości w danym elemencie (zasilania lub chłodzenia). 6. Obudowa posiada widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii macierzy. 7. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów dyskowych dla dalszej rozbudowy w co najmniej trzech wariantach: a. maksimum 2U przy gęstości upakowania minimum 24 dysków 2,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków SAS, SSD w pojedynczej półce); b. maksimum 2U przy gęstości upakowania minimum 12 dysków 3,5” typu hotplug lub 4U przy gęstości upakowania minimum 24 dyski 3,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków NL-SAS, SSD); c. maksimum 4U przy gęstości upakowania minimum 60 dysków 3,5” typu hotplug; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji półek dyskowych typu a, b, c; (np. jednoczesne użycie półek gęstego upakowania typu c. i półek 2U dla dysków 2,5” typu a. w jednej macierzy).

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		8. Wszystkie zewnętrzne połączenia kablowe pomiędzy modułami muszą zapewniać komunikację nawet w przypadku awarii dowolnej z półek ze wszystkimi pozostałymi półkami/dyskami. 9. Połączenia kablowe SAS 12Gb pomiędzy modułami muszą zapewniać przepustowość minimum 48Gb/s w ramach pojedynczego połączenia.
2.	Pojemność	1. Model oferowanej macierzy obsługuje minimum 260 dysków wykonanych w technologii hot-plug bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami.
3.	Kontrolery	1. Kontrolery macierzy obsługują tryb pracy w układzie active-active lub mesh-active. Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. 2. Każdy z kontrolerów macierzy posiada po minimum 64 GB pamięci podręcznej Cache – zawartość pamięci Cache musi być identyczna dla wszystkich kontrolerów macierzy. 3. Macierz musi posiadać możliwość rozbudowy pamięci podręcznej cache dla operacji odczytu do minimum 800 GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności dysków SSD. 4. Macierz musi być wyposażona w zabezpieczenie stanu pamięci cache np. na wypadek awarii zasilania – zapis stanu pamięci cache na dyski flash lub równoważny nośnik nie wymagający zasilania. Czas przechowywania kopii pamięci flash nie może być ograniczony czasowo. 5. Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia – wymaganie w przypadku konfiguracji z min. 2 kontrolerami. 6. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. 7. Macierz musi umożliwiać wymianę minimum 1 kontrolera bez konieczności wyłączania zasilania całego urządzenia. 8. Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN: a. Sama deduplikacja wybranego LUN; b. Sama kompresja wybranego LUN; c. Kombinacja technologii kompresji i deduplikacji dla wybranego LUN; d. Brak użycia technologii kompresji i deduplikacji dla wybranego LUN; Jeżeli do uruchomienia wymaganych funkcjonalności deduplikacji i kompresji są wymagane jakiekolwiek licencje lub elementy hardware wymaga się ich dostarczenia dla maksymalnej obsługiwanej przez macierz pojemności. Deduplikacja i kompresja realizowane w trybie in-line lub on-line dla danych blokowych udostępnianych za pośrednictwem FC/iSCSI/SAS. Dane muszą być od razu zapisane na dyski w postaci zdeduplikowanej/skompresowanej. Deduplikacja i kompresja musi być wspierana przez macierz na dowolnym typie obsługiwanych dysków – co najmniej NL-SAS, SAS, SSD. 9. Macierz posiada minimum 4 dedykowane interfejsy RJ-45 Ethernet 1Gb/s dedykowane dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. 10. Każdy z kontrolerów macierzy wyposażony co najmniej w procesor wykonany w technologii wielordzeniowej z minimum 8 rdzeniami.

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		11. Każdy kontroler macierzy pozwala na konfigurację interfejsów niezbędnych dla współpracy w sieci LAN, FC SAN oraz NAS.
4.	Interfejsy	1.Oferowana macierz musi mieć minimum 4 porty FC 16Gbit/s (z wkładkami światłowodowymi) wyprowadzone na każdy kontroler RAID. Porty przeznaczone do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN. 2. Dla komunikacji blokowej I/O z serwerami (front-end), oferowany model macierzy wyposażony w oferowaną ilość kontrolerów musi obsługiwać wymiennie co najmniej następujące protokoły i porty: a. Możliwość instalacji minimum 16 portów FC 16Gbit/s b. Możliwość instalacji minimum 8 portów FC 32Gbit/s c. Możliwość instalacji minimum 8 portów iSCSI 10 Gbit/s SFP+ lub RJ-45 d. Możliwość instalacji minimum 8 portów iSCSI 1 Gbit/s RJ-45 Musi istnieć możliwość jednoczesnego wykorzystania różnych typów interfejsów. 3. Oferowany model macierzy umożliwia wymianę portów do transmisji danych z serwerami (front-end) na porty obsługujące protokoły: iSCSI 1 Gb/s, FC 16 Gb/s, FC 32Gb/s,. Wymiana portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, w przypadku konieczności licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencją na instalację i obsługę każdego z wymienionych protokołów transmisji danych. 4. Dla komunikacji plikowej NAS z serwerami oferowany model macierzy wyposażony w oferowaną ilość kontrolerów musi obsługiwać co najmniej następujące protokoły i porty: CIFS, NFS oraz interfejsy Ethernet 1Gbit/s i 10Gbit/s. Oferowany model macierzy musi umożliwiać jednoczesne użytkowanie portów do komunikacji blokowej i plikowej. W obecnym postępowaniu wymagana jest macierz z aktywnym dostępem blokowym oraz możliwością rozbudowy o dostęp realizowany na poziomie plikowym.
5.	Poziomy RAID	1. Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1 , 10, 5 , 50, 6 . 2. Macierz musi być wyposażona w nadmiarowe mechanizmy badania integralności składowanych danych.
6.	Wspierane dyski	1. Oferowana macierz wspiera co najmniej następujące typy dysków hot-plug: - dyski elektroniczne SSD SAS o pojemności minimum 30TB - dyski elektroniczne SSD SAS SED lub FDE o pojemności minimum 4TB - dyski mechaniczne HDD SAS o pojemności minimum 900GB i prędkości 15 tysięcy obrotów na minutę - dyski mechaniczne HDD SAS o pojemności minimum 2,4TB, 10k RPM - dyski mechaniczne HDD NL-SAS o pojemności minimum 18TB 7.2k RPM 2. Macierz obsługuje dyski hot-plug SSD i HDD wyposażone w porty SAS 12Gb/s. 3. Wszystkie dyski wspierane przez oferowany model macierzy wykonane są w technologii hot-plug i posiadają podwójne porty SAS obsługujące tryb pracy full-duplex. 4. Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5” 5. Wymagane jest dostarczenie macierzy zawierającej: - 17 dysków 2.5” SSD SAS 12Gb/s o pojemności min. 1,92 TB każdy 6. Macierz umożliwia skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach:

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		- hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID - hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID lub zapewnia możliwość skonfigurowania równoważnej przestrzeni zapasowej. 7. W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk. 8. Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych na zainstalowanych dyskach dowolnego typu – funkcjonalność realizowana bezpośrednio przez kontrolery macierzy dla danych blokowych – minimum AES 256. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy.
7.	Opcje software'owe	1. Macierz wyposażona jest w system kopii migawkowych umożliwiających wykonanie minimum 4000 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy. 2. Macierz musi umożliwiać zdefiniowanie minimum 4096 woluminów tzw. LUN. 3.Macierz umożliwia aktualizację oprogramowania wewnętrznego, kontrolerów i dysków bez konieczności wyłączania macierzy i bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych serwerów. 4. Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, alokowanie woluminu na inną grupę dyskową 5. Model macierzy musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server /2016/2019/2022, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, VMWare , Citrix XEN Server. 6. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI. 7. Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności minimum 16TB. 8. Macierz umożliwia obsługę mechanizów QoS (ang. Quality of Services) dla skonfigurowanych hostów, LUN-ów, portów do hostów. 9. Macierz umożliwia rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD. 10. Macierz musi posiadać wsparcie dla mechanizmów Offloaded Data Transfer i Space Reclamation. 11. Macierz obsługuje mechanizmy Thin Provisioning czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. Jeżeli taka funkcjonalność

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		wymaga dodatkowych licencji to należy je dostarczyć wraz z macierzą dla maksymalnej pojemności dyskowej oferowanej macierzy. 12. Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy trzech różnych technologiach dyskowych równocześnie: SSD, SAS, NLSAS. Macierz musi pozwalać na definiowanie minimum 120 różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 13. Model macierzy musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych jest zapewniona z poziomu oprogramowania wewnętrznego macierzy. Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 14. Model oferowanej macierzy musi wspierać rozwiązania klasy „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać poziomy RAID: 1,10,5,6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i zapasową. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover).

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Funkcjonalność „wysokiej dostępności" musi wspierać dwukierunkowe przełączanie macierzy podstawowej na zapasową tj. przypadek, gdy każda z tych macierzy obsługuje własne środowisko produkcyjne, a rolę jej macierzy zapasowej pełni druga z macierzy. Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 15. Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror). Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność.
8.	Konfiguracja, zarządzanie	1.Oprogramowanie do zarządzania zintegrowane jest z systemem operacyjnym macierzy zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI) jak i do obsługi transmisji protokołami CIFS oraz NFS (nie dopuszcza się tzw. główek czy dodatkowych serwerów podłączonych do macierzy w celu realizacji obsługi dostępu protokołami CIFS i NFS do danych znajdujących się na macierzy). 2. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą odbywa się w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. Zdalne zarządzanie macierzą odbywa się bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora. 3. Wbudowane oprogramowanie macierzy obsługuje połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.
9.	Gwarancja i serwis	1. Macierz dyskowa musi zostać objęta minimum 60 miesięcznym okresem gwarancji producenta w trybie onsite z gwarantowanym czasem reakcji, najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email (w ofercie należy podać dedykowany adres email serwisu producenta macierzy do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. W formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		zweryfikować dedykowany numer telefonu do obsługi zgłoszeń serwisowych. Wymagane jest oświadczenie Producenta oferowanej macierzy, iż wymagany poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta macierzy na potrzeby oferty w niniejszym postępowaniu. 2. Macierz musi być zaoferowana z serwisem producenta macierzy, który w przypadku wymiany dysków twardych HDD/SSD, umożliwia pozostawienie wszystkich uszkodzonych nośników u Zamawiającego. Serwis taki musi dotyczyć wszystkich oferowanych półek dyskowych i przewidywać ich uzupełnienie do maksymalnej pojemności poprzez dodanie dowolnych typów obsługiwanych dysków przez macierz bez konieczności ponoszenia żadnych dodatkowych kosztów przez Zamawiającego z tytułu gwarancji „pozostawienie dysku" dla tych dysków zainstalowanych w macierzy jak i dodatkowych dysków możliwych do zainstalowania w obrębie oferowanych półek dyskowych. Wymagane jest oświadczenie Producenta oferowanej macierzy, iż wymagany poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta macierzy na potrzeby oferty w niniejszym postępowaniu; 3. Serwis gwarancyjny obejmuje dostęp do poprawek i nowych wersji firmware, które są elementem zamówienia przez cały okres obowiązywania gwarancji. 4. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje; 5. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną linię telefoniczną wsparcia technicznego w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej (telefon stacjonarny lub 0-800/0-801 , nie dopuszcza się numerów o podwyższonej płatności - specjalnych, komórkowych, itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. Po podaniu numeru seryjnego macierzy można zweryfikować telefonicznie co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia, jak również zgłosić problem/zapytanie techniczne związane z urządzeniem – w formularzu ofertowym należy podać pełen numer telefonu linii wsparcia technicznego producenta 6. Macierz musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu o usterce przez samo urządzenie (poprzez dedykowany system wbudowany w macierz - bez pośrednictwa administratora, nie dopuszcza się użycia ogólnodostępnych mechanizmów - poczty email w tym m.in. protokołu SNMP i SMTP, nie dopuszcza się SMS – Zamawiający nie dopuszcza możliwości komunikacji z/do macierzy poprzez pocztę email/SNMP/SMTP itp. z powodów bezpieczeństwa). Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy. 7. Oferowana macierz musi być fabrycznie nowa, Macierz pochodzi z legalnego kanału sprzedaży producenta na terenie Polski i reprezentuje model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych. 8. Urządzenie wykonane jest zgodnie z europejskimi dyrektywami RoHS i WEEE. 9. Oferowana macierz musi pochodzić z autoryzowanego kanału producenta na terenie Polski oraz być fabrycznie nowa (nie dopuszcza się urządzeń odnawianych, używanych, itp.) 10. Przed podpisaniem protokołu ilościowo-jakościowego Wykonawca dostarczy pisemne potwierdzenie wykupienia i uruchomienia gwarancji producenta macierzy obowiązującej na terenie Polski, zgodnej co najmniej z wymaganiami specyfikacji i ze złożoną przez niego ofertą.

6.2.3 System kopii zapasowych

Dostarczony system kopii zapasowych musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

Wykonawca dostarczy system składający się z serwera, oprogramowania systemowego oraz oprogramowania do wykonywania kopii zapasowych.

Lp.	Parametr lub warunek	Minimalne wymagania
1	Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Możliwość zainstalowania 12 dysków twardych hot plug 3,5”; • Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; • Zainstalowane 2 szt. dyski SSD M.2 SATA lub M.2 NVMe SSD 240GB podpięte do sprzętowego kontrolera RAID-1; • Możliwość zainstalowania dedykowanego napędu optycznego.
2	Płyta główna	• Dwuprocesorowa; • Wyprodukowana i zaprojektowana przez producenta serwera • Możliwość zainstalowania modułu TPM 2.0; • Min 7 złącz PCI Express generacji 4:w tym: o 4 fizyczne złącza o prędkości x16; o 3 fizyczne złącza o prędkości x8; o Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości; o Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; Lub o 6 fizycznych złącz o prędkości x8 o 2 fizyczne złącza o prędkości x16 • 32 gniazda pamięci RAM; • Obsługa minimum 4TB pamięci RAM DDR4; • Obsługa minimum 8TB pamięci RAM DDR4 + pamięć nieulotna • Wsparcie dla technologii:

		○ Memory Scrubbing lub równoważne ○ SDDC lub równoważne ○ ECC lub równoważne ○ Memory Mirroring lub równoważne ○ ADDDC lub równoważne; • Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) • Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;
3	Procesory	• Zainstalowany minimum jeden procesor maksymalnie 8-sto rdzeniowy • Taktowanie 2,8 GHz • architektura x86_64 osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 81pkt (wynik osiągnięty dla zainstalowanego jednego procesora). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html
4	Pamięć RAM	• 32 GB pamięci RAM • DDR4 Registered • 3200Mhz • Możliwość rozbudowy do 256GB pamięci RAM przez dołożenie kolejnych modułów bez konieczności wymiany zainstalowanych
5	Kontrolery LAN	• Karta LAN wyposażona minimum w interfejsy: 2x 10Gbit SFP+,
	Kontrolery dyskowe	• Zainstalowany kontroler SAS 3.0 RAID 0,1,5,50
		• Zainstalowane 6 dysków SATA 7.2K RPM o pojemności 6TB GB każdy, dyski Hotplug;
7	Porty	• Zintegrowana karta graficzna ze złączem VGA; • 2 port USB 3.0 wewnętrzne; • 2 porty USB 3.0 dostępne z tyłu serwera; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; • 1 porty USB 3.0 na panelu przednim
8	Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimalnej 800W; • Redundantne wentylatory hotplug;
9	Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera; ○ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ○ Dostęp poprzez przeglądarkę Web, SSH; ○ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ○ Zarządzanie alarmami (zdarzenia poprzez SNMP) ○ Możliwość przejęcia konsoli tekstowej ○ Możliwość zarządzania przez 6 administratorów jednocześnie

		○ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) ○ Obsługa serwerów proxy (autentykacja) ○ Obsługa VLAN ○ Obsługa protokołów TLS 1.2, SSL v3 ○ Obsługa protokołu LDAP ○ Integracja z HP SIM ○ Synchronizacja czasu poprzez protokół NTP • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • BIOS UEFI w specyfikacji 2.7;
10	Wspierane OS	• Microsoft Windows Server 2022, 2019, 2016 • VMWare vSphere 6.7, 7.0 • Suse Linux Enterprise Server 15 • Red Hat Enterprise Linux 7.9, 8.2 • Hyper-V Server 2016, 2019
	System operacyjny	Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 12 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading lub równoważny. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

		11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika na przykład typu certyfikatu użytego do logowania, - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 11 c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: - Dystrybucję certyfikatów poprzez http - Konsolidację CA dla wielu lasów domeny,

		- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wsparcie dla algorytmów Suite B (RFC 4869), l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych. - Obsługi 4-KB sektorów dysków - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
	System Backupu	1. Oprogramowanie do wykonywania kopii zapasowych musi być produktem przeznaczonym do obsługi środowisk DataCenter. 2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji, 6.5, 6.7 i 7.0 oraz Microsoft Hyper-V 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej 3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. 4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. 5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. 6. Dostarczona licencja ma umożliwić backup 10 maszyn wirtualnych. Licencje dożywotnie z minimum 5 letnim wsparciem producenta w trybie 24/7 (w tym prawo do upgrade oprogramowania do najnowszej wersji)

		7. Oprogramowanie do wykonywania kopii zapasowych musi być w pełni kompatybilne z zaoferowanym oprogramowaniem do wirtualizacji. 9. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej 10. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków 11. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) 12. 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 13. 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. 14. 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. 15. 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. 16. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania 17. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. 18. 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) 19. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu 20. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API 21. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji 22. 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 23. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania 24. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) 25. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. 26. Wymagania RPO 27. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej 28. Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

		29. 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 30. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru 31. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora 32. Oprogramowanie 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 i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage. 33. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. 34. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn 35. Oprogramowanie musi posiadać wsparcie dla NDMP 36. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 37. 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. 38. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. 39. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. 40. Repozytoria oparte o XFS muszą pozwalać na niezmienność danych przez określoną ilość czasu (tzw Immutability) 41. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. 42. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. 43. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwosc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 44. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik 45. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) 46. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) 47. Wymagania RTO 48. Oprogramowanie musi umożliwiać jednoczesne 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 dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. 49. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 50. 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 51. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre 52. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków 53. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2. 54. 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 55. 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. 56. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: 57.-Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs 58.-BSD: UFS, UFS2 59.-Solaris: ZFS, UFS 60.-Mac: HFS, HFS+ 61.-Windows: NTFS, FAT, FAT32, ReFS 62.-Novell OES: NSS 63. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. 64. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 65. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. 66. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. 67. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), 68. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska 69. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych 70. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska 71. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych 72. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.

		73. 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. 74. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego 75. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN 76. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA 77. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN 78. Ograniczenie ryzyka 79. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. 80. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. 81. 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 82. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere 83. 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. 84. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. 85. Monitoring 86. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich 87. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji, 6.5, 6.7 i 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie 88. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. 89. System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware 90. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter 91. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn 92. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel 93. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

		94. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora 95. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów 96. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) 97. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna 98. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego 99. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta 100. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. 101. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. 102. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware 103. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x 104. Raportowanie 105. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi, 6.5, 6.7 i 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-, 2016 oraz 2019 106. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. 107. System musi być certyfikowany przez VMware i posiadać status „VMware Ready” 108. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V 109. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF 110. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc 111. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach 112. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów 113. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych 114. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych 115. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury 116. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta

		117. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. 118. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. 119. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware 120. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) 121. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie
11	Gwarancja	• 60 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną reakcją serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. • Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; • Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki;
12	Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; • Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; • Zgodność z normami: RoHS, WEEE, CE;

6.2.4 Przełącznik typ 1

Dostarczone przełączniki typ 1 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Przełącznik posiadający min. 48 portów 1/10/25 Gbps SFP lub SFP28
1.2. Przełącznik posiadający min. 6 portów 100 Gbps QSFP28
1.3. Wysokość urządzenia 1U
1.4. Nieblokująca architektura o wydajności przełączania min. 4 Tb/s
1.5. Tablica MAC adresów min. 92 000
1.6. Pamięć operacyjna: minimum 16 GB pamięci DRAM
1.7. Pamięć SSD minimum 64 GB
1.8. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4059
1.9. Obsługa 802.1v VLAN Klasyfikacja per Protokół oraz port
1.10. Obsługa Q-in-Q IEEE 802.1ad
1.11. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
1.12. Przełącznik musi posiadać dwa redundantne zasilacze o mocy minimum 650 W. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika.
1.13. Przepływ powietrza w przełączniku: przód-tył
1.14. Moduł wentylatorów zapewniający ich redundancję
1.15. Wbudowany DHCP Serwer i klient
1.16. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
1.17. Wbudowany port konsolowy RJ-45 do zarządzania przełącznikiem
1.18. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
1.19. Port USB do podpięcia zewnętrznego storage

2. Obsługa Routingu IPv4

1.1. Sprzętowa obsługa routingu IPv4 - forwarding
1.2. Pojemność tabeli routingu min. 16 tys. wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego IPv4
   a. RIP v1/v2
   b. OSPFv2
   c. BGP4, BGP+
   d. IS-IS
1.5. Minimum 256 instancji VRF

3. Obsługa Routingu IPv6

1.1. Sprzętowa obsługa routingu IPv6 - forwarding
1.2. Pojemność tabeli routingu min. 7,5 tys. wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego dla IPv6
   a. OSPF v3
   b. BGPv6
   c. IS-IS
1.5. Ping dla IPv6
1.6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
1.7. Obsługa MLDv2 (Multicast Listener Discovery version 2)
1.8. Minimum 256 instancji VRF

4. Obsługa Multicastów

1.1. Statyczne przyłączanie do grupy multicast
1.2. Obsługa PIM-SM
1.3. Obsługa PIM-SSM
1.4. Obsługa IGMP v1
1.5. Obsługa IGMP v2
1.6. Obsługa IGMP v3
1.7. Obsługa IGMP oraz MLD snooping

1.8. Obsługa IETF RFC1112 Host Extensions for IP Multicasting

5. Bezpieczeństwo

1.1. Obsługa RADIUS Authentication (RFC 2138)
1.2. Obsługa RADIUS Accounting (RFC 2139)
1.3. Obsługa IETF RFC5176 Dynamic Authorization Extensions to RADIUS
1.4. Obsługa 802.1AE Media Access Control Security
1.5. Obsługa SNMPv1/v2/v3
1.6. Obsługa 802.1X Port-based Network Access Control
1.7. Klient SSH2
1.8. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na
1.9. Obsługa DHCP Option 82
1.10. Ograniczanie przepustowości per port – w zakresie 1Mbps – 100 Gbps
1.11. Obsługa IETF RFC 2474

6. Bezpieczeństwo sieciowe

1.1. Obsługa redundancji routingu VRRP (dla IPv4 i IPv6)
1.2. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
1.3. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
1.4. Obsługa Link Aggregation LACP
1.5. Obsługa 802.1AX Link Aggregation

7. Zarządzanie

1.1. Obsługa IETF RFC5905 NTPv4: Protocol and Algorithms Specification
1.2. Zarządzanie przez SNMP v1/v2/v3
1.3. Zarządzanie przez przeglądarkę WWW – protokół http i https
1.4. Możliwość zarzadzania przełącznikiem z poziomu CLI
1.5. Zarządzanie z dedykowanej aplikacji zarządzającej
1.6. Telnet Serwer/Klient
1.7. SSH2 Serwer/Klient
1.8. Ping dla IPv4 / IPv6
1.9. Traceroute dla IPv4 / IPv6
1.10. Obsługa SYSLOG
1.11. Sprzętowa obsługa sFlow lub netflow
1.12. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events

8. Inne

1.1. Obsługa VXLAN: IETF RFC7358
1.2. Obsługa VXLAN Gateway
1.3. Obsługa 802.1Qbp Equal-Cost Multi-Path (Shortest Path Bridging)
1.4. Obsługa 802.1ag Connectivity Fault Management
1.5. Obsługa 802.1ah Provider Backbone Bridges

6.2.5 Przełącznik typ 2

Dostarczone przełączniki typ 2 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.6. Przełącznik wyposażony w minimum 48 portów SFP lub SFP28 pracujących z prędkościami 1G/10G/25G oraz minimum 6 portów QSFP28 pracujących z prędkościami 40G//100G.
1.1. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone.
1.2. Wysokość urządzenia 1U montowana w standardowym 19” Rack.

1.3. Przełącznik musi posiadać możliwość instalacji dwóch zasilaczy, które umożliwiają uzyskanie redundancji zasilania. Niedopuszczalna jest instalacja zasilaczy zewnętrznych. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika bez wpływu na jego pracę.
1.4. Wraz z przełącznikiem należy dostarczyć 2 zasilacze 230V
1.5. Przełącznik musi posiadać wymienne w czasie pracy wentylatory
1.6. Przełącznik musi zapewniać pobór powietrza z przodu i wyrzut powietrza z tyłu przełącznika – chłodzenie przód-tył.
1.7. Architektura o zagregowanej przepustowości min. 4 Tb/s
1.8. Szybkość przełączania min. 1 milion pakietów na sekundę
1.9. Temperatura pracy przełącznika w zakresie min. 0o do 40o C
1.10. Tablica MAC adresów min. 92 tys.
1.11. Pamięć operacyjna: min. 16 GB pamięci DRAM
1.12. Pamięć SSD: min. 64 GB pamięci
1.13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000
1.14. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
1.15. Wsparcie dla ramek Jumbo Frames
1.16. Obsługa Q-in-Q IEEE 802.1ad
1.17. Obsługa Quality of Service
    a. Rozpoznawanie i przełączanie ramek zgodnie z priorytetem ustawionym w ramach IEEE 802.1p
    b. Rozpoznawanie i przełączanie pakietów zgodnie z priorytetem ustawionym w ramach DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
    d. Obsługa kolejek Strict Priority
    e. Obsługa kolejek Weighted Round Robin
    f. Obsługa WRED (Weighted Random Early Detection)
1.18. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
1.19. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
1.20. Obsługa CDPv2 z obsługą Voice VLAN
1.21. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
1.22. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
1.23. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci SSD
1.24. Możliwość monitorowania zajętości CPU oraz pamięci z CLI oraz SNMP
1.25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
1.26. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
1.27. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
1.28. Dedykowany port konsoli szeregowej RJ45
1.29. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika
1.30. Obsługa Data Center Bridging
    a. DCBx Data Center Bridging Exchange Protocol
    b. PFC Priority Flow Control
    c. ETS Enhanced Transmission Selection
1.31. Obsługa VXLAN Tunneling End Point (VTEP)

2. Obsługa Routingu IPv4

1.1. Sprzętowa obsługa routingu IPv4 - forwarding
1.2. Pojemność sprzętowej tabeli routingu min. 128 tys. wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego IPv4
    a. RIP v1/v2
    b. OSPFv2 - możliwość rozszerzenia przez licencje

   c. BGPv4 - możliwość rozszerzenia przez licencje
   d. IS-IS - możliwość rozszerzenia przez licencje
1.5. Policy Based Routing dla IPv4
1.6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

3. Obsługa Routingu IPv6

1.1. Sprzętowa obsługa routingu IPv6 - forwarding
1.2. Pojemność tabeli routingu min. 32 tys. wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego dla IPv6
   a. OSPF v3 – możliwość rozszerzenia przez licencje
   b. BGPv4 – możliwość rozszerzenia przez licencje
   c. IS-IS – możliwość rozszerzenia przez licencje
1.5. Obsługa tuneli 6to4 (RFC 3056)
1.6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
1.7. Obsługua MLDv2 (Multicast Listener Discovery version 2)
1.8. Policy Based Routing dla IPv6
1.9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

4. Obsługa Multicastów

1.1. Statyczne przyłączanie do grupy multicast
1.2. Filtrowanie IGMP
1.3. Obsługa PIM-SM – możliwość rozszerzenia przez licencje
1.4. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
1.5. Obsługa Multicast VLAN Registration - MVR
1.6. Obsługa IGMP v1 - RFC 1112
1.7. Obsługa IGMP v2 - RFC 2236
1.8. Obsługa IGMP v3 - RFC 3376
1.9. Obsługa IGMP v1/v2/v3 snooping
1.10. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

5. Bezpieczeństwo

1.1. Obsługa logowania do sieci Network Login
   a. IEEE 802.1x based Network Login
   b. MAC based Network Login
   c. Web-based Network Login
1.2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
1.3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
1.4. Przydział sieci VLAN dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
1.5. Przydział ACL dla uwierzytelnionego użytkownika lub urządzenia podczas logowania do sieci IEEE 802.1x, MAC authentication
1.6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
1.7. Obsługa Guest VLAN dla IEEE 802.1x
1.8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
1.9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
1.10. Obsługa TACACS+ (RFC 1492)
1.11. Obsługa RADIUS Authentication (RFC 2138)
1.12. Obsługa RADIUS Accounting (RFC 2139)
1.13. RADIUS per-command Authentication
1.14. Obsługa RADIUS over TLS (RadSec) – RFC 6614

1.15. Bezpieczeństwo MAC adresów
   a. ograniczenie liczby MAC adresów na porcie
   b. zatrzaśnięcie MAC adresu na porcie
   c. możliwość wpisania statycznych MAC adresów na port/vlan
1.16. Możliwość wyłączenia MAC learning
1.17. Zabezpieczenie przełącznika przed atakami DoS
   a. Networks Ingress Filtering RFC 2267
   b. SYN Attack Protection
   c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
1.18. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
   a. Adres MAC źródłowy i docelowy plus maska
   b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
   c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
   d. Numery portów źródłowych i docelowych TCP, UDP
   e. Zakresy portów źródłowych i docelowych TCP, UDP
   f. Identyfikator sieci VLAN - VLAN ID
   g. Quality of Service IEEE 802.1p oraz DiffServ
   h. Flagi TCP
   i. Obsługa fragmentów
1.19. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
1.20. Możliwość konfiguracji min. 8 000 reguł na wejściu i 1 000 reguł na wyjściu
1.21. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
1.22. Obsługa bezpiecznego transferu plików SCP/SFTP
1.23. Obsługa DHCP Option 82
1.24. Obsługa IP Security – Trusted DHCP Server
1.25. Obsługa IP Security – DHCP Snooping and Guard
1.26. Obsługa IP Security - Gratuitous ARP Protection
1.27. Obsługa IP Security – DHCP Secured ARP/ARP Validation
1.28. Obsługa IP Security – IP Source guard
1.29. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
1.30. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

6. Bezpieczeństwo sieciowe

1.1. Możliwość konfiguracji portu głównego i zapasowego
1.2. Obsługa redundancji routingu VRRP
1.3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
1.4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
1.5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
1.6. Obsługa PVST+
1.7. Obsługa ERPS / G.8032
1.8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
1.9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
1.10. Obsługa LACP w ramach MLAG

7. Zarządzanie

1.1. Obsługa synchronizacji czasu SNTP lub NTP
1.2. Zarządzanie przez SNMP v1/v2/v3
1.3. Zarządzanie przez przeglądarkę WWW – protokół http i https

1.4. Telnet Serwer/Klient dla IPv4 / IPv6
1.5. SSH2 Serwer/Klient dla IPv4 / IPv6
1.6. Ping dla IPv4 / IPv6
1.7. Traceroute dla IPv4 / IPv6
1.8. Obsługa SYSLOG z możliwością definiowania wielu serwerów
1.9. Wsparcie SYSLOG over TLS
1.10. Sprzętowa obsługa sFlow
1.11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
1.12. Obsługa RMON2 (RFC 2021)
1.13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

8. Inne

1.1. Możliwość rozszerzenia funkcjonalności o MPLS poprzez wymianę oprogramowania lub licencję. Wymagane wsparcie dla następujących funkcjonalności: MPLS/VPLS, MPLS/VPWS, LDP, RSVP-TE, Fast Reroute
1.2. Możliwość uruchomienia wirtualizacji na przełączniku z bezpośrednim dostępem do chipsetu przełącznika – przepustowość min. 10 Gb/s
1.3. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
1.4. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
1.5. Obsługa skryptów CLI
1.6. Obsługa funkcji TCL/Tk w skryptach CLI
1.7. Obsługa skryptów Python
1.8. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
1.9. Możliwość uruchamiania skryptów
   a. Ręcznie
   b. O określonym czasie lub co wskazany okres czasu
   c. Na podstawie wpisów w logu systemowym

6.2.6 Przełącznik typ 3

Dostarczone przełączniki typ 3 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Przełącznik wyposażony w 48 portów 10/100/1000BASE-T
1.2. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
1.3. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
1.4. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
1.5. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana
1.6. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
1.7. Wysokość urządzenia 1U montowana w standardowym 19” Rack
1.8. Przełącznik musi posiadać zasilacz 230V. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
1.9. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
1.10. Możliwość łączenia do 8 przełączników w stos
1.11. Nieblokująca architektura o wydajności przełączania min. 256 Gb/s
1.12. Szybkość przełączania min. 190 Milionów pakietów na sekundę
1.13. Temperatura pracy przełącznika w zakresie min. 0o do 40o C
1.14. Tablica MAC adresów min. 32 tys.
1.15. Pamięć operacyjna: min. 1 GB pamięci DRAM
1.16. Pamięć flash: min. 1 GB pamięci Flash
1.17. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000

1.18. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
1.19. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów)
1.20. Obsługa Q-in-Q IEEE 802.1ad
1.21. Obsługa Quality of Service
    a. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
    b. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
    d. Obsługa kolejek Strict Priority
    e. Obsługa kolejek Weighted Round Robin
    f. Obsługa WRED (Weighted Random Early Detection)
1.22. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
1.23. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
1.24. Obsługa CDPv2 z obsługą Voice VLAN
1.25. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
1.26. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
1.27. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
1.28. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
1.29. Możliwość monitorowania zajętości CPU oraz pamięci
1.30. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
1.31. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
1.32. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
1.33. Dedykowany port konsoli szeregowej RJ45
1.34. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

2. Obsługa Routingu IPv4

1.1. Sprzętowa obsługa routingu IPv4 - forwarding
1.2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego IPv4
    a. RIP v1/v2
    b. OSPFv2 - możliwość rozszerzenia przez licencje
    c. BGPv4 - możliwość rozszerzenia przez licencje
    d. IS-IS - możliwość rozszerzenia przez licencje
1.5. Policy Based Routing dla IPv4
1.6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

3. Obsługa Routingu IPv6

1.1. Sprzętowa obsługa routingu IPv6 - forwarding
1.2. Pojemność tabeli routingu min. 2 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3 – możliwość rozszerzenia przez licencje
    c. BGPv4 – możliwość rozszerzenia przez licencje
    d. IS-IS – możliwość rozszerzenia przez licencje
1.5. Obsługa 6to4 (RFC 3056)
1.6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
1.7. Obsługua MLDv2 (Multicast Listener Discovery version 2)

1.8. Policy Based Routing dla IPv6
1.9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

4. Obsługa Multicastów

1.1. Statyczne przyłączanie do grupy multicast
1.2. Filtrowanie IGMP
1.3. Obsługa PIM-SM
1.4. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
1.5. Obsługa Multicast VLAN Registration - MVR
1.6. Obsługa IGMP v1 - RFC 1112
1.7. Obsługa IGMP v2 - RFC 2236
1.8. Obsługa IGMP v3 - RFC 3376
1.9. Obsługa IGMP v1/v2/v3 snooping
1.10. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

5. Bezpieczeństwo

1.1. Obsługa logowania do sieci Network Login
   a. IEEE 802.1x based Network Login
   b. MAC based Network Login
   c. Web-based Network Login
1.2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
1.3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
1.4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
1.5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink.
1.6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
1.7. Obsługa Guest VLAN dla IEEE 802.1x
1.8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
1.9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
1.10. Obsługa TACACS+ (RFC 1492)
1.11. Obsługa RADIUS Authentication (RFC 2138)
1.12. Obsługa RADIUS Accounting (RFC 2139)
1.13. RADIUS per-command Authentication
1.14. Bezpieczeństwo MAC adresów
   a. ograniczenie liczby MAC adresów na porcie
   b. zatrzaśnięcie MAC adresu na porcie
   c. możliwość wpisania statycznych MAC adresów na port/vlan
1.15. Możliwość wyłączenia MAC learning
1.16. Zabezpieczenie przełącznika przed atakami DoS
   a. Networks Ingress Filtering RFC 2267
   b. SYN Attack Protection
   c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
1.17. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
   a. Adres MAC źródłowy i docelowy plus maska
   b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
   c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
   d. Numery portów źródłowych i docelowych TCP, UDP
   e. Zakresy portów źródłowych i docelowych TCP, UDP
   f. Identyfikator sieci VLAN - VLAN ID
   g. Quality of Service IEEE 802.1p oraz DiffServ

h. Flagi TCP
i. Obsługa fragmentów

1.18. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
1.19. Możliwość konfiguracji min. 5200 reguł na wejściu i 1 000 reguł na wyjściu
1.20. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
1.21. Obsługa bezpiecznego transferu plików SCP/SFTP
1.22. Obsługa DHCP Option 82
1.23. Obsługa IP Security – Trusted DHCP Server
1.24. Obsługa IP Security – DHCP Snooping and Guard
1.25. Obsługa IP Security - Gratuitous ARP Protection
1.26. Obsługa IP Security – DHCP Secured ARP/ARP Validation
1.27. Obsługa IP Security – IP Source guard
1.28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
1.29. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

6. Bezpieczeństwo sieciowe

1.1. Możliwość konfiguracji portu głównego i zapasowego
1.2. Obsługa redundancji routingu VRRP
1.3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
1.4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
1.5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
1.6. Obsługa PVST+
1.7. Obsługa ERPS / G.8032
1.8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
1.9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
1.10. Obsługa LACP w ramach MLAG

7. Zarządzanie

1.1. Obsługa synchronizacji czasu SNTP lub NTP
1.2. Zarządzanie przez SNMP v1/v2/v3
1.3. Zarządzanie przez przeglądarkę WWW – protokół http i https
1.4. Możliwość zarządzania przez protokół XML
1.5. Telnet Serwer/Klient dla IPv4 / IPv6
1.6. SSH2 Serwer/Klient dla IPv4 / IPv6
1.7. Ping dla IPv4 / IPv6
1.8. Traceroute dla IPv4 / IPv6
1.9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
1.10. Sprzętowa obsługa sFlow
1.11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
1.12. Obsługa RMON2 (RFC 2021)
1.13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

8. Inne

1.1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
1.2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
1.3. Obsługa skryptów CLI
1.4. Obsługa funkcji TCL/Tk w skryptach CLI

1.5. Obsługa skryptów Python
1.6. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
1.7. Możliwość uruchamiania skryptów
   a. Ręcznie
   b. O określonym czasie lub co wskazany okres czasu

Na podstawie wpisów w logu systemowym

6.2.7 Przełącznik typ 4

Dostarczone przełączniki typ 4 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Przełącznik wyposażony w 24 porty 10/100/1000BASE-T
1.2. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
1.3. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
1.4. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
1.5. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana
1.6. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
1.7. Wysokość urządzenia 1U montowana w standardowym 19” Rack
1.8. Przełącznik musi posiadać zasilacz 230V. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
1.9. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
1.10. Możliwość łączenia do 8 przełączników w stos
1.11. Nieblokująca architektura o wydajności przełączania min. 208 Gb/s
1.12. Szybkość przełączania min. 154 Milionów pakietów na sekundę
1.13. Temperatura pracy przełącznika w zakresie min. 0o do 40o C
1.14. Tablica MAC adresów min. 32 tys.
1.15. Pamięć operacyjna: min. 1 GB pamięci DRAM
1.16. Pamięć flash: min. 1 GB pamięci Flash
1.17. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000
1.18. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
1.19. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów)
1.20. Obsługa Q-in-Q IEEE 802.1ad
1.21. Obsługa Quality of Service
   a. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
   b. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
   c. 8 kolejek priorytetów na każdym porcie wyjściowym
   d. Obsługa kolejek Strict Priority
   e. Obsługa kolejek Weighted Round Robin
   f. Obsługa WRED (Weighted Random Early Detection)
1.22. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
1.23. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
1.24. Obsługa CDPv2 z obsługą Voice VLAN
1.25. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
1.26. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
1.27. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
1.28. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
1.29. Możliwość monitorowania zajętości CPU oraz pamięci
1.30. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)

1.31. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
1.32. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
1.33. Dedykowany port konsoli szeregowej RJ45
1.34. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

2. Obsługa Routingu IPv4

1.1. Sprzętowa obsługa routingu IPv4 - forwarding
1.2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego IPv4
   a. RIP v1/v2
   b. OSPFv2 - możliwość rozszerzenia przez licencje
   c. BGPv4 - możliwość rozszerzenia przez licencje
   d. IS-IS - możliwość rozszerzenia przez licencje
1.5. Policy Based Routing dla IPv4
1.6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

3. Obsługa Routingu IPv6

1.1. Sprzętowa obsługa routingu IPv6 - forwarding
1.2. Pojemność tabeli routingu min. 6 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego dla IPv6
   a. RIPng
   b. OSPF v3 – możliwość rozszerzenia przez licencje
   c. BGPv4 – możliwość rozszerzenia przez licencje
   d. IS-IS – możliwość rozszerzenia przez licencje
1.5. Obsługa 6to4 (RFC 3056)
1.6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
1.7. Obsługua MLDv2 (Multicast Listener Discovery version 2)
1.8. Policy Based Routing dla IPv6
1.9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

4. Obsługa Multicastów

1.1. Statyczne przyłączanie do grupy multicast
1.2. Filtrowanie IGMP
1.3. Obsługa PIM-SM
1.4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
1.5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
1.6. Obsługa Multicast VLAN Registration - MVR
1.7. Obsługa IGMP v1 - RFC 1112
1.8. Obsługa IGMP v2 - RFC 2236
1.9. Obsługa IGMP v3 - RFC 3376
1.10. Obsługa IGMP v1/v2/v3 snooping
1.11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

5. Bezpieczeństwo

1.1. Obsługa logowania do sieci Network Login
   a. IEEE 802.1x based Network Login
   b. MAC based Network Login

c. Web-based Network Login

1.2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
1.3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
1.4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
1.5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink.
1.6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
1.7. Obsługa Guest VLAN dla IEEE 802.1x
1.8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
1.9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
1.10. Obsługa TACACS+ (RFC 1492)
1.11. Obsługa RADIUS Authentication (RFC 2138)
1.12. Obsługa RADIUS Accounting (RFC 2139)
1.13. RADIUS per-command Authentication
1.14. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
1.15. Możliwość wyłączenia MAC learning
1.16. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
1.17. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    a. Adres MAC źródłowy i docelowy plus maska
    b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    d. Numery portów źródłowych i docelowych TCP, UDP
    e. Zakresy portów źródłowych i docelowych TCP, UDP
    f. Identyfikator sieci VLAN - VLAN ID
    g. Quality of Service IEEE 802.1p oraz DiffServ
    h. Flagi TCP
    i. Obsługa fragmentów
1.18. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
1.19. Możliwość konfiguracji min. 5200 reguł na wejściu i 1 000 reguł na wyjściu
1.20. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
1.21. Obsługa bezpiecznego transferu plików SCP/SFTP
1.22. Obsługa DHCP Option 82
1.23. Obsługa IP Security – Trusted DHCP Server
1.24. Obsługa IP Security – DHCP Snooping and Guard
1.25. Obsługa IP Security - Gratuitous ARP Protection
1.26. Obsługa IP Security – DHCP Secured ARP/ARP Validation
1.27. Obsługa IP Security – IP Source guard
1.28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
1.29. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

6. Bezpieczeństwo sieciowe

1.1. Możliwość konfiguracji portu głównego i zapasowego
1.2. Obsługa redundancji routingu VRRP
1.3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
1.4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
1.5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
1.6. Obsługa PVST+
1.7. Obsługa ERPS / G.8032
1.8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
1.9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
1.10. Obsługa LACP w ramach MLAG

7. Zarządzanie

1.1. Obsługa synchronizacji czasu SNTP lub NTP
1.2. Zarządzanie przez SNMP v1/v2/v3
1.3. Zarządzanie przez przeglądarkę WWW – protokół http i https
1.4. Możliwość zarządzania przez protokół XML
1.5. Telnet Serwer/Klient dla IPv4 / IPv6
1.6. SSH2 Serwer/Klient dla IPv4 / IPv6
1.7. Ping dla IPv4 / IPv6
1.8. Traceroute dla IPv4 / IPv6
1.9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
1.10. Sprzętowa obsługa sFlow
1.11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
1.12. Obsługa RMON2 (RFC 2021)
1.13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

8. Inne

1.1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
1.2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
1.3. Obsługa skryptów CLI
1.4. Obsługa funkcji TCL/Tk w skryptach CLI
1.5. Obsługa skryptów Python
1.6. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
1.7. Możliwość uruchamiania skryptów
   a. Ręcznie
   b. O określonym czasie lub co wskazany okres czasu
   c. Na podstawie wpisów w logu systemowym

6.2.8 Przełącznik typ 5

Dostarczone przełączniki typ 5 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Przełącznik wyposażony w 24 porty PoE+ 10/100/1000BASE-T
1.2. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
1.3. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
1.4. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
1.5. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana

1.6. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
1.7. Wysokość urządzenia 1U montowana w standardowym 19” Rack
1.8. Przełącznik musi posiadać zasilacz 230V. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
1.9. PoE+ zgodne ze standardem IEEE 802.3at.
1.10. Budżet mocy dla PoE+ min. 370W z jednego i 720W z dwóch zasilaczy.
1.11. Możliwość konfiguracji priorytetów wyłączenia PoE+ w przypadku braku budżetu mocy wynikającego np. z uszkodzenia pojedynczego zasilacza.
1.12. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
1.13. Możliwość łączenia do 8 przełączników w stos
1.14. Nieblokująca architektura o wydajności przełączania min. 208 Gb/s
1.15. Szybkość przełączania min. 154 Milionów pakietów na sekundę
1.16. Temperatura pracy przełącznika w zakresie min. 0o do 40o C
1.17. Tablica MAC adresów min. 32 tys.
1.18. Pamięć operacyjna: min. 1 GB pamięci DRAM
1.19. Pamięć flash: min. 1 GB pamięci Flash
1.20. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000
1.21. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
1.22. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów)
1.23. Obsługa Q-in-Q IEEE 802.1ad
1.24. Obsługa Quality of Service
    a. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
    b. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
    d. Obsługa kolejek Strict Priority
    e. Obsługa kolejek Weighted Round Robin
    f. Obsługa WRED (Weighted Random Early Detection)
1.25. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
1.26. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
1.27. Obsługa CDPv2 z obsługą Voice VLAN
1.28. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
1.29. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
1.30. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
1.31. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
1.32. Możliwość monitorowania zajętości CPU oraz pamięci
1.33. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
1.34. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
1.35. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
1.36. Dedykowany port konsoli szeregowej RJ45
1.37. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

2. Obsługa Routingu IPv4

1.1. Sprzętowa obsługa routingu IPv4 - forwarding
1.2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego IPv4
    a. RIP v1/v2
    b. OSPFv2 - możliwość rozszerzenia przez licencje

c. BGPv4 - możliwość rozszerzenia przez licencje
d. IS-IS - możliwość rozszerzenia przez licencje

1.5. Policy Based Routing dla IPv4
1.6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

3. Obsługa Routingu IPv6

1.1. Sprzętowa obsługa routingu IPv6 - forwarding
1.2. Pojemność tabeli routingu min. 2 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego dla IPv6
a. RIPng
b. OSPF v3 – możliwość rozszerzenia przez licencje
c. BGPv4 – możliwość rozszerzenia przez licencje
d. IS-IS – możliwość rozszerzenia przez licencje
1.5. Obsługa 6to4 (RFC 3056)
1.6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
1.7. Obsługua MLDv2 (Multicast Listener Discovery version 2)
1.8. Policy Based Routing dla IPv6
1.9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

4. Obsługa Multicastów

1.1. Statyczne przyłączanie do grupy multicast
1.2. Filtrowanie IGMP
1.3. Obsługa PIM-SM
1.4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
1.5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
1.6. Obsługa Multicast VLAN Registration - MVR
1.7. Obsługa IGMP v1 - RFC 1112
1.8. Obsługa IGMP v2 - RFC 2236
1.9. Obsługa IGMP v3 - RFC 3376
1.10. Obsługa IGMP v1/v2/v3 snooping
1.11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

5. Bezpieczeństwo

1.1. Obsługa logowania do sieci Network Login
a. IEEE 802.1x based Network Login
b. MAC based Network Login
c. Web-based Network Login
1.2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
1.3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
1.4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
1.5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink
1.6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
1.7. Obsługa Guest VLAN dla IEEE 802.1x
1.8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
1.9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
1.10. Obsługa TACACS+ (RFC 1492)
1.11. Obsługa RADIUS Authentication (RFC 2138)

1.12. Obsługa RADIUS Accounting (RFC 2139)
1.13. RADIUS per-command Authentication
1.14. Bezpieczeństwo MAC adresów
   a. ograniczenie liczby MAC adresów na porcie
   b. zatrzaśnięcie MAC adresu na porcie
   c. możliwość wpisania statycznych MAC adresów na port/vlan
1.15. Możliwość wyłączenia MAC learning
1.16. Zabezpieczenie przełącznika przed atakami DoS
   a. Networks Ingress Filtering RFC 2267
   b. SYN Attack Protection
   c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
1.17. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
   a. Adres MAC źródłowy i docelowy plus maska
   b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
   c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
   d. Numery portów źródłowych i docelowych TCP, UDP
   e. Zakresy portów źródłowych i docelowych TCP, UDP
   f. Identyfikator sieci VLAN - VLAN ID
   g. Quality of Service IEEE 802.1p oraz DiffServ
   h. Flagi TCP
   i. Obsługa fragmentów
1.18. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
1.19. Możliwość konfiguracji min. 5200 reguł na wejściu i 1 000 reguł na wyjściu
1.20. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
1.21. Obsługa bezpiecznego transferu plików SCP/SFTP
1.22. Obsługa DHCP Option 82
1.23. Obsługa IP Security – Trusted DHCP Server
1.24. Obsługa IP Security – DHCP Snooping and Guard
1.25. Obsługa IP Security - Gratuitous ARP Protection
1.26. Obsługa IP Security – DHCP Secured ARP/ARP Validation
1.27. Obsługa IP Security – IP Source guard
1.28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
1.29. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

6. Bezpieczeństwo sieciowe

1.1. Możliwość konfiguracji portu głównego i zapasowego
1.2. Obsługa redundancji routingu VRRP
1.3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
1.4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
1.5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
1.6. Obsługa PVST+
1.7. Obsługa ERPS / G.8032
1.8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
1.9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
1.10. Obsługa LACP w ramach MLAG

7. Zarządzanie

1.1. Obsługa synchronizacji czasu SNTP lub NTP
1.2. Zarządzanie przez SNMP v1/v2/v3

1.3. Zarządzanie przez przeglądarkę WWW – protokół http i https
1.4. Możliwość zarządzania przez protokół XML
1.5. Telnet Serwer/Klient dla IPv4 / IPv6
1.6. SSH2 Serwer/Klient dla IPv4 / IPv6
1.7. Ping dla IPv4 / IPv6
1.8. Traceroute dla IPv4 / IPv6
1.9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
1.10. Sprzętowa obsługa sFlow
1.11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
1.12. Obsługa RMON2 (RFC 2021)
1.13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

8. Inne

1.1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
1.2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
1.3. Obsługa skryptów CLI
1.4. Obsługa funkcji TCL/Tk w skryptach CLI
1.5. Obsługa skryptów Python
1.6. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
1.7. Możliwość uruchamiania skryptów
   a. Ręcznie
   b. O określonym czasie lub co wskazany okres czasu

Na podstawie wpisów w logu systemowym

6.2.9 Przełącznik typ 6

Dostarczone przełączniki typ 6 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Przełącznik wyposażony w min. 12 portów PoE 100/1G/2,5GBASE-T 802.3bt
1.2. Przełącznik wyposażony w 32 porty PoE 10/100/1000BASE-T 802.3at
1.3. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
1.4. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
1.5. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
1.6. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana
1.7. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
1.8. Wysokość urządzenia 1U montowana w standardowym 19” Rack
1.9. Przełącznik musi siadać zasilacz 230V. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
1.10. Budżet mocy dla PoE+ min. 960W z jednego i 1800W z dwóch zasilaczy.
1.11. Możliwość konfiguracji priorytetów wyłączenia PoE+ w przypadku braku budżetu mocy wynikającego np. z uszkodzenia pojedynczego zasilacza.
1.12. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
1.13. Możliwość łączenia do 8 przełączników w stos
1.14. Nieblokująca architektura o wydajności przełączania min. 304 Gb/s
1.15. Szybkość przełączania min. 225 Milionów pakietów na sekundę
1.16. Temperatura pracy przełącznika w zakresie min. 0o do 40o C
1.17. Tablica MAC adresów min. 32 tys.
1.18. Pamięć operacyjna: min. 1 GB pamięci DRAM
1.19. Pamięć flash: min. 1 GB pamięci Flash
1.20. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000
1.21. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci

1.22. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów)
1.23. Obsługa Q-in-Q IEEE 802.1ad
1.24. Obsługa Quality of Service
   a. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
   b. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
   c. 8 kolejek priorytetów na każdym porcie wyjściowym
   d. Obsługa kolejek Strict Priority
   e. Obsługa kolejek Weighted Round Robin
   f. Obsługa WRED (Weighted Random Early Detection)
1.25. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
1.26. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
1.27. Obsługa CDPv2 z obsługą Voice VLAN
1.28. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
1.29. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
1.30. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
1.31. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
1.32. Możliwość monitorowania zajętości CPU oraz pamięci
1.33. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
1.34. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
1.35. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
1.36. Dedykowany port konsoli szeregowej RJ45
1.37. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

2. Obsługa Routingu IPv4

1.1. Sprzętowa obsługa routingu IPv4 - forwarding
1.2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego IPv4
   a. RIP v1/v2
   b. OSPFv2 - możliwość rozszerzenia przez licencje
   c. BGPv4 - możliwość rozszerzenia przez licencje
   d. IS-IS - możliwość rozszerzenia przez licencje
1.5. Policy Based Routing dla IPv4
1.6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

3. Obsługa Routingu IPv6

1.1. Sprzętowa obsługa routingu IPv6 - forwarding
1.2. Pojemność tabeli routingu min. 6 000 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego dla IPv6
   a. RIPng
   b. OSPF v3 – możliwość rozszerzenia przez licencje
   c. BGPv4 – możliwość rozszerzenia przez licencje
   d. IS-IS – możliwość rozszerzenia przez licencje
1.5. Obsługa 6to4 (RFC 3056)
1.6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
1.7. Obsługa MLDv2 (Multicast Listener Discovery version 2)
1.8. Policy Based Routing dla IPv6
1.9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

4. Obsługa Multicastów

1.1. Statyczne przyłączanie do grupy multicast
1.2. Filtrowanie IGMP
1.3. Obsługa PIM-SM
1.4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
1.5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
1.6. Obsługa Multicast VLAN Registration - MVR
1.7. Obsługa IGMP v1 - RFC 1112
1.8. Obsługa IGMP v2 - RFC 2236
1.9. Obsługa IGMP v3 - RFC 3376
1.10. Obsługa IGMP v1/v2/v3 snooping
1.11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

5. Bezpieczeństwo

1.1. Obsługa logowania do sieci Network Login
   a. IEEE 802.1x based Network Login
   b. MAC based Network Login
   c. Web-based Network Login
1.2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
1.3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
1.4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
1.5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink.
1.6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
1.7. Obsługa Guest VLAN dla IEEE 802.1x
1.8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
1.9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
1.10. Obsługa TACACS+ (RFC 1492)
1.11. Obsługa RADIUS Authentication (RFC 2138)
1.12. Obsługa RADIUS Accounting (RFC 2139)
1.13. RADIUS per-command Authentication
1.14. Bezpieczeństwo MAC adresów
   a. ograniczenie liczby MAC adresów na porcie
   b. zatrzaśnięcie MAC adresu na porcie
   c. możliwość wpisania statycznych MAC adresów na port/vlan
1.15. Możliwość wyłączenia MAC learning
1.16. Zabezpieczenie przełącznika przed atakami DoS
   a. Networks Ingress Filtering RFC 2267
   b. SYN Attack Protection
   c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
1.17. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
   a. Adres MAC źródłowy i docelowy plus maska
   b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
   c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
   d. Numery portów źródłowych i docelowych TCP, UDP
   e. Zakresy portów źródłowych i docelowych TCP, UDP
   f. Identyfikator sieci VLAN - VLAN ID
   g. Quality of Service IEEE 802.1p oraz DiffServ
   h. Flagi TCP

i. Obsługa fragmentów

1.18. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
1.19. Możliwość konfiguracji min. 5200 reguł na wejściu i 1 000 reguł na wyjściu
1.20. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
1.21. Obsługa bezpiecznego transferu plików SCP/SFTP
1.22. Obsługa DHCP Option 82
1.23. Obsługa IP Security – Trusted DHCP Server
1.24. Obsługa IP Security – DHCP Snooping and Guard
1.25. Obsługa IP Security - Gratuitous ARP Protection
1.26. Obsługa IP Security – DHCP Secured ARP/ARP Validation
1.27. Obsługa IP Security – IP Source guard
1.28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
1.29. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

6. Bezpieczeństwo sieciowe

1.1. Możliwość konfiguracji portu głównego i zapasowego
1.2. Obsługa redundancji routingu VRRP
1.3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
1.4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
1.5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
1.6. Obsługa PVST+
1.7. Obsługa ERPS / G.8032
1.8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
1.9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
1.10. Obsługa LACP w ramach MLAG

7. Zarządzanie

1.1. Obsługa synchronizacji czasu SNTP lub NTP
1.2. Zarządzanie przez SNMP v1/v2/v3
1.3. Zarządzanie przez przeglądarkę WWW – protokół http i https
1.4. Możliwość zarządzania przez protokół XML
1.5. Telnet Serwer/Klient dla IPv4 / IPv6
1.6. SSH2 Serwer/Klient dla IPv4 / IPv6
1.7. Ping dla IPv4 / IPv6
1.8. Traceroute dla IPv4 / IPv6
1.9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
1.10. Sprzętowa obsługa sFlow
1.11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
1.12. Obsługa RMON2 (RFC 2021)
1.13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

8. Inne

1.1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
1.2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
1.3. Obsługa skryptów CLI
1.4. Obsługa funkcji TCL/Tk w skryptach CLI
1.5. Obsługa skryptów Python

1.6. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
1.7. Możliwość uruchamiania skryptów
   a. Ręcznie
   b. O określonym czasie lub co wskazany okres czasu
   c. Na podstawie wpisów w logu systemowym

6.2.10 Przełącznik typ 7

Dostarczone przełączniki typ 7 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Przełącznik posiadający 12 portów 10/100/1000BASE-T
1.2. 2 porty port 1G/10G SFP+, działające z prędkością 1/10 Gb/s
1.3. Wysokość urządzenia 1U
1.4. Przełącznik musi być wyposażony we wbudowany zasilacz AC 230V. Nie dopuszcza się stosowania zewnętrznego zasilacza
1.5. Wydajności przełączania min. 104 Gb/s
1.6. Szybkość przełączania min. 77 Milionów pakietów na sekundę
1.7. Możliwość łączenia do 8 przełączników w stos z wydajnością 10 Gb/s za pomocą portów 10G SFP+ lub za pomocą dedykowanych połączeń stakujących.
1.8. Tablica MAC adresów min. 16k
1.9. Pamięć operacyjna: min. 1GB pamięci DRAM
1.10. Pamięć flash: min. 4GB pamięci Flash
1.11. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000
1.12. Obsługa sieci wirtualnych protokołowych IEEE 802.1v
1.13. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
1.14. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów)
1.15. Obsługa Q-in-Q IEEE 802.1ad
1.16. Obsługa Quality of Service
   a. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
   b. Rozpoznawanie i realizacja priorytetów ustawionych w DiffServ
   c. 8 kolejek priorytetów na każdym porcie wyjściowym
   d. Obsługa kolejek Strict Priority
   e. Obsługa kolejek Weighted Round Robin
   f. Obsługa WRED (Weighted Random Early Detection)
1.17. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
1.18. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
1.19. Obsługa CDPv2 z obsługą Voice VLAN
1.20. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
1.21. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcja 43, 60, 78 itp.)
1.22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
1.23. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
1.24. Możliwość monitorowania zajętości CPU oraz pamięci
1.25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
1.26. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.

2. Obsługa Routingu IPv4

1.1. Sprzętowa obsługa routingu IPv4 – forwarding
1.2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 480 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego IPv4
   a. RIPv1/v2
   b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

3. Obsługa Routingu IPv6

1.1. Sprzętowa obsługa routingu IPv6 – forwarding
1.2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 240 wpisów
1.3. Routing statyczny
1.4. Obsługa routingu dynamicznego dla IPv6
   a. RIPng
   b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
1.5. Obsługa MLDv1 (Multicast Listener Discovery version 1)
1.6. Obsługa MLDv2 (Multicast Listener Discovery version 2)

4. Obsługa Multicastów

1.1. Statyczne przyłączenie do grupy multicast
1.2. Filtrowanie IGMP
1.3. Obsługa Multicast VLAN Registration - MVR
1.4. Obsługa IGMP v1/v2/v3 snooping

5. Bezpieczeństwo

1.1. Obsługa Network Login
   a. IEEE 802.1x
   b. Web-based Network Login
   c. MAC based Network Login
1.2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
1.3. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
1.4. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login – również dla wielu klientów na jednym porcie (np. jeden klient przydzielony do VLAN X, drugi klient przydzielony do sieci VLAN Y)
1.5. Obsługa Guest VLAN dla IEEE 802.1x
1.6. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
1.7. Obsługa TACACS+ (RFC 1492)
1.8. Obsługa RADIUS Authentication (RFC 2138)
1.9. Obsługa RADIUS Accounting (RFC 2139)
1.10. RADIUS and TACACS+ per-command Authentication
1.11. Bezpieczeństwo MAC adresów
   a. ograniczenie liczby MAC adresów na porcie
   b. zatrzaśnięcie MAC adresu na porcie
   c. możliwość wpisania statycznych MAC adresów na port/vlan
1.12. Możliwość wyłączenia MAC learning
1.13. Obsługa SNMPv1/v2/v3
1.14. Klient SSH2
1.15. Zabezpieczenie przełącznika przed atakami DoS
   a. Networks Ingress Filtering RFC 2267
   b. SYN Attack Protection
   c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
1.16. Dwukierunkowe listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
   a. Adres MAC źródłowy i docelowy plus maska
   b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
   c. Protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
   d. Numery portów źródłowych i docelowych TCP, UDP
   e. Zakresy portów źródłowych i docelowych TCP, UDP
   f. Identyfikator sieci VLAN – VLAN ID
   g. Flagi TCP
   h. Obsługa fragmentów

1.17. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
1.18. Możliwość konfiguracji min. 1024 reguł na wejściu i 256 reguł na wyjściu.
1.19. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania
1.20. Obsługa bezpiecznego transferu plików SCP/SFTP
1.21. Obsługa DHCP Option 82
1.22. Obsługa IP Security - Gratuitous ARP Protection
1.23. Obsługa IP Security - Trusted DHCP Server
1.24. Obsługa IP Security - DHCP Snooping
1.25. Obsługa IP Security - DHCP Secured ARP/ARP Validation
1.26. Obsługa IP Security – IP Source Guard
1.27. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s
1.28. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

6. Bezpieczeństwo sieciowe

1.1. Możliwość konfiguracji portu głównego i zapasowego
1.2. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
1.3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
1.4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
1.5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
1.6. Obsługa PVST+
1.7. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
1.8. Obsługa ERPS / G.8032
1.9. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.
1.10. Obsługa MLAG - połączenie Link Aggregation do dwóch niezależnych przełączników.
1.11. Obsługa LACP w ramach MLAG
1.12. Obsługa MVRP w ramach MLAG

7. Zarządzanie

1.1. Obsługa synchronizacji czasu SNTP (Simple Network Time Protocol)
1.2. Obsługa synchronizacji czasu NTP
1.3. Zarządzanie przez SNMP v1/v2/v3
1.4. Zarządzanie przez przeglądarkę WWW – protokół http i https
1.5. Telnet Serwer/Klient dla IPv4 / IPv6
1.6. SSH2 Serwer/Klient dla IPv4 / IPv6
1.7. Ping dla IPv4 / IPv6
1.8. Traceroute dla IPv4 / IPv6
1.9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
1.10. Sprzętowa obsługa sFlow
1.11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
1.12. Obsługa RMON2 (RFC 2021)
1.13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, SYSLOG oraz RADIUS

8. Inne

1.1. Obsługa skryptów CLI
1.2. Obsługa funkcji TCL/Tk w skryptach CLI
1.3. Obsługa skryptów Python
1.4. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)

1.5. Wsparcie dla OpenFlow – poprzez rozszerzenie licencji
1.6. Możliwość uruchamiania skryptów
   a. Ręcznie
   b. O określonym czasie lub co wskazany okres czasu
   c. Na podstawie wpisów w logu systemowym

6.2.11 Przełącznik typ 8

Dostarczone przełączniki typ 8 muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Switch musi posiadać 8 portów 10/100/1000BASE-T
1.2. Switch musi posiadać co najmniej 2 porty 1000/10GBaseX SFP+
1.3. Switch musi posiadać port konsoli RS 232 w postaci portu RJ-45
1.4. Switch musi posiadać port USB
1.5. Wydajności przełączania minimum 40 Gb/s
1.6. Szybkość przełączania min. 29 Milionów pakietów na sekundę
1.7. Switch musi być w pełni zarządzany z aplikacji zarządzającej
1.8. Możliwość połączenia w kaskadzie do 4 urządzeń
1.9. Wsparcie dla Zero Touch Provisioning (ZTP)
1.10. Połączenie ze switchem corowym poprzez porty 1000/10GBaseX SFP+
1.11. Wsparcie dla autentykacji użytkowników 802.1x oraz MAC autentykacji

6.2.12 Bezprzewodowy punkt dostępowy

Dostarczone bezprzewodowe punkty dostępowe muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania podstawowe

1.1. Punkt dostępowy przeznaczony do instalacji wewnątrz pomieszczeń
1.2. Punkt dostępowy musi posiadać trzy interfejsy radiowe pozwalające na obsługę:
   a. Pasma 2.4 GHz min. 2x2:2 MIMO
   b. Pasma 5 GHz min. 4x4:4 MIMO
   c. Sensor pracujący w paśmie 2.4 GHz oraz 5 GHz
1.3. Punkt dostępowy musi zapewniać możliwość pracy w trybie dual 5 GHz
1.4. Punkt dostępowy musi zapewniać prawidłową pracę w zakresie temperatur od 00C do +400C
1.5. Punkt dostępowy musi być zgodny ze standardem WiFi6 – IEEE 802.11ax.
1.6. Punkt dostępowy musi posiadać możliwość zabezpieczenia z wykorzystaniem systemu Kensington
1.7. Punkt dostępowy musi być przeznaczony do montaż na suficie, suficie podwieszanym oraz na ścianie
1.8. Punkt dostępowy musi posiadać wbudowane diody LED sygnalizujące stan pracy.
1.9. Punkt dostępowy musi posiadać możliwość centralnego wyłączenia diod LED sygnalizujących stan pracy oraz włączenia lokalizacji (charakterystyczna sekwencja świecenia diod LED) punktu dostępowego
1.10. Punkt dostępowy musi być wyposażony w 1 interfejs Ethernet 10/100/1000BASE-T . Musi zapewniać możliwość zasilenia punktu dostępowego przez PoE+ (IEEE 802.3at – min 21W).
1.11. Przynajmniej jeden z powyższych interfejsów Ethernet musi wspierać Multi-rate min. 2.5 Gb/s.
1.12. Punkt dostępowy musi posiadać interfejs min. USB 2.0
1.13. Punkt dostępowy musi zapewniać obsługę min. 8 SSID na każdym radiu WiFi
1.14. Punkt dostępowy musi zapewniać możliwość dołączenia min. 500 klientów na każdym radiu
1.15. Punkt dostępowy musi zapewniać możliwość pracy z wykorzystaniem dedykowanego kontrolera sieci bezprzewodowej i/lub z wykorzystaniem systemu chmurowego producenta punktu dostępowego.

1.16. Producent musi zapewniać dedykowane kontrolery zarówno w postaci sprzętowej jak i wirtualnej możliwej do instalacji w środowisku opisanym w pkt 4.2.1 i 4.2.2
1.17. Punkt dostępowy musi posiadać mechanizmy zapewniające współpracę z min. dwoma kontrolerami zapewniającymi odporność na awarie i możliwość dalszej pracy w przypadku uszkodzenia pojedynczego kontrolera.
1.18. Punkt dostępowy musi posiadać możliwość konfiguracji suplikanta IEEE 802.1x i pozwalać na uwierzytelnianie z wykorzystaniem min. PEAP oraz EAP-TLS (certyfikat zainstalowany na punkcie dostępowym)
1.19. Punkt dostępowy musi zapewniać możliwość terminowania połączeń bezprzewodowych bezpośrednio na punkcie dostępowym i wpuszczania ruchu do wskazanej sieci VLAN (sieć VLAN musi być konfigurowalna dla każdego SSID z osobna oraz musi być możliwość jej przekazania dla każdego klienta uwierzytelnianego z wykorzystaniem systemu RADIUS w ramach RFC 3580).
1.20. Punkt dostępowy musi zapewniać możliwość tunelowania ruchu klienta bezprzewodowego przez sieć LAN do kontrolera i wpuszczania ruchu do wskazanej sieci VLAN na kontrolerze (sieć VLAN musi być konfigurowalna dla każdego SSID z osobna oraz musi być możliwość jej przekazania dla każdego klienta uwierzytelnianego z wykorzystaniem systemu RADIUS w ramach RFC 3580).
1.21. Punkt dostępowy musi zapewniać obsługę tunelowania ruchu.
1.22. Ruch kontrolny oraz tunelowany pomiędzy punktem dostępowym a kontrolerem musi mieć możliwość zabezpieczenia z wykorzystaniem IPSec.
1.23. Punkt dostępowy musi zapewniać możliwość konfiguracji puli sieci VLAN dla obsługi dużej liczby klientów z zapewnieniem ich separacji w sieci LAN z wykorzystaniem wielu sieci VLAN.
1.24. Punkt dostępowy musi zapewniać realizację filtrowania ruchu dla dołączonych klientów bezprzewodowych. Filtracja musi być możliwa dla każdego SSID z osobna oraz musi być możliwość przekazania informacji o filtracji dla każdego klienta uwierzytelnionego z wykorzystaniem systemu RADIUS.
1.25. Punkt dostępowy musi zapewniać wsparcie IEEE 802.11r, IEEE 802.11k oraz IEEE 802.11v
1.26. Punkt dostępowy musi umożliwiać współpracę z dedykowanym systemem IDS oraz IPS
1.27. Punkt dostępowy musi zapewniać możliwość uwierzytelniania klientów bezprzewodowych z wykorzystaniem IEEE 802.1x i protokołów min.: EAP-TLS, EAP-TTLS, PEAP
1.28. Punkt dostępowy musi zapewniać obsługę WPA3
1.29. Punkt dostępowy musi zapewniać możliwość uwierzytelniania klientów z wykorzystaniem MAC Authentication
1.30. Punkt dostępowy musi zapewniać współpracę z serwerami RADIUS Authentication oraz RADIUS Accounting
1.31. Punkt dostępowy musi zapewniać realizację priorytetów dla rozwiązań VoIP
1.32. Punkt dostępowy musi zapewniać wsparcie zabezpieczenia ramek kontrolnych zgodnie ze standardem IEEE 802.11w
1.33. Punkt dostępowy musi być wyposażony w moduł TPM
1.34. Punkt dostępowy musi posiadać Certyfikat CE lub Deklarację zgodności
1.35. Punkt dostępowy musi posiadać tzw. dożywotnią gwarancję, czyli zapewnienie wymiany w przypadku awarii do min. 5 lat po zakończeniu produkcji urządzenia.
1.36. Punt dostępowy musi zostać dostarczony z modułem montażowym

6.2.13 Kontroler sieci bezprzewodowej

Dostarczony kontroler sieci bezprzewodowej musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Kontroler bezprzewodowy dostarczony jako
   a. Kontroler sprzętowy w formie klastra odpornego na awarie (opcja 1)
      ii. Kontroler musi być przeznaczony do montażu w szafie Rack 19”
      iii. Kontroler musi być wyposażony w dwa zasilacz 230V zapewniające odporność na awarie w przypadku jednego z nich.
      iv. Kontroler musi być wyposażony w min. 2 porty 10 Gigabit Ethernet SFP+ do podłączenia do przełączników znajdujących się w Głównym Punkcie Dystrybucyjnym

v. Kontroler musi być wyposażone w inne niezbędne porty, jeśli są wymagane do stworzenia odpornego na awarie klastra

b. Kontroler wirtualny (opcja 2)

iv. Kontroler musi być przeznaczony do instalacji w systemie wirtualizacji opisanym w pkt 4.2.1 i 4.2.2 .

v. Kontroler musi zapewniać alternatywnie możliwość instalacji w systemie VMware

2. Niezależnie od powyższych opcji kontroler musi być dostarczony w postaci odpornego na awarie klastra
3. Kontroler musi zapewnić skalowalność do min. 1000 punktów dostępowych
4. Kontroler musi zapewnić skalowalność niezbędną do obsługi min. 8 tys jednoczesnych użytkowników sieci bezprzewodowej.
5. Kontroler musi zapewniać obsługę sieci VLAN zgodnych z IEEE 802.1Q
6. Kontroler musi być zarządzany przez przeglądarkę www bez konieczności instalacji aplikacji na stacji zarządzającej jak np. Java
7. Kontroler musi zapewniać obsługę wielu Lokalizacji z wizualizacją ich stanu, liczby sieci bezprzewodowych (SSID) oraz liczby obsługiwanych punktów dostępowych w każdej lokalizacji.
8. Kontroler musi zapewniać widzialność wszystkich dołączonych do kontrolera punktów dostępowych z następującymi informacjami:
   a. Nazwa punktu dostępowego – konfigurowalna nazwa punktu (Host Name)
   b. Typ punktu dostępowego
   c. Numer seryjny punktu dostępowego
   d. MAC adres punktu dostępowego
   e. Adres IP punktu dostępowego
   f. Status punktu dostępowego
   g. Przypisanie do lokalizacji
   h. Informacje o kanałach pracy poszczególnych interfejsów radiowych
   i. Informacje o liczbie klientów na poszczególnych interfejsach radiowych
   j. Informacje o aktualnej mocy ustawionej na poszczególnych interfejsach radiowych
   k. Informacji o szerokości kanału ustawionej na poszczególnych interfejsach radiowych
   l. Informacji o poziomie szumu dla poszczególnych interfejsów radiowych
9. Kontroler musi zapewniać możliwość filtracji prezentowanych informacji o punktach dostępowych na podstawie dowolnych parametrów
10. Kontroler musi zapewniać możliwość konfiguracji sieci bezprzewodowych, ich przydziału do grup punktów dostępowych, a następnie do lokalizacji
11. Kontroler musi zapewniać automatyczne wykrywanie i konfigurowanie nowych punktów dostępowych
12. Kontroler musi być zarządzany przez SNMPv1/v2/v3 oraz SSHv2.
13. Kontroler musi obsługiwać RADIUS authentication oraz RADIUS accounting.
14. Kontroler musi zapewniać obsługę: 802.11i, WPA, WPA2, TKIP oraz AES, WPA3
15. Kontroler musi zapewniać obsługę rozwiązania OWE (Opportunistic Wireless Encryption) zapewniającego bezpieczeństwo w sieciach „otwartych”
16. Kontroler musi zapewniać obsługę IEEE 802.1x oraz autentykację: EAP-TLS, EAP-TTLS, PEAP, EAP-MD5 oraz EAP-SIM.
17. Obsługa mechanizmów roaming oraz handover (wstępne uwierzytelnienie, OKC)
18. Kontroler musi zapewniać obsługę najnowszych standardów realizacji roamingu IEEE 802.11r
19. Kontroler musi zapewniać obsługę Neighbor Report w ramach standardu IEEE 802.11k
20. Kontroler musi zapewniać obsługę mechanizmów Roaming Assist zgodnych ze standardem IEEE 802.11v
21. Kontroler musi zapewniać obsługę mechanizmów IEEE 802.11w
22. Kontroler musi zapewniać przesyłanie danych z sieci WLAN do sieci przewodowej w następujących architekturach:
   a. bridging na kontrolerze – kontroler zapewnia przełączanie ruchu z sieci bezprzewodowej do wskazanej sieci wirtualnej przewodowej dołączonej do kontrolera
   b. bridging na punkcie dostępowym – w tym trybie ruch z sieci bezprzewodowej jest kierowany bezpośrednio do wskazanej sieci wirtualnej przyłączonej bezpośrednio do punktu dostępowego
   c. bridging na punkcie dostępowym wraz z sygnalizacją niezbędnych sieci VLAN z wykorzystaniem IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging (PBB)
   d. bridging na punkcie dostępowym z zapewnieniem tunelowania ruchu poprzez VxLAN
23. Kontroler bezprzewodowy musi zapewniać możliwość ustawiania następujących parametrów w ramach każdej sesji klienckiej:

a. indywidualne raguły filtrowania ruchu
   b. przypisanie sieci VLAN
   c. QoS
   d. ograniczenia transmisji wejściowej i wyjściowej
   e. wyboru topologii (bridging na kontrolerze, bridging na punkcie dostępowym, tunel VxLAN, IEEE 802.1Qcj)

24. Kontroler musi zapewniać obsługę konfiguracji punktów dostępowych w trybie Client Bridge, który będzie wykorzystywał punkt dostępowych jako klienta do sieci bezprzewodowej przy wykorzystaniu jednego z interfejsów radiowych (2.4 GHz lub 5 GHz) jednocześnie udostępniając obydwa interfejsy radiowe dla klientów bezprzewodowych oraz dostępne interfejsy Ethernet do przyłączenia urządzeń nieposiadających interfejsu bezprzewodowego do sieci bezprzewodowej
25. Kontroler musi zapewniać możliwość centralnej konfiguracji przyłączenia punktów dostępowych do infrastruktury sieciowej zabezpieczonej przez IEEE 802.1x i protokoły PEAP oraz EAP-TLS (IEEE 802.1x supplicant na porcie Ethernet punktu dostępowego)
26. Kontroler musi zapewniać możliwość konfiguracji rozwiązania Mesh
27. Kontroler musi zapewniać obsługę standardu Hotspot 2.0
28. Kontroler musi zapewniać współpracę z systemem Eduroam
29. Kontroler musi zapewniać obsługę Captive Portal pozwalającego na obsługę gości jak i uwierzytelnianie klientów bezprzewodowych z wykorzystaniem Captive Portal – np. nieposiadających suplikanta IEEE 802.1x
30. Kontroler musi zapewniać możliwość rejestracji gości w oparciu o portal www znajdujący się na kontrolerze.
31. Portal rejestracji gości musi zapewniać możliwość stworzenia i akceptacji regulaminu przez rejestrujących się gości
32. Kontroler musi zapewniać przynajmniej podstawową konfigurację wyglądu Captive Portal – zmiana kolorów itp.
33. Kontroler musi zapewniać możliwość automatycznej, centralnej aktualizacji oprogramowania punktów dostępowych zaadoptowanych do kontrolera.
34. Kontroler musi zapewniać możliwość konfiguracji blokowania ruchu pomiędzy klientami sieci bezprzewodowej.
35. Kontroler musi zapewniać autoryzację użytkowników IEEE 802.1x w oparciu o zewnętrzny serwer RADIUS z możliwością definicji różnych serwerów RADIUS dla różnych identyfikatorów SSID
36. Kontroler musi zapewniać przydzielanie klientów do wskazanych sieci wirtualnych na podstawie informacji przesyłanej z serwera RADIUS zgodnie z RFC3580
37. Kontroler musi zapewniać możliwość przydzielania do sieci VLAN na podstawie przynależności klientów bezprzewodowych do grup użytkowników zdefiniowanych w LDAP
38. Kontroler musi zapewniać przydzielanie Polityki zawierającej QoS (Quality of Service), list kontroli dostępu ACL. Przydzielane polityki muszą być realizowane na punktach dostępowych w przypadku ruchu, który jest wpuszczany do sieci bezpośrednio na punkcie dostępowym.
39. Kontroler musi zapewniać konfigurację roamingu pomiędzy punktami dostępowymi.
40. Kontroler musi zapewniać konfigurację oszczędzania energii UAPSD (Unscheduled Automatic Power Save Delivery).
41. Kontroler musi obsługiwać QBSS (informacja o zbyt dużym obciążeniu zostanie przekazana klientowi dla obsługi inteligentnego roamingu)
42. Kontroler musi obsługiwać funkcjonalność FCA (Flexible Client Access) zwiększającą prędkość transmisji klientów IEEE 802.11n w sieci z urządzeniami IEEE 802.11/a/b/g.
43. Kontroler musi obsługiwać funkcjonalność CAC (Call Admission Control), pozwalającą na sprawdzenie czy zestawienie nowego połączenia telefonii VoIP nie wpłynie na jakość dotychczasowych połączeń.
44. Kontroler musi zapewniać obsługę preferencji pasma polegającą na automatycznym przenoszeniu klientów na pasmo 5 GHz.

6.2.14 System zarządzania

Dostarczony system zarządzania musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.
   a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub Windows oraz jaka aplikacja dedykowana dla systemu wirtualizacyjnego.
   b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
   c. Dostarczenie oprogramowanie zarządzające musi być obsługiwanego ze standardowej przeglądarki www bez konieczności instalacji dodatkowego klienta lub wymagania instalacji dodatkowego oprogramowania jak np. Java
2. Aplikacja zarządzająca musi obsługiwać minimum 2500 urządzeń (adresów IP zarządzanych przez SNMP) przy czym oprogramowanie musi być dostarczone z licencjami niezbędnymi do zarządzania dostarczonych urządzeń.
3. Aplikacja zarządzająca musi zapewniać możliwość zarządzania dowolnymi urządzeniami posiadającymi obsługę protokołu SNMP i/lub dostęp poprzez CLI (Telnet i/lub SSH)
4. Aplikacja zarządzająca musi zapewniać możliwość jednoczesnego podłączenia się do platformy zarządzającej min. 10 użytkowników. W skład tych użytkowników będą wchodzić administratorzy sieci
5. Aplikacja zarządzająca musi mieć możliwość definiowania grup użytkowników i definicji praw dostęp do różnych funkcji oprogramowania. Aplikacja musi zapewniać możliwość przydziału użytkowników systemu do różnych grup użytkowników
6. Aplikacja zarządzająca musi mieć możliwość integracji uwierzytelniania i autoryzacji użytkowników za pomocą LDAP i/lub Radius.
7. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
8. Aplikacja zarządzająca musi zezwalać na zarządzanie urządzeniami z wykorzystaniem protokołów SNMPv1, SNMPv2c, SNMPv3. SNMPv3 musi zapewniać uwierzytelnianie za pomocą protokołów MD5 oraz SHA, szyfrowanie za pomocą protokołów DES oraz AES.
9. Aplikacja musi pozwalać na tworzenie profili dostępu do urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu. Profil musi zawierać konfigurację SNMP dla danego urządzenia z podziałem na pełny dostęp, dostęp dla zapisu i odczytu oraz dostęp tylko do odczytu.
10. Dodatkowo profil dostępu do urządzeń musi zawierać możliwość konfiguracji dostępu do urządzenia z wykorzystaniem CLI – np. poprzez Telnet lub SSH.
11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
12. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
13. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
14. Aplikacja musi zapewniać możliwość konfiguracji widoków zawierających wskazane obiekty SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych. Przykładowo możliwość włączania/wyłączania portów, konfiguracji opisu portu (alias), włączenie/wyłączenie IEEE 802.1x, prezentację obciążenia portów PoE+ i inne dostępne w SNMP MIB OID dowolnego producenta.
15. Aplikacja musi zezwalać na modyfikację wyżej wymienionych obiektów SNMP MIB OID jeśli są to obiekty pozwalające na zapis i odczyt informacji.
16. Aplikacja musi posiadać wbudowany Syslog serwer pozwalający na gromadzenie logów przesyłanych przez zarządzane urządzenia.
17. Aplikacja musi posiadać możliwość konfiguracji Alarmów w reakcji na przychodzące trapy SNMP lub informacje z Syslog.
18. Alarmy muszą zapewniać możliwość wysłania emaila, wysłania trapu SNMP do innego systemu zarządzającego lub systemu automatyzacji, wpisu do Syslog lub uruchomienia skryptu.
19. Aplikacja zarządzająca musi zapewniać możliwość tworzenia skryptów CLI dla automatyzacji często wykonywanych zadań na zarządzanych urządzeniach. Skrypty muszą zapewniać możliwość wydawania komend CLI do wskazanych urządzeń lub grup urządzeń.
20. Aplikacja zarządzająca musi zapewniać możliwość tworzenia prostych skryptów CLI nie wymagających od administratora wiedzy programistycznej jak również bardziej zaawansowanych skryptów z wykorzystaniem TCL i Python.
21. Aplikacja zarządzająca musi w ramach powyższych skryptów zapewniać mechanizmy pozwalające na uzyskanie informacji z systemów firm trzecich z wykorzystaniem REST API

22. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
23. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
24. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń.
25. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
    a. Lokalizacji urządzeń np. poszczególne lokalizacje, budynki, piętra itp.
    b. Wizualizacja sieci musi zapewniać możliwość podłożenia rysunku kampusu lub piętra
    c. Połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem numerów portów po obydwu stronach łącza
    d. Połączeń Link Aggregation
    e. Wizualizacji skonfigurowanych sieci VLAN na poszczególnych urządzeniach
26. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a. adres IP urządzenia
    b. adresu MAC urządzenia
    c. nazwy urządzenia
    d. wersji oprogramowania
    e. wersji bootrom
    f. lokalizacji urządzenia
    g. danych kontaktowych administratora
    h. numeru seryjnego
    i. dodatkowych pól konfigurowanych przez użytkownika pozwalających na skonfigurowanie np. numerów inwentarzowych
27. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej (np. codziennie, co tydzień) realizacji backup'u konfiguracji urządzeń o wskazanym czasie (np. o 01:00).
    b. możliwość odtworzenia wskazanej konfiguracji urządzenia
    c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych
    d. możliwość porównywania różnic w ramach jednego urządzania z różnych backup'ów konfiguracji oraz w ramach różnych urządzeń.
    e. możliwość obsługi urządzeń sieciowych różnych producentów
28. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych różnych producentów (przy założeniu dostępu SSH/Telnet).
29. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30. Aplikacja musi zapewniać możliwość tworzenia profili bezpieczeństwa, które zawierają konfigurację sieci VLAN, ACL, QoS i mogą być przypisywane statycznie do portów przełączników sieciowych.
31. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
    a. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
    b. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
    c. generowanie raportów
32. System zarządzający musi mieć wbudowane API do komunikacji z systemami firm trzecich.
33. Ilość licencji system zarządzania musi odpowiadać ilość dostarczonych urządzeń i zapewniać pełne zarządzanie dostarczonymi urządzeniami I oprogramowaniem
34. System zarządzania musi być objęty 5 letnim wsparciem serwisowym producenta i musi zapewniać również dostęp do poprawek oraz nowych wersji oprogramowania oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia technicznego przez telefon, e-mail lub stronę www trybie 24x7x365 przez okres co najmniej 5 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowanego partnera serwisowego.

6.2.15 System kontroli dostępu

Dostarczony system kontroli dostępu musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. System kontroli dostępu musi zapobiegać przed nieautoryzowanym dostępem użytkowników lub urządzeń do sieci LAN oraz sieci WLAN. Dodatkowo systemu musi zapewniać kontrolę dostępu do zarządzania urządzeń sieciowych poprzez Telnet, SSH, CLI
2. System kontroli dostępu musi zapewniać możliwość instalacji wielu serwerów fizycznych lub wirtualnych zapewniających uwierzytelnianie i autoryzację użytkowników w sieci przy jednoczesnej centralnej konfiguracji wszystkich serwerów. Jeśli liczba serwerów kontroli dostępu jest osobno licencjonowana to wymagane jest dostarczenie licencji na min. 2 instancje
2. System kontroli dostępu musi zapewniać możliwość dodawania urządzeń (np. przełącznik, kontroler bezprzewodowy), które będą korzystały z systemu kontroli dostępu i pozwolić na konfigurację serwerów, z których będzie korzystać konkretne urządzenie. Dla każdego dodawanego urządzenia musi być zapewniona możliwość konfiguracji zestawu atrybutów RADIUS wysyłanych jako odpowiedź z autoryzacją oraz mechanizm realizacji reauthentykacji CoA.
3. System kontroli dostępu musi zapewniać możliwość reauthentykacji dla poszczególnych urządzeń z wykorzystaniem standardowego CoA RFC 3576/5176 lub z wykorzystaniem SNMP
4. System kontroli dostępu musi zapewniać obsługę RADIUS Accounting, który pozwoli na informowanie systemu kontroli dostępu o stanie dołączonego urządzenia – podłączone/niepodłączone.
5. System kontroli dostępu musi zapewniać uwierzytelnianie dołączonych do przełączników sieciowych lub bezprzewodowych punktów dostępowych z wykorzystaniem IEEE 802.1x oraz MAC Authentication.
6. System kontroli dostępu w ramach IEEE 802.1x musi zapewniać możliwość wykorzystywania następujących protokołów uwierzytelniania:
    a. EAP-TLS
    b. EAP-TTLS
    c. PEAP
    d. EAP-MD5
    e. PAP
    f. CHAP
    g. MS-CHAP
7. System kontroli dostępu musi zapewniać możliwość wizualizacji dołączanych systemów końcowych do sieci LAN i WLAN z możliwością prezentacji następujących parametrów:
    a. Stan systemu końcowego – np. włączony/wyłączony, błąd uwierzytelniania bądź autoryzacji
    b. MAC adres systemu końcowego
    c. Adres IP systemu końcowego
    d. Nazwa systemu końcowego – Hostname
    e. Typ systemu końcowego wraz z systemem operacyjnym – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows, MAC OS, IOS, Android
    f. Nazwa urządzenia, do którego dołączony jest system końcowy – może to być np. nazwa przełącznika sieciowego lub nazwa punktu dostępowego w przypadku sieci bezprzewodowej
    g. Adres IP urządzenia, do którego dołączony jest system końcowy –adres IP przełącznika sieciowego lub adres IP kontrolera bezprzewodowego, który przeprowadził uwierzytelnienie i autoryzację.
    h. Identyfikację portu, do którego dołączony jest system końcowy – identyfikacja sieci bezprzewodowej (SSID) lub portu przełącznika sieciowego.
    i. Typ uwierzytelniania systemu końcowego np. MAC authentication, IEEE 802.1x – EAP-TLS, PEAP, EAP-TTLS, EAP-MD5, Kerberos snooping itp.
    j. Nazwa przydzielonego profilu bezpieczeństwa.
8. System kontroli dostępu musi zapewniać możliwość wybrania z powyższej wizualizacji dowolnego systemu końcowego i wykonanie na nim następujących operacji:
    a. wymuszenie ponownego uwierzytelnienia
    b. sprawdzenie dostępności urządzenia z wykorzystaniem mechanizmu „ping”
    c. otworzenie okna terminala do urządzenia, które zrealizowało uwierzytelnienie – przełącznik, kontroler bezprzewodowy

d. otworzenie zarządzania http/https do urządzenia, które zrealizowało uwierzytelnienie – przełącznik, kontroler bezprzewodowy
e. przeniesienie systemu końcowego do wcześniej stworzonej grupy (np. wskazanie wykrytej drukarki i przeniesienie jej do grupy drukarek)
f. symulację procesu uwierzytelniania i autoryzacji – wizualizacja jak proces przebiegał i jakie warunki zadziałały dla danego systemu końcowego
g. usunięcie systemu końcowego z bazy danych
h. otworzenie mapy wskazującej lokalizację systemu końcowego (w przypadku przełącznika ma być wskazany przełącznik, gdzie nastąpiło uwierzytelnienie, a w przypadku sieci bezprzewodowej powinna być wskazana lokalizacja uwierzytelnionego urządzenia na mapie z wykorzystaniem triangulacji

9. System kontroli dostępu musi zapewniać przechowywanie historii uwierzytelnionych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana profilu bezpieczeństwa itp.
10. System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
11. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List
12. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
13. System kontroli dostępu do sieci musi posiadać informacje podsumowujące zawierające:
    a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
    b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
    c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
    d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
    e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
14. System kontroli dostępu do sieci, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 3000 urządzeń klienckich (adresów MAC).
15. System zarządzania musi być objęty 5 letnim wsparciem serwisowym producenta i musi zapewniać również dostęp do poprawek oraz nowych wersji oprogramowania oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia technicznego przez telefon, e-mail lub stronę www trybie 24x7x365 przez okres co najmniej 5 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowanego partnera serwisowego.
16. System zarządzania musi zapewniać wizualizację analityki aplikacji działających w sieci LAN
17. Poszczególne dodatkowe komponenty systemu zarządzania powinny być zintegrowane z podstawowym systemem zarządzającym i posiadać wspólny interfejs zarządzania www. W przypadku zaproponowania odrębnych systemów konieczne jest zapewnienie pojedynczego logowania do wszystkich systemów z wykorzystaniem Single Sign-On.
18. System musi zostać dostarczony z licencją dla 2000 użytkowników

6.2.16 System analizy aplikacji działających w sieci LAN i WLAN

Dostarczony System analizy aplikacji musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. System ma za zadanie wykrywanie i prezentowanie informacji o aplikacjach wykorzystywanych przez użytkowników sieci przewodowej oraz bezprzewodowej
2. System musi współpracować z dostarczonymi przełącznikami oraz punktami dostępowymi, które muszą dostarczać niezbędne informacje na potrzeby wykrywania aplikacji działających w sieci.

3. System analizy aplikacji musi zapewniać możliwość wykrywania aplikacji działających w sieci LAN i WLAN na podstawie dostarczonych wraz z systemem sygnatur ruchu sieciowego. Liczba sygnatur ruchu sieciowego nie może być mniejsza niż kilkanaście tysięcy i musi pozwalać na wykrywanie kilku tysięcy aplikacji
4. System analizy aplikacji musi zapewniać możliwość tworzenia własnych sygnatur wykrywania aplikacji na wartswie 7
5. System analizy aplikacji musi zapewniać możliwość tworzenia własnych sygnatur również poprzez definiowanie portu TCP/UDP, zakresu portów TCP/UDP, adresu IP serwera, zakresu adresów IP serwera oraz HTTP URL
6. Wykrywanie aplikacji musi się odbywać do warstwy 7 modelu OSI pozwalając na rozróżnianie aplikacji działających z wykorzystaniem tego samego portu TCP/UDP.
7. System musi zapewniać możliwość pomiaru czasu odpowiedzi sieci oraz czasu odpowiedzi aplikacji, co pozwoli na jednoznaczne określenie miejsca występujących problemów – sieć LAN, WLAN, czy sama aplikacja lub serwer, na którym aplikacja jest uruchomiona
8. System analizy aplikacji musi zapewniać możliwość monitorowania krytycznych dla pracy sieci aplikacji takich jak: DNS, DHCP, Radius, Kerberos, LDAP. Odbiegające od normy lub przekroczenie zdefiniowanych czasów odpowiedzi aplikacji musi być raportowane w postaci alarmów. Obsługa alarmów musi być zapewniona zgodnie z wymaganiami opisanymi dla platformy zarządzającej.
9. System analizy aplikacji musi zapewniać możliwość śledzenia wybranych lub własnych zdefiniowanych aplikacji.
10. System musi zapewniać możliwość tworzenia raportu zawierającego najgorzej działające aplikacje w sieci lub jej fragmencie (poprzez podanie lokalizacji). Identyfikacja najgorzej działającej aplikacji powinna się odbywać poprzez analizę czasów odpowiedzi sieci i czasów odpowiedzi aplikacji
11. System musi zapewniać możliwość uzyskania informacji o wykorzystaniu sieci przez poszczególne aplikacje w określonym czasie z uwzględnieniem.
    a. Zajmowanego pasma
    b. Liczby przepływów (flow)
    c. Liczby klientów
12. System musi zapewniać możliwość przeszukiwania gromadzonych informacji i wyświetlania raportów z możliwością filtrowania informacji na podstawie:
    a. Lokalizacji
    b. Grupy aplikacji – np. Mail, Cloud Storage, Social Networking, VPN itp.
    c. Wskazanej konkretnej aplikacji – np. Facebook, Google Mail, Google Calendar, Microsoft Office 365
    d. Rodziny urządzeń klienckich – np. Windows, Android, Linux,
    e. Zalogowanego klienta – przykładowo wszystkie aplikacje wykorzystywane przez użytkownika Jan Kowalski (nazwa użytkownika wynika z loginu użytkownika)
13. Wyszukiwane powyżej dane muszą mieć możliwość prezentacji w formie tabelarycznej lub w postaci wykresów
14. System musi posiadać mechanizmy do automatycznego, periodycznego wysyłania raportów pod wskazany adres email.
15. System musi posiadać możliwość wyświetlenia wszystkich przepływów (flow) otrzymanych z urządzeń sieciowych ze wskazaniem adresów źródłowego i docelowego, aplikacji, grupy aplikacji, czasu odpowiedzi sieci i czasu odpowiedzi aplikacji, lokalizacji oraz nazwy użytkownika pochodzącej z systemu kontroli dostępu.

6.2.17 System firewall – cluster

Dostarczony system firewall musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

1. Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

2. Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

3. Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 18 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP+ 10 Gb/s.
   - 8 gniazdami SFP 1Gb/s
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. Oprócz wkładek potrzebnych do podłączenia systemu firewall do przełączników typ 1 Zamawiający wymaga dostarczenia dodatkowych 4 wkładek SFP+ 10Gb
4. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
5. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
6. System musi być wyposażony w dwa zasilanie AC.

4. Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 7,7 mln. jednoczesnych połączeń oraz 490 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 77 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 50 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 9 Gbps.
6. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps.

5. Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 25 tokenów sprzętowych lub programowych, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

6. Polityki, Firewall

14. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
15. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
16. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
17. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
18. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

7. Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    - Obsługa protokołu Diffie-Hellman grup 19 i 20.
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

8. Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

9. Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

10. Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

11. Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

12. Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

13. Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

14. Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

15. Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

16. Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

17. Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

18. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

19. Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

20. Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

7 Wymagania funkcjonalne dla całości dostarczonego sprzętu i oprogramowania.

1. Wszystkie przełączniki, system zarządzania, system kontroli dostępu muszą pochodzić od jednego producenta
2. Wszystkie urządzenia: kontroler sieci bezprzewodowej, bezprzewodowe punkty dostępowe muszą pochodzić od jednego producenta
3. Wszystkie moduły światłowodowe oraz kable typu DAC muszą być produkcji producenta przełączników lub być przez niego certyfikowane
4. Wykonawca dostarczy odpowiednią ilość modułów światłowodowych potrzebnych do połączenia i wybudowania całej infrastruktury.
5. Przełączniki dystrybucyjne w punktach dystrybucyjnych IDFx muszą być ze sobą zestakowane za pomocą dedykowanych portów stackujących - zgodnie z zaleceniami producenta
6. Stos przełączników w punkcie dystrybucyjny IDFx musi być połączony z przełącznikami Typ1 w GPD za pomocą co najmniej 2 łączy 10Gb/s. Wymagane jest aby połączenia te były terminowane na 2 przełącznikach Typ1
7. W przypadku punktów dystrybucyjnych IDFx w których występuje pojedynczy przełącznik wymagane jest aby został połączony do GPD z wykorzystaniem 2 portów 10Gb/s. Połączenia muszą być terminowane na 2 przełącznikach Typ 1
8. W punkcie dystrybucyjnym IDF22 Zamawiający dopuszcza zastosowanie przełącznika Typ 7 (w tym przypadku wymagane jest aby został połączony do GPD do przełącznika typ 1 z wykorzystaniem 2

portów 10Gb/s) lub przełącznika Typ 8 (w tym przypadku wymagane jest aby został połączony do stosu przełącznika nadrzędnego Typ 6 w GPD z wykorzystaniem 2 portów 10Gb/s)

9. Wszystkie urządzenia muszą być objęte co najmniej 5 letnią gwarancją i wsparciem technicznym producenta obejmującym co najmniej: bezpłatną aktualizację oprogramowani, dostęp do wsparcia technicznego producenta (możliwość zgłaszania incydentów, rozwiązywanie problemów), dostęp do bazy wiedzy technicznej, wymianę uszkodzonego urządzenia w trybie NBD AHR.

8 Dodatkowe wymagania oraz warunki dostawy sprzętu i oprogramowania

1. Wykonawca opracuje plan dostaw realizowanych przez Wykonawcę. Plan dostaw musi zawierać:
   1.1. szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego,
   1.2. procedurę odbioru jakościowego,
   1.3. procedurę zmian terminów w trakcie realizacji dostaw,
   1.4. procedurę obsługi uszkodzeń sprzętu w trakcie dostawy,
   1.5. specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostaw.
2. Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego w godzinach od 8:00 do 15:00 w dni robocze od poniedziałku do piątku.
3. Odbiory sprzętu odbędą się w umówionym terminie przy obecności wyznaczonych pracowników Zamawiającego
4. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
5. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
6. Wykonawca zapewni we własnym zakresie środki transportu oraz zasoby ludzkie umożliwiające rozładunek i transport sprzętu do pomieszczeń wskazanych przez Zamawiającego.

7. Wykonawca jest zobowiązany do wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania.
8. Wykonawca ponosi koszt dostawy i zużycia mediów tj. energii elektrycznej, wody oraz innych mediów niezbędnych do wykonania zamówienia, przez cały czas trwania realizacji prac. Rozliczenie odbywać się będzie z Generalnym Wykonawcą, na podstawie odczytu z olicznikowanych przez Wykonawcę przyłączy wg stawek, które Generalny Wykonawca płaci za korzystanie z w/w mediów.
9. Wykonawca musi zapewnić, że wszystkie dostarczane sprzęty jak i oprogramowania są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca.
10. Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) niezbędny do jego prawidłowego podłączenia z siecią energetyczną Zamawiającego o parametrach: 230 V ± 10% , 50 Hz.
11. Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej, urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania.
12. Urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
13. Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
14. Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz wszystkie muszą być objęte gwarancją producenta.
15. Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
16. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
17. Wykonawca dostarczy wszystkie licencje i klucze licencyjne wymagane do działania dostarczanego sprzętu i oprogramowania.
18. W przypadku, gdy licencja oprogramowania objęta jest opłatą okresowej opieki wówczas Wykonawca poda wszystkie dane umożliwiające przedłużenie czasu opieki przez Zamawiającego

9 Rozwiązania równoważne

1. W sytuacji, gdy w opisie przedmiotu zamówienia wskazywane by były znaki towarowe wskazujące na konkretne rozwiązania, w myśl artykułu 29 ust. 3 ustawy PZP, Zamawiający dopuszcza składanie ofert na produktach równoważnych, pochodzących od innych producentów, spełniających minimalne wymagania określone w niniejszym Opisie Przedmiotu Zamówienia. Udowodnienie równoważności rozwiązań spoczywa na Wykonawcy.
2. Zawarte w dokumentacji nazwy producenta mają na celu jedynie wskazanie oczekiwanego przez Zamawiającego wzorca jakości przedmiotu Zamówienia.
3. Zamawiający stosując nazwy produktów wskazuje jedynie jakościowe wymagania, przez co dopuszcza składanie ofert zawierających równoważnych o parametrach jakościowych oraz cechach użytkowych, spełniających co najmniej przedstawione wymagania.
4. Obowiązkiem oferenta jest udowodnienie że produkt, przez niego zaproponowany spełnia te wymagania. Służyć mogą temu zapisy zawarte w ogólnie dostępnych źródłach, katalogach lub stronach internetowych producentów.
5. Wykonawca do udowodnienia równoważności jest zobowiązany do wykazania że oferowane przez niego urządzenia oraz ich części składowe spełniają wymagania minimalne poprzez dostarczenie kart charakterystyki technicznej, certyfikatów, katalogów, opisów technicznych dotyczących tych urządzeń oraz ich elementów. Zamawiający zastrzega sobie możliwość wezwania Wykonawcy do przedstawienia oferowanego rozwiązania w celu udowodnienia jego równoważności.

10 Dokumentacja powykonawcza

1. Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis połączeń zainstalowanych komponentów, instalacji i konfiguracji zainstalowanych komponentów dostarczonego rozwiązania. Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej, a także w wersji pdf. Na żądanie Zamawiającego Wykonawca dostarczy dokument w wersji drukowanej.
2. Dodatkowo Wykonawca opracuje dokumentację dla administratorów IT
3. Dokumentacja ta powinna zawierać co najmniej:
   3.1. Procedury aktualizacji standardowych elementów dostarczonego sprzętu
   3.2. Procedury włączenia i wyłączenia całości dostarczanego sprzętu w przypadku prac planowych.
4. Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji oprogramowania typu firmware. Procedury muszą obejmować wszystkie czynności, jakie należy

wykonać w celu monitorowania i utrzymania dostarczonej infrastruktury w poprawnym działaniu i zgodności z najnowszymi wersjami komponentów. Procedury zostaną przetestowane przez Zamawiającego przy udziale inżyniera Wykonawcy.

5. Dokumentacja dostarczona w trakcie realizacji zamówienia musi być wykonana w sposób spójny, zgodnie z dobrymi praktykami i zaleceniami budowy tego typu dokumentów.

10.1 Cechy dokumentacji dostarczonej w ramach projektu

1. Dokumentacja musi zawierać spis treści, strony dokumentów muszą posiadać numerację, załączniki muszą zostać opisane w sposób jasny i ułatwiający ich identyfikacje.
2. Całość dokumentacji projektowej musi być dostarczona w segregatorze umożliwiającym wypięcie dowolnej strony z dokumentacji i wpięcie jej z powrotem oraz dodatkowo w wersji elektronicznej w postaci pliku tekstowego w popularnym formacie (Microsoft Office, OpenOffice etc.).
3. Wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzować się muszą wysoką jakością, na którą będą miały wpływ takie czynniki jak:
   3.1. Czytelna i zrozumiała struktura zarówno poszczególnych dokumentów jak i całej dokumentacji z podziałem na rozdziały, podrozdziały i sekcje;
   3.2. Zachowanie standardów, a także sposób pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów oraz fragmentów tego samego dokumentu jak również całej dokumentacji;
   3.3. Kompletność dokumentu, rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia. Oznacza to w szczególności jednoznaczne i wyczerpujące przedstawienie wszystkich zagadnień w odniesieniu do systemu.
   3.4. Spójność i niesprzeczność dokumentu, rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
   3.5. Nomenklatura użyta w dokumentacji musi być spójna z dokumentacją przetargową.
4. Cała dokumentacja, o której mowa powyżej, musi być zaakceptowana przez Zamawiającego. Wykonawca przeniesie na Zamawiającego całość majątkowych praw autorskich do stworzonej dokumentacji.

11 Szkolenie

1. W ramach prowadzonego postępowania Wykonawca zapewni i opracuje:

1.1. szkolenia i warsztaty z dostarczanych produktów infrastruktury techniczno-systemowej. Przewidywana ilość uczestników warsztatów to do 3 osób wskazanych przez Zamawiającego,

1.2. plan warsztatów/szkoleń z zakresu wdrażanej infrastruktury. Warsztaty z zakresu każdego z typów urządzeń dostarczanych w ramach przedmiotowego postępowania powinny trwać przynajmniej:

LP	Nazwa	Ilość godzin*
1	Przełączniki	16
2	System kopii zapasowej	8
3	Sieć bezprzewodowa	8
4	System zarządzania	8
5	System kontroli dostępu	8
6	System firewall	8
7	Wirtualizacja	8

**Przy czym szkolenie nie może trwać dłużej niż 8 godzin dziennie*

2. Dodatkowo szkolenia powinny uwzględniać uwarunkowania montażu i instalacji sprzętu w infrastrukturze Zamawiającego.
3. Warsztaty odbędą się w siedzibie Zamawiającego lub online. Warsztaty będą prowadzone w języku polskim. Osoba prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne umożliwiające przekazanie informacji z zakresu wdrożonych rozwiązań. Wykonawca zobowiązany będzie do przygotowania i przedstawienia Zamawiającemu, co najmniej na 5 dni przed rozpoczęciem warsztatów, odpowiednich materiałów szkoleniowych oraz harmonogram warsztatów, włączając w to materiały dla uczestników. Zamawiający zastrzega sobie prawo do żądania wprowadzenia poprawek i zmian do materiałów szkoleniowych. Harmonogram zajęć powinien zawierać:
   3.1. informacje dotyczące czasu i miejsca realizacji danego warsztatu lub szkolenia,
   3.2. informacje dotyczące tematyki prowadzonych zajęć z podziałem na zajęcia teoretyczne i praktyczne
   3.3. informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy po zakończeniu szkoleń i warsztatów.
4. Każdy uczestnik szkolenia otrzyma certyfikat jego ukończenia. W ramach warsztatów/szkoleń uczestnicy otrzymają komplet materiałów szkoleniowych w wersji papierowej oraz elektronicznej obejmujących swoim zakresem całe szkolenie. Wszystkie materiały szkoleniowe muszą być w języku polskim lub angielskim. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych
5. Szkolenia/warsztaty mogą zostać zrealizowane w postaci voucherów z zakresu wdrażanych rozwiązań sprzętowych. Vouchery będą ważne co najmniej 12 miesięcy od dnia podpisania Protokołu Odbioru Końcowego.

6. Ponadto Zamawiający oczekuje dostawy 2 szt voucherów na szkolenia, z każdego niżej wymienionego zakresu. Vouchery muszą być ważne min. 12 miesięcy od daty dostawy. Vouchery będą uprawniać do odbycia szkolenia w autoryzowanych Centrach Szkoleniowych Producentów na terenie Polski:

LP	Nazwa
1	Wirtualizacja
2	Przełączniki
3	Sieć bezprzewodowa
4	System kopii zapasowej

12 Wdrożenie

Wykonawca jest zobowiązany przestrzegać obowiązujących norm oraz przepisów związanych z realizacją przedmiotu Zamówienia.

Wykonawca odpowiada za wszelkie uszkodzenia powstałe w ramach jego prac oraz jest zobowiązany do ich naprawy na własny koszt.

12.1 Prace wdrożeniowe

Zakres prac do wykonania:

- Instalacja dostarczonych urządzeń wchodzących w skład zaprojektowanej infrastruktury w istniejących szafach rack.
- Uporządkowanie połączeń kablowych w szafach
- Aktualizacja oprogramowania systemowego na wszystkich nowo dostarczanych przełącznikach do wersji wynikającej z projektu.
- Aktualizacja oprogramowania systemowego na wszystkich nowo dostarczanych serwerach i macierzach do wersji wynikającej z projektu.
- Aktualizacja oprogramowania systemowego na wszystkich nowo dostarczanych kontrolerach i bezprzewodowych punktach dostępowych sieci bezprzewodowej do wersji zalecanej przez producenta
- Aktualizacja oprogramowania systemowego na wszystkich nowo dostarczanych firewallach do wersji zalecanej przez producenta
- Podłączenie urządzeń do sieci LAN/WAN oraz oznaczenie połączeń (wykonanie trwałych etykiet na istotnych połączeniach kablowych w szafie z wykorzystaniem drukarki do wykonywania etykiet).
- Konfiguracja przełączników siec LAN zgodna z projektem.
- Konfiguracja infrastruktury serwerowo macierzowej wraz z wirtualizacją tej infrastruktury
- Konfiguracja systemu firewall zgodnie z projektem
- Konfiguracja systemów zarządzania, kontroli dostępu i systemu analizy aplikacji zgodnie z projektem
- Instalacja i konfiguracja kontrolerów sieci bezprzewodowej zgodnie z projektem
- Instalacja i konfiguracja bezprzewodowych punktów dostępowych zgodnie z projektem oraz załączonym planowaniem radiowym.
- Podłączenie urządzeń do zasilania.

- Wszystkie kable i przewody potrzebne do wybudowania działającej infrastruktury zgodnej z projektem są po stronie Wykonawcy oraz zawierają się w cenie oferty
- Fizyczna instalacja bezprzewodowych punktów dostępowych oraz niezbędne okablowanie do ich instalacji musi być wliczona w cenę oferty
- Zamawiający informuje, że gniazda dla bezprzewodowych punktów dostępowych zabudowane zostaną za sufitem podwieszanym z siatki cięto ciągnionej. Instalacja punktów dostępowych musi odbywać się w porozumieniu i w czasie uzgodnionym z aktualnym wykonawcą budowlanym obiektu. Zamawiający zaznacza, że Wykonawca musi podłączyć punkt dostępowy do gniazda w przestrzeni sufitowej oraz zamontować urządzenie na suficie z siatki cięto ciągnionej. Na etapie wdrożenie zostanie przedłożona instrukcja dotyczącą demontażu i montażu elementów podwieszanego sufitu.
- Zamawiający oczekuje by po wdrożeniu cała infrastruktura opisana w pkt 4.2 była gotowa do pracy
- Zamawiający zaznacza, że niektóre pomieszczenia (np. sale wystawowe) mają wysokość ok 10 metrów
- W niektórych pomieszczeniach (np. Sale wystawowe) bezprzewodowe punkty dostępowe muszą zostać przymocowane do kratownicy dachu.
- Instalacja i konfiguracja usług katalogowych oraz przygotowanie szablonów grup użytkowników. Dodatkowo Zamawiający wymaga integracji usług katalogowych z posiadaną przez Zamawiającego usługą Microsoft 365
- Przygotowanie szablonów nowych maszyn wirtualnych

13 Gwarancja wraz ze wsparciem technicznym

W ramach gwarancji zakres projektu modernizacji musi być objęty następującymi warunkami.

1. Całość dostarczonego sprzętu i oprogramowanie musi być objęta 5 letnim serwisem i gwarancją producenta.
2. Zgłoszenia awarii następować będzie w trybie 8/5/NBD i musi być dokonywane w postaci: zgłoszenia telefonicznego, z wykorzystaniem serwisu www lub za pomocą poczty elektronicznej. Wszystkie wymienione kanały komunikacji muszą być świadczone w języku polskim.
3. W ramach gwarancji Wykonawca zapewni następujące usługi:
   3.1. zdalne wsparcie techniczne Wykonawcy i producenta,
   3.2. wsparcie w miejscu instalacji,
   3.3. części zamienne oraz ich instalację,
   3.4. uaktualnienia oraz instalację oprogramowania firmware, jeżeli takie uaktualnienia są rekomendowane przez Producenta,
   3.5. dostęp do internetowych narzędzi serwisowych.
4. Wykonawca jest zobowiązany do niezwłocznego potwierdzenia przyjęcia zgłoszenia na adres poczty elektronicznej podany przez Zamawiającego lub telefonicznie - na numer podany podczas rejestracji zgłoszenia (czas reakcji).

5. Zamawiający musi mieć możliwość bezpośredniego zgłaszania awarii do producenta sprzętu oraz samodzielnej aktualizacji oprogramowania.
6. W okresie obowiązywania serwisu gwarancyjnego wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Uszkodzone dyski podlegające gwarancji stanowią własność Zamawiającego i pozostają u Zamawiającego, nie podlegają zwrotowi w ramach usługi gwarancyjnej.
7. Usługi gwarancyjne muszą być realizowane przez autoryzowany serwis producenta albo przez Wykonawcę na terenie Polski.

W ramach wsparcia technicznego Zamawiający wymaga:

1. Od momentu podpisania protokołu odbioru przez 12 miesięcy Wykonawca będzie realizował usługi wsparcia technicznego pracowników Zamawiającego w zakresie dostarczonego rozwiązania.
2. Usługa będzie świadczona na podstawie zgłoszeń rejestrowanych przez Zamawiającego w dedykowanym systemie 24h/d; 7 dni w tygodniu lub telefonicznie, na wskazany przez Wykonawcę numer telefonu: w dni robocze, od poniedziałku do piątku w godzinach 8:00-16:00. Zamawiający wymaga by czas rozwiązania błędów o wysokim priorytecie wynosił do 8 godzin w dni robocze.
3. Za zgłoszenie błędów o wysokim priorytecie uznawane będą wszelkie zgłoszenia wpływające na działanie wdrożonej infrastruktury w sposób uniemożliwiający korzystanie z całości lub części funkcjonalności. Dotyczy w szczególności sytuacji gdy oprogramowanie działa w ograniczonym zakresie, brak jest dostępności części infrastruktury, zmniejszona jest znacząco wydajność utrudniająca pracę użytkownikom.
4. Zamawiający przewiduje, że znacząca większość prac będzie wykonywana zdalnie. W tym celu Zamawiający umożliwi Wykonawcy zestawienie bezpiecznego tunelu VPN do połączenia z elementami infrastruktury Zamawiającego. W przypadku prac realizowanych na miejscu Zamawiający umożliwi dostęp do infrastruktury Wykonawcy najpóźniej w ciągu 2 dni roboczych od zgłoszenia.
5. W ramach usługi utrzymania Wykonawca będzie realizował następujące zadania:
   5.1. Przygotowywanie okresowych raportów i statystyk działania systemu
   5.2. Analizę logów oraz podejmowanie działań naprawczych
   5.3. pomoc w rozwiązywaniu problemów z działaniem wdrożonego systemu
   5.4. konsultacje w zakresie zmian konfiguracji elementów wdrożonego systemu
   5.5. Przekazywanie zgłoszeń do serwisu producenta i nadzór nad ich obsługą
   5.6. Zarządzanie bezpieczeństwem, analiza logów pod kątem zdarzeń z obszaru bezpieczeństwa i podejmowanie niezbędnych działań

5.7. Realizacja procedur i wytycznych dostarczonych przez Zamawiającego

5.8. Weryfikację poprawności wykonywania polityk i podejmowanie działań korekcyjnych

5.9. Współpracę z innymi administratorami usług i innymi podmiotami świadczącymi usługi informatyczne

5.10. Optymalizacje sytemu w celu poprawy wydajności.