F.H.U. EBIT
ul. Lubelska 28/3
35-233 Rzeszów
Tel. 17 86-11-353
Internet: www.biuro21.pl
e-mail: ebit@biuro21.pl

Rzeszów, 22.10.2014r.

Projekt wykonawczy

Temat: Remont istniejącej sieci internetowej w DS LAURA i DS Filon w Rzeszowie, ul. Cicha 2,4.

Inwestor: Uniwersytet Rzeszowski, al. Rejtana 16c, 35-959 Rzeszów

Zawartość

SPIS RYSUNKÓW

SPIS TABEL

1 Wstęp

Dokument ten stanowi projekt wykonawczy konfiguracjami sieci LAN oraz sieci Wi-Fi w akademikach Uniwersytetu Rzeszowskiego. W dokumencie tym zostały opisane elementy i wymagania:

- elementy, jakie wchodzą w skład sieci LAN i Wi-Fi
- sposób konfiguracji urządzeń
- sposób integracji z istniejącymi systemami na Uniwersytecie Rzeszowskim

Celem opracowania jest zaprojektowanie nowoczesnej sieci LAN, Wi-Fi spełniającej oczekiwania inwestora. Głównymi celami Zamawiającego są:

- remont sieci istniejącej – kablowej z umożliwieniem z korzystania z sieci Wi-Fi przeznaczonej dla mieszkańców akademików URZ, będącymi studentami uczelni
    - sieć Wi-Fi powinna być oparta o kontroler umożliwiającym zarządzenie całością infrastruktury Wi-Fi oraz AP-tami
- remont sieci istniejącej – kablowej z umożliwieniem z korzystania z sieci Wi-Fi przeznaczonej dla mieszkańców akademików URZ niebędących studentami URZ
- wymiana istniejących przełączników na nowe, obsługujące istniejącą sieć LAN oraz umożliwiającą podłączenia AP-tów po portach PoE+
- wymiana urządzenia dostępowego do sieci Internet(systemu bezpieczeństwa) umożliwiającego jednocześnie identyfikację użytkowników korzystających z sieci oraz umożliwiającemu logowanie sesji/ruchu użytkowników
- montaż AP wraz z doprowadzeniem okablowania w celu połączenia urządzeń do sieci LAN
- integracja z obecnie wykorzystywanym Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej oraz istniejącą siecią Wi-Fi „eduroam”
- konfiguracja sieci LAN umożliwiająca
    - blokowanie mac adresów na portach dostępowych
    - blokowanie obcych serwerów DHCP
    - blokowanie statycznych adresów IP na portach przełączników(użytkownicy mają otrzymywać adresy IP z uczelnianego serwera DHCP)

2 Wykaz urządzeń niezbędnych do realizacji projektu

W celu realizacji projektu należy zdemontować wymieniane urządzenia pozostawiając je inwestorowi oraz dostarczyć niżej wymiennie urządzenia w podziale na poszczególne kategorie.

2.1 System Firewall

Wykaz interfejsów i modułów:

- Liczba interfejsów GE RJ45: 8
- Liczba interfejsów GE SFP: 8
- Port konsoli RJ45
- Urządzenie wyposażone w dysk SSD o pojemności min. 100GB

Wydajność firewall-a(minimalne wartości):

- Przepustowość IPv4 dla pakietów 1518 bajtów: 15Gbps
- Przepustowość IPv4 dla pakietów 64 bajtów: 15Gbps
- Opóźnienie dla pakietów 64 bajty: 3us
- Przepustowość liczona w pakietach/s: 22Mpps
- Ilość jednoczesnych sesji TCP: 5,5 milionów
- Ilość nowych sesji/s: 250000
- Ilość polityk: 8000
- Przepustowość VPN-a IPSEC: 12Gbps
- Przepustowość VPN-a SSL: 400Mbps
- Liczba użytkowników VPN SSL: 400
- Przepustowość IPS-a: 4,5Gbps
- Możliwość podłączenia AP-tów(funkcja kontrolera): co najmniej 500, w tym 250 w trybie tunelowania
- Możliwość pracy w klastrze Active-Active oraz Active-standby

Funkcjonalność Firewall-a:

- Antywirus – skanowanie ruchu w poszukiwaniu zainfekowanych plików
- IPS – skanowanie ruchu, detekcja anomalii
- Filtracja stron WWW – możliwość filtracji, monitorowania, blokowania stron internetowych
- Kontrola aplikacji – możliwość monitorowania/blokowania ruchu ze zdefiniowanych aplikacji
- Ochrona przed wyciekiem danych

- Kontroler sieci bezprzewodowej, możliwość podłączenia i zarządzania AP-tami oraz możliwość kreowania sieci bezprzewodowych z poziomu firewall-a
- Praca w trybie NAT/transparent
- Optymalizacja WAN
- Możliwość monitorowania i raportowania w „Chmurze"
- Możliwość autoryzacji z wykorzystaniem tokenów
- Możliwość tworzenia VPN-ów IPSec Site-to-Site
- Możliwość tworzenia VPN-ów IPSec Klient-to-Site
- Możliwość tworzenia VPN-ów SSL-owych
- W zakresie realizowanych funkcjonalności VPN, wymagane jest:
    - Tworzenie połączeń w topologii Site-to-Site oraz możliwość definiowania połączeń Client-to-Site
    - Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
    - Obsługa SSL VPN w trybach portal oraz tunel
- Integracja ze środowiskiem Active Directory, z możliwością autoryzacji użytkowników w trybie SSO
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
- Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
- Możliwość budowy 2 oddzielnych instancji systemów bezpieczeństwa (fizycznych lub logicznych) w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
- Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
- Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 4500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość

wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

- Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
- Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 50 kategorii. W ramach filtra powinny być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
- Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
- System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    - 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
    - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

2.2 Systemem zbierania logów

Urządzenie powinno pochodzić od tego samego producenta, co firewall. Urządzenie powinno spełniać następujące wymagania:

- 3 porty Gbps
- Zainstalowane dwa dyski twarde o pojemności 2TB
- Możliwość zapisu min. 14,5GB logów/dzień
- Obsługa, co najmniej 50M sesji/dzień
- Predefiniowane raporty dostosowane do potrzeb administratorów umożliwiające:
    - Monitorowanie wykorzystania polityk
    - Identyfikowanie wzorców ataków
- Korelacja zdarzeń sieciowych umożliwiająca szybką identyfikację na zagrożenia i zdarzenia bezpieczeństwa

- Możliwość przeglądania logów wysyłanych z urządzeń w podziale na
    - Rodzaj urządzenia
    - Log z ruchu użytkowników
    - Log zdarzeń zarejestrowanych przez urządzenie
    - Log z profili ochrony
- Możliwość archiwizacji(http, FTP, MAIL)

2.3 Przełączniki sieciowe

W ramach realizacji projektu należy dostarczyć 3 rodzaje przełączników. Przełączniki te musza pochodzić od jednego producenta oraz muszą mieć możliwość klastrowania/łączenia urządzeń w stos po linkach 10Gbps. Należy również dostarczyć moduły, kable i inne elementy niezbędne do podłączenia urządzeń w stos/klaster oraz połączenia urządzeń ze sobą po linkach światłowodowych.

2.3.1 Przełącznik sw_type_1 o parametrach:

- 48 portów 10/100/1000Base-T
- Możliwość zasilania urządzeń końcowych jak AP-ty, telefony z przełącznika poprzez funkcję PoE+
- 4 porty SFP+
- Zasilacz o mocy nie mniejszej niż 350W
- Możliwość instalacji modułów 1Gbps SFP oraz modułów 10Gbps SFP+
- Możliwość kastrowania do 9 przełączników tego samego typu po linkach 10Gbps
- Wyposażony w min. 1GB pamięci RAM
- Wyposażony w min. 128 MB pamięci flash
- Wydajność na poziomie nie mniejszym niż 130 Mpps
- Wydajność przełączania nie mniejsza niż 170Gbps
- Wsparcie dla protokołu Openflow
- Możliwość zarządzania przez:
    - SSH
    - WEB
    - SNMP v2 oraz SNMP v3
    - Specjalizowane oprogramowanie producenta sprzętu
- Obsługa routingu statycznego, protokołu routingu RIP

- Wsparcie dla protokołów/standardów:
    - IEEE 802.1w
    - IEEE 802.1ad Q-in-Q
    - IEEE 802.1D MAC Bridges
    - IEEE 802.1p Priority
    - IEEE 802.1Q VLANs
    - IEEE 802.1s Multiple Spanning Trees
    - IEEE 802.3ab 1000BASE-T
    - IEEE 802.3ad Link Aggregation Control Protocol(LACP)
    - IEEE 802.3ae 10-Gigabit Ethernet
    - IEEE 802.3af Power over Ethernet
    - IEEE 802.3u 100BASE-X
    - IEEE 802.3x Flow Control
    - IEEE 802.3z 1000BASE-X
    - RFC 768 UDP
    - RFC 791 IP
    - RFC 792 ICMP
    - RFC 793 TCP
    - RFC 826 ARP
    - RFC 854 TELNET

2.3.2 Przełącznik sw_type_2 o parametrach:

- 48 portów 10/100/1000Base-T
- 4 porty SFP+
- Zasilacz o mocy nie mniejszej niż 350W
- Możliwość instalacji modułów 1Gbps SFP oraz modułów 10Gbps SFP+
- Możliwość kastrowania do 9 przełączników tego samego typu po linkach 10Gbps
- Wyposażony w min. 1GB pamięci RAM
- Wyposażony w min. 128 MB pamięci flash
- Wydajność na poziomie nie mniejszym niż 130 Mpps
- Wydajność przełączania nie mniejsza niż 170Gbps
- Możliwość zarządzania przez:
    - Ssh
    - WEB
    - SNMP v2 oraz SNMP v3
    - Specjalizowane oprogramowanie producenta sprzętu
- Obsługa routingu statycznego, protokołu routingu RIP
- Wsparcie dla protokołów/standardów:
    - IEEE 802.1w
    - IEEE 802.1ad Q-in-Q
    - IEEE 802.1D MAC Bridges
    - IEEE 802.1p Priority
    - IEEE 802.1Q VLANs
    - IEEE 802.1s Multiple Spanning Trees
    - IEEE 802.3ab 1000BASE-T
    - IEEE 802.3ad Link Aggregation Control Protocol(LACP)
    - IEEE 802.3ae 10-Gigabit Ethernet
    - IEEE 802.3u 100BASE-X
    - IEEE 802.3x Flow Control
    - IEEE 802.3z 1000BASE-X
    - RFC 768 UDP
    - RFC 791 IP
    - RFC 792 ICMP
    - RFC 793 TCP

- RFC 826 ARP
- RFC 854 TELNET

2.3.3 Przełącznik sw_type_3 o parametrach:

- 4 porty SFP+
- 16 portów SFP 1Gbps
- 8 portów 100/1000Base-T
- Dwa zasilacz wbudowane umożliwiające redundancje na wypadek awarii jednego z nich
- Możliwość instalacji modułów 1Gbps SFP oraz modułów 10Gbps SFP+
- Możliwość kastrowania do 9 przełączników tego samego typu po linkach 10Gbps
- Wyposażony w min. 1GB pamięci RAM
- Wyposażony w min. 128 MB pamięci flash
- Wydajność na poziomie nie mniejszym niż 95 Mpps
- Wydajność przełączania nie mniejsza niż 120Gbps
- Możliwość zarządzania przez:
    - Ssh
    - WEB
    - SNMP v2 oraz SNMP v3
    - Specjalizowane oprogramowanie producenta sprzętu
- Obsługa routingu statycznego, protokołu routingu RIP
- Wsparcie dla protokołów/standardów:
    - IEEE 802.1w
    - IEEE 802.1ad Q-in-Q
    - IEEE 802.1D MAC Bridges
    - IEEE 802.1p Priority
    - IEEE 802.1Q VLANs
    - IEEE 802.1s Multiple Spanning Trees
    - IEEE 802.3ab 1000BASE-T
    - IEEE 802.3ad Link Aggregation Control Protocol(LACP)
    - IEEE 802.3ae 10-Gigabit Ethernet
    - IEEE 802.3u 100BASE-X
    - IEEE 802.3x Flow Control
    - IEEE 802.3z 1000BASE-X
    - RFC 768 UDP
    - RFC 791 IP
    - RFC 792 ICMP

- RFC 793 TCP
- RFC 826 ARP
- RFC 854 TELNET

2.4 *Oprogramowanie do monitorowania i zarządzania dostarczanymi przełącznikami*

System zbudowany w architekturze klient – serwer. Licencja na system umożliwi zarządzanie urządzeniami sieciowymi różnych producentów. System zbudowany modułowo, tak, aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność.

System zarządzania posiada podstawowe funkcje:

- Automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet
- Monitorowanie stanu urządzeń po protokole SNMP
- Konfiguracja urządzeń po protokole SNMP
- Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach
- Konfiguracja VLANów na zarządzanych urządzeniach
- Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania
- Zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń
- Zarządzenie infrastrukturą Wi-Fi z wykorzystaniem kontrolerów bezprzewodowych
- Możliwość wysyłania alarmów np. mailem lub SMS'em
- Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta
- Obrazowanie sieci w postaci mapki wraz z wyróżnianiem kolorami występujących alarmów
- Lokalizowanie użytkowników po adresie IP lub MAC
- Możliwość zdefiniowania polityki zmieniającej ustawienia sieci w przypadku wykrycia ataku sieciowego
- Możliwość utworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym
- Funkcja Telnet / SSH proxy umożliwiająca zarządzanie CLI przez przeglądarkę Internetową.
- Funkcja zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem android.
- Dla wszystkich obsługiwanych standardowo urządzeń dostępne nie tylko monitorowanie, ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń.

- Dostęp do sytemu zarządzania realizowany przez przeglądarkę internetową.
- System zarządzania podłączy się i importuje dane z LDAP / Active Directory.
- System ma możliwość autentykacji użytkowników w oparciu o LDAP i Radius.
- System ma możliwość zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, Email.
- Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń.
- System ma możliwość zarządzania siecią wirtualną poprzez integracje SOAP z VMWare VirtualCenter Server.
- System wspiera zarządzanie, co najmniej dla 6000 modeli urządzeń.
- System ma możliwość automatycznej aktualizacji przez Internet.
- System ma możliwość implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.
- System posiada kontekstową funkcje pomocy zmieniającą zawartość w zależności od wyświetlanego kontekstu.

Dostępne moduły umożliwiają rozbudowę i integrację systemu o następujące funkcjonalności:

- Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x
- Zarządzanie klientami na stacjach roboczych w ramach implementacji technologii Network Access Control
- Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA
- Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników
- Zarządzenie systemem telefonii IP
- Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS
- Zarządzanie dostępem zdalnym Ipsec/VPN
- Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych SFLOW, NetSream v5 oraz analizy kontentu pakietów SMTP, FTP, HTTP

2.5 Access Point-y

W ramach realizacji projektu należy dostarczyć AP-ty o parametrach:

- AP do zastosowań wewnątrz budynków
- Liczba radia: 2
- Liczba anten wewnętrznych/wbudowanych: 4
- Częstotliwości dla radia 1-wszego:
  - 2.4 GHz b/g/n lub 5 GHz a/n
- Częstotliwości dla radia 2-go:
  - 5 GHz a/n/ac
- Wydajność:
  - Radio 1 – do to 300 Mbps,
  - Radio 2 – do to 500 Mbps
- Port 10/100/1000Base-T
- Strumienie TX / RX:
  - 2x2 MIMO
- Możliwość zasilenia AP-ta przez PoE
- Liczba jednoczesnych SSID: 13
- Wsparcie dla protokołów EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
- Wsparcie dla autentykacja użytkowników/urządzeń: WPA, WPA2 z 802.1x lub Preshared key, WEP, Web Captive Portal
- Wsparcie standardów IEEE: 802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11n, 802.1X, 802.3af, 802.11ac
- Urządzenie jako tzw. cienki punkt dostępowy zarządzany z poziomu kontrolera sieci bezprzewodowej. W celu zapewnienia spójności zarządzania i uzyskania wymaganego poziomu bezpieczeństwa kontroler sieci wireless uruchomiony jest w obrębie systemu realizującego funkcję firewall/ platformy bezpieczeństwa gwarantującej ochronę dla obsługiwanych sieci wireless i przewodowych.
- Kompaktowa obudowa z tworzywa sztucznego umożliwiającą montaż na suficie lub ścianie wewnątrz budynku. Interfejs sieciowy i inne gniazda - jeśli występują-zlokalizowane na ściance od strony montażowej urządzenia.

2.6 Serwer

Należy dostarczyć serwer o parametrach:

LP	Parametr lub warunek	Opis
1	Obudowa	-Typu Rack, wysokość 2U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack;
3	Procesory	-Zainstalowany procesor w architekturze x86
4	Pamięć RAM	-Zainstalowane min. 24 GB pamięci RAM DDR3 LV Registered -Wsparcie dla technologii zabezpieczania pamięci o najmniej Advanced ECC, Memory Scrubbing, SDDC; -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing"; -min. 24 gniazda pamięci RAM na płycie głównej, obsługa min. 1536GB pamięci RAM;
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 2.0 RAID min. 0,1,5,6,50,60, min. 1024MB pamięci podręcznej cache,
6	Dyski twarde	-Zainstalowane min. 3 dyski SAS 2.0 o pojemności min. 300GB każdy, min. 10K RPM dyski Hotplug; -min. 8 wnęk dla dysków twardych Hotplug 2,5; -Obsługa dysków SAS, SATA, SSD; -Możliwość rozbudowy dostarczonego serwera do obsługi min. 16 wewnętrznych dysków twardych Hotplug 2,5;
7	Kontrolery LAN	-2x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot i teamingu, RJ-45;
8	Porty	-zintegrowana karta graficzna ze złączem VGA; -USB 2.0, w tym minimum 2 na panelu przednim, minimum 4 z tyłu; -1x RS-232;
10	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug -Redundantne wentylatory hotplug;

11	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; Dostęp poprzez przeglądarkę Web (także SSL, SSH) Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii Zarządzanie alarmami (zdarzenia poprzez SNMP) Możliwość przejęcia konsoli tekstowej Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) 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 itd.).
12	Wspierane OS	- VMWare
14	Oprogramowanie	Licencje oprogramowania potrzebnego do uruchomienia systemu MGMT i Radius

2.7 *Komputer stacjonarny do prezentacji informacji*

Komputer stacjonarny do prezentacji informacji (Kiosk informacyjny) wyposażony w klawiaturę metalową, o wzmocnionej konstrukcji odpornej na uszkodzenia mechaniczne:

Element	**Opis**	
Obudowa	• konstrukcja wykonana z blachy stalowej • monitor odchylony od pionu pod kątem 45 stopni (+/- 5 stopni) • dostęp serwisowy realizowany od tyłu kiosku przez drzwi uchylne stalowe, zamykane zamkiem. • podstawa kiosku dwuwarstwowa stalowa, malowana proszkowo • kolorystyka dopasowana do wymagań Inwestora • demontażu (wymiany) wszystkich elementów poszycia kiosku bez użycia elektronarzędzi. • podświetlane logo (każdy komputer/terminal spersonalizowane poprzez polakierowanie na dowolny, wskazany przez Inwestora kolor z palety, jak również umieszczenie na nim elementów identyfikacji wizualnej w formie podświetlanego logo zgodne z wymogami Inwestora – księga znaku). Personalizacja według uzgodniona z oferentem.	
Monitor	monitor dotykowy - przekątna monitora: 21''	
Jednostka sterująca kioskiem	Procesor	Procesor zgodny z architekturą x64
	Pamięć RAM	Min. 4 GB; z możliwością rozbudowy min. 32 GB, min. 2 wolne złącza dla rozszerzeń pamięci
	Dysk twardy	Min. 320GB, min. 32MB Cache,
	Karta dźwiękowa	zintegrowana
	Porty I/O	8 portów USB 2.0
	Karta sieciowa	Zintegrowana 10/100/1000 MBit/s
	Karta graficzna	Karta graficzna zintegrowana, z możliwością dynamicznego przydzielania pamięci.
Wyposażenie dodatkowe	• wrzutnik monet • Głośniki • Czytnik kart stykowych (smartcard) zamontowany z przodu Kiosku • Klawiatura o wzmocnionej konstrukcji odpornej na uszkodzenia mechaniczne z manipulatorem kulkowym	
Zasilanie	• 230V, 50 Hz,	
Certyfikaty i dokumenty	• Deklaracja zgodności CE	

a) Parametry funkcjonującego u Zamawiającego Systemu Kiosków Informacyjnych

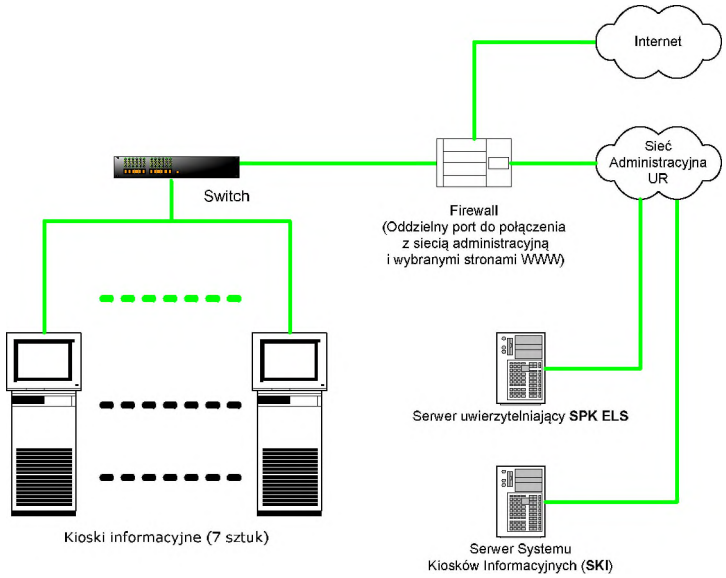
Dostarczone kioski informacyjne należy zintegrować z istniejącym i działającym u Zamawiającego Systemem Kiosków Informacyjnych o poniższych parametrach:

System Kiosków Informacyjnych – tzw. „Infomatów" – tworzą:

- serwer aplikacji zwany dalej serwerem Systemu Kiosków Informacyjnych (serwer SKI);
- kioski informacyjne

Serwer Systemu Kiosków Informacyjnych (SKI) znajduje się w chronionej sieci administracyjnej UR. Serwer SKI nawiązuje połączenia z serwerem uwierzytelniającym ELS (znajdującym się wewnątrz sieci administracyjnej UR) oraz z wybranymi witrynami zewnętrznymi (sieć Internet i Intranet). Infomaty znajdują się w odrębnej sieci Infomatów oddzielonej od sieci Administracyjnej poprzez firewall.
Kioski Informacyjne, które zostaną dostarczone muszą współpracować z posiadanym przez Inwestora Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej .

Dostarczone Kioski Informacyjne umożliwiać zapis, odczyt, wykorzystanie kodu PIN zapisanego w strukturach funkcjonujących na Uniwersytecie Rzeszowskim kart ELS, ELD, EKP do uwierzytelniania.
Oprogramowanie Kiosku przygotowuje ELS, ELD i EKP do obsługi PKI w kioskach informacyjnych.
Oprogramowanie Kiosku umożliwia zalogowanie się użytkownika przy pomocy certyfikatu (PKI).
Oprogramowanie Kiosku ma możliwość obsługi Bezobsługowego Centrum Wydruku - BCW (m.in. ładowanie impulsów na karty ELS, ELD, EKP)



Rysunek 1: Schemat ideowy Systemu Kiosków Informacyjnych

b) Oprogramowanie do nowych dostarczanych kiosków informacyjnych:

1	Kiosk informacyjny wykorzystuje sterowniki do obsługi czytnika kart elektronicznych zgodnych z normą ISO/IEC 7816 lub równoważną oraz standardem PC/S.C. lub równoważnym, a w szczególności legitymacji ELS o specyfikacji zgodnej z rozporządzeniem Ministerstwa Szkolnictwa Wyższego - Dziennik Ustaw z dnia 8 grudnia 2006 r. (Nr 224, poz. 1634) Rozporządzenie wydano na podstawie art. 192 ust. 1 ustawy z dnia 27 lipca 2005 r. -Prawo o szkolnictwie wyższym.
2	Kiosk informacyjny autoryzuje i uwierzytelnia użytkownika na podstawie danych zapisanych w specjalnej, przewidzianej do tego strukturze danych przechowywanej na legitymacji ELS lub przy pomocy logowania z hasłem, umożliwiające dostęp do stron zawierających dane osobiste, które mogą pochodzić z innych systemów uczelnianych (np. systemu dziekanatowego lub bibliotecznego).
3	Kiosk informacyjny obsługuje procesorowe karty serwisowe, umożliwiające konfigurację serwisu informacyjnego kiosku przy pomocy stron WWW.
4	Powłoka użytkownika (shell) oprogramowania kiosku jest wykonana w postaci aplikacji wykonanej w technologii „cienkiego klienta", współpracująca z dedykowaną bazą danych, umożliwiającą tworzenie kont użytkowników i zarządzanie ich uprawnieniami, przechowywanie indywidualnej konfiguracji kiosków, itp.
	Inne funkcje oprogramowania kiosku informacyjnego
5	Autoryzacja użytkownika odbywająca się na podstawie legitymacji ELS z kodem PIN lub w oparciu o login i hasło. Niedopuszczalne jest autoryzowanie użytkownika na podstawie jedynie numeru numeru seryjnego karty ELS. W przypadku braku karty ELS w czytniku Infokiosku lub gdy użytkownik nie zalogował się za pośrednictwem Infokiosku dostęp użytkownika ograniczony jest jedynie do: - strony głównej (wraz z podstronami);

	- rozkładów jazdy PKP, PKS, etc.; - innych witryn włączanych sukcesywnie przez administratora ze strony Zamawiającego do grupy witryn nie wymagających autoryzowanego dostępu. Oprogramowanie ma możliwość zastosowania struktury PKI (Infrastruktury Klucza Publicznego) do uwierzytelniania.
6	Kiosk informacyjny zapewnia automatyczne wylogowanie użytkownika (przejście do strony głównej systemu) w przypadku: - wyjęcia karty ELS z czytnika; - utraty połączenia z serwerem kiosków informacyjnych (wyświetlenie stosownego komunikatu dla użytkownika); - przekroczenia limitu czasu bezczynności (określanego przez administratora systemu w zakresie od 1 minuty do 60 minut z krokiem 1 minuta).
7	Kiosk informacyjny pozwala na cykliczne odświeżanie konfiguracji programowej urządzenia, rozumiane jako zdalne załadowanie parametrów konfiguracyjnych dla przeglądarki internetowej działającej na kiosku w charakterze klienta.
8	Kiosk informacyjny pozwala na ochronę kiosku poprzez restrykcje systemowe (blokowanie możliwości uruchamiania wskazanych aplikacji).
9	Kiosk informacyjny pozwala na obsługę klawiatury ekranowej dostosowanej do ekranów dotykowych (duże przyciski), umożliwiającej jedynie wprowadzanie tekstów, z zablokowaną możliwością wykonywania funkcji sterujących (skrótów klawiszowych).
10	Kiosk informacyjny pozwala na aktywowanie klawiatury ekranowej poprzez ustawienie kursora w polu edycji lub poprzez wywołanie dedykowanym przyciskiem.
11	Kiosk informacyjny pozwala na obsługę modułów bezpieczeństwa
12	Kiosk informacyjny pozwala na zapisywanie danych na kartach procesorowych, które są zabezpieczone kluczami 3DES (również kluczami zdywersyfikowanymi 3DES). Dodatkowo pozwala na poszerzanie funkcjonalności karty poprzez tworzenie dodatkowych struktur danych na karcie.
13	Kiosk informacyjny pozwala na przechowywanie kluczy 3DES w bezpiecznym magazynie chronionym.
System operacyjny infokiosku	
Platforma	Zainstalowany 64 bitowy system operacyjny (klasy PC).

Dostawa, instalacja, montaż, szkolenie:

W ramach dostawy przewiduje się:

- wykonanie montażu kiosków w miejscu wskazanym przez Inwestora
- wykonanie instalacji urządzeń wraz z infrastrukturą potrzebną do ich uruchomienia (kable połączeniowe i zasilające, PEL)
- instalacja i konfiguracja oprogramowania systemowego i oprogramowania zarządzająco - sterującego
- szkolenia w zakresie obsługi urządzenia i zainstalowanego oprogramowania dla administratorów

- dostarczenie instrukcji obsługi w języku polskim dotyczącej eksploatacji kiosku i postępowania w przypadku awarii,
- dostarczenie instrukcji w języku polskim dotyczącej konfiguracji oprogramowania
- dokonywanie zmian konfiguracji przez Inwestora

2.8 *Urządzenie przenośne do diagnostyki i konfiguracji sieci*

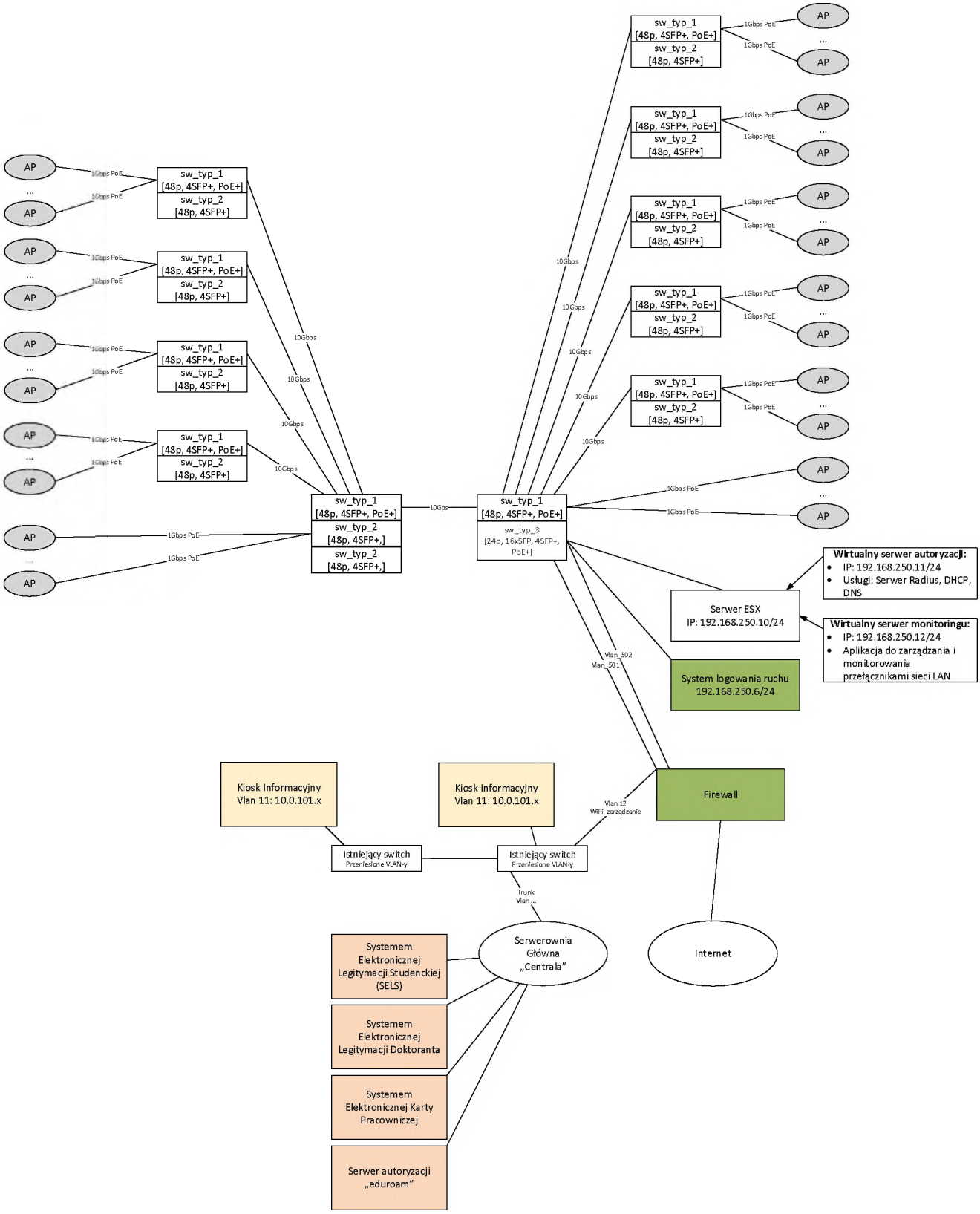
Należy dostarczyć urządzenie przenośne do diagnostyki i konfiguracji sieci o parametrach:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Procesor osiągający w teście PassMark PerformanceTest co najmniej wynik min. 2500 punktów PassMark CPU Mark (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net).
Płyta główna	Oparta na chipsecie rekomendowanym przez producenta procesora.
Matryca	Przekątna matrycy: min. 12,1" - max. 14,1"
Pamięć operacyjna	Zainstalowane min. 4 GB RAM, możliwość rozbudowy
Parametry pamięci masowej	Min. 500 GB
Sloty zewnętrzne	Czytnik kart pamięci min. SD i MMC
Połączenia i karty sieciowe	Port sieci LAN 10/100/1000 Ethernet RJ 45 zintegrowany z płytą główną oraz WLAN 802.11b/g/n, zintegrowany z płytą główną lub w postaci wewnętrznego modułu mini-PCI Express. Bluetooth
Wymagane zintegrowane złącza	Min. 2x USB; Min. 1 x VGA lub 1x HDMI; wyjście słuchawkowe; wejście mikrofonu; Min. 1 x sieć (RJ-45)
Bateria	Min. 4 cell Li-Ion zapewniająca pracę minimum przez 4h
System operacyjny	Zainstalowany system operacyjny w wersji polskiej. Dopuszczalny jest system operacyjny dla komputerów PC, spełniający następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; 2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; 3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; 4. Internetowa aktualizacja zapewniona w języku polskim; 5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;

	7. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) 8. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer 9. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 13. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. 14. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 15. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 16. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 17. Wbudowany system pomocy w języku polskim; 18. Certyfikat producenta oprogramowania na dostarczany sprzęt; 19. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 20. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 21. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; 22. Graficzne środowisko instalacji i konfiguracji; 23. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; 24. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 25. Udostępnianie modemu;

	26. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; 27. Możliwość przywracania plików systemowych; 28. System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)
Dodatkowo	Przejściówka USB -> COM Torba do dostarczonego urządzenia: przegroda z pianki, pasek na ramię, kolor ciemny

3 Schemat rozwiązania



Rysunek 2: Schemat rozwiązania

4 Podział sieci na VLAN-y

W ramach konfiguracja sieci LAN i Wi-Fi należy wykonać konfigurację następujących nowych VLAN-ów:

Tabela 1: Konfiguracja VLAN-ów

VLAN ID	Nazwa	Adres IP	Maska	Brama domyślna	Przenaczenie
501	MGMT	192.168.250.0	255.255.255.0	192.168.250.1	MGMT, adresacja urządzeń aktywnych - switche, przełączniki
502	Firewall	10.10.10.0	255.255.255.248	10.10.10.1	dwupunkt SW-FG
511	WiFi_eduroam	10.200.0.0	255.255.240.0	10.200.0.1	Podpięcie uzytkowników sieci WiFi eduroam
512	WiFi_hotel	10.200.100.0	255.255.252.0	10.200.100.1	Podpięcie uzytkowników sieci WiFi
520	Laura_0	10.100.100.0	255.255.255.0	10.100.100.1	Podłączenie użytkowników LAN, akademik Laura parter
521	Laura_1	10.100.101.0	255.255.255.0	10.100.101.1	Podłączenie użytkowników LAN, akademik Laura 1-piętro
522	Laura_2	10.100.102.0	255.255.255.0	10.100.102.1	Podłączenie użytkowników LAN, akademik Laura
523	Laura_3	10.100.103.0	255.255.255.0	10.100.103.1	Podłączenie użytkowników LAN, akademik Laura
524	Laura_4	10.100.104.0	255.255.255.0	10.100.104.1	Podłączenie użytkowników LAN, akademik Laura
525	Laura_5	10.100.105.0	255.255.255.0	10.100.105.1	Podłączenie użytkowników LAN, akademik Laura
526	Laura_6	10.100.106.0	255.255.255.0	10.100.106.1	Podłączenie użytkowników LAN, akademik Laura
527	Laura_7	10.100.107.0	255.255.255.0	10.100.107.1	Podłączenie użytkowników LAN, akademik Laura
528	Laura_8	10.100.108.0	255.255.255.0	10.100.108.1	Podłączenie użytkowników LAN, akademik Laura
529	Laura_9	10.100.109.0	255.255.255.0	10.100.109.1	Podłączenie użytkowników LAN, akademik Laura
530	Laura_10	10.100.110.0	255.255.255.0	10.100.110.1	Podłączenie użytkowników LAN, akademik Laura 10-piętro
531	Filon_0	10.100.111.0	255.255.255.0	10.100.111.1	Podłączenie użytkowników LAN, akademik Filon parter
532	Filon_1	10.100.112.0	255.255.255.0	10.100.112.1	Podłączenie użytkowników LAN, akademik Filon 1-piętro
533	Filon_2	10.100.113.0	255.255.255.0	10.100.113.1	Podłączenie użytkowników LAN, akademik Filon
534	Filon_3	10.100.114.0	255.255.255.0	10.100.114.1	Podłączenie użytkowników LAN, akademik Filon
535	Filon_4	10.100.115.0	255.255.255.0	10.100.115.1	Podłączenie użytkowników LAN, akademik Filon
536	Filon_5	10.100.116.0	255.255.255.0	10.100.116.1	Podłączenie użytkowników LAN, akademik Filon
537	Filon_6	10.100.117.0	255.255.255.0	10.100.117.1	Podłączenie użytkowników LAN, akademik Filon
538	Filon_7	10.100.118.0	255.255.255.0	10.100.118.1	Podłączenie użytkowników LAN, akademik Filon
539	Filon_8	10.100.119.0	255.255.255.0	10.100.119.1	Podłączenie użytkowników LAN, akademik Filon
540	Filon_9	10.100.120.0	255.255.255.0	10.100.120.1	Podłączenie użytkowników LAN, akademik Filon
541	Filon_10	10.100.121.0	255.255.255.0	10.100.121.1	Podłączenie użytkowników LAN, akademik Filon 10-piętro

VLAN-y 520 do 541 przeznaczone są do podpięcia użytkowników sieci LAN. Jedne VLAN-an przeznaczony jest na jedno piętro w każdym z akademików.

Dodatkowo należy przekonfigurować istniejące połączenie pomiędzy lokalizacją serwerownia główna Uniwersytetu Rzeszowskiego, a akademikami. Połączenie to należy tak przekonfigurować, aby możliwa była komunikacja pomiędzy zasobami zlokalizowanymi w serwerowni głównej, a dostarczanymi urządzeniami: Kioskami informacyjnymi, instalowanymi systemami.

W tym celu należy wykonać połączenie umożliwiające przeniesienie wymaganych VLAN-ów:

Tabela 2: VLAN-y - przeniesienie

VLAN ID	Nazwa	Adres IP	Maska	Brama domyślna	Przeznaczenie
10	LAN_k_sels_v10	10.0.100.0	255.255.255.0	10.0.100.1	Sieć obsługi legitymacji studenckiej
11	LAN_k_kiosk_tv_v11	10.0.101.0	255.255.255.0	10.0.101.1	Sieć kiosków
12	LAN_wifi_zarz_v12	10.0.116.0	255.255.255.0	10.0.116.1	Sieć bezprzewodowa - zarządzanie

W obu akademikach(na parterze) istnieje również sieć pracownicza przeznaczona dla pracowników akademików/pracowników URZ. Sieć tą należy zostawić, powinna ona być wydzielona z sieci przeznaczonej dla mieszkańców akademików. Jeżeli zajdzie potrzeba rekonfiguracji urządzeń, rekonfiguracji połączeń urządzeń należy ją również wykonać.

5 Konfiguracja sieci LAN

W ramach konfiguracji sieci LAN należy:

- Zdemontować istniejące przełączniki sieciowe
    - Przełączniki należy złożyć w wyznaczonym przez Inwestora miejscu
- Zamontować nowo dostarczone przełączniki, klastry przełączników zgodnie z schematem sieci LAN
- Wykonać podłączenie po linkach światłowodowych
- Podłączyć istniejące gniazda, wskazane przez Zamawiającego do nowych przełączników
- Wykonać pełną konfigurację przełączników, szczegółowo opisaną w punktach poniżej

Inwestor posiada sieć światłowodową:

- pomiędzy punktami dystrybucyjnymi, a głównym punktem w każdym z akademików
- połączenie światłowodowe pomiędzy głównymi punktami zlokalizowanymi w obu akademikach
- Połączenie światłowodowe pomiędzy akademikiem, a serwerownią główną Uniwersytetu Rzeszowskiego

5.1 Szczegóły konfiguracji przełączników sieciowych

Należy wykonać następującą konfigurację przełączników sieciowych:

- W każdym z punktów dystrybucyjnych należy połączyć przełączniki w stos/klaster, tak, aby zarządzanie nimi odbywało się z jednego adresu IP
- VLAN-y
    - Na każdym z urządzeń należy skonfigurować vlan-y pod obsługę użytkowników, AP-tów i innych urządzeń. VLAN-y zostały opisane w punkcie powyżej
    - Porty dostępowe należy przypisać do odpowiednich vlan-ów, w zależności od ich przeznaczenia
    - Porty wykorzystywane do połączeń pomiędzy urządzeniami należy skonfigurować w tryb przenoszenia wszystkich vlan-ów
- Routing
    - Na stosie przełączników w głównym punkcie dystrybucyjnym należy uruchomić routing
    - Na przełącznikach tych należy skonfigurować interfejsy vlan_x i nadać im adresację zgodne z wykazem vlan-ów:
        - VLAN_502: 10.10.10.2/255.255.255.248
        - VLAN_520: 10.100.100.1/255.255.255.0
        - VLAN_521: 10.100.101.1/255.255.255.0

- VLAN_522: 10.100.102.1/255.255.255.0
- VLAN_523: 10.100.103.1/255.255.255.0
- VLAN_524: 10.100.104.1/255.255.255.0
- VLAN_525: 10.100.105.1/255.255.255.0
- VLAN_526: 10.100.106.1/255.255.255.0
- VLAN_527: 10.100.107.1/255.255.255.0
- VLAN_528: 10.100.108.1/255.255.255.0
- VLAN_529: 10.100.109.1/255.255.255.0
- VLAN_530: 10.100.110.1/255.255.255.0
- VLAN_531: 10.100.111.1/255.255.255.0
- VLAN_532: 10.100.112.1/255.255.255.0
- VLAN_533: 10.100.113.1/255.255.255.0
- VLAN_534: 10.100.114.1/255.255.255.0
- VLAN_535: 10.100.115.1/255.255.255.0
- VLAN_536: 10.100.116.1/255.255.255.0
- VLAN_537: 10.100.117.1/255.255.255.0
- VLAN_538: 10.100.118.1/255.255.255.0
- VLAN_539: 10.100.119.1/255.255.255.0
- VLAN_540: 10.100.120.1/255.255.255.0
- VLAN_541: 10.100.121.1/255.255.255.0

  - Na przełączniku należy skonfigurować statyczne trasy routingu
    - ip route 0.0.0.0 0.0.0.0 10.10.10.1
  - Należy skonfigurować trasę domyślną tak, aby możliwe było wyjście do Internetu
  - Na przełączniku korowym należy również przygotować access-listy zabraniające komunikacji IP pomiędzy VLAN-ami 520-541. Access listy te mają za zadanie uniemożliwić komunikacje między sobą użytkowników z różnych VLAN-ów, w przypadku występowania problemów w sieci LAN.

- DHCP Relay
  - Zapytania DHCP z poszczególnych sieci LAN należy przekierować do serwera DHCP zlokalizowanego w sieci zarządzającej poprzez odpowiednią konfigurację parametrów DHCP Relay na wszystkich urządzeniach pośrednich biorących udział w komunikacji
- Konfiguracja portów typu TRUNK – do połączenia pomiędzy urządzeniami
  - Połączenia pomiędzy przełącznikami mają przepuszczać wszystkie vlan-y
- Konfiguracja portów dostępowych

- Wszystkie porty dostępowe użytkowników zostaną skonfigurowane w tryb szybkiego uruchamiania się w przypadku uruchomienia protokołu STP
- Porty te zostaną przypisane do odpowiedniego vlan-u, w zależności od podłączanego urządzenia
  - Inwestor wskaże/ustali z wykonawcą, które porty dostępowe użytkowników mają być skonfigurowane w odpowiednim VLAN-ie
- Na portach tych należy wykonać konfigurację odpowiednich parametrów, aby możliwe było osiągnięcie zabezpieczeń opisanych w punktach poniżej w szczególności zabezpieczenie przed pętlami w sieci LAN, sztormami broadcastowymi, podłączeniem obcego serwera DHCP

- Konfiguracja zabezpieczeń
  - Blokowanie obcych serwerów DHCP
    - Porty dostępowe należy skonfigurować tak, aby nie było możliwe rozgłaszanie adresów IP z urządzeń podłączonych do tych portów
  - Blokowanie statycznych adresów IP
    - Wszyscy użytkownicy sieci LAN, Wi-Fi muszą używać dynamicznych adresów IP
  - Blokowanie MAC adresów – możliwy dostęp tylko jednego MAC adresu na porcie dostępowym
  - Blokowanie portów dostępowych po otrzymaniu pakietów BPDU
    - W przypadku wykrycia na porcie dostępowych pakietów BPDU, port taki zostanie zablokowany
  - Zabezpieczenie instancji spanning tree poprzez mechanizm obrony root-a w sieci
    - W przypadku podłączenia urządzenia z włączonym protokołem STP, port taki nie będzie brał udziału w wyborze root-a w protokole STP
  - Blokowanie/ograniczenie ruchu broadcastowego na portach dostępowych
    - W przypadku przekroczenia ruchu broadcastowego na portach dostępowych, ruch ten zostanie zablokowany/ograniczony lub port zostanie wyłączony
  - Zabezpieczenie przed wystąpieniem pętli w sieci LAN
- Zabezpieczenie dostępu do urządzeń aktywnych
  - Uruchomienie protokołów ssh, https
    - Zostaną uruchomione bezpieczne protokoły do zarządzania urządzeniami w raz z ograniczeniem do adresów IP, z jakich można takie połączenie wykonywać

5.2 *Adresacja przełączników*

Wszystkie przełączniku, stosy przełączników zostaną zaadresowane w VLAN-ie zarządzającym zgodnie z poniższą tabelą(nazwy przełączników zostaną określone przez Inwestora na etapie konfiguracji urządzeń):

Tabela 3: Adresacja przełączników

Adres IP	Rodzaj urządzenia	Interfejs	Nazwa urządzenia
192.168.250.21	Switch	VLAN_501	
192.168.250.22	Switch	VLAN_501	
192.168.250.23	Switch	VLAN_501	
192.168.250.24	Switch	VLAN_501	
192.168.250.25	Switch	VLAN_501	
192.168.250.26	Switch	VLAN_501	
192.168.250.27	Switch	VLAN_501	
192.168.250.28	Switch	VLAN_501	
192.168.250.29	Switch	VLAN_501	
192.168.250.30	Switch	VLAN_501	
192.168.250.31	Switch	VLAN_501	
192.168.250.32	Switch	VLAN_501	
192.168.250.33	Switch	VLAN_501	
192.168.250.34	Switch	VLAN_501	
192.168.250.35	Switch	VLAN_501	
192.168.250.36	Switch	VLAN_501	
192.168.250.37	Switch	VLAN_501	
192.168.250.38	Switch	VLAN_501	
192.168.250.39	Switch	VLAN_501	
192.168.250.40	Switch	VLAN_501	
192.168.250.41	Switch	VLAN_501	
192.168.250.42	Switch	VLAN_501	
192.168.250.43	Switch	VLAN_501	
192.168.250.44	Switch	VLAN_501	
192.168.250.45	Switch	VLAN_501	
192.168.250.46	Switch	VLAN_501	
192.168.250.47	Switch	VLAN_501	
192.168.250.48	Switch	VLAN_501	
192.168.250.49	Switch	VLAN_501	
192.168.250.50	Switch	VLAN_501	

6 Konfiguracja sieci Wi-Fi

Należy wykonać montaż wszystkich urządzeń wchodzących w skład systemu Wi-Fi oraz dokonać ich konfiguracji w celu osiągnięcia następujących założeń działania sieci:

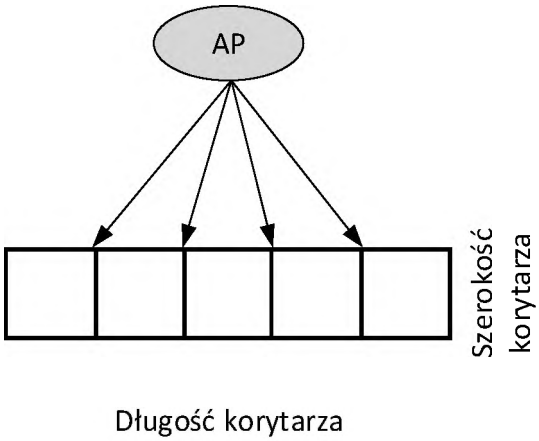
- Rozgłaszanie dwóch sieci Wi-Fi
    - rozbudowa sieci eduroam
    - sieć Wi-Fi dla gości akademików
- autoryzacja dostępu do obu sieci Wi-Fi poprzez konieczność podania użytkownik/hasło z wykorzystaniem bezpiecznych protokołów uniemożliwiających przejęcie tych danych
- logowanie i przechowywanie informacji:
    - logowanie autoryzacji użytkowników
    - logowanie dzierżawy adresów z serwera DHCP
    - logowanie sesji/ruchu użytkowników do sieci Internet

6.1 Rozmieszczenie AP-tów

W obu akademikach należy zamontować dostarczane AP-ty we wskazanych miejscach(4-ry Access Pointy na piętro). Do AP-tów należy doprowadzić okablowanie kategorii 6 zakończone gniazdem obok miejsca montażu AP-ta oraz zakończonym na panelu w najbliższym punkcie dystrybucyjnym, do którego będzie ono prowadzone. Kable należy umieści w korytkach.
Należy wykonać pomiary dynamiczne wszystkich nowo prowadzonych połączeń kablowych pod AP-ty oraz kioski informacyjne. Pomiary te należy dołączyć do końcowej dokumentacji powykonawczej.
Przed wykonaniem prac wymagana jest wizja lokalna na obiektach w celu ustalenia z Zamawiającym sposobu prowadzenia tras kablowych.

Access Pointy należy rozmieścić w akademikach zgodnie z założeniami:

- 4-ry AP-ty na piętro
- Instalacja AP-tów zgodnie z rysunkiem:



Rysunek 3: Rozmieszczenie AP-tów

6.2 Podłączenie AP-tów do kontrolera

Wszystkie zamontowane AP-ty należy podłączyć do pierwszych portów PoE przełącznika do VLAN-u zarządzającego. AP-ty należy nazwać i zaadresować zgodnie z poniższą tabelą:

Tabela 4: Adresacja AP-tów

Nazwa urządzenia	Budynek	Piętro
AP01	Akademik Laura	Parter
AP02	Akademik Laura	Parter
AP03	Akademik Laura	Parter
AP04	Akademik Laura	Parter
AP05	Akademik Laura	Piętro I
AP06	Akademik Laura	Piętro I
AP07	Akademik Laura	Piętro I
AP08	Akademik Laura	Piętro I
AP09	...	...
...	...	...
AP87	Akademik Filon	Piętro X
AP88	Akademik Filon	Piętro X

Dostęp do konsoli zarządzającej WEB, SSH każdego z AP-ów należy zabezpieczyć poprzez zmianę domyślnego hasła, na hasło uzgodnione z Zamawiającym.

AP-ty należy podłączyć do kontrolera sieci Wi-Fi w celu ich monitorowania i zarządzania nimi. Z poziomu kontrolera należy udostępnić możliwość tworzenia i rozgłaszania sieci bezprzewodowych oraz zmianę ich parametrów.

Moc AP-tów należy ustanowić na 100%, z możliwością ich zmiany definiowanej na kontrolerze Wi-Fi.

6.3 Konfiguracja kontrolera sieci Wi-Fi

Do kontrolera należy dołączyć wszystkie montowane AP-ty. Z poziomu jego interfejsu graficznego umożliwić zarządzanie AP-tami oraz możliwość kreowania sieci Wi-Fi z różnego rodzaju zabezpieczeniami. Na kontrolerze Wi-Fi należy stworzyć odpowiedni interfejs w celu zarządzania i obsługi ruchu związanego z sieciami bezprzewodowymi.

6.3.1 Konfiguracja sieci Wi-Fi - SSID

Na kontrolerze należy stworzyć dwie sieci bezprzewodowe:

- sieć bezprzewodowa do obsługi użytkowników sieci eduroam charakteryzująca się parametrami:
    - SSID: „eduroam"
    - Zabezpieczenie WPA2 Enterprise
    - Autoryzację użytkowników tej sieci WiFi należy zintegrować z już istniejącym systemem użytkowanym w URZ do obsługi studentów oraz pracowników uczelni.
    - Ruch sieci Wi-Fi od AP-tów do kontrolera przesyłany w trybie tunelowania
    - Adresy IP użytkowników sieci Wi-Fi przydzielane przez serwer DHCP instalowany i konfigurowany w ramach projektu
    - Do zadań wykonawcy należy również rekonfiguracja istniejących systemów URZ oraz urządzeń aktywnych pośredniczących w komunikacji w celu podłączenia tworzonej sieci.
    - Ruch do sieci Internet, autoryzacja użytkowników oraz dzierżawy DHCP należy logować zgodnie z wymogami sieci eduroam
- Sieć bezprzewodowa do obsługi gości akademików charakteryzująca się parametrami
    - Autoryzacja użytkowników poprzez „Captive Portal"
    - Użytkownicy konfigurowani na serwerze RADIUS, instalowanym i konfigurowanym w ramach projektu
    - SSID: „akademiki" w trybie rozgłaszania
    - Ruch użytkowników sieci WiFi tunelowany z AP-tów do kontrolera
    - Adresy IP użytkowników sieci Wi-Fi przydzielane przez serwer DHCP instalowany i konfigurowany w ramach projektu
    - Ruch użytkowników, autoryzacja użytkowników i dzierżawy DHCP logowane i przechowywane na dostarczanych systemach

7 Instalacja i konfiguracja serwera

Na dostarczanym serwerze należy zainstalować darmową wersję systemu ESXi w najnowszej dostępnej wersji znajdującej się na stronie producenta. Serwer ten należy nazwać, zaadresować i podłączyć do sieci LAN zgodnie z danymi:

Tabela 5: ESX - parametry serwera

Parametr	Wartość
Nazwa	Esx
Adres IP/Maska	192.168.250.10/24
Brama domyślna	192.168.250.1

Na serwerze tym należy zainstalować:

- Serwer do obsługi zapytań DHCP i autoryzacji użytkowników – nazwa „Radius”
- Serwer monitoringu sieci LAN – nazwa „MGMT”

7.1 Konfiguracja serwera autoryzacji

Na serwerze ESX należy zainstalować serwer o parametrach:

Tabela 6: Serwer Radius - parametry

Serwer Radius	
Parametr	**Wartość**
Nazwa	Radius
Adres IP/Maska	192.168.250.11/24
Brama domyślna	192.168.250.1
Ilość procesorów	1
Pojemność dyskowa	60GB
Ilość pamięci RAM	8GB
System operacyjny	

Na serwerze tym należy uruchomić usługi:

- NPS, usługa wykorzystywana do autoryzacji użytkowników sieci przewodowych i bezprzewodowych
- DHCP, usługa wykorzystywana do przydzielania dynamicznych adresów IP użytkownikom sieci przewodowej oraz sieci bezprzewodowej

7.1.1 Konfiguracja usługi NPS

Głównym założeniem wykorzystania serwera Radius jest konieczność autoryzacji użytkowników w dostępie do sieci bezprzewodowej oraz autoryzacji użytkowników korzystających z sieci przewodowej przy dostępie do Internetu.

W tym celu należy wykonać pełną konfigurację usługi NPS w szczególności:

- Konfiguracja klientów usługi Radius – należy ograniczyć możliwość korzystania z usług do firewall-a oraz kontrolera sieci bezprzewodowej
- Konfiguracja zasad żądań połączeń
- Konfiguracja zasad sieciowych,

w celu uzyskania następujących funkcjonalności:

- Możliwość autoryzacji użytkowników sieci Wi-Fi „akademiki”
    - Autoryzacja z wykorzystaniem portalu „Captive Portal” dostępnym na urządzeniu brzegowym
- Możliwość autoryzacji użytkowników sieci LAN przewodowej,
    - Autoryzacja ma odbywać się na Firewallu przy próbie wyjścia do Internetu.
    - Autoryzacja poprzez portal WEB-owy bez konieczności dodatkowej konfiguracji urządzeń użytkowników końcowych
    - Autoryzacja poprzez podanie prawidłowego użytkownika i hasła na portalu WEB-owym
        - Autoryzacja na serwerze lokalnym Radius, w przypadku gości
        - Autoryzacja na serwerach URZ w przypadku użytkowników posiadających już konta w istniejących systemach
- Autoryzacja użytkowników należących do grupy „Internet” zdefiniowanym na serwerze,
- Ograniczenie możliwości autoryzacji z urządzeń biorących udział w komunikacji LAN, Wi-Fi oraz ograniczenie do autoryzacji użytkowników sieci LAN przewodowej i bezprzewodowej Wi-Fi

Logi z autoryzacji użytkowników mają być zapisywane do plików z możliwością ich archiwizacji.

7.1.2 Konfiguracja usługi DHCP

Na serwerze należy uruchomić usługę DHCP. Należy wykonać pełną konfiguracją serwera DHCP oraz urządzeń pośrednich tak, aby użytkownicy tworzonych sieci LAN i Wi-Fi pobierali adresy IP z konfigurowanego serwera(w szczególności konfiguracja parametrów DHCP Relay na przełącznikach oraz reguł na firewall-u).

Na serwerze należy stworzyć następujące pule adresów o parametrach:

Tabela 7: Serwer DHCP - parametry konfiguracji

Nazwa puli	Zakres od	Zakres do	Serwer DNS	Brama domyślna	Czas dzierżawy
VLAN_511	10.200.0.11	10.200.15.254	10.200.0.1	10.200.0.1	8h
VLAN_512	10.200.100.11	10.200.103.254	10.200.100.1	10.200.100.1	8h
VLAN_520	10.100.100.11	10.100.100.254	10.100.100.1	10.100.100.1	8h
VLAN_521	10.100.101.11	10.100.101.254	10.100.101.1	10.100.101.1	8h
VLAN_522	10.100.102.11	10.100.102.254	10.100.102.1	10.100.102.1	8h
VLAN_523	10.100.103.11	10.100.103.254	10.100.103.1	10.100.103.1	8h
VLAN_524	10.100.104.11	10.100.104.254	10.100.104.1	10.100.104.1	8h
VLAN_525	10.100.105.11	10.100.105.254	10.100.105.1	10.100.105.1	8h
VLAN_526	10.100.106.11	10.100.106.254	10.100.106.1	10.100.106.1	8h
VLAN_527	10.100.107.11	10.100.107.254	10.100.107.1	10.100.107.1	8h
VLAN_528	10.100.108.11	10.100.108.254	10.100.108.1	10.100.108.1	8h
VLAN_529	10.100.109.11	10.100.109.254	10.100.109.1	10.100.109.1	8h
VLAN_530	10.100.110.11	10.100.110.254	10.100.110.1	10.100.110.1	8h
VLAN_531	10.100.111.11	10.100.111.254	10.100.111.1	10.100.111.1	8h
VLAN_532	10.100.112.11	10.100.112.254	10.100.112.1	10.100.112.1	8h
VLAN_533	10.100.113.11	10.100.113.254	10.100.113.1	10.100.113.1	8h
VLAN_534	10.100.114.11	10.100.114.254	10.100.114.1	10.100.114.1	8h
VLAN_535	10.100.115.11	10.100.115.254	10.100.115.1	10.100.115.1	8h
VLAN_536	10.100.116.11	10.100.116.254	10.100.116.1	10.100.116.1	8h
VLAN_537	10.100.117.11	10.100.117.254	10.100.117.1	10.100.117.1	8h
VLAN_538	10.100.118.11	10.100.118.254	10.100.118.1	10.100.118.1	8h
VLAN_539	10.100.119.11	10.100.119.254	10.100.119.1	10.100.119.1	8h
VLAN_540	10.100.120.11	10.100.120.254	10.100.120.1	10.100.120.1	8h
VLAN_541	10.100.121.11	10.100.121.254	10.100.121.1	10.100.121.1	8h

Dzierżawy adresów IP uzyskiwane przez użytkowników należy logować z możliwością ich archiwizacji.

7.2 Konfiguracja systemu monitoringu sieci LAN(MGMT)

Na serwerze ESX należy zainstalować serwer o parametrach:

Tabela 8: Serwer monitoringu - parametry

Serwer MGMT	
Parametr	**Wartość**
Nazwa	MGMT
Adres IP/Maska	192.168.250.12/24
Brama domyślna	192.168.250.1
Ilość procesorów	1
Pojemność dyskowa	120GB
Ilość pamięci RAM	8GB
System operacyjny	

Na serwerze tym należy zainstalować dostarczone oprogramowanie do zarządzania przełącznikami sieciowymi.

7.2.1 Konfiguracja oprogramowania do zarządzania przełącznikami sieciowymi

Zainstalowane oprogramowanie należy zarejestrować oraz należy zainstalować dostarczone licencje. Należy dokonać konfiguracji i integracji z przełącznikami sieciowymi(konfiguracja oprogramowania oraz przełączników sieciowych), w szczególności należy:

- Zarządzanie przełącznikami z wykorzystaniem protokołów:
    - SNMP v2 lub SNMPv3 z ograniczeniem możliwości logowania poprzez ten protokół do adresu IP serwera MGMT z możliwością odczytywania i zmiany parametrów podpiętych urządzeń – uprawnienia Read/Write
    - SSH, logowanie poprzez użytkownika i hasło z możliwością wykonywania skryptów

Szczegóły wyżej wymienionych parametrów zostaną określone na etapie integracji.

Należy wykonać konfigurację oprogramowania tak, aby:

- Uzyskać mapę połączeń pomiędzy dostarczonymi urządzeniami
- Monitorować stan podpiętych urządzeń:
    - Dostępność
    - Obciążenie procesora
    - Wykorzystanie pamięci RAM
    - Wykorzystanie uplinków
- Otrzymywać alerty w przypadku awarii urządzeń i ich elementów
- Otrzymywać alerty w przypadku przekroczenia zdefiniowanych progów

- Wykonać aktualizację przełącznika z poziomu GUI/Portalu WEB oprogramowania
- Wykonać archiwizację konfiguracji przełącznika
- Wykonać konfiguracja portów przełączników m.in. przypisanie portu dostępowego do określonego VLAN-u
- Wykonać konfigurację nowych VLAN-ów

8 Rekonfiguracja systemów elektronicznych legitymacji

W ramach projektu wymagana jest integracja nowo tworzonej struktury sieci LAN oraz sieci Wi-Fi z istniejącym Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej.

Celem, jaki należy osiągnąć jest:

- Możliwość logowania się studentom, pracownikom oraz innym użytkownikom do sieci „eduroam" konfigurowanej w ramach projektu
- Możliwość autoryzacji użytkowników sieci LAN przy wyjściu do Internetu. Każdy z użytkowników powinien podać dane do autoryzacji po pojawieniu się strony internetowej w przeglądarce.

W ramach prowadzonych prac należy wykonać konfigurację wszystkich elementów wchodzących w skład systemu oraz wszystkich urządzeń pośredniczących w komunikacji, w szczególności:

- Konfiguracja Systemu Elektronicznej Legitymacji Studenckiej (SELS),
- Konfiguracja Systemu Elektronicznej Legitymacji Doktoranta
- Konfiguracja Systemu Elektronicznej Karty Pracowniczej
- Konfiguracja kontrolera sieci Wi-Fi
- Konfiguracja firewalla
- Konfiguracja połączenia z zasobami w centrali – reguły na centralnym firewall-u w celu przepuszczenia ruchu

8.1 Podłączenie kiosków – integracja z Systemem Kiosków Informacyjnych

W ramach projektu należy zainstalować dwa kioski informacyjne w akademikach(po jednym kiosku w akademiku). Kioski należy zamontować na parterze, we wskazanym przez Zamawiającego miejscu. Do kiosków należy doprowadzić nowe okablowanie ETH kategorii 6 zakończone gniazdem w miejscu instalacji kiosku oraz na panelu w punkcie dystrybucyjnym zlokalizowanym na parterze. W celu zasilenia kiosku informacyjnego należy podłączyć się do istniejącego gniazda zasilającego zlokalizowanego w pobliżu miejsca instalacji kiosku.

Kioski informacyjne należy zaadresować i podłączyć do VLAN-u obecnie wykorzystywanego na URZ. Należy wykonać pełną konfiguracje kiosku oraz systemu informatycznego do jego obsługi, aby uzyskać pełną funkcjonalność, jaka w chwili obecnej jest wykorzystywana w pozostałych lokalizacjach, w szczególności:

- Kioski Informacyjne, które zostaną dostarczone muszą współpracować z posiadanym przez Zamawiającego Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej. Dostarczone Kioski

Informacyjne muszą umożliwiać zapis, odczyt, wykorzystanie kodu PIN zapisanego w strukturach funkcjonujących u Zamawiającego kart ELS, ELD, EKP do uwierzytelniania. Oprogramowanie Kiosku musi przygotować ELS, ELD i EKP do obsługi PKI w kioskach informacyjnych. Oprogramowanie Kiosku umożliwi zalogowanie się użytkownika przy pomocy certyfikatu (PKI).

9 Konfiguracja Firewall-a i systemu logowania

Dostarczone urządzenia należy zamontować w głównym punkcie dystrybucyjnym zlokalizowanym na parterze. Firewall-a należy w pełni skonfigurować tak, aby uzyskać następującą funkcjonalność:

- Dwa dostarczone firewalle należy połączyć w klaster Active-Active
- Zapewnić wyjście do Internetu użytkownikom sieci LAN oraz sieci Wi-Fi
- Wyjście do Internetu powinno być zabezpieczone koniecznością autoryzacji użytkowników na firewall-u
    - W przypadku użytkowników sieci Wi-Fi autoryzacja realizowana będzie
        - w trakcie podpinania się do sieci „eduroam”
        - poprzez „Captive Portal” w przypadku sieci bezprzewodowej „akademiki”
    - w przypadku użytkowników sieci LAN autoryzacja realizowana będzie poprzez portal WEB-owy
        - Dla VLAN-ów 520-541 autoryzacja użytkowników odbywa się na lokalnym serwerze Radius w przypadku użytkowników zakładanych lokalnie, jeżeli użytkownik korzysta z już istniejącego konta założonego w systemach do obsługi legitymacji, autoryzacja zostanie przesłana do serwerów zlokalizowanych w URZ – serwery do obsługi legitymacji
- należy zapewnić logowanie:
    - Autoryzacji użytkowników
    - Ruch użytkowników do/z Internetu oraz pomiędzy sieciami, których ruch przechodzi przez firewall-a.
- Firewall-a należy zintegrować z dostarczanym urządzeniem do zbierania i archiwizacji logów

9.1 Szczegółowa konfiguracja firewall-a

W ramach projektu należy wykonać konfigurację firewall-a zgodnie z poniższymi danymi:

- Adresacja interfejsów firewall-a zgodnie z tabelą:

Adresacja interfejsów fizycznych			
Numer portu	**Przeznaczenie**	**Adres IP**	**Maska**
Port_1	WAN		
Port_2	MGMT	192.168.250.1	255.255.255.0
Port_3	LAN	10.10.10.1	255.255.255.248
Port_4	LAN_WiFi	10.0.116.X	255.255.255.0

Adresacja interfejsów logicznych			
Numer portu	**Przeznaczenie**	**Adres IP**	**Maska**
511	WiFi_eduroam	10.200.0.0	255.255.240.0
512	WiFi_akademiki	10.200.100.1	255.255.252.0

Adresacja interfejsów WAN oraz LAN_WiFi zostanie ustalona przed przystąpieniem do konfiguracji urządzenia.

- Konfiguracja routingu na firewall-u

  ip route 10.100.0.0 255.255.0.0 10.10.10.2
  ip route 0.0.0.0 0.0.0.0 WAN1

  Dodatkowy routing:

  - Należy skonfigurować routing do zasobów i systemów zlokalizowanych w centrali poprzez port LAN_WiFi

- Konfiguracja polityk bezpieczeństwa
  - Dla każdej z tworzonych sieci LAN należy skonfigurować politykę bezpieczeństwa, która zapewni:
    - Dostęp do Internetu
    - NAT-towanie adresów prywatnych na dostępną pulę adresów publicznych
    - Logowanie ruchu użytkowników
    - Autoryzację użytkowników sieci LAN
    - Dostęp do systemów URZ należy zablokować dla użytkowników końcowych, ruch ten zezwolony będzie wyłącznie dla administratorów systemów oraz urządzeń biorących udział w komunikacji
  - Konfiguracja QoS-a

- Stworzenie profilu QoS przypisanie go do polityk bezpieczeństwa o parametrach:
  - Maksymalny transfer z jednego adresu IP – 5120Kbps
  - Maksymalna ilość sesji z jednego IP – 10000

9.2 Szczegóły konfiguracji systemu logowania ruchu

Dostarczone urządzenie należy zainstalować w głównym punkcie dystrybucyjnym. Urządzenie to należy nazwać/zaadresować zgodnie z tabelą:

System logowania	
Nazwa	FW_LOG
Adres IP	192.168.250.6/24
Brama domyślna	192.168.250.1

System ten należy zintegrować z firewall-em. Opis integracji został opisany w punktach powyżej.