Załącznik nr 1

Szczegółowy Opis Przedmiotu Zamówienia

Instytucja:
Sąd Okręgowy w Rzeszowie
Plac Śreniawitów 3, 35-959 Rzeszów

Rzeszów, wrzesień 2020

Spis treści

1 Opis stanu aktualnego.

Sieć komputerowa Sądu Okręgowego w Rzeszowie zbudowana jest w większości w oparciu o okablowanie strukturalne kat 5e. Okablowanie strukturalne sieci LAN posiada stosowne certyfikaty i pomiary. Sieć LAN wykorzystuje 4 punkty dystrybucyjne (PD). Pomiędzy PD występują połączenia światłowodowe. W obrębie sieci LAN Sądu działa również jednostka zdalna – połączenie vDSL.

1.1 Centralny punkt dystrybucyjny – stan obecny.

Tabela 1. Zestawienie pozycji dla CPD.

Szafa nr 1				
Lp.	Nazwa	Opis	ilość	Ilość portów
1	3Com 4900 12 port	12 portów 1000BASE-SX	1	12
2	3Com 4228G	24 x 10/100 + 2 x GBIC + 2 x 10/100/1000	1	24
3	CISCO C2960G-24TC-L	24 x Port 10/100/1000	2	48
4	3Com 4200	24 x network node - Ethernet 10Base-T/100Base-TX - RJ-45	1	24
5	D-Link DES-3852	48 x 10/100Mbps	1	48
			Razem:	156
Szafa nr 2				
1	D-Link DES-3052P	48 x RJ-45 10/100 Mbps	2	96

Źródło: opracowanie własne

1.2 Punkt dystrybucyjny – PD1 – stan obecny.

Tabela 2. Zestawienie pozycji dla PD1.

Szafa nr 1				
Lp.	Nazwa	Opis	ilość	Ilość portów
1	D-Link DES-3828	24 x 10/100 + 2 x 10/100/1000 Combo	1	24
2	3Com 4228G	24 x 10/100 + 2 x GBIC + 2 x 10/100/1000	1	24
3	D-Link DES-3852	48 x 10/100Mbps	1	48
			Razem:	96
Szafa nr 2				
1	D-Link DES-3052P	48 x RJ-45 10/100 Mbps	1	48
2	HP 2620-48	48 x RJ-45 10/100 Mbps	1	48
			Razem:	96

Źródło: opracowanie własne

1.3 Punkt dystrybucyjny – PD2 – stan obecny.

Tabela 3. Zestawienie pozycji dla PD2.

Szafa nr 1				
Lp.	Nazwa	Opis	ilość	Ilość portów
1	D-Link DES-3828	24 x 10/100 + 2 x 10/100/1000 Combo	1	24
2	3Com 4228G	24 x 10/100 + 2 x GBIC + 2 x 10/100/1000	2	48

3	3Com 4200	24 x network node - Ethernet 10Base-T/100Base-TX - RJ-45	1	24
4	D-Link DES-3852	48 x 10/100Mbps	1	48
			Razem:	144

Źródło: opracowanie własne

1.4 Punkt dystrybucyjny – PD3 – stan obecny.

Tabela 4. Zestawienie pozycji dla PD3.

Szafa nr 1				
Lp.	Nazwa	Opis	ilość	Ilość portów
1	D-Link DES-3828	24 x 10/100 + 2 x 10/100/1000 Combo	1	24
2	HP 2620-48	48 x RJ-45 10/100 Mbps	1	48
3	3Com 4200	24 x network node - Ethernet 10Base-T/100Base-TX - RJ-45	1	24
4	3Com 4228G	24 x 10/100 + 2 x GBIC + 2 x 10/100/1000	1	24
5	D-Link DES-3052P	48 x RJ-45 10/100 Mbps	1	48
			Razem:	168

Źródło: opracowanie własne

1.5 Punkt dystrybucyjny – Punkt zdalny – stan obecny.

Tabela 5. Zestawienie pozycji dla punktu zdalnego.

Szafa nr 1				
Lp.	Nazwa	Opis	ilość	Ilość portów
1	3Com 4200	24 x network node - Ethernet 10Base-T/100Base-TX - RJ-45	1	24
			Razem:	24

Źródło: opracowanie własne

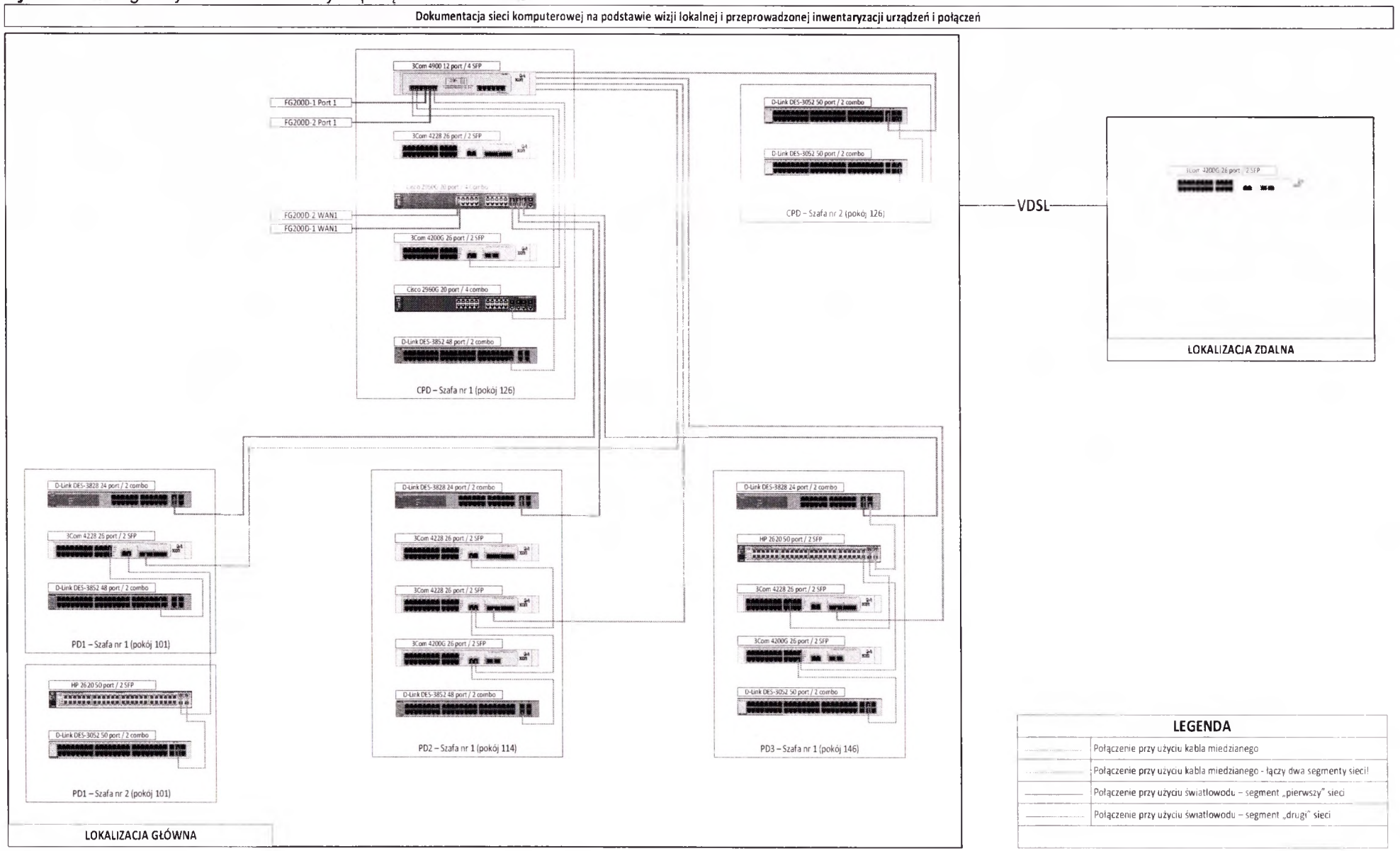
Na poniższych schematach Zamawiający przedstawił obecny schemat logiczny sieci LAN wraz z używanymi przełącznikami sieci LAN, oraz zaprezentował istniejące okablowanie strukturalne w zakresie łączy światłowodowych.

Wykonawca zobowiązany jest wykorzystać istniejące okablowanie światłowodowe do łączenia punktów PD.

Na bazie istniejącego okablowania światłowodowego Wykonawca musi dobrać odpowiednie moduły GBIC (SFP/SFP+) do zaoferowanych w postepowaniu przełączników sieciowych celem spełnienia wymogów połączeniowych na zaprezentowanym docelowym logicznym schemacie połączeń sieci LAN.

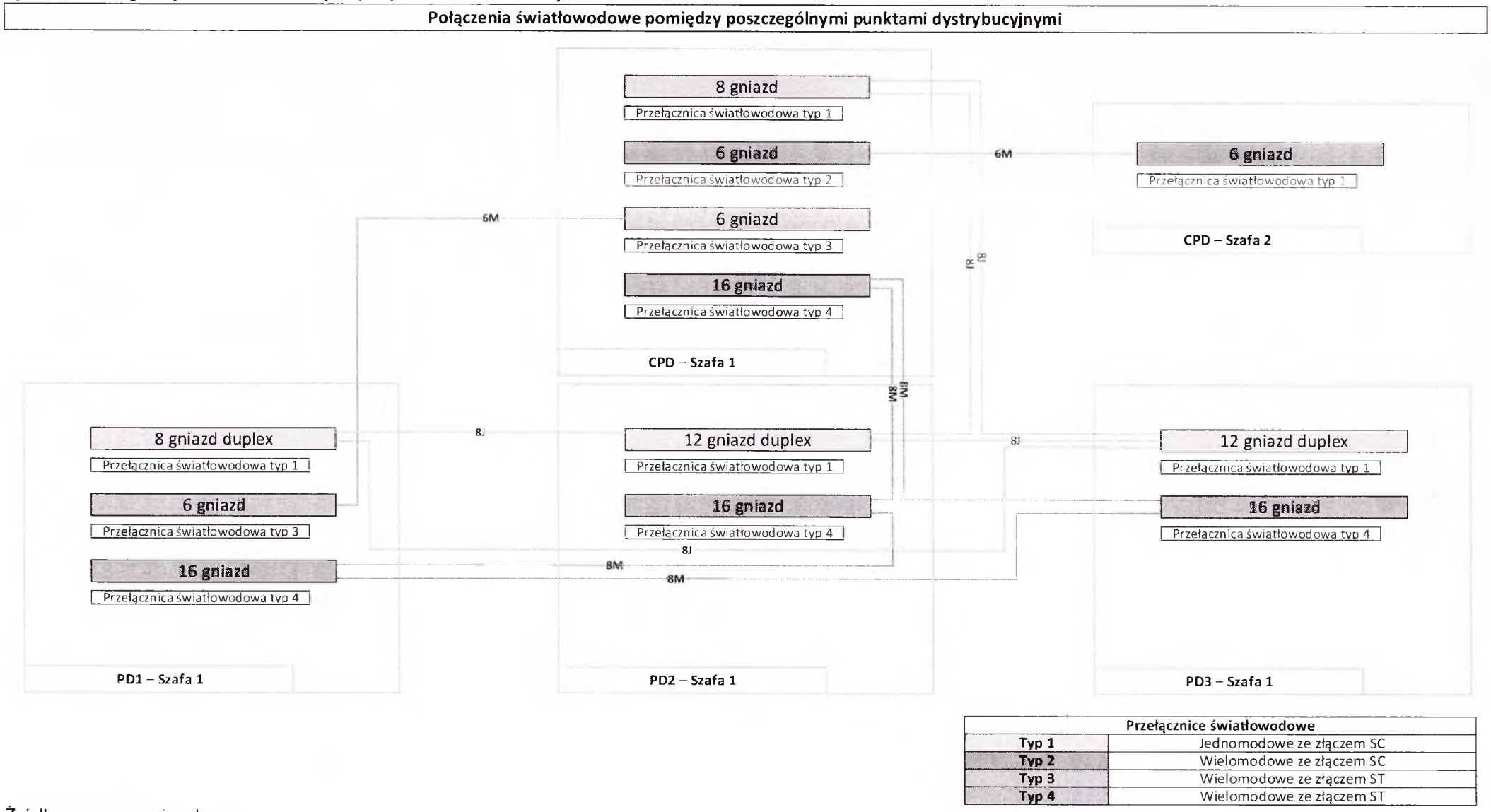
Koszty związane z modułami GBIC oraz patchordami Wykonawca musi uwzględnić w ofercie jako element wyposażenia przełącznika sieci LAN.

Rysunek 1. Logiczny schemat aktualnych połączeń sieci LAN.



Źródło: opracowanie własne

Rysunek 2. Logiczny schemat aktualnych połączeń światłowodowych.



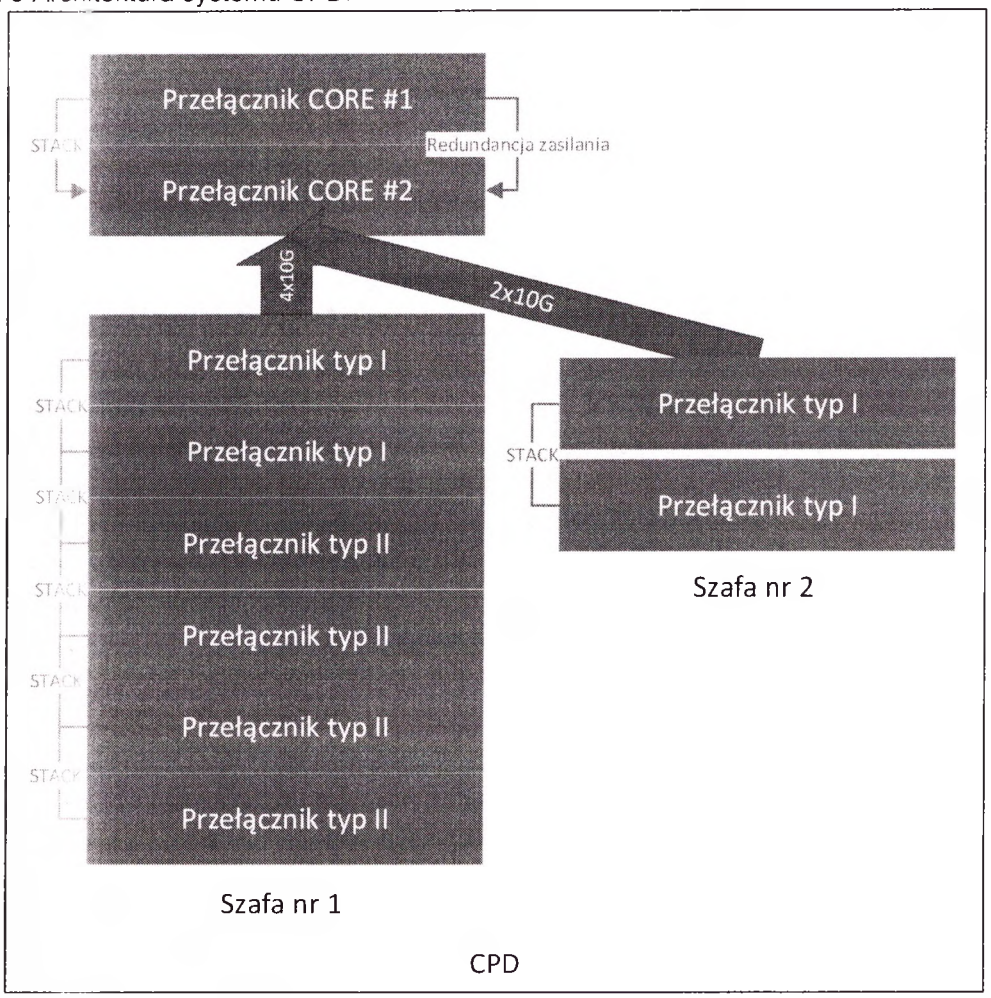
Przełącznice światłowodowe	
Typ 1	Jednomodowe ze złączem SC
Typ 2	Wielomodowe ze złączem SC
Typ 3	Wielomodowe ze złączem ST
Typ 4	Wielomodowe ze złączem ST

Źródło: opracowanie własne

1.6 Niezbędna infrastruktura.

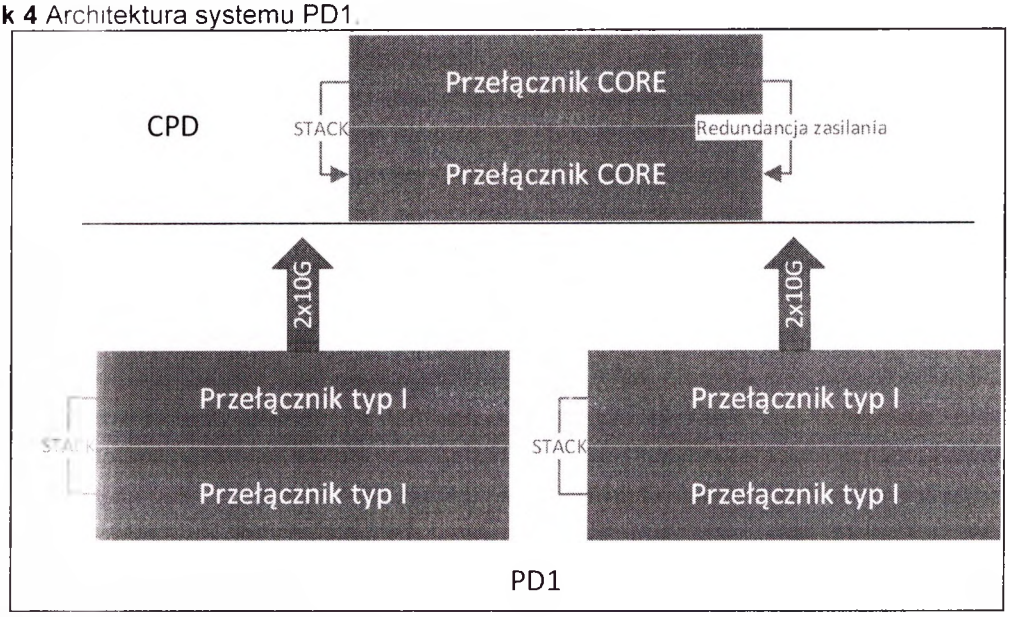
Celem zobrazowania przyjętych przez Zamawiającego w niniejszym projekcie, postepowaniu przetargowym rozwiązań technicznych i technologicznych, na poniższym schemacie przedstawiono architekturę wymaganego systemu do zrealizowania przez Wykonawcę.

Rysunek 3 Architektura systemu CPD.



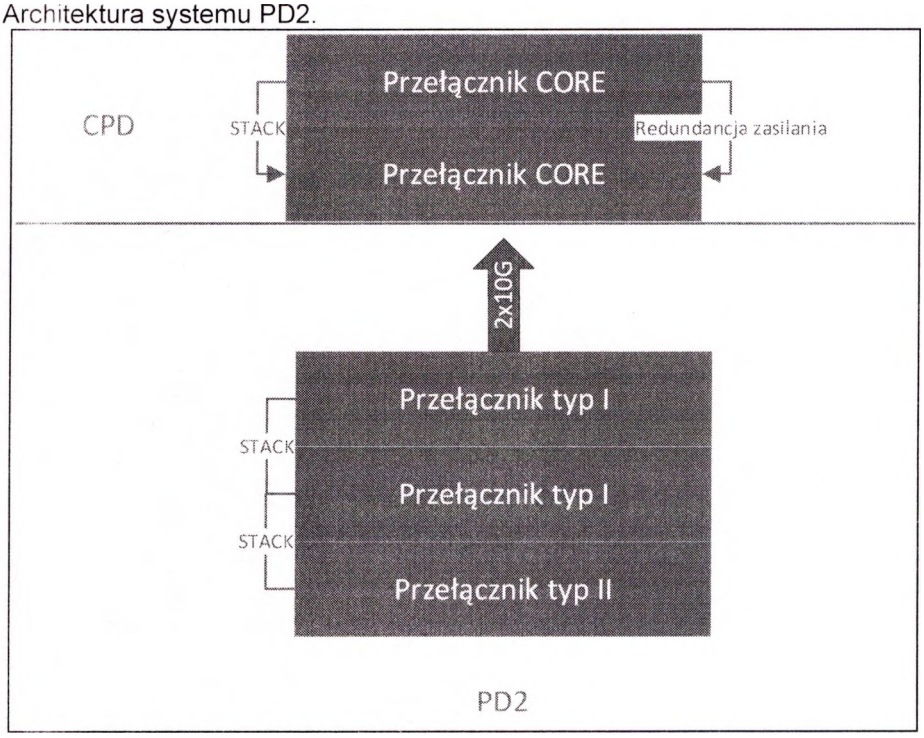
Źródło: opracowanie własne

Rysunek 4 Architektura systemu PD1.



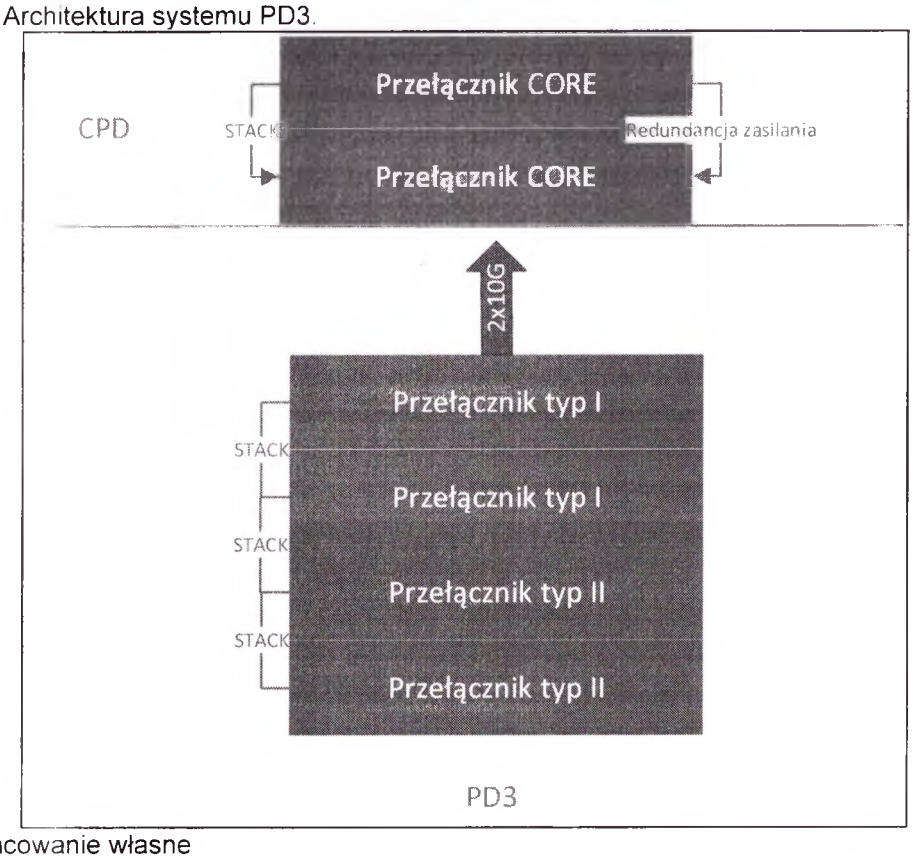
Źródło: opracowanie własne

Rysunek 5 Architektura systemu PD2.



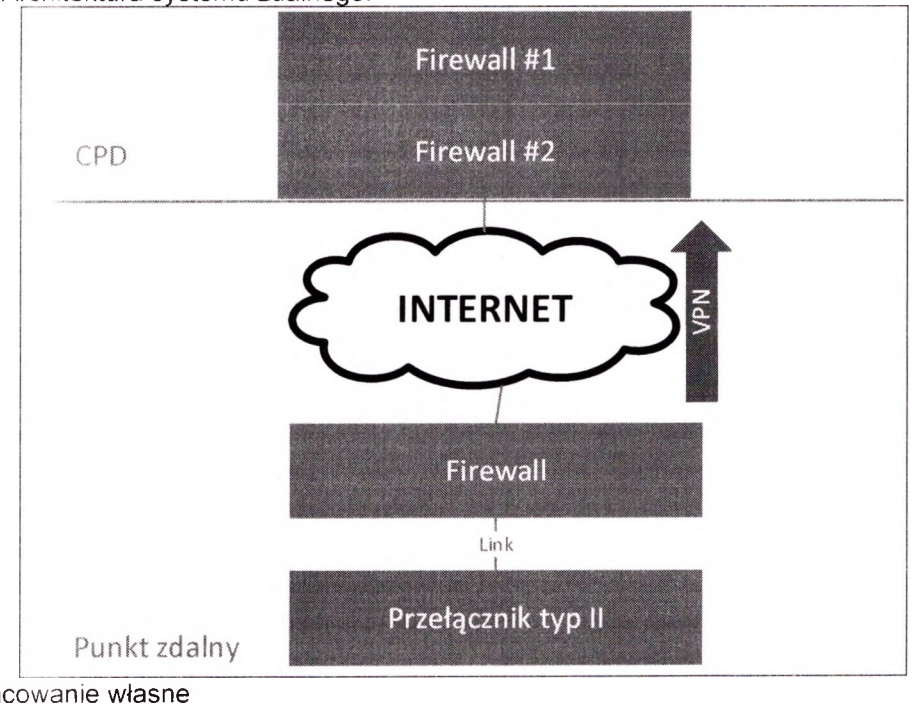
Źródło: opracowanie własne

Rysunek 6 Architektura systemu PD3.



Źródło: opracowanie własne

Rysunek 7 Architektura systemu zdalnego.



Źródło: opracowanie własne

2 Zadanie: Modernizacja sieci LAN – urządzenia aktywne przełączniki.

Zadaniem Wykonawcy jest modernizacja obecnej sieci LAN Sądu Okręgowego w Rzeszowie. Należy to wykonać poprzez wymianę istniejących urządzeń aktywnych w punktach PD na nowe urządzenia aktywne wymagane przez Zamawiającego. Poniżej przedstawiono wymagania techniczne dla nowych urządzeń – przełączniki sieci LAN - w zestawieniu całościowym oraz z podziałem na PD. Dodatkowo opisano wymogi w stosunku do ich instalacji i konfiguracji wraz z opisem gwarancji, asysty stanowiskowej oraz opieki serwisowej.

Tabela 6. Zestawienie pozycji dla zadania modernizacja sieci LAN.

lp.	Nazwa	ilość	ilość portów na przełącznik	ilość portów	Komentarz
1	Przełącznik CORE	2	12	24	**Przełącznik szkieletowy 10G.** Każdy z punków pośrednich zostanie zapięty do tego przełącznika. Przełączniki będą pracowały w stacku - dedykowany link połączeniowy.
2	Przełącznik typ I	12	48	576	**Przełącznik dostępowy** oraz zapewniający dostęp do przełącznika szkieletowego 10G.
3	Przełącznik typ II	8	48	384	**Przełącznik dostępowy** - pracujący w stacku.

Źródło: Opracowanie własne

Tabela 7. Zestawienie przełączników – CPD po modernizacji.

Szafa nr 1				
lp.	**Nazwa**	**ilość**	**ilość portów na przełącznik/razem**	**Komentarz**
1	Przełącznik CORE	2	12/24	**Przełącznik szkieletowy 10G.** Każdy z punków pośrednich zostanie zapięty do tego przełącznika. Przełączniki będą pracowały w stacku - dedykowany link połączeniowy.
2	Przełącznik typ I	2	48/96	**Przełącznik dostępowy** oraz zapewniający dostęp do przełącznika szkieletowego 10G.
3	Przełącznik typ II	4	48/192	**Przełącznik dostępowy** - pracujący w stacku.
Szafa nr 2				
lp.	**Nazwa**	**ilość**	**ilość portów na przełącznik/razem**	**Komentarz**
1	Przełącznik typ I	2	48/96	**Przełącznik dostępowy** oraz zapewniający dostęp do przełącznika szkieletowego 10G.

Źródło: opracowanie własne

Tabela 8. Zestawienie przełączników – PD1 po modernizacji.

Szafa nr 1				
lp.	**Nazwa**	**ilość**	**ilość portów na przełącznik/razem**	**Komentarz**
1	Przełącznik typ I	2	48/96	**Przełącznik dostępowy** oraz zapewniający dostęp do przełącznika szkieletowego 10G.
Szafa nr 2				
lp.	**Nazwa**	**ilość**	**ilość portów na przełącznik/razem**	**Komentarz**
1	Przełącznik typ I	2	48/96	**Przełącznik dostępowy** oraz zapewniający dostęp do przełącznika szkieletowego 10G.

Źródło: opracowanie własne

Tabela 9. Zestawienie przełączników – PD2 po modernizacji.

Szafa nr 1				
lp.	**Nazwa**	**ilość**	**ilość portów na przełącznik/razem**	**Komentarz**
1	Przełącznik typ I	2	48/96	**Przełącznik dostępowy** oraz zapewniający dostęp do przełącznika szkieletowego 10G.
2	Przełącznik typ II	1	48/48	**Przełącznik dostępowy** - pracujący w stacku.

Źródło: opracowanie własne

Tabela 10. Zestawienie przełączników – PD3 po modernizacji.

Szafa nr 1				
lp.	**Nazwa**	**ilość**	**ilość portów na przełącznik/razem**	**Komentarz**
1	Przełącznik typ I	2	48/96	**Przełącznik dostępowy** oraz zapewniający dostęp do przełącznika szkieletowego 10G.
2	Przełącznik typ II	2	48/96	**Przełącznik dostępowy** - pracujący w stacku.

Źródło: opracowanie własne

Tabela 11. Zestawienie przełączników – Punkt zdalny po modernizacji.

Szafa nr 1				
lp.	**Nazwa**	**ilość**	**ilość portów na przełącznik/razem**	**Komentarz**
1	Przełącznik typ II	1	48/48	**Przełącznik dostępowy**.

Źródło: opracowanie własne

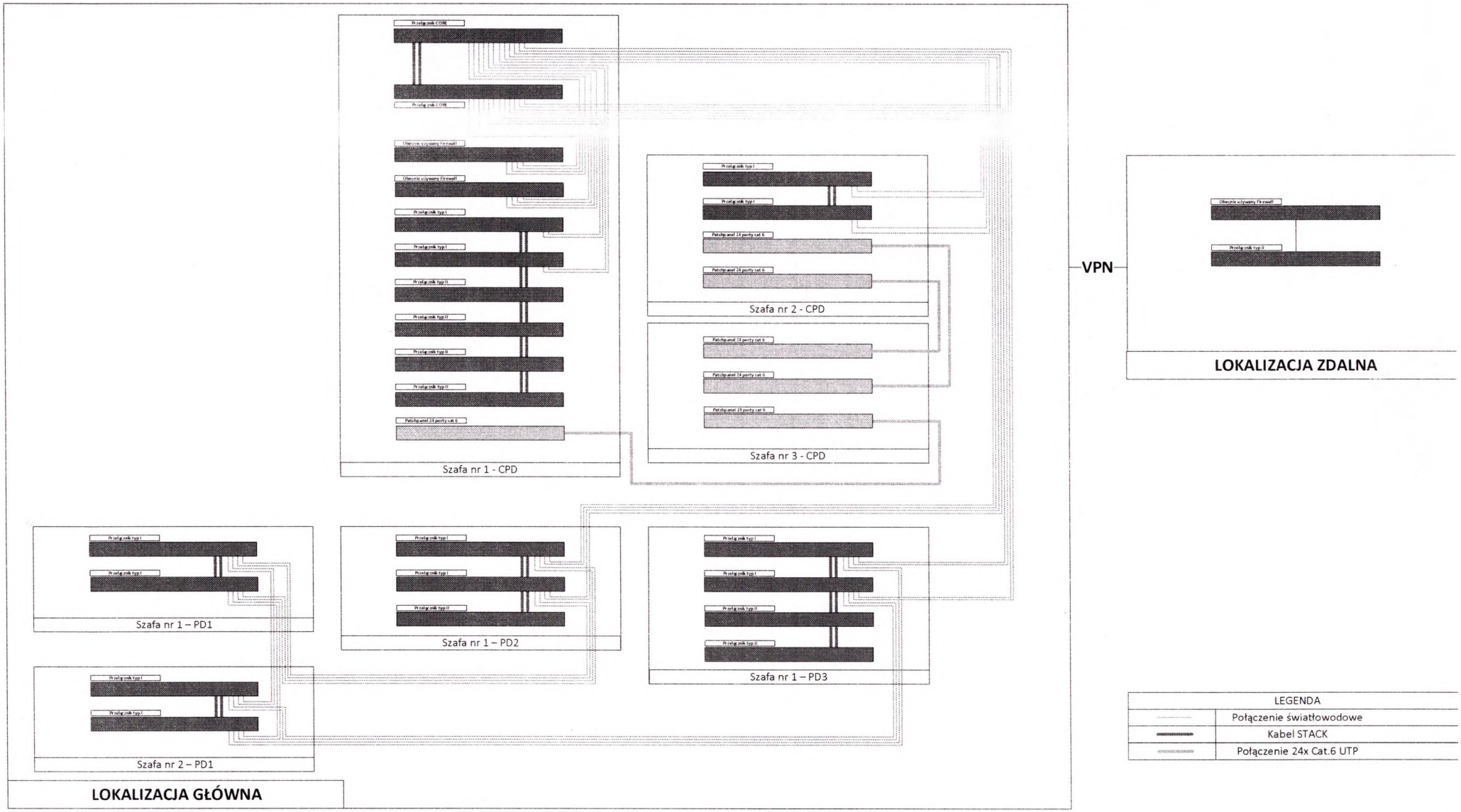
Modernizacja sieci LAN ma uwzględniać w miarę możliwości eliminację pojedynczego punktu awarii (np.: redundancja połączeń poprzez zastosowanie podwójnych linków sieciowych w przełącznikach, zastosowanie mechanizmu stackowania – łączenia logicznego, podwójnych zasilaczy itp.).

Wizualizacja oczekiwanego rozwiązania schematu połączeń znajduje się na poniższym rysunku.

Zakłada się zrealizowanie połączeń bezpośrednich z CPD do punktów dostępowych PD2 i PD3 a następnie, z braku bezpośredniego połączenia światłowodem jednomodowym z CPD do PD1, z wykorzystaniem PD2 i PD3. Utworzony zostanie w ten sposób pierścień, który zostanie rozpięty przez protokół STP, a którego głównym węzłem będzie CPD – przełączniki CORE.

Rysunek 8. Logiczny schemat połączeń sieci LAN po zmianach.

Koncepcja topologii sieciowej proponowanego rozwiązania zorientowana na redundancję połączeń i wysoką niezawodność



Źródło: opracowanie własne

2.1 Przełączniki sieci LAN – wymagania minimalne.

W niniejszym postepowaniu przewiduje się zakup urządzeń aktywnych do sieci LAN (switche – element dostępu do sieci). Urządzenia te powinny na bazie okablowania strukturalnego sieci LAN utworzyć platformę komunikacji (wymiany danych) dla systemów informatycznych Sądu Okręgowego w Rzeszowie.
Projekt zakłada wykorzystanie przełączników z modułami SFP/SFP+ (1/10Gbps). Do przełączników zostaną podłączone miedzy innymi:

- Serwery,
- Porty zarządzające macierzy,
- Komputery.

Przełączniki będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokoły STP (protokół drzewa rozpinającego).

Zamawiający wymaga aby Wykonawca zrealizował w ramach projektu dołączenie i konfigurację stworzonej infrastruktury sieci LAN (przełączniki LAN) do istniejącego klastra Firewall pracującego w trybie HA. Zapewniając komunikacje na warstwie trzeciej modelu ISO/OSI – L3 (warstwa sieciowa) wraz z dostępem do Internetu.

Tabela 12. Opis funkcjonalności przełącznika CORE.

Szczegółowy opis wymagań minimalnych dla przełącznika CORE – 2 szt.
1. Przełącznik stackowalny wyposażony w 12 portów SFP+
2. Przełącznik musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco" (ang. hot swap). Dostępny minimum 4-portowy moduł 10Gigabit Ethernet z gniazdami SFP+
3. Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000Base-SX, 1000Base-LX/LH zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH)
4. Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów: a. Przepustowość w ramach stosu min. 480Gb/s b. Min. 8 urządzeń w stosie c. Zarządzanie poprzez jeden adres IP d. Możliwość tworzenia połączeń cross-stack EtherChannel (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad e. Przełączniki muszą umożliwiać współdzielenie mocy zasilaczy tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE)
5. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów
6. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne. Przełącznik musi być wyposażony w drugi redundantny zasilacz.
8. Przełącznik musi posiadać możliwość rozbudowy o funkcję kontrolera sieci bezprzewodowej WiFi: a. Przełącznik musi zapewniać centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415), w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym (RRM) po zainstalowaniu odpowiedniej licencji b. Przepustowość dla sieci WiFi nie mniejsza niż 20Gb/s c. Obsługa minimum 2000 klientów sieci WiFi
9. Szybkość przełączania minimum 220 Mpps dla pakietów 64-bajtowych, 320 Gbps.
10. Minimum 4GB pamięci DRAM i 4GB pamięci flash
11. Obsługa minimum : a. 1.000 sieci VLAN b. 32.000 adresów MAC

c. 24.000 tras routingu
12. Obsługa protokołu NTP
13. Obsługa IGMPv1/2/3
14. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree
    b. IEEE 802 1s Multi-Instance Spanning Tree
15. Obsługa protokołu LLDP i LLDP-MED
17. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
18. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    g. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
    h. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)
    i. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    j. Możliwosc autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
    k. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
19. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    b. Implementacja co najmniej 4 kolejek dla ruchu wyjściowego dla sieci WLAN dla obsługi ruchu o różnej klasie obsługi
    c. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek
    d. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    e. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    f. Mozliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik
    g. Kontrola sztormów dla ruchu broadcast/multicast/unicast
    h. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
21. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych
22. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)

23. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 24.000 . Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow
24. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
25. Dedykowany port Ethernet do zarządzania out-of-band
26. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
27. Urządzenie musi być wyposażone w port konsoli USB
28. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją
29. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
30. Możliwość montażu w szafie rack 19". Wysokość urządzenia nie może przekraczać 1 RU
31. Moduły SFP/SFP+ w ilości zgodnej ze schematem połączenia. Moduły SFP/SFP+ od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia
32. Moduły stakujące w ilości zgodnej ze schematem połączenia. Moduły od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia.
33. Kable stakujace w ilości zgodnej ze schematem połączenia. Kable od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia.

Źródło: opracowanie własne

Tabela 13. Opis funkcjonalności przełącznika dostępowego typ I.

Szczegółowy opis wymagań minimalnych dla przełącznika dostępowego typ I – 12 szt.
1. Typ i liczba portów: 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP
2. Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami) 740W/1440W
3. Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: 3.1. Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U 3.2. Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
4. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: 4.1. Przepustowość w ramach stosu - 80Gb/s 4.2. 8 urządzeń w stosie 4.3. Zarządzanie poprzez jeden adres IP 4.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5. Zasilanie i chłodzenie 5.1. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap) 5.2. Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia 5.3. Redundantne wentylatory
6. Parametry wydajnościowe: 6.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) 6.2. Bufor pakietów – 6MB 6.3. Pamięć DRAM – 2GB 6.4. Pamięć flash – 4GB 6.5. Obsługa 6.5.1 1024 sieci VLAN

6.5.2. 16.000 adresów MAC
6.5.3 3.000 tras IPv4
6.5.4. 1.500 tras IPv6

7. Obsługa protokołu NTP
8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
9. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   9.1. IEEE 802.1w Rapid Spanning Tree
   9.2. Per-VLAN Rapid Spanning Tree (PVRST+)
   9.3. IEEE 802.1s Multi-Instance Spanning Tree
   9.4. Obsługa 64 instancji protokołu STP
10. Obsługa protokołu LLDP i LLDP-MED.
11. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
12. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
13. Możliwość uruchomienia funkcji serwera DHCP
14. Mechanizmy związane z bezpieczeństwem sieci:
    14.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
    14.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    14.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    14.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    14.5. Mozliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    14.6. Mozliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    14.7. Mozliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
    14.8. Mozliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
    14.9. 1500 wpisów dla list kontroli dostępu (Security ACE)
    14.10. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)
    14.11. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    14.12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
    14.13. Mozliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
    14.14. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
    14.15. mozliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host)
    14.16. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)
    14.17. Funkcja Private VLAN
15. Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania
    16.1. Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne, jednoukładowe rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny
    16.2. Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego
    16.3. Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane.

Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.

16. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    16.1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    16.2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek
    16.3. Mozliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    16.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    16.5. Mozliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting)
    16.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast
    16.7. Mozliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
17. Obsługa protokołów routingu:
    17.1. Routing statyczny dla IPv4 i IPv6
    17.2. Routing dynamiczny – RIP, OSPF
    17.3. Policy-based routing (PBR)
    17.4. Obsługa protokołu redundancji bramy (VRRP)
18. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
19. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
20. Możliwość uruchamiania skryptów Python poprzez Embedded Event Manager
21. Zarządzanie
    21.1. Port konsoli
    21.2. Dedykowany port Ethernet do zarządzania out-of-band
    21.3. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
    21.4. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
    21.5. Mozliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
    21.6. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych
    21.7. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą
    21.8. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
22. Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU
23. Wsparcie dla protokołu LISP zgodnie z RFC 6830
24. Obsługa zaawansowanych protokołów routingu
    24.1. IS-IS dla IPv4
    24.2. Routing multicastów - PIM-SM, PIM-SSM
    24.3. Multicast Source Discovery Protocol (MSDP)
    24.4. VRF-Lite
25. Możliwość enkapsulacji ruchu w pakiety VXLAN
26. próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 16.000 strumieni
27. Wbudowany analizator pakietów
28. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie [Oprogramowanie DNA Advantage]
29. Możliwość integracji urządzenia z systemem SDN dla sieci LAN w celu zbierania statystyk, występujących trendów w sieci, monitorowania zdrowia urządzenia jak i podłączonych do urządzenia klientów
30. Wyposażenie urządzenia

30.1. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy –
30.2. Moduły SFP/SFP+ w ilości zgodnej ze schematem połączenia. Moduły SFP/SFP+ od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia
32. Moduły stakujące w ilości zgodnej ze schematem połączenia. Moduły od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia.
33. Kable stakujace w ilości zgodnej ze schematem połączenia. Kable od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia.

Źródło: opracowanie własne

Tabela 14. Opis funkcjonalności przełącznika dostępowego typ II.

Szczegółowy opis wymagań minimalnych dla przełącznika dostępowego typ II – 8 szt.
1. Typ i liczba portów: 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x1G SFP lub RJ45
2. Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami) 740W/1440W
3. Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: 3.1. Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U 3.2. Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
4. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: 4.1. Przepustowość w ramach stosu - 80Gb/s 4.2. 8 urządzeń w stosie 4.3. Zarządzanie poprzez jeden adres IP 4.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5. Zasilanie i chłodzenie 5.1. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap) 5.2. Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia 5.3. Redundantne wentylatory
6. Parametry wydajnościowe: 6.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) 6.2. Bufor pakietów – 6MB 6.3. Pamięć DRAM – 2GB 6.4. Pamięć flash – 4GB 6.5. Obsługa 6.5.1. 1024 sieci VLAN 6.5.2. 16.000 adresów MAC 6.5.3. 3.000 tras IPv4 6.5.4. 1.500 tras IPv6
7. Obsługa protokołu NTP
8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
9. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: 9.1. IEEE 802.1w Rapid Spanning Tree 9.2. Per-VLAN Rapid Spanning Tree (PVRST+) 9.3. IEEE 802.1s Multi-Instance Spanning Tree 9.4. Obsługa 64 instancji protokołu STP
10. Obsługa protokołu LLDP i LLDP-MED.
11. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
12. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
13. Możliwość uruchomienia funkcji serwera DHCP
14. Mechanizmy związane z bezpieczeństwem sieci:

14.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
14.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
14.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
14.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
14.5. Mozliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
14.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
14.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
14.8. Mozliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
14.9. 1500 wpisów dla list kontroli dostępu (Security ACE)
14.10. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)
14.11. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
14.12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
14.13. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
14.14. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
14.15. Mozliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host)
14.16. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)
14.17. Funkcja Private VLAN

15. Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania
16.1 Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne, jednoukładowe rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny
16.2. Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego
16.3. Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.

16. Mechanizmy związane z zapewnieniem jakości usług w sieci:
16.1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
16.2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek
16.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
16.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
16.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting)
16.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast
16.7. Mozliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

17. Obsługa protokołów routingu:

17.1. Routing statyczny dla IPv4 i IPv6
17.2. Routing dynamiczny – RIP, OSPF
17.3. Policy-based routing (PBR)
17.4. Obsługa protokołu redundancji bramy (VRRP)
18. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
19. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
20. Możliwość uruchamiania skryptów Python poprzez Embedded Event Manager
21. Zarządzanie
21.1. Port konsoli
21.2. Dedykowany port Ethernet do zarządzania out-of-band
21.3. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
21.4. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
21.5. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
21.6. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych
21.7. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą
21.8. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
22. Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU
23. Wsparcie dla protokołu LISP zgodnie z RFC 6830
24. Obsługa zaawansowanych protokołów routingu
24.1. IS-IS dla IPv4
24.2. Routing multicastów - PIM-SM, PIM-SSM
24.3. Multicast Source Discovery Protocol (MSDP)
24.4. VRF-Lite
25. Możliwość enkapsulacji ruchu w pakiety VXLAN
26. próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 16.000 strumieni
27. Wbudowany analizator pakietów
28. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
29. Możliwość integracji urządzenia z systemem SDN dla sieci LAN w celu zbierania statystyk, występujących trendów w sieci, monitorowania zdrowia urządzenia jak i podłączonych do urządzenia klientów
30. Wyposażenie urządzenia
30.1. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy –
30.2. Moduły SFP/SFP+ w ilości zgodnej ze schematem połączenia. Moduły SFP/SFP+ od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia
32. Moduły stakujące w ilości zgodnej ze schematem połączenia. Moduły od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia.
33. Kable stakujace w ilości zgodnej ze schematem połączenia. Kable od producenta przełącznika celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzenia.

Źródło: opracowanie własne

2.2 Wymagania dotyczące instalacji i konfiguracji.

Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa.

Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.

W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową.

Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:

1) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia
2) Sporządzenia Dokumentacji Systemu według której nastąpi realizacja.
3) Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia W szczególności:
    a) testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności,
    b) sposób odbioru uzgodniony z Zamawiającym,
    c) listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu.
    d) opis przypadków, w których projekt dopuszcza niedziałanie systemu,

Realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą. Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.

2.2.1 Miejsce i termin instalacji.

Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego. z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji zamówienia, w ramach jednego weekendu (Piątek godz. 16:00 – Niedziela godz. 22:00) po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym.

Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci dwóch osób w siedzibie Zamawiającego w ciągu pierwszych dwóch dni roboczych następujących po pracach wdrożeniowo – instalacyjnych w godzinach od 7.30 do 16.00.

W tym czasie przedstawiciele Wykonawcy zobowiązani są do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji.

Dodatkowo przedstawiciele Wykonawcy dokonają także przeszkolenia dwóch pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań.

2.2.2 Montaż i fizyczne uruchomienie systemu.

Zamawiający wymaga zainstalowania całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:

a) Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
b) Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
c) Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
d) Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
e) Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
f) Dla urzadzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.

g) Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
h) Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).

2.2.3 Połączenia sieciowe.

Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami PD (punktami dystrybucyjnymi) występującymi w projekcie według topologii gwiazdy, oraz zaproponowanego schematu.

Połączenia światłowodowe pomiędzy lokalizacjami powinny zostać zakończone (podłączone) na portach SFP/SFP+:

- pomiędzy lokalizacjami z wykorzystaniem istniejących łączy światłowodowych, należy wykorzystać istniejące patchpanele zakończone w istniejących szafach,
- przełączników CORE – na dwa przełączniki celem zapewnienia niezawodności, redundancja i agregacji połączeń,
- punktów pośrednich - połączenie (lokalizacja zdalna – serwerownia centralna) powinno zostać zrealizowane poprzez 2 połączenia SFP/SFP+ (porty) (4 włókna) z wykorzystaniem redundancji i agregacji połączeń.

Zamawiający wymaga wykonania połączeń sieciowych (łącznika), który należy wykonać w oparciu o okablowanie miedziane kat. 6U/UTP pomiędzy:

- szafa nr 2 – szafa nr 3 – pomieszczenie CPD (liczba połączeń 48 szt.; 2xpatchpanel 24 porty RJ45 kat 6. U/UTP na szafę; szacowana długość 5 m).
- szafa nr 1 – szafa nr 3 – pomieszczenie CPD (liczba połączeń 24 szt.; 1xpatchpanel 24 porty RJ45 kat 6. U/UTP na szafę; szacowana długość 15 m).

Wykonane połączenia mają służyć do podłączenia urządzeń serwerowych zlokalizowanych w szafie nr 3 do nowej, zmodernizowanej struktury sieci LAN.

Wykonawca wraz z przełącznikami musi dostarczyć:

- odpowiednie porty (GBIC – SFP/SFP+) dla uzyskania połączeń światłowodowych o wymaganych przepustowościach oraz redundancji.
- odpowiednie moduły i okablowanie do stackowania.
- odpowiednie patchordy światłowodowe i miedziane.

2.2.4 Instalacja i konfiguracja.

Konfiguracja dostarczanych przełączników w zakresie:

a) Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów.
b) Stworzenia odpowiednich konfiguracji redundancji zasilania dla przełączników CORE (zapewnienie zasilania przełącznika CORE #1 z wykorzystaniem zasilaczy przełącznika CORE #2 i odwrotnie) .
c) Konfiguracja protokołu STP.
d) Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu, ale nie mniej niż:
    - VLAN'y Pracownicze (odzwierciedlające strukturę organizacyjną),
    - VLAN WLAN,
    - VLAN Klient,
    - VLAN Serwer,
    - VLAN Public,
    - VLAN DMZ,
    - VLAN SAN – dla ruchu do systemu macierzowego SAN.
e) Konfiguracja połączeń pomiędzy przełącznikami sieci LAN z wykorzystaniem połączeń światłowodowych oraz miedzianych.
f) Agregacja połączeń celem uzyskania pasma nx1/10Gbps w obu kierunkach ruchu.

g) Dołączenie i konfiguracja przełączników CORE do istniejących urządzeń firewall – klaster (urządzenia firmy Fortinet: Fortigate 100F).
h) Konfiguracja klastra HA firewall:
    a. Modernizacja konfiguracja klastra HA firewall w trybie active-active.
    b. Segmentacja sieci w oparciu o protokół 802.1q.
    c. Konfiguracja routingu pomiędzy sieciami VLAN.
    d. Konfiguracja polityk dostępu pomiędzy strefami.
    e. Konfiguracja dostępu zdalnego dla różnych grup użytkowników z wykorzystaniem zewnętrznego serwera RADIUS.
    f. Konfiguracja uwierzytelniania dwuskładnikowego dla wybranych użytkowników.
    g. Konfiguracja funkcji bezpieczeństwa w zakresie: skanowanie antywirusowe, moduł IPS, moduł web-filter, inspekcja protokołu https.
    h. Konfiguracja połączenia VPN – pomiędzy lokalizacja główną a punktem zdalnym.
    i. Konfiguracja automatycznego backupu konfiguracji.
i) Konfiguracja serwerów DHCP na przełącznikach na użytek urządzeń końcowych, które zostaną przyłączone do portów w poszczególnych sieciach VLAN
j) Implementacja mechanizmów bezpieczeństwa sieci LAN:
    - Mechanizm monitorowania przydziału adresów IP przez serwery DHCP, ochrona przed nieautoryzowanymi serwerami DCHP.
    - Mechanizm monitorowania prawidłowego użycia protokołu ARP przez stacje końcowe w celu zapobieżenia nadużyciom oraz atakom typu „man in the middle".
    - Mechanizm filtrujący ruch na portach dostępowych, do których przyłączone zostaną stacje końcowe, zezwalając na ruch jedynie z adresu IP przydzielonego przez serwer DHCP.
    - Implementacja mechanizmów 802.1x na wybranych portach z wykorzystaniem dostarczanego serwera uwierzytelniającego wbudowanego w system domenowy, tak aby w przypadku braku autoryzacji dozwolony był ruch np. tylko do Internetu, a w przypadku poprawnej autoryzacji możliwy był dostęp do zasobów sieciowych. Uwierzytelnienie powinno zostać oparte o certyfikat komputera jak i użytkownika (dynamiczna zmiana sieci VLAN w oparciu o przynależność do grupy użytkowników w systemie domenowym).
k) Konfiguracja dostępu do urządzeń z wykorzystaniem mechanizmów AAA w oparciu o serwer uwierzytelniający wbudowany w istniejący system domenowy. Administrator ma podlegać autentykacji, autoryzacji wykonywanych operacji administracyjnych lub konfiguracyjnych na urządzeniu oraz wszelkie wykonywane operacje mają być logowane na serwerze uwierzytelniającym.
l) Zapewnienie bezpiecznego środowiska zarządzającego dla urządzeń – dostęp jedynie z dedykowanej stacji zarządzającej, jeżeli to możliwe zbudowanie odseparowanego segmentu zarządzającego wykorzystującego interfejsy kart zarządzających out-of-band management (jezeli zaproponowane urządzenia będą posiadać interfejsy tego typu).
m) Implementacja dostępnych mechanizmów Quality of Service:
    - Konfiguracja kolejkowania traktującego ruch pochodzący od serwerów oraz ruch zarządzający jako priorytetowy.
    - Implementacja mechanizmów zapobiegających wysycaniu pasma na łączach pomiędzy przełącznikami, routerami oraz firewall'em poprzez niepożądany ruch sieciowy np. ruch generowany przez stacje zainfekowane wirusem (Scaveger QoS).
n) Przepięcie obecnej infrastruktury serwerowo-macierzowej Sądu Okręgowego w Rzeszowie na nową sieć LAN.
o) Testowanie obsługi ruchu sieciowego.
p) Testowanie skuteczności zabezpieczeń.

2.3 Opracowanie dokumentacji powykonawczej.

Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.

1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów.
2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).

3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.
4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.
5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.

2.4 Warunki gwarancji i dostępności serwisu.

Warunki gwarancji i wsparcia technicznego dla sprzętu i oprogramowania:

a) Dostarczone przełączniki powinny posiadać gwarancje lifetime (ograniczona gwarancja dożywotnia do 5 lat od wycofania z produkcji / sprzedaży przez producenta).
b) Na dostarczany sprzęt musi być udzielony min. 12-miesięczne wsparcie oparta na gwarancji producenta rozwiązania; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas naprawy i reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym oraz zakończenie naprawy) nie może przekroczyć jednego dnia roboczego - NBD;
c) Tryb gwarancji 7/24;
d) Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producent;
e) Całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producenta;
f) Całość kupowanego sprzętu musi być nowa, (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana we wcześniejszych projektach;
g) Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań;
h) W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie, na czas naprawy, sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
i) Zamawiający otrzyma dostęp do pomocy technicznej producenta (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego w okresie trwania wsparcia;
j) Zamawiający otrzyma dostęp do aktualizacji oprogramowania układowego firmware przełączników w okresie trwania wsparcia.

2.5 Asysta stanowiskowa.

Asysta stanowiskowa ma obejmować 40 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 5 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.
Asysta musi zostać podzielona na bloki dziedzinowe:

- Blok pierwszy (2 dni – 16 godzin) musi zostać przeprowadzony w centrum kompetencyjnym (poza terenem Sądu) i mieć na celu zapoznanie uczestników z elementami technologicznymi, które składają się na całość rozwiązania modernizacji sieci LAN.
- Blok drugi (3 dni – 24 godziny) musi zostać przeprowadzony w siedzibie Zamawiającego i musi ściśle dotyczyć podstawowych procedur administracyjnych, które są typowe dla codziennej pracy administratora celem zapewnienia poprawnej pracy wdrożonego rozwiązania sprzętowego jako platformy teleinformatycznej.

Zakres asysty stanowiskowej:

- Architektura sieci LAN – przełączniki sieciowe.
- Punkt styku z Internetem – firewall.

Asysta będzie skierowana do administratorów sieci LAN Sądu Okręgowego w Rzeszowie (2 osoby).

Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego.

Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. Wykonawcę oraz Zamawiającego.

2.6 Opieka serwisowa.

Zamawiający wymaga świadczenia opieki serwisowej przez okres minimum 12 miesięcy od dnia podpisania protokołu odbioru końcowego (telefoniczna, zdalna, mailowa, na miejscu u klienta) z czasem reakcji na zaistniałe problemy wynoszącym 2 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych. Zamawiający wymaga świadczenia pomocy technicznej i merytorycznej dla dostarczonego i wdrożonego rozwiązania modernizacji sieci LAN. Okres opieki serwisowej stanowi jedno z kryteriów oceny ofert, Wykonawca może zaoferować dłuższy okres opieki serwisowej niż 12 miesięcy. Szczegółowe zasady przyznawania punktów zostały opisane w SIWZ.

Wykonawca zapewni przyjmowanie zgłoszeń w Godzinach Roboczych, przez które rozumie się godziny od 7.00 do 17.00 w Dni Robocze.

Prace serwisowe mogą być realizowane po godzinach pracy Sądu w tym również w dni wolne. Termin realizacji prac wyznacza Zamawiający, a Wykonawca je przyjmuje.

W ramach opieki serwisowej Zamawiający wymaga dwóch wizyt serwisowych w siedzibie Sądu. Czas pojedynczej wizyty serwisowej 8 godz. – jeden dzień roboczy. Liczba wizyt będzie uwarunkowana zaoferowanym przez Wykonawcę okresem opieki serwisowej przy założeniu że jedna wizyta przypada na okres 6 miesięcy.

W przypadku jeżeli producent sprzętu komputerowego udostępni jakiekolwiek aktualizacje, nowe wersje, patche, zmiany itp. (dalej łącznie zwane aktualizacjami), Wykonawca w ramach Usług Serwisu zapewni Zamawiającemu takie aktualizacje niezwłocznie po ich udostępnieniu.

Łączny wymiar usług związanych z opieką serwisową nie przekroczy 240 godzin przy założeniu – okresu 12 miesięcznej opieki serwisowej.

Przygotował:

25.09.2020r. Paweł Jaźwa
(data i podpis)

Zatwierdzam:

Dyrektor Sądu Okręgowego
w Rzeszowie
28.09.2020 Małgorzata Niedzielska
(data i podpis)

3 Spis rysunków

4 Spis tabel