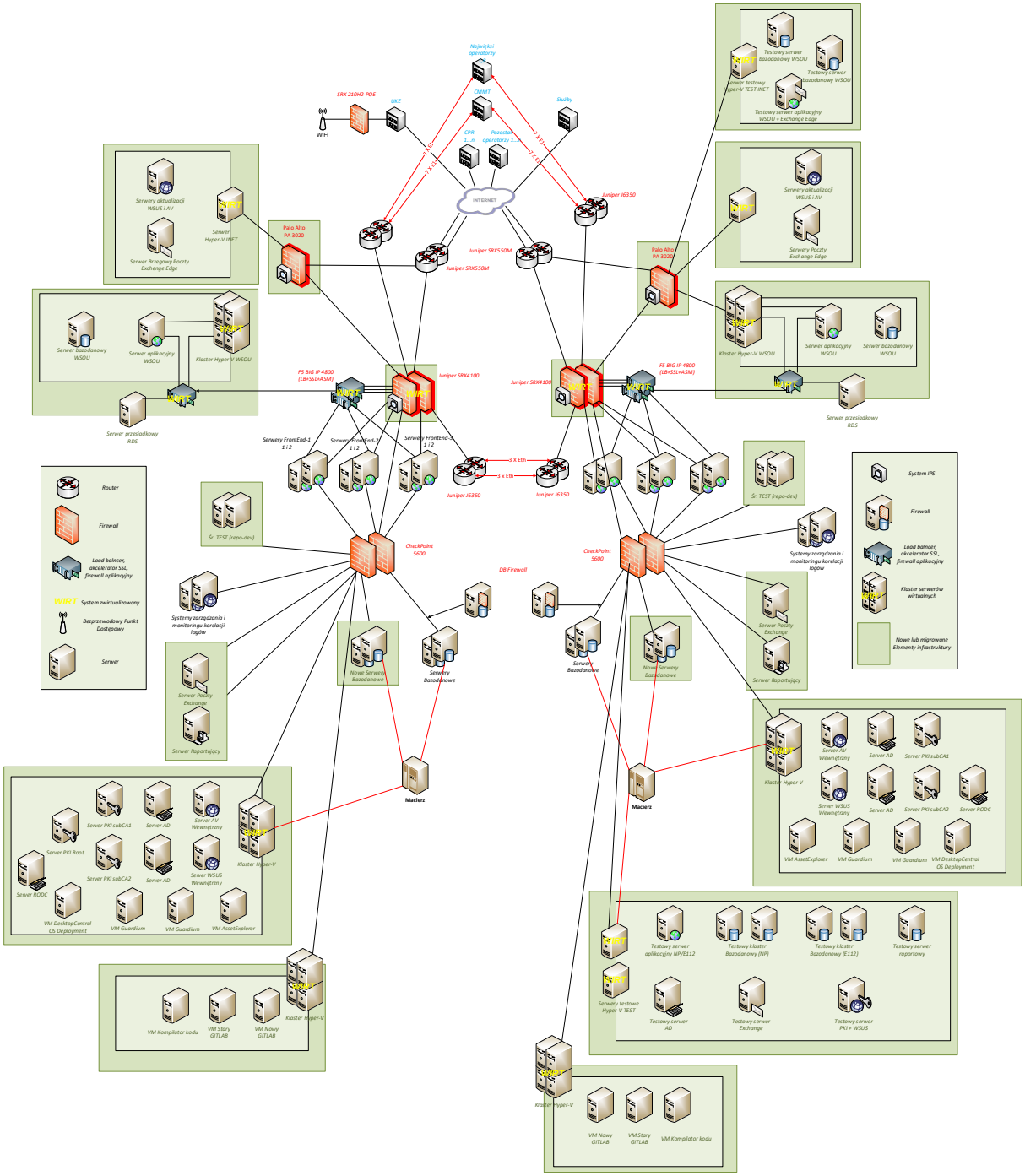
Załącznik D. Opis środowiska sieciowego LAN

Warszawa, 2023

Spis treści

Architektura rozwiązania

Poniższy diagram prezentuje ogólną wdrożoną architekturę rozwiązania:



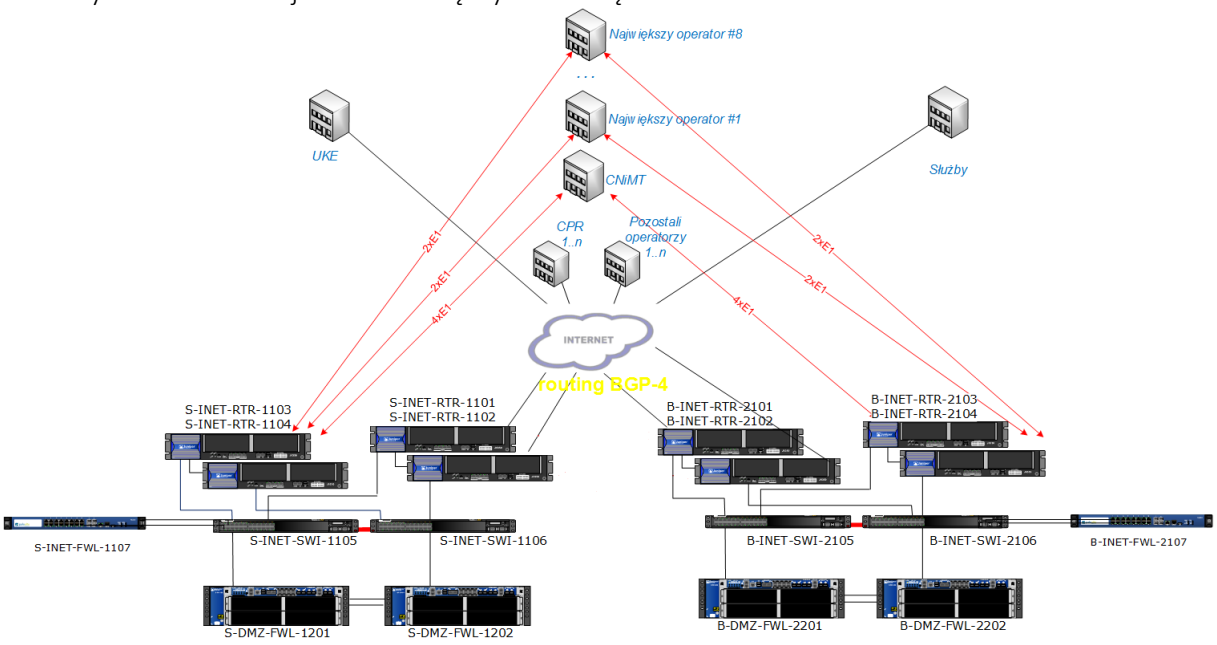
Rys. 1. Architektura

1. Strefa INET

1.1 W strefie styku z siecią internet uruchomiono w każdym z ośrodków

- 2 routery Juniper SRX550M - Routery dostępowe do sieci internet
- 2 routery Juniper J6350 - Routery dostępowe dla dużych operatorów/służb
- 2 przełączniki Juniper EX3300
- 2 zapory sieciowe *firewall* Juniper SRX 4100 - Węzeł I. linii ochrony
  (zapora sieciowa *firewall* + IPS) [cześć wspólna dla Strefy styku z siecią internet i DMZ]
- zapora sieciowa *firewall* Palo Alto PA-3020 – ochrona wyjścia do sieci internet

Poniższy schemat ilustruje architekturę styku z siecią internet:



Rys. 2. Strefa dostępu do internetu

1.2 Routery internetowe

W celu zapewnienia redundantnego dostępu do sieci internet, w każdym z ośrodków zainstalowano po dwa routery Juniper SRX550M. Każdy z routerów do obsługi ruchu internetowego posiada następującą specyfikację sprzętową:

Numer elementu	Opis	Liczba
SRX550M	Juniper SRX550M, 8GB Compact Flash 4GB RAM, Sprzętowa enkrypcja, 0 dodatkowych kart interfejsów (PIM), 1 zasilacz AC, oprogramowanie JUNOS	1

1.3 Routery dostępowe

Połączenia do największych operatorów i centrum CP SCPR (OST112) zrealizowane są z wykorzystaniem dwóch routerów dostępowych w każdym z Ośrodków. Do każdego z największych operatorów

telekomunikacyjnych (z wyjątkiem operatora T-mobile – posiada po dwa łącza Ethernet) oraz CP SCPR zestawione są po dwa łącza E1 z każdego Ośrodka – po jednym łączu E1 do każdego routera dostępowego.

Każdy z routerów dostępowych posiada następującą specyfikację sprzętową:

Numer elementu	Opis	Liczba
J-6350-JB	Juniper J6350, Pamięć Compact Flash 512 MB, Sprzętowe szyfrowanie, 0 dodatkowych kart interfejsów (PIM), 2 zasilacze AC, Oprogramowanie JUNOS, Pamięć wewnętrzna: 1 GB Compact Flash dla serii J-Series (JX-CF-1G-S), Moduł interfejsów: 8 portów Gigabit Ethernet 10/100/1000 Copper Universal PIM (JXU-8GE-TX-S)	1
JX-2Serial-S	Karta (PIM) do dwóch interfejsów szeregowych (2x V.35)	5
JX-CBL-V35-DTE	Kabel V.35 cable (DTE)	10
SSG-PS-AC	Dodatkowy zasilacz AC dla Juniper J6350	1

1.4 Przełączniki w strefie INET

W celu realizacji połączeń drugiej warstwy w strefie INET, w każdym Ośrodku zastosowano dwa przełączniki EX3300. Przełączniki połączone zostały w jeden przełącznik wirtualny z wykorzystaniem technologii Virtual Chassis, za pomocą dedykowanych portów VCP (*Virtual Chassis Port*). W każdym przełączniku wykorzystane zostały oba porty VCP w celu zestawienia stosu uodpornionego na awarię jednego z połączeń w obrębie Virtual Chassis. Przełączniki pełnią następujące role w Virtual Chassis:

- Jeden przełącznik w funkcji Master – nadzór nad połączeniem Virtual Chassis, obsługa protokołów kontrolnych
- Jeden przełącznik w funkcji Backup – przejmuje rolę Master w przypadku jego awarii

Każdy z przełączników posiada następującą konfiguracje sprzętową:

Numer elementu	Opis	Liczba
EX3300-24T	Juniper EX 3300 24 porty 10/100/1000BaseT	1
650-063365	4x GE/XE SFP+	1
740-013111	SFP-1GE-T	4

1.5 Zapora sieciowa

W celu zabezpieczenia Systemu Obsługi Użytkownika i systemu poczty elektronicznej oraz umożliwienie dostępu do sieci internet zostały dostarczone dwa urządzenia Palo Alto PA-3020. Urządzenia te zabezpieczają następujące połączenia pomiędzy strefami DMZ i internet:

- dostęp z internetu do aplikacji SOU
- dostęp z/do internetu dla serwerów pocztowych przez aplikację MS Exchange

- dostęp do internetu do pobierania poprawek przez system MS WSUS
- dostęp do internetu do pobierania sygnatur antywirusów AV
- dostęp do internetu dla aplikacji do pobierania słownika TERYT

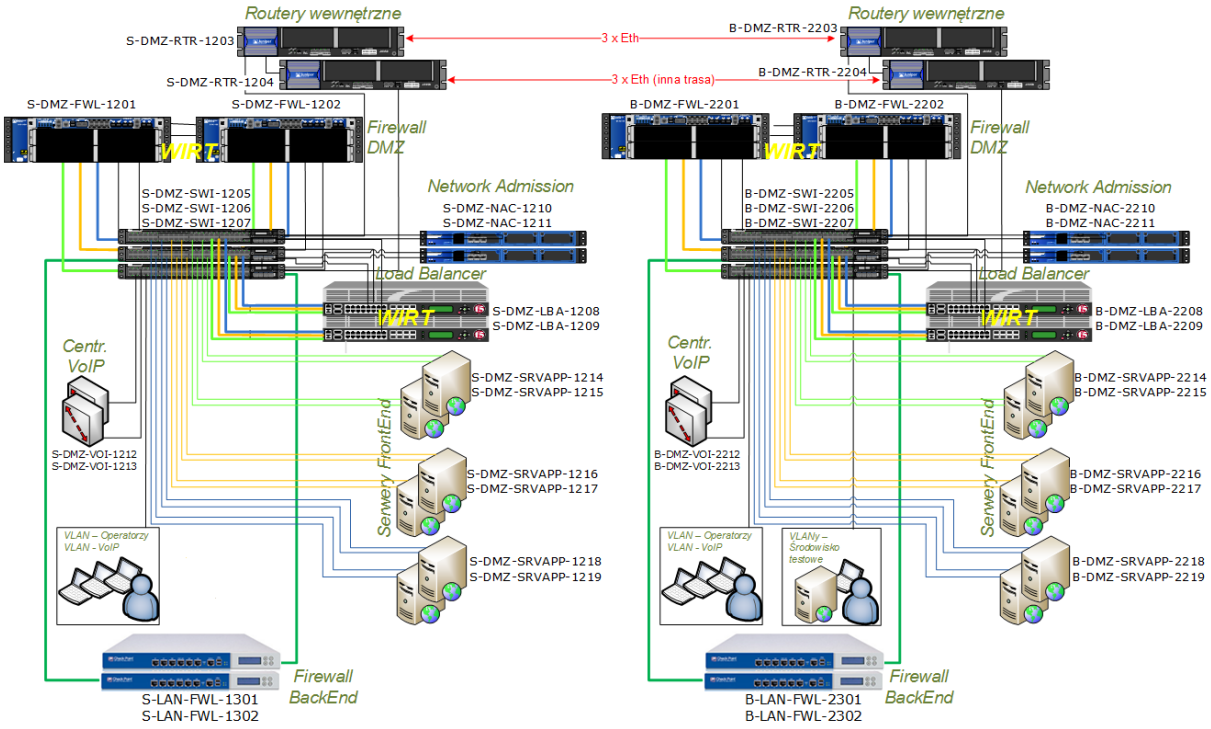
Specyfikacja dostarczanych urządzeń Palo Alto PA-3020:
Urządzenie zapory sieciowej *firewall*: Palo Alto Networks PA-3020 (PAN-PA-3020)
Abonament na funkcjonalność IPS i AV: Threat prevention subscription 3-year prepaid
Abonament na funkcjonalność filtracji stron WWW: URL filtering subscription 3-year prepaid (PAN-PA-3020-URL2-3YR)

2. Strefa DMZ

W strefie DMZ w każdym z Ośrodków zainstalowano:

- dwie (2) zapory sieciowe *firewall* Juniper SRX4100 - Węzeł I. linii ochrony (zapora sieciowa *firewall* + IPS)
  [cześć wspólna dla Strefy styku z siecią internet i DMZ]
- dwa (2) routery Juniper J6350 – Routery wewnętrzne
- trzy (3) przełączniki Juniper EX4200 - Przełączniki DMZ
- dwie (2) zapory sieciowe *firewall* CheckPoint 5600 - Węzeł II. linii ochrony [cześć wspólna dla Strefy DMZ i BackEnd]
- dwa (2) urządzenia równoważenia obciążenia (*load balancer*) F5 Big-IP 4800 – realizujące również funkcjonalność zakończenia połączeń szyfrowanych SSL oraz zapory sieciowej *firewall* aplikacyjnej sieci *WEB*
- dwa (2) urządzenia Pulse Secure Appliance 3000 – realizujące funkcjonalność kontroli dostępu do sieci (*Network Admission Control*)
- Stacje robocze administratorów

Poniższy schemat ilustruje architekturę strefy DMZ:



Rys. 3. Strefa DMZ

2.1 Specyfikacja urządzeń SRX4100

- **Półka bazowa**: SRX 4100 Chassis, Midplane, Fan, RE, SFB-12GE, AC PEM (SRX4100BASE-AC)
- **Karta usług sieciowych**: Network Processing Card for SRX 4000 (SRX4K-NPC)
- **Karty usług bezpieczeństwa**: 2x Services Processing Card for SRX 4000, Single Processor, 1 GHz, 4 GB Memory/CPU (SRX4K-SPC-1-10-40)
- **Redundantny zasilacz**: 2x 650W redundant AC-DC/DC-DC PSU
- **Przewody zasilające**: 2x Power Cord, AC, Continental Europe, C19, 16 A/250 V, 2,5 m, RA (CBL-PWR-C19S-162-EU)
- **Licencja na systemy wirtualne**: 2x SRX4100 5 Incremental Logical Systems License (SRX-4100-LSYS-5)
- **Moduł tworzenia klastra**: Clustering Module for SRX 4000 (SRX4K-CRM)
- **Abonament na funkcjonalność IPS**: Three year IDP signature subscription for SRX 4000 (SRX4K-IDP-3)

2.2 Specyfikacja urządzeń EX4200

Każdy z przełączników EX4200 w strefie DMZ posiada następującą konfiguracje sprzętową:

Numer elementu	Opis	Liczba
EX4200-48T	Juniper EX 4200, 48 porty 10/100/1000 BaseT (8 portów z PoE), Zasilacz 320 W AC, Kabel tworzenia stosu 50 cm	1
EX-PWR-320-AC	Dodatkowy zasilacz 320 W AC	1
EX-UM-2X4SFP	dwa porty 10G SFP+ / cztery porty 1G SFP Uplink Module dla EX4200 i EX3200	1

2.3 Urządzenia równoważenia obciążenia ruchu (load ballancer) f5 Big-IP

Urządzenia F5 Big-IP pełnią w systemie PLI-CBD następujące role:

- zakończanie ruchu szyfrowanego SSL
- Ochrona aplikacyjna serwerów sieci *WEB* (WAF)
- Równoważenie obciążenia ruchem (rozdzielanie zapytań do konkretnych serwerów aplikacji)
- Obsługa certyfikatów klienckich

W każdej z lokalizacji zainstalowane zostały po dwa urządzenia w klastrze aktywny/oczekujący (*active*/*standby*).

Dla każdego z urządzeń równoważenia obciążenia ruchu (*load ballancer*) została zapewniona następująca konfiguracja sprzętowa:

F5-BIG-LTM-I4800-AS-R	BIG-IP 4800 Local Traffic Manager, Application Security Edition (pamięć 8 GB) RoHS
F5-UPG-RACK2U-R	BIG-IP Rack Mount Rails (2U, Field Upgrade)

2.4 Routery wewnętrzne

Połączenie w strefie DMZ pomiędzy Ośrodkami zrealizowane zostało z wykorzystaniem 6 łączy Ethernet 48 Mbit/s i dwóch routerów wewnętrznych w każdym z Ośrodków.

Każdy z routerów wewnętrznych posiada następującą specyfikację sprzętową:

Numer elementu	Opis	Liczba
J-6350-JB	Juniper J6350, Pamięć Compact Flash 512 MB, Sprzętowe szyfrowanie, 0 dodatkowych kart interfejsów (PIM), 2 zasilacze AC, oprogramowanie JUNOS, Pamięć wewnętrzna: 1 GB Compact Flash for J-Series (JX-CF-1G-S), Moduł interfejsów: 8 portów Gigabit Ethernet 10/100/1000 Copper Universal PIM (JXU-8GE-TX-S)	1
JX-2Serial-S	Karta (PIM) do dwóch interfejsów szeregowych (2x V.35)	2
JX-CBL-V35-DTE	Kabel V.35 cable (DTE)	4
SSG-PS-AC	Dodatkowy zasilacz AC dla Juniper J6350	1

2.5 System kontroli dostępu do sieci - Network Admission Control

W każdej z lokalizacji został wdrożony system NAC oparty o klaster dwa urządzenia Pulse Secure Appliance 3000. Wraz z urządzeniami zostały dostarczone odpowiednie licencje, pozwalające na obsługę 100 równoległych Klientów na każde urządzenie.
Rozwiązanie to pozwala zarówno na kontrolę dostępu w warstwie II ISO/OSI (integracja z przełącznikami sieciowymi), jak i kontrolę dostępu w warstwie III ISO/OSI (integracja z systemami firewall)

Poniżej przedstawiono specyfikację dostarczanego systemu – do zbudowania klastra w każdej z lokalizacji, został dostarczony następujący zestaw urządzeń / licencji:

Numer elementu	Opis	Liczba
PSA 3000	Pulse Secure Appliance 3000 Base System	2
POLSEC-ADD-100U	Junos Pulse Policy Secure License 100 Concurrent Sessions-Perpetual	2

2.6 Centrale VoIP

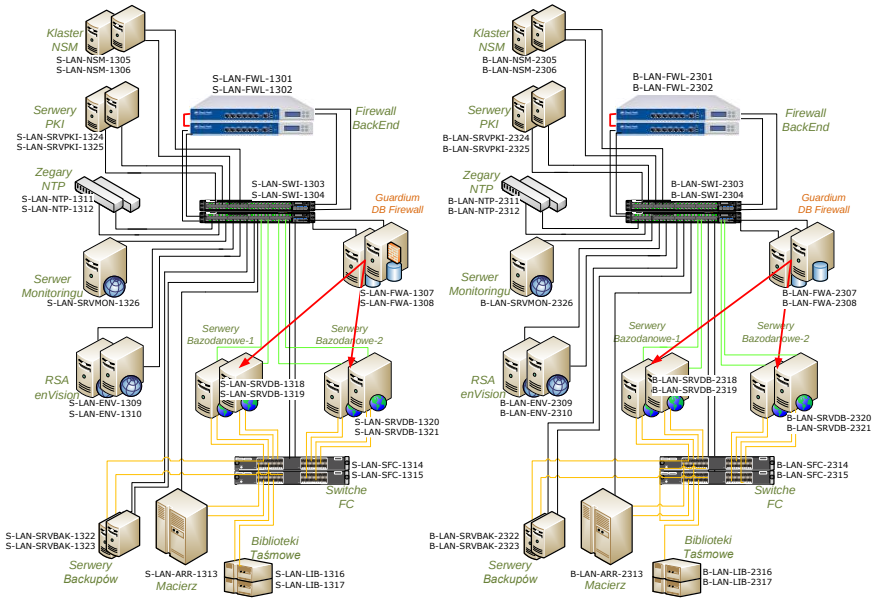
Funkcję zintegrowanej centrali telefonicznej pełni rozwiązanie Cisco® CallManager Express zainstalowane na routerze Cisco 2811. Jest to jednolite rozwiązanie zapewniające rejestrację telefonów IP, jak i obsługę połączeń VoIP. Dzięki dodatkowym modułom Network Module (NM) lub Advanced Integration Module (AIM) możliwe jest również zapewnienie użytkownikom funkcjonalności skrzynek głosowych. Urządzenie to zostało dostarczone wraz z licencją na 15 użytkowników. Na zaproponowanej platformie istnieje możliwość obsługi maksymalnie do 35 telefonów IP jedynie poprzez zakupienie odpowiedniej licencji.

3. Strefa BackEnd

W strefie BackEnd w każdym z Ośrodków zainstalowano:

- dwie (2) zapory sieciowe *firewall* CheckPoint 5600 - Węzeł II. linii ochrony [cześć wspólna dla Strefy DMZ i BackEnd]
- dwa (2) przełączniki Juniper EX4200 - Przełączniki LAN

- system zarządzania siecią Junos Space, składający się z pakietów:
  - Junos Space 21.1R1.4
  - Network Director 5.1R1.98
  - Security Director 21.1R1
  - Log Collector 20.1.1.22
- dwa (2) urządzenia RSA enVision ES-560 Appliance - System centralnej kolekcji i korelacji zdarzeń
- dwa (2) urządzenia Guardium SQL Guard (G2000) - System ochrony baz danych
- dwa (2) zegary czasu – odpowiadających za synchronizację czasu



Rys. 4. Strefa BackEnd

Wszystkie połączenia logiczne dla sieci IP w strefie BackEnd są obsługiwane w każdej lokalizacji przez parę przełączników EX4200 połączonych w stos (S-LAN-SWI-1303/1304 / B-LAN-SWI-2303/2304). Do przełączników tych zostały podłączone serwery bazodanowe, serwery monitoringu, serwery logów (RSA), serwery czasu, serwery PKI, serwer zarządzania siecią Junos Space oraz klaster zapór sieciowych *firewall* strefy BackEnd (CheckPoint 5600).
Połączenia do serwerów bazodanowych (oznaczone kolorem zielonym) składają się z dwóch połączeń fizycznych (mechanizm równoważenia obciążenia i przełączenia na drugie łącze (*teaming*[1])) w celu zwiększenia niezawodności. Pozostałe serwery, z uwagi na zdublowanie swoich funkcji oraz fakt, iż nie działają na nich systemy czasu rzeczywistego (od których zależy bezpośrednio działanie aplikacji PLI CBD), zostały podłączone pojedynczymi łączami.

3.1 Klaster zapór sieciowych firewall CheckPoint

Klaster dwóch urządzeń CheckPoint 5600 pełni funkcję systemu separacji dla strefy BackEnd w każdej z lokalizacji.
Urządzenia zostały w każdej z lokalizacji połączone w klaster typu Active-Standby z synchronizacją stanu.

[1] LBFO (ang. *Load Balancing and FailOver*)

3.2 Przełącznik EX4200

W celu realizacji połączeń drugiej warstwy w strefie BackEnd, w każdym z Ośrodków zainstalowano dwa przełączniki EX4200. Przełączniki połączone zostały w jeden przełącznik wirtualny z wykorzystaniem technologii Virtual Chassis, za pomocą dedykowanych portów VCP (*Virtual Chassis Port*). W każdym przełączniku wykorzystane zostały oba porty VCP w celu zestawienia stosu uodpornionego na awarię jednego z połączeń w obrębie Virtual Chassis. Przełączniki pełnią następujące role w Virtual Chassis:

- Jeden przełącznik w funkcji Master – nadzór nad połączeniem Virtual Chassis, obsługa protokołów kontrolnych
- Jeden przełącznik w funkcji Backup – przejmuje rolę Master w przypadku jego awarii

Każdy z przełączników posiada następującą konfiguracje sprzętową:

Numer elementu	Opis	Liczba
EX4200-48T	Juniper EX 4200, 48 portów 10/100/1000 BaseT (8 portów z PoE) Zasilacz 320 W AC, Kabel tworzenia stosu 50 cm	1
EX-PWR-320-AC	Dodatkowy zasilacz 320 W AC	1
EX-UM-2X4SFP	dwa porty 10G SFP+ / cztery porty 1G SFP Uplink Module dla EX4200 i EX3200	1

3.3 System zarządzania siecią Junos Space

Na potrzeby zarządzania urządzeniami Juniper, w każdej z lokalizacji został wdrożony system Junos Space składający się z pakietów w wersjach:

- Junos Space 21.1R1.4
- Network Director 5.1R1.98
- Security Director 21.1R1
- Log Collector 20.1.1.22

Wszystkie komponenty systemu Junos Space zostały zainstalowane na wirtualizatorze KVM (Kernel-based Virtual Machine) opartego o system CentoOS 7. Zainstalowano to na serwerze o adresie 10.10X.0.195. Do instalacji wykorzystano dwie wirtualne maszyny, odpowiednio dla modułów Space, Network Director i Security Director jedną, a dla Log Collector'a drugą.

3.4 Synchronizacja czasu

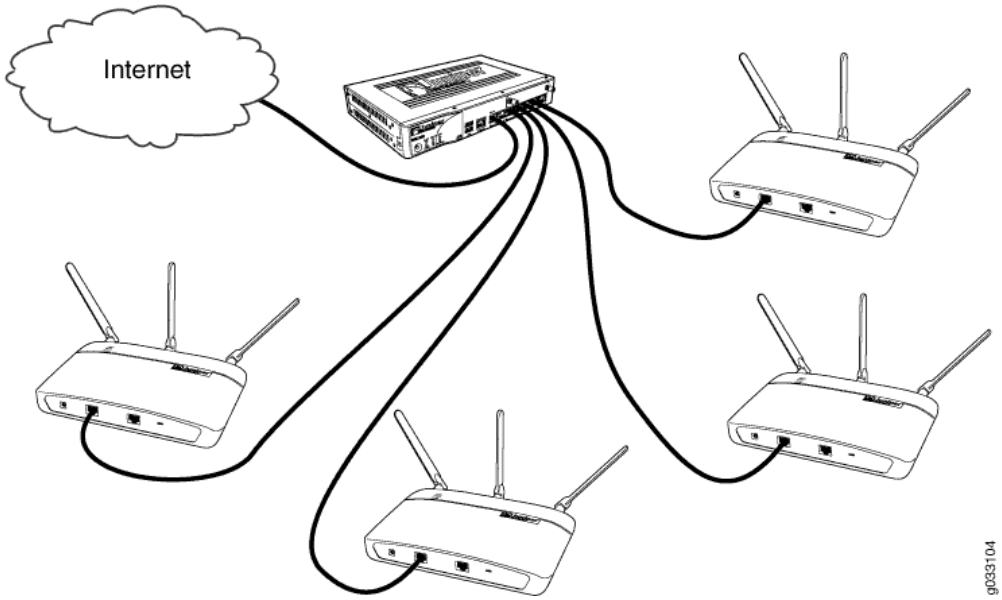
Wszystkie urządzenia posiadają synchronizację czasu opierając się na mechanizmie protokołu NTP. Funkcję serwerów czasu pełnią po dwa urządzenia Spectracom Netclock 9383 (pobierają czas z satelity i z internetu) umieszczone w strefie BackEnd każdej z lokalizacji.

4. Lokalizacja w centrali UKE w Warszawie

W celu wykonania sieci logicznej w Centrali UKE w Warszawie Wykonawca dostarczył firewall Juniper SRX210 HE2-POE i 4 bezprzewodowe punkty dostępowe Aruba IAP-305-RW w oparciu, o które wykonana została sieć bezprzewodowa WiFi.

W ramach budowanego rozwiązania dostarczone zostały następujące elementy:

- **Urządzenie firewall:** SRX services gateway 210 with 2xGE + 6xFE ports, 1xmini-PIM slot, 2GB DRAM and 2GB Flash and 4 ports of POE (SRX210HE2-POE)
- **Licencję na dziesięciu użytkowników VPN:** Dynamic VPN Svc: 10 Sim Access Mgr Usrs
- **Zestaw montażowy SRX210:** SRX210 Rack mount kit for 19" rack(SRX210-RMK)
- Bezprzewodowe punkty dostępowe: 4x Aruba IAP-305-RW



Rys. 5. Schemat sieci w Centrali UKE