Załącznik nr 1 do Opisu Przedmiotu Zamówienia Specyfikacji Istotnych Warunków Zamówienia pn. Zaprojektowanie i wdrożenie zapasowej serwerowni systemów projektu Podlaskiego Systemu Informacyjnego e-Zdrowie w Urzędzie Marszałkowskim Województwa Podlaskiego

DOKUMENTACJA TECHNICZNA WDROŻENIA URZĄDZEŃ SIECIOWYCH, SERWERÓW, PAMIĘCI MASOWYCH ORAZ BEZPIECZEŃSTWA

Miejsce wdrożenia: Urząd Marszałkowski

Województwa Podlaskiego

Ul. Kardynała Stefana Wyszyńskiego 1, 15-888 Białystok

SPIS TREŚCI

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

SPIS RYSUNKÓW

SPIS TABEL

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

1. Opis architektury UMWP[1]

1.1. Architektura sprzętowo-systemowa UMWP

Rysunek 1 przedstawia architekturę sprzętową, sieciową i systemową dla projektu PSIeZ w części regionalnej. Serwery fizyczne oznaczono kolorem czarnym. Czerwonym kolorem zaznaczono systemy przeznaczone do wirtualizacji, wraz z szacowaną, dedykowaną dla nich wielkością przestrzeni dyskowej macierzy. Obszar wirtualny zostanie zainstalowany na dwóch serwerach o dużej mocy, połączonych poprzez FCoE i zwirtualizowane karty CNA do macierzy dyskowych. Macierz będzie udostępniała powierzchnie szybkich dysków SAS zastosowanych ze względu na systemy wirtualne i chęć zapewnienia poprawnego działania mechanizmu vMotion lub równoważnego, oferującego tą samą funkcjonalność.

Obszar ciemnoniebieski na rysunku to system bazy danych, udostępniający dane dla systemów transakcyjnych. System ten umieszczony jest na dwóch serwerach połączonych do macierzy danych poprzez FCoE i karty CNA. System ten będzie korzystał z szybkich dysków SAS.

Obszar zielony to wolny i pojemny obszar macierzy, zainstalowany na dyskach SATA, dla systemów baz danych plikowych, zainstalowanych na dwóch serwerach w klastrze active passive. Serwery te również są połączone poprzez karty CNA. Serwery te będą zabezpieczać się wzajemnie, tj. jeden będzie aktywnie obsługiwać żądania transakcyjne, a drugi będzie aktywnie obsługiwać żądania plikowe. W przypadku awarii jednego z serwerów, drugi przejmie jego rolę. Serwer plikowy będzie przechowywał dane medyczne z podmiotów leczniczych na dodatkowej szyfrowanej przez macierz półce dyskowej z dyskami SATA.

Wszystkie serwery inne niż bazy danych zostaną zwirtualizowane. Dzięki takiemu rozwiązaniu ilość wymaganych serwerów fizycznych w projekcie jest minimalna, ponieważ każdy z systemów może zostać umieszczony na przestrzeni zwirtualizowanej i podłączony do jednej z dwóch baz danych. W przestrzeni wirtualnej zostanie dodatkowo umieszczony serwer LDAP pełniący rolę master root serwera domeny, a także udostępniający kontenery trust'ów dla kopii lokalnych; tych serwerów w podmiotach leczniczych.

W przestrzeni wirtualnej zostanie umieszczony serwer backupu dla baz danych i snapshotów systemów zwirtualizowanych wykonujący backupy danych na taśmy DLT biblioteki taśmowej, przy lub bez pomocy dodatkowej pamięci dyskowej macierzy. Dane backupu będą przekazywane do macierzy poprzez dodatkowy odrębny kanał Fibre Channel. Serwery fizyczne zostaną połączone do sieci za pomocą kart CNA i NIC do przełączników 10 Gbit. Sieci zostaną odseparowane od siebie VLANami, a ruch pomiędzy VLANami będzie filtrowany przez sprzętowe urządzenia typu Firewall. Ruch na każdym z portów będzie dodatkowo sprawdzany poprzez IPS. Ruch na styku z siecią Internet będzie monitorowany przez oddzielny IPS i Firewall.

[1] Opis na podstawie OPZ

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Dodatkowo, na potrzeby wdrażanego systemu dostarczone zostaną również serwery zarządzania i monitoringu sieci oraz zaawansowane serwery bezpieczeństwa typu appliance. Systemy udostępniające dane i systemy portalowe zostaną odseparowane fizycznie od reszty systemów i umieszczone w strefach DMZ. Systemy obsługujące warstwę integracyjną zostaną umieszczone w strefie DMZ WAN (VLAN WAN). Założono, że przed przesłaniem danych do systemów w sieci WAN, zostaną one poddane deduplikacji poprzez urządzenia akceleracji WAN. Wszystkie dane w WAN będą szyfrowane z wykorzystaniem algorytmu AES o długości klucza 256-bit.

Macierz dyskowa zostanie podłączona do przełącznika FCoE poprzez karty FC 8 Gbit. Karty 1 Gbit zostały przewidziane do celów zarządzania macierzą.

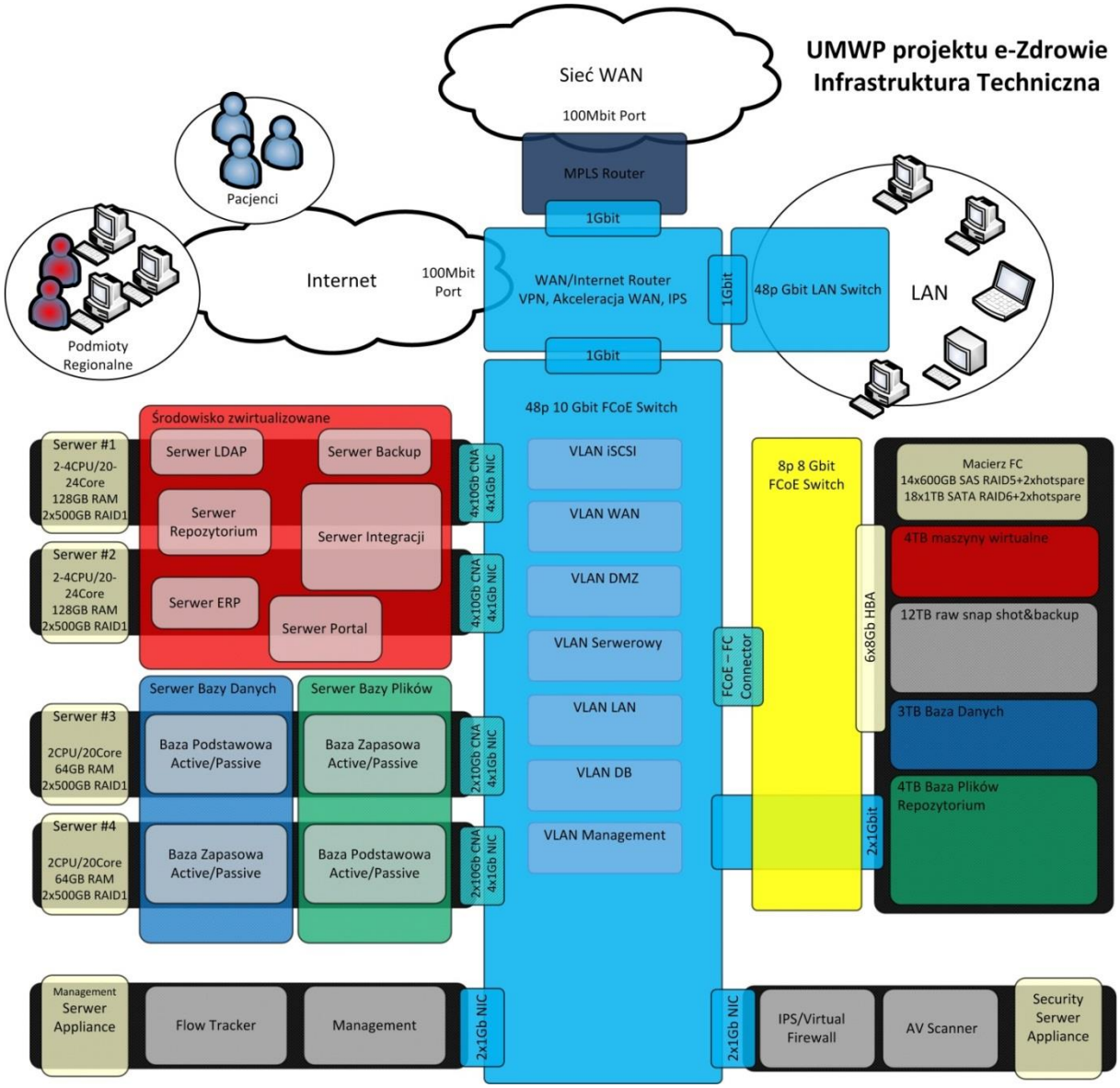
System do zarządzania serwerami wirtualnymi zostanie umieszczony na jednym z serwerów wirtualnych. Dostęp do wszystkich systemów będzie odbywał się poprzez model uprawnień grupowych przyznawanych poprzez wzajemne zaufanie domen i kontenery domen.

Użytkownicy systemów portalowych będą się do nich logować za pomocą przeglądarki z wykorzystaniem SSL wykorzystując wewnętrzną, inna niż wewnętrzny system LDAP, bazę danych użytkowników portalu.

Do połączenia wszystkich elementów sieci będą zastosowane switche core L3 oraz dostępowe FCoE.

Infrastruktura zostanie skonfigurowana tak, aby w przyszłości dało się ją zdublować do innej serwerowni.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 1 Architektura logiczna sprzętowo-sieciowa systemów projektu e-Zdrowie w części regionalnej systemu w UMWP;

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

2. Urządzenia w projekcie

Poniższa tabela zawiera spis urządzeń dostarczonych w projekcie e-zdrowie dla UMWP.

Funkcja	PN	Opis	Ilosć
WAN + Akceleracja			
router	CISCO2951-SEC/K9	Cisco 2951 Security Bundle w/SEC license PAK	1
Akcelerator WAAS	WAVE-694-K9	Wide Area Virtualization Engine 694	1
WAAS Central Manager	WAVE-294-K9	Wide Area Virtualization Engine 294	1
Firewall			
zabezpieczenie aplikacji	ASA5585-S10X-K9	ASA 5585-X Chas with SSP10,8GE,2SFP+,2GE Mgt,2 AC,3DES/AES	1
	SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter	2
zabezpieczenie styku do Internetu	ASA5515-IPS-K9	ASA 5515-X with IPS, SW, 6GE Data, 1GE Mgmt, AC, 3DES/AES	1
LAN			
przełącznik core	WS-C3750X-24T-S	Catalyst 3750X 24 Port Data IP Base	1
	C3KX-PWR-350WAC/2	Catalyst 3K-X 350W AC Secondary Power Supply	1
	C3KX-NM-10G	Catalyst 3K-X 10G Network Module option PID	1
	SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter	2
Serwerownia			
Serwer dla systemu wirtualnego RACK	UCSC-C240-M3L		2
Serwer baz danych RACK	UCSC-C240-M3L		2
Serwer pod system monitoringu LAN/WAN	UCSC-C240-M3L		1
przełącznik Eth/FCoE/FC	N5K-C5548UP-FA	Nexus 5548 UP Chassis, 32 10GbE Ports, 2 PS, 2 Fans	1
Macierz FC RACK	FAS3240-R5		1
Biblioteka taśmowa Backup	IBM TL3100	TS3100 Tape Library	

Tabela 1 Zestawienie sprzętu dostarczonego w ramach projektu E-Zdrowie

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

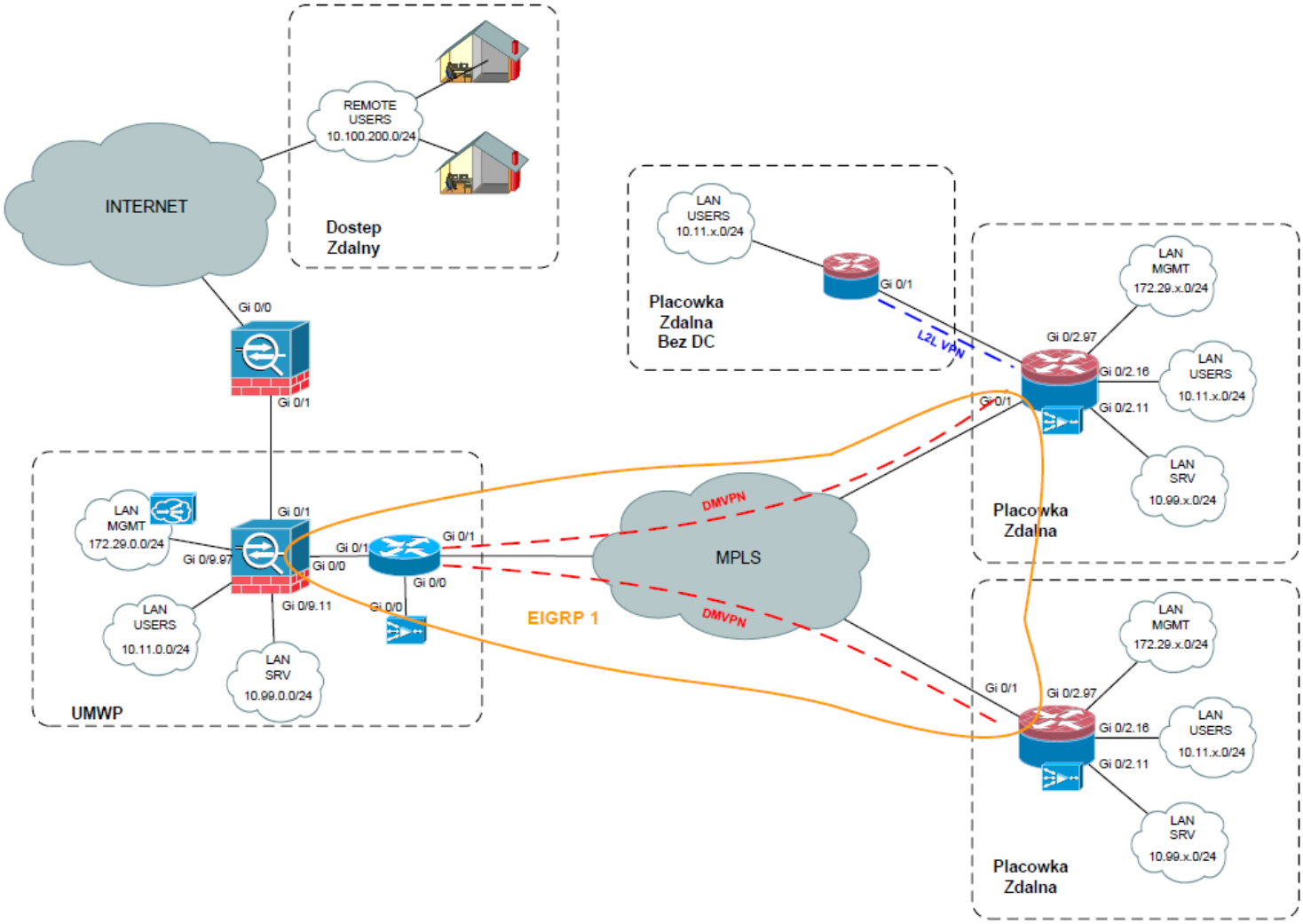
3. Architektura sieci WAN

W projekcie ePodlasie sieć rozległa WAN ma za zadanie zapewnienie komunikacji w warstwie trzeciej pomiędzy wszystkimi lokalizacjami. Każda z lokalizacji jest wyposażona w router klasy Cisco 2900, posiadający trzy interfejsy Ethernet i zapewniający styk pomiędzy siecią WAN i LAN. Połączenie pomiędzy routerami zrealizowane jest w technologii MPLS, dostarczonej przez Service Provider'a - firmę NETIA.

Do podłączenia się do sieci MPLS routery wykorzystują sieci połączeniowe z długością maski 30 bitów, których adresacja jest narzucona przez Service Providera. Dodatkowo Provider rozgłasza w sieci MPLS adresację interfejsów Loopback0 z klasy adresowej 10.128.0.0/24. Ostatni oktet adresu interfejsu Loopback 0 odpowiada umownemu numerowi placówki.

Sieć WAN zbudowana jest w architekturze HUB-AND-SPOKE. W projekcie rolę Huba pełni router zlokalizowany w Urzędzie Marszałkowskim Województwa Podlaskiego w Białymstoku. Poniższy rysunek przedstawia logiczny schemat połączeń za pośrednictwem sieci WAN pomiędzy placówkami medycznymi a Urzędem Marszałkowskim.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 2 Schemat logiczny połączeń sieci WAN i LAN – rys koncepcyjny

Router w każdej z placówek medycznych nawiązuje połączenie z routerem w Urzędzie Marszałkowskim wykorzystując w tym celu dynamicznie zestawiane tunele w technice DMVPN.

W warstwie fizycznej do połączenia z siecią MPLS, wykorzystuje interfejs GigabitEthernet 0/1. Poniżej ogólny schemat konfiguracji interfejsów wykorzystywanych w połączeniu MPLS.

W celu zapewnienia komunikacji na poziomie adresacji MPLS, router UMWP ma skonfigurowany routing statyczny do sieci 192.168.255.0/24 oraz 10.128.0.0/24.

3.1. Szyfrowanie

Jednym z wymogów projektowych było zapewnienie bezpiecznej transmisji danym poprzez sieć WAN z wykorzystaniem szyfrowania oraz ograniczenie komunikacji pomiędzy placówkami. Osiągnięto to

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

zestawiając szyfrowane kanały pomiędzy placówkami a lokalizacją centralną UMWP. Z punktu widzenia ruchu w kanałach szyfrowanych powstała topologia gwiazdy z centralnym punktem w lokalizacji UMWP. Szyfrowanie zrealizowano w technologii opracowanej przez firmę Cisco - DMVPN w fazie pierwszej. W technologii DMVPN w fazie pierwszej do zestawiania połączeń wykorzystuje się kanały GRE zestawione pomiędzy centralnym punktem a lokalizacjami zdalnym, zabezpieczone protokołem IPSec. Kanały zestawiane są dynamicznie w przypadku dostępności obu węzłów i wykorzystują jako punkty końcowe interfejsy Loopback0. Do budowy tunelu użyto interfejsu logicznego Tunnel0 z adresacją IP z klasy 10.128.1.0/24. Każda ze zdalnych lokalizacji w topologii gwiazdy ma analogiczną konfigurację, dodanie kolejnej placówki wymaga jedynie zmiany adresu IP.

Na potrzeby protokołu IPSec na routerze w lokalizacji centralnej UMWP, został skonfigurowany urząd certyfikacji CA, który wystawia certyfikaty dla urządzeń w lokalizacjach zdalnych. Takie rozwiązanie zapewnia elastyczny sposób uwierzytelniania routerów i zestawiania szyfrowanej transmisji w oparciu o IPSec.

Protokół IPSec skonfigurowano w oparciu o uwierzytelnianie w pierwszej fazie z wykorzystaniem PKI i algorytmu szyfrowania AES_256.

Z uwagi na wydajność transmisji w fazie drugiej do szyfrowania użyto algorytmu 3DES.

3.2. Realizacja Routingu pomiędzy placówką medyczną a Urzędem Marszałkowskim

W topologii powstałej po zestawieniu tuneli szyfrowanych, uruchomiono protokół routingu EIGRP, który odpowiedzialny jest za dynamiczne rozgłaszanie sieci w poszczególnych placówkach. Każdy z routerów rozgłasza sieci w jego zasięgu jedynie poprzez interfejs Tunnel 0 (X-nr placówki)

Natomiast router w UMWP z perspektywy protokołu EIGRP wymienia się trasami z wykorzystanie dwóch interfejsów - Tunnael 0 oraz GigabitEthernet0/2.501.

W konfiguracji protokołu EIGRP zawarto również redystrybucję tras statycznych z wykorzystaniem route mapy STATIC_TO_EIGRP. Redystrybuuje ona statyczne trasy, które mieszczą się w zakresie listy prefiksów zawartych w REDI_STATIC, do których skonfigurowano trasy statyczne . W chwili obecnej redystrybuowana jest klasa adresowa wykorzystywana w profilu VPN.

Od strony sieci LAN router łączy się z systemem firewall za pośrednictwem subinterfejsu GigabitEthernet0/2.501 na interfejsie fizycznym GigabitEthernet0/2.

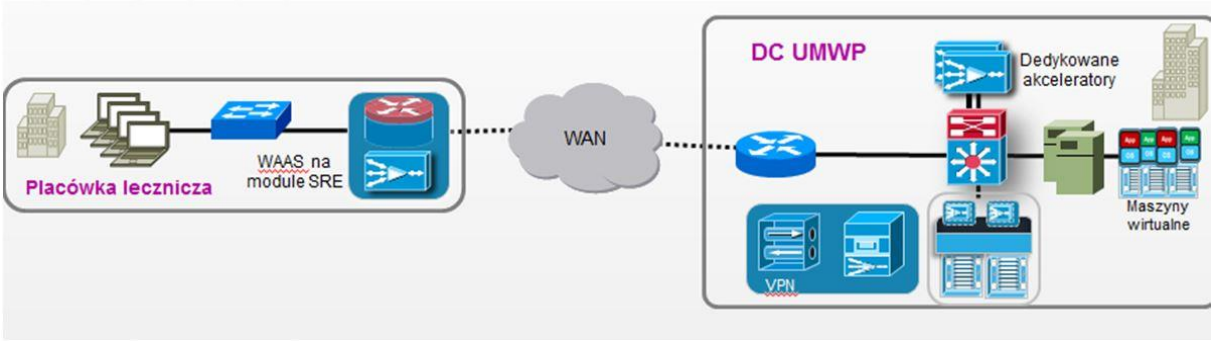
Zastosowanie subinterfejsu daje możliwość przyszłego wykorzystanie interfejsu fizycznego do połączenia z dodatkowymi segmentami sieci.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

3.3. Realizacja optymalizacji transmisji w sieci WAN przy wykorzystaniu Cisco WAAS

W celu podniesienia wydajności pracy w sieci WAN, routery są wyposażone w sprzętowe moduły akceleracji ruchu, natomiast w placówce UMWP zastosowano dedykowaną platformę sprzętową podłączoną ro routera z wykorzystaniem interfejsu GigabitEthernet0/0.

Akceleracja dotyczy ruchu przesyłanego pomiędzy serwerami w lokalizacji centralnej i lokalizacjami zdalnymi. Poniższy schemat przedstawia model działania optymalizacji w projekcie E-Zdrowie.



Rysunek 3 Schemat działania akceleratorów WAAS

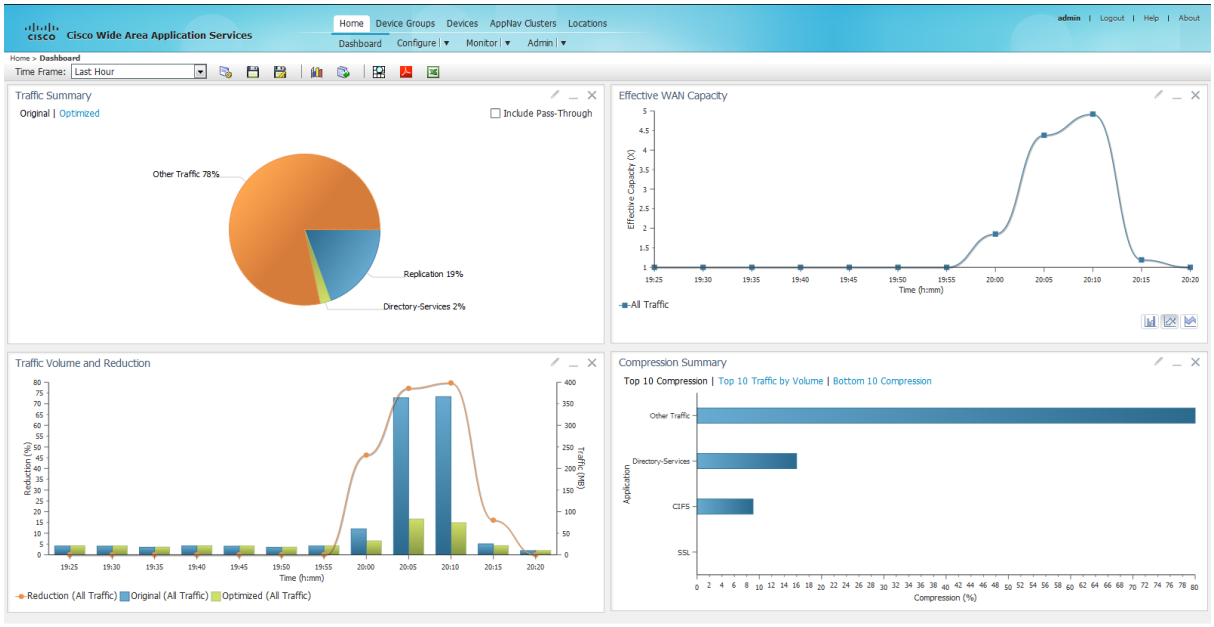
Komunikacja pomiędzy routerami i modułami akcelerującymi wykorzystywany jest protokół WCCP oraz grupa 61 i 62.

Do kwalifikowania ruchu przeznaczonego do akceleracji używana jest lista dostępu.

Akcelerator w UMWP jest zarządzany centralnie. Jego minimalna konfiguracja pozwalająca na uruchomienie jest przedstawiona poniżej.

W celu zarządzania infrastrukturą akceleratorów w lokalizacji UMWP znajduje się centralny system zarządzania - Central Manager - za pomocą, konfigurujemy oraz monitorujemy pracę wszystkich akceleratorów uruchomionych w sieci WAN ePodlasie. Zarządzanie Centrall Managerem odbywa się z wykorzystaniem interfejsu graficznego, dostępnego poprzez przeglądarkę internetową.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 4 Interfejs Central Manager Cisco WAAS

Zarządzanie samym Centrall Managerem odbywa się również z poziomu konsoli graficznej. Z użyciem interfejsu CLI mamy możliwość skonfigurowania jedynie poniższych parametrów podstawowych umożliwiających podłączenie się poprzez przeglądarkę internetową.

3.4. Reguły bezpieczeństwa z wykorzystaniem Firewall'a Cisco ASA

W lokalizacji centralnej UMWP z uwagi na wydajność zastosowano sprzętowy firewall jako oddzielne urządzenie Cisco ASA. Jest to wydajna platforma sprzętowa pozwalająca na inspekcję ruchu w wyższych warstwach. W lokalizacji UMWP firewall łączy ze sobą segmenty sieci LAN, WAN oran styku z siecią Internet. Firewall ASA pracuje w oparciu o przypisane do interfejsów poziomy zaufania, przepuszczając domyślnie jedynie ruch przychodzący z interfejsu o większym poziomie zaufania w kierunku interfejsu o mniejszym poziomie zaufania. Takie podejście minimalizuje podstawową konfigurację. Poniżej konfiguracja interfejsów urządzenia wraz z przypisanymi im poziomami zaufania.

Firewall posiada również uruchomioną inspekcję podstawowych protokołów, które tego wymagają co zapewnia im poprawną pracę.

W celu zapewnienia poprawnej i optymalnej dostępności placówek zdalnych poprzez sieć WAN, analogicznie jak w przypadku routerów, na urządzeniu firewall uruchomiono protokół routingu EIGRP. W ramach protokołu aktywny jest interfejs GigabitEthernet0/0 od strony sieci WAN.

Ponadto skonfigurowano domyślną trasę routingu w kierunku sieci Internet.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Oprócz domyślnych mechanizmów ochrony skonfigurowano na poszczególnych interfejsach listy dostępu jak poniżej. Należy wziąć pod uwagę, że na tym etapie projektu, nie jesteśmy w stanie określić poprawnie wymaganego ruchu związanego z przyszłymi aplikacjami pracującymi na wdrażanej infrastrukturze data center. W związku z tym przyjęto założenie, że listy dostępu powinny umożliwiać bezproblemowe prace wdrożeniowe i w chwili obecnej nie mają one charakteru uszczelnienia w sposób maksymalny ruchu sieciowego pomiędzy lokalizacjami w ramach sieci WAN ePodlasie. Samo skonfigurowanie list dostępu wraz z polityką inspekcji zapewnia bazę do późniejszych prac administracyjnych.

3.5. Styk z Internetem

Lokalizacja centralna UMWP posiada w ramach projektu dostęp do sieci Internet. W celu zabezpieczenia sieci e Podlasie od strony Internetu zdecydowano się na zastosowanie odseparowanego sprzętowo firewalla Cisco ASA. Funkcjonalnie firewall na styku z Internetem jest takim samym urządzeniem jak opisywane w poprzednim akapicie i pracuje również w oparciu o poziom zaufania poszczególnych interfejsów i zasadę dopuszczania domyślnie jedynie ruchu przychodzącego z interfejsu o większym poziomie zaufania i wychodzącego interfejsem o mniejszym poziomie zaufania.

Urządzenie posiada skonfigurowane dwa interfejsy, jeden od strony sieci Internet i jeden od strony sieci ePodlasie, co czyni je podstawowym i spójnym punktem demarkacyjnym.

W systemie skonfigurowano routing statyczny z domyślną trasą w kierunku sieci Internet oraz z trasami do sieci stosowanych w sieci ePodlasie.

W celu zapewnienia dostępu do Internetu z sieci wewnętrznej zastosowano funkcję natowania adresacji wykorzystywanych klas prywatnych na adres publiczny interfejsu.

W chwili obecnej nie dopuszczono żadnego ruchu od strony sieci Internet do wewnątrz sieci ePodlasie. Pomimo tego została założona lista dostępu na interfejsie od strony sieci Internet, w której skonfigurowano możliwość wykorzystania protokołu ICMP, celem ułatwienia diagnozowania ewentualnych problemów z połączeniem sieciowym.

Firewall Cisco ASA pełni również funkcję koncentratora VPN zapewniając bezpieczny zdalny dostęp do zasobów ePodlasia. Wstępna konfiguracja umożliwia zdalne połączenie typu "remote warrior" z wykorzystaniem klienta IPSec VPN.

Lista dostępu zapewnia separację sieci ruchu sieci lokalnej i sieci zdalnej z perspektywy użytkownika połączonego poprzez VPN.

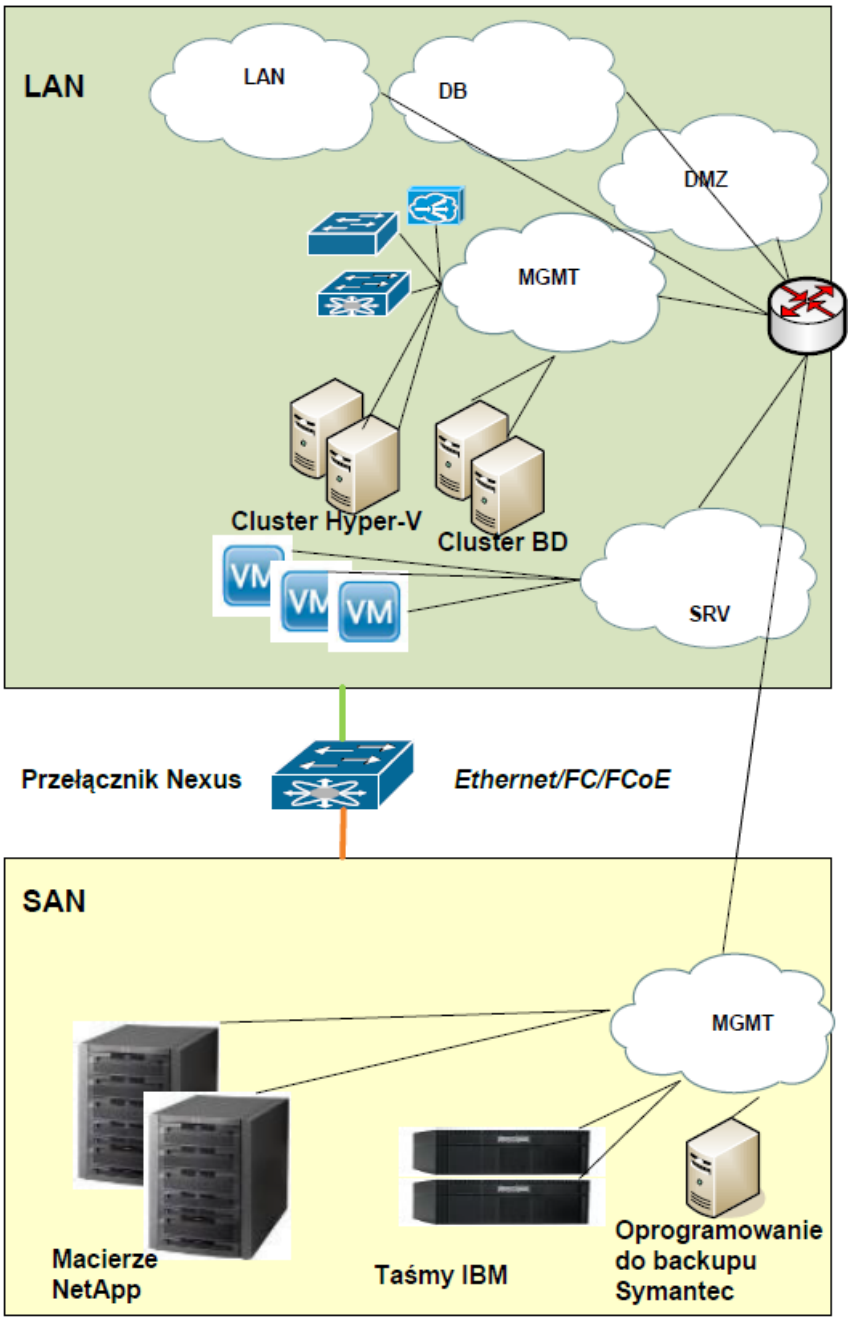
Należy mieć na uwadze, że powyższa konfiguracja sytemu firewall jest konfiguracją bazową zapewniającą bezpieczeństwo i funkcjonalność na etapie wdrażania aplikacji. Systemy firewall wymagają monitorowania i wprowadzania zmian w przypadku zmiany w środowiskach sieciowych i aplikacyjnych.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

4. Architektura sieci LAN/SAN

4.1. Koncepcja budowy sieci

Topologia sieci w UMWP przedstawiona została na poniższym diagramie:



Rysunek 5 Topologia sieci UMWP– schemat poglądowy

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

4.2. Warstwa fizyczna sieci

Zbudowana w UMWP sieć oparta została o różnego typu okablowanie. Niektóre połączenia realizowane są za pomocą skrętki miedzianej, inne za pomocą światłowodów a jeszcze inne za pomocą kabli typu Twinax. Różne medium transmisji zostało przede wszystkim podyktowane wykorzystaniem różnych protokołów transmisji (Ethernet, FC, FCoE).

4.2.1. Połączenia na poszczególnych portach urządzeń

Fizyczne połączenia pomiędzy poszczególnymi urządzeniami przedstawiono w tabelach.

Poniższa tabela przedstawia połączenia fizyczne wychodzące z przełącznika sw-1-umwp.

port	podłączone urządzenie	port podłączonego urządzenia[2]	typ połączenia
Gi/01	BRAK	N/A	N/A
Gi/02	BRAK	N/A	N/A
Gi/03	BRAK	N/A	N/A
Gi/04	BRAK	N/A	N/A
Gi/05	UPS_1	Ethernet	miedź
Gi/06	UPS_2	Ethernet	miedź
Gi/07	FW-UMWP	Gi0/0	miedź
Gi/08	rtr-1-umwp?	Gi0/2	miedź
Gi/09	BRAK	N/A	N/A
Gi/10	UMWP-DC0	Port Ethernet	miedź
Gi/11	fas3220-1	e0b	miedź
Gi/12	WAAS CM	Ge0/0	miedź
Gi/13	IBM Tape1	Port Ethernet	miedź
Gi/14	IBM Tape2	Port Ethernet	miedź
Gi/15	VPM/NPA	LOM#1	miedź
Gi/16	VPM/NPA	Port CIMC	miedź

[2] W celu zlokalizowania odpowiedniego portu konkretnego urządzenia należy odwołać się do Instrukcji Obsługi dostarczonej w ramach projektu

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Gi/17	UMWP-HOST1	port CIMC	miedź
Gi/18	UMWP-HOST2	port CIMC	miedź
Gi/19	UMWP-B1	port CIMC	miedź
Gi/20	UMWP-B2	port CIMC	miedź
Gi/21	fas3220-1	e0M	miedź
Gi/22	fas3220-2	e0M	miedź
Gi/23	fas3220-1	e0a	miedź
Gi/24	fas3220-2	e0b	miedź
Porty uplink			
Ge1			
Ge2/Te1	SW-N5K-UMWP	Ethernet 20	Twinax
Ge3			
Ge4/Te2			

Tabela 2 Połączenia fizyczne przełącznika sw-1-umwp

Poniższa tabela przedstawia połączenia fizyczne wychodzące z przełącznika Nexus N5k-umwp.

port	Podłączone urządzenie	Port podłączonego urządzenia	Typ połączenia
Eth1	UMWP-HOST1	PORT0/dolny	Twinax
Eth 2	UMWP-HOST2	PORT0/dolny	Twinax
Eth 3	UMWP-B1	PORT0/dolny	Twinax
Eth 4	UMWP-B2	PORT0/dolny	Twinax
Eth 5	fas3220-1	PORT1/górny	Twinax
Eth 6	fas3220-2	PORT1/górny	Twinax
Eth 7	IBM-BACKUP	PORT0	Twinax
Eth 8	BRAK	N/A	N/A
Eth 9	BRAK	N/A	N/A
Eth 10	BRAK	N/A	N/A
Eth 11	BRAK	N/A	N/A

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Eth 12	BRAK	N/A	N/A
Eth 13	UMWP-HOST1	PORT1/dolny	Twinax
Eth 14	UMWP-HOST2	PORT1/dolny	Twinax
Eth 15	UMWP-B1	PORT1/dolny	Twinax
Eth 16	UMWP-B2	PORT1/dolny	Twinax
Eth 17	IBM-BACKUP	PORT1	Twinax
Eth 18	BRAK	N/A	N/A
Eth 19	BRAK	N/A	N/A
Eth 20	Sw-1-UMWP	TenGigabit1/1/1	Twinax
Eth 21	BRAK	N/A	N/A
Eth 22	FW-UMWP	TenGigabit 9	Twinax
Eth 23	BRAK	N/A	N/A
Eth 24	BRAK	N/A	N/A
Eth 25	BRAK	N/A	N/A
Eth 26	BRAK	N/A	N/A
Eth 27	BRAK	N/A	N/A
Eth 28	BRAK	N/A	N/A
Eth 29	TS3100-1	Port FC	Światłowód
Eth 30	TS3100-2	Port FC	Światłowód
Eth 31	IBM-BACKUP	Port 0 – FC	Światłowód
Eth 32	BRAK	N/A	N/A

Tabela 3 Połączenia fizyczne przełącznika n5k-umwp

Poniższa tabela przedstawia połączenia fizyczne wychodzące z routera rtr-1-umwp.

Port routera	Podłączone urządzenie	Port podłączanego urządzenia
GE0/0	WAE-UMWP	Ge0/0
GE0/1	MPLS	
GE0/2	sw-1-umwp	Ge0/8

Tabela 4 Połączenia fizyczne routera rtr-1-umwp

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Poniższa tabela przedstawia połączenia fizyczne wychodzące z firewalla aplikacyjnego FW-UMWP.

Port FW-UMWP	Podłączone urządzenie	Port podłączanego urządzenia
Ethernet 0	sw-1-umwp	Ge0/7
Ethernet 1	FW-INET-UMWP	Ethernet 1
TenGigabitEthernet 0/9	SW-N5K-UMWP	Ethernet 22

Tabela 5 Połączenia fizyczne firewalla FW-UMWP

Poniższa tabela przedstawia połączenia fizyczne wychodzące z firewalla internetowego FW-INET-UMWP.

Port FW-INET-UMWP	Podłączone urządzenie	Port podłączanego urządzenia
Ethernet 0	Internet	
Ethernet 1	FW-UMWP	Ethernet 1

Tabela 6 Połączenia fizyczne firewalla FW-INET-UMWP

Poniższa tabela przedstawia bezpośrednie połączenia fizyczne pomiędzy serwerami UMWP-HOST1 oraz UMWP-HOST2.

Port Serwera UMWP-HOST1	Podłączone urządzenie	Port podłączanego urządzenia
LOM#2	UMWP-HOST2	LOM#2
LOM#4	UMWP-HOST2	LOM#4

Tabela 7 Połączenia fizyczne pomiędzy serwerami HOST1 i HOST2

Poniższa tabela przedstawia bezpośrednie połączenia fizyczne pomiędzy serwerami UMWP-B1 oraz UMWP-B2.

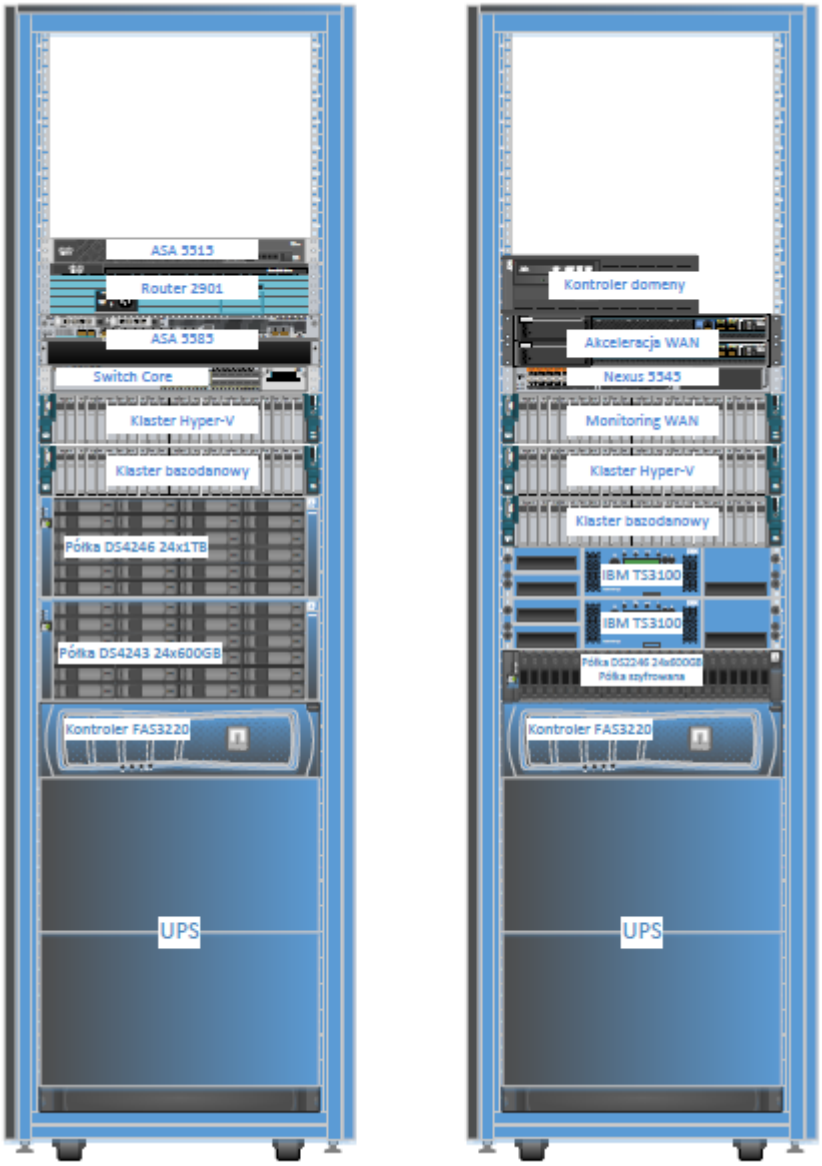
Port Serwera UMWP-B1	Podłączone urządzenie	Port podłączanego urządzenia
LOM#2	UMWP-B2	LOM#2
LOM#4	UMWP-B2	LOM#4

Tabela 8 Połączenia fizyczne pomiędzy serwerami B1 i B2

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

4.2.2. Rozmieszczenie urządzeń w szafach

Do Urzędu Marszałkowskiego dostarczone zostały dwie szafy rack z przeznaczeniem zainstalowania w nich dostarczonych w ramach projektu urządzeń.



Rysunek 6 Rozmieszczenie urządzeń w szafach rack

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

4.3. Wykorzystywane protokoły sieciowe – opis i konfiguracja

4.3.1. FC i FCoE – Fiber Channel (over Ethernet)

Zastosowany w projekcie przełącznik 10 GigabitEthernet Cisco Nexus 5000 pozwala na jednoczesne dołączenie sieci FC (SAN) i Ethernet, poprzez jeden interfejs i z prędkością 10GE (FCoE).

FCoE to metoda przesyłania ruchu FC z wykorzystaniem ramki Ethernet. Typową ramkę FC (max 2112 bajty) opakowuje się w nagłówek/końcówkę Ethernet (razem max 2180 bajtów) i przesyła poprzez interfejs Ethernet, tyle że w obrębie zdefniowanej specjalnej klasy ruchu (CoS), zapewniającej transmisję bez utraty nawet pojedynczych ramek i z gwarantowanym pasmem.

Poza realizacją Ethernetu, przełącznik ten jednocześnie jest przełącznikiem Fibre Channel, implementującym takie standardowe mechanizmy sieci FC jak adresacja WWN, topologia w oparciu o FSPF, *Name Server*, *Zoning*,.

Dzięki implementacji dwóch typów protokołów, możliwe było dołączenie do tych urządzeń zarówno serwerów wykorzystujących interfejsy *FC over Ethernet* jak i urządzeń z klasycznymi interfejsami FC .

Zastosowanie FCoE umożliwiło konsolidację portów IP oraz SAN w serwerach. Zamiast osobnych kart Ethernet NIC (Network Interface Card) oraz FC HBA (Host Bus Adaptor) zostały zastosowane karty CNA (Converged Network Adaptor). Dzięki takiemu rozwiązaniu ilość kart, kabli i portów na przełączniku została zredukowana.

Ruch FCoE realizowany jest na pierwszych siedmiu interfejsach, do których podłączone są serwery, macierze i serwer IBM.

Natywny FiberChannel realizowany jest na czterech ostatnich interfejsach (liczba portów pracujących jako FiberChannel wymuszona przez system). Do trzech z nich podłączone są systemy IBM backup. Na urządzeniu skonfigurowane zostały dwie sieci SAN. Przy czym vfc to wirtualne interfejsy FC odpowiedzialne za transport danych typu storage przez porty FCoE. W celu uzyskania dostępu poszczególnych serwerów do zasobów macierzy na przełączniku Nexus skonfigurowane zostały zony.

4.3.2. VTP – VLAN Trunking Protocol

W sieci używany jest protokół VTP, służący do wymiany informacji o konfiguracji VLAN pomiędzy przełącznikami. VTP jest protokołem informacyjnym warstwy drugiej, który dzięki umożliwieniu przełącznikom wymiany informacji o konfiguracji VLAN, zachowuje spójną konfigurację VLAN w sieci.

Dzięki mechanizmowi oferowanemu przez protokół VTP, konfiguracja VLAN może być dokonywana przez administratora systemu na jednym przełączniku a pozostałe przełączniki w sieci automatycznie nauczą się takiej konfiguracji.

Każdy z przełączników Cisco może pracować w jednym z trzech trybów protokołu VTP. Różnice w funkcjonalności przedstawia poniższa tabelka.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Funkcja	Server Mode	Client Mode	Transparent Mode
Inicjalizuje ogłaszanie VTP	Tak	Nie	Nie
Aktualizuje lokalną bazę VLAN na podstawie odebranego ogłoszenia VTP	Tak	Tak	Nie
Przekazuje ogłoszenie VTP do sąsiadujących przełączników	Tak	Tak	Tak
Zapisuje konfigurację VLAN w pamięci NVRAM lub w pliku VLAN.DAT	Tak	Nie	Tak
Umożliwia tworzenie, modyfikację oraz kasowanie VLANów za pomocą poleceń konfiguracyjnych	Tak	Nie	Tak

Tabela 9 Funkcjonalność trybów pracy protokołu VTP

*Istnieje także czwarty tryb protokołu VTP, jest to stan 'wyłączony', w którym przełącznik nie tworzy, nie nasłuchuje i nie przekazuje ogłoszeń VTP.

Proces aktualizacji VTP rozpoczyna się w chwili gdy administrator przełącznika doda, zmodyfikuje lub usunie konfigurację VLAN, na przełączniku pracującym w trybie VTP Server. Jeśli takie zdarzenie nastąpi, VTP Server zwiększy tzw. *VTP revision number* (numer wersji bazy VTP) o 1 oraz rozpocznie ogłaszanie całej bazy VLAN, łącznie z nowym *VTP revision number*.

VTP revision number pozwala przełącznikom rozpoznać że nastąpiła zmiana bazy VLAN. Po otrzymaniu ogłoszenia VTP, jeśli revision number odebranego ogłoszenia jest większy niż bieżący revision number, przełącznik uznaje nową wersję bazy VLAN.

Przełączniki Cisco domyślnie pracują w trybie VTP Server, jednak nie wysyłają ogłoszeń VTP dopóki nie zostanie skonfigurowana nazwa domeny VTP. Po ustawieniu nazwy domeny VTP, przełącznik wysyła ogłoszenia VTP z aktualizacjami i nowym, rosnącym *revision number*, po każdej modyfikacji konfiguracji VLAN. Ogłoszenia VTP wysyłane są poprzez wszystkie aktywne porty, pracujące w trybie trunk (ISL lub 802.1Q).

Jeśli parametr *VTP domin name*, przełącznika pracującego w trybie VTP Client, nie zostanie skonfigurowany, przełącznik uzna, że pracuje w domenie VTP odczytanej z pierwszego ogłoszenia, jakie odbierze.

W celu uzyskania większej niezawodności systemu rekomendowane jest użycie przynajmniej dwóch przełączników w trybie VTP Server. Umożliwi to zachowanie oraz modyfikacje konfiguracji VLAN nawet podczas niedostępności któregoś z serwerów VTP

Ponieważ revision number oraz VTP domain name mogą być w prosty sposób podsłuchane oprogramowaniem typu Sniffer, aby zabezpieczyć system przed atakami typu Denial of Service, należy ustawić hasło VTP. Ustawianie hasła uruchomi mechanizm kodowania komunikatów VTP używając algorytmu MD5.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

W konfiguracji zastosowano mechanizm VTP Pruning, który powoduje zmniejszenie ilości ogłoszeń VTP. Informacje o VLANach nie będą rozsyłane do przełączników, które nie mają portów w danych VLANach.

4.3.3. VLAN – konfiguracja

W niniejszym projekcie utworzono następujące VLANy:

VLAN ID	Nazwa VLANu	Adres IP sieci	Maska sieci	Brama domyślna	Opis
97	Mgmt	X.X.X.X	255.255.255.0	X.X.X.X	Sieć do zarządzania
16	LAN	X.X.X.X	255.255.255.0	X.X.X.X	Sieć dla użytkowników lokalnych
11	SRV	X.X.X.X	255.255.255.0	X.X.X.X	Sieć serwerowa (m.in.. LDAP, Backup, Antywirus..)
12	DB	X.X.X.X	255.255.255.0		Sieć do komunikacji z Bazą danych
10	WAN	X.X.X.X	255.255.255.0		M.in.. Serwer integracji
63	DMZ	X.X.X.X	255.255.255.0		do systemu portalowego

Tabela 10 Lista utworzonych VLANów

Tabela zawiera dodatkowo informacje:

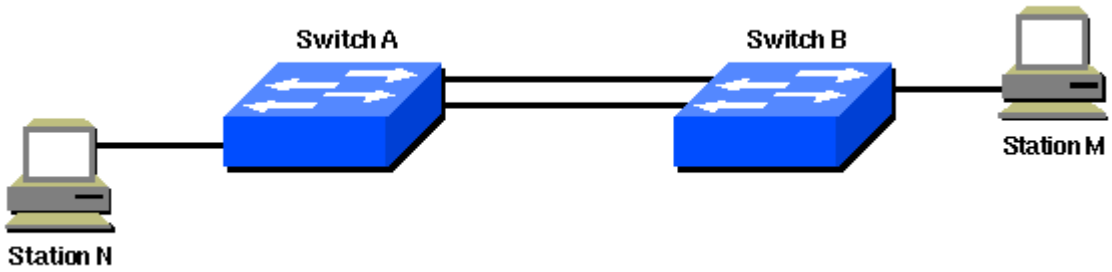
- Obsługiwana sieć przez dany VLAN
- Konfiguracja interfejsów L3 umożliwiających routing pomiędzy VLANami

4.3.4. STP – Spanning Tree Protocol

Spanning Tree Protocol (STP) jest protokołem warstwy drugiej działającym na przełącznikach oraz bridge'ach. Specyfikacja protokołu Spanning Tree jest zawarta w IEEE 802.1D. Podstawowym celem STP jest nie dopuścić do powstawania pętli w sieci LAN przy zastosowaniu redundantnych ścieżek pomiędzy przełącznikami. Powstanie pętli w sieci powoduje tzw. broadcast storm, co może spowodować zablokowanie funkcjonowania infrastruktury LAN.

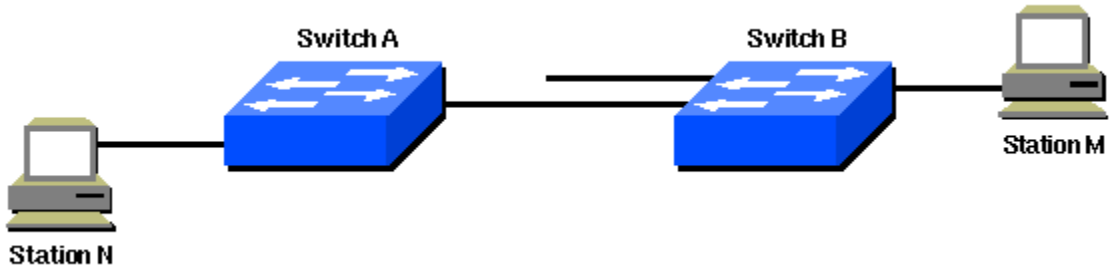
Protokołu STP używamy w sytuacji, gdy potrzebujemy zbudować redundantne połączenia ale jednocześnie uniknąć powstania pętli. Redundantne połączenia są niezwykle istotne dla wysoko dostępnej infrastruktury sieciowej, zapewnia zapasowe połączenia w przypadku awarii części połączeń sieciowych. Awaria łączy głównych aktywuje połączenia zapasowe co umożliwia kontynuację użytkowania sieci przez użytkowników. Brak protokołu STP na przełącznikach może być przyczyną awarii (niedostępności sieci) spowodowanej pojawieniem się pętli.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



W sieci widocznej na powyższym diagramie istnieje redundantne połączenie pomiędzy przełącznikiem A oraz przełącznikiem B. W konfiguracji brakuje mechanizmu STP, dlatego zapasowe połączenie powoduje powstanie pętli. Pakiet typu broadcast lub multicast wysłany przez komputer M przeznaczony dla komputera N, będzie krążył pomiędzy obydwoma przełącznikami.

W przypadku zastosowania algorytmu STP na obu przełącznikach, struktura logiczna sieci będzie wyglądała jak na poniższym diagramie.



W celu zapewnienia potrzeby istnienia redundantnych połączeń i uniknięcia powstania pętli, STP definiuje tzw. drzewo rozpinające wszystkie przełączniki w sieci. Spanning Tree wymusza przejście niektórych połączeń w stan *standby* (blocked) a inne zostawia w trybie *forwarding*. Jeśli połączenie w trybie forwarding będzie niedostępne np. z powodu awarii przełącznika, STP przekonfiguruje sieć i zbuduje nową sieć połączeń (drzewo rozpinające), aktywując odpowiednie porty będące w trybie standby.

Istotnym elementem konfiguracji STP jest wybór tzw. root switch. Przełącznik taki stanie się centralnym punktem sieci z punktu widzenia protokołu STP. Wszystkie decyzje jak wybór portów dla trybów forwarding czy blocked następują z perspektywy root switcha. Istnieje mechanizm automatycznej elekcji root switcha, jednak wysoce wskazane jest aby wybór taki dokonany był świadomie przez administratora systemu, i mający na uwadze topologię sieci. Rekomendowane jest aby root switchem był przełącznik znajdujący się w najbardziej centralnym punkcie sieci. Zazwyczaj są to przełączniki core'owe.

Każdy VLAN musi mieć ustawiony swój własny root switch, ponieważ każdy VLAN stanowi oddzielną domenę rozgłoszeniową. Root switchem dla poszczególnych VLANów może zostać jeden fizyczny przełącznik lub różne przełączniki.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Wybór root switcha dokonywany jest na podstawie parametru bridge priority. Przełącznik o najmniejszym bridge priority w sieci zostanie root switchem. Domyślna wartość parametru bridge priority w przełącznikach Cisco to 32768.

Jako 'root switche' dla sieci w projekcie e-zdrowie zostały wybrane przełączniki szkieletowe. Ustalone priorytety wskazują w pierwszej kolejności przełącznik PLKR-SW-CORE1. W przypadku jego awarii, rolę 'root switcha' przejmie przełącznik PLKR-SW-CORE2. Pozostałe przełączniki mają domyślny bridge-priority.

Dodatkowo wszystkie porty dostępowe, czyli takie, do których nie będą podłączane inne przełączniki a jedynie urządzenia końcowe typu laptop, desktop, zostały ustawione w trybie *forwarding*. Poleceniem:

Operacja taka znacząco przyspiesza podłączenie urządzenia końcowego, gdyż w takim przypadku negocjacja Spinning Tree może zostać wyłączona.

4.3.5. DTP - Dynamic Trunking Protocol

Przełączniki Cisco Catalyst używają protokołu Dynamic Trunk Protocol (DTP) do automatycznego rozpoznawania czy urządzenie po drugiej stronie połączenia może być trunkiem, jeśli tak to, jakiego protokołu użyć do zestawienia trunku.

Przełączniki Cisco domyślnie używają protokołu DTP w trybie *desirable*, co oznacza, że przełącznik inicjuje wysyłanie komunikatu DTP, mając nadzieję, że urządzenie po drugiej stronie połączenia odpowie innym komunikatem DTP. Jeśli odpowiedź zostanie odebrana, DTP może ustalić czy oba przełączniki mogą utworzyć trunk między sobą oraz za pomocą jakiego protokołu. Jeśli oba przełączniki wspierają zarówno enkapsulację ISL oraz 802.1Q, do zestawienia trunku zostanie wybrana ISL.

Dzięki trybowi DTP desirable, przełączniki mogą być w prosty sposób łączone ze sobą a porty dynamicznie będą pracować w trybie trunk.

W niniejszym projekcie zastosowano precyzyjną konfigurację portów, rezygnując z automatycznego dostosowywania parametrów co podyktowane zostało względami bezpieczeństwa.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

5. System monitoringu LAN/WAN

Wdrożenie systemu monitorowania sieci komputerowej w nowoczesnym środowisku informatycznym ma na celu poprawę funkcjonowania sieci IP w aspekcie wydajności przepływu ruchu aplikacji będących w użyciu jednostek korzystających z sieci, jak również prawidłowego wykorzystania urządzeń oraz optymalizacji istniejących łączy LAN/WAN.

Przedmiotem opisywanego wdrożenia był system monitoringu sieci TruView firmy Fluke Networks. W sieci klienta wdrożono system monitoringu w wersji wirtualnej, złożony z dwóch komponentów logicznych:

- **Kolektor vTVF(virtual TruView Flow)** - źródło danych wykorzystujące protokół Netflow/IPFIX, bazujący na interpretacji ruchu sieciowego w postaci przepływów (ang. flow-based network monitoring)
- **Portal dostępowy TVC(TruView Central)** – serwer WWW oraz platforma dostępowa do źródeł danych odpowiedzialna za korelację i prezentację danych pomiarowych, jak również pozwalająca na zarządzanie dostępem do systemu przez wielu użytkowników

Obydwa komponenty logiczne występują w postaci maszyn wirtualnych pracujących w oparciu o platformę wirtualizacyjną VMware 5.1. Platformą fizyczną natomiast jest serwer UCS C240 M3L (specyfikacja serwera znajduje się w dokumencie „Specyfikacja systemu monitoringu LAN_WAN”).

Dzięki wdrożeniu systemu do monitoringu sieci możliwe jest osiągnięcie następujących celów:

- Określenie listy aplikacji używanych w sieci korporacyjnej oraz stopnia wykorzystania zasobów sieciowych przez każdą z nich
- Obserwowanie wpływu wybranych aplikacji na siebie w wybranym (np. tym samym) obszarze sieci
- Kształtowanie obciążeń i priorytetyzacja ruchu dostępnych zasobów tak, aby spełnione zostały wymagania SLA
- Utrzymanie ciągłości pracy jednostek wykorzystujących zasoby sieciowe
- Skrócenie czasu rozwiązywania zaistniałych problemów w prawidłowym funkcjonowaniu sieci w czasie rzeczywistym
- Analizowanie pełnych danych historycznych na potrzeby raportowania menedżerskiego oraz kształtowania polityki inwestycyjnej i rozwoju zasobów sieci korporacyjnej
- Analiza parametrów TCP związanych z ruchem IP w ramach poszczególnych aplikacji

Należy zwrócić uwagę, że wdrożone rozwiązanie dzięki unikalnej architekturze, posiada bogate spektrum możliwości generowania raportów i statystyk, które mogą posłużyć jako podstawa tworzonej dokumentacji, a także forma informowania pionu zarządzającego o obecnym stanie pracy sieci.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

5.1. Opis systemu

TruView Central umożliwia łatwą integrację informacji pochodzących z różnych źródeł. Uwzględnia dane pochodzące z TruView Flow, a także wszelkich rozwiązań działających w oparciu o technologię www, w tym systemów do zarządzania klasy korporacyjnej oraz tradycyjnych źródeł danych pomocnych w usuwaniu problemów.

Architektura udostępnia unikatowe widoki dzięki korelacji danych pochodzących z różnych źródeł w obrębie rozwiązania. Ujednolicony system do monitorowania pracy sieci i serwerów zapewnia wysoki stopień widoczności. System pozwala departamentom IT na monitorowanie wydajności na podstawie kompleksowego podglądu ruchu sieciowego oraz zrozumienie jego wpływu na wydajność usług.

Funkcjonalność rozwiązania TruView Central przydatna w pracy wydziałów IT:

- Zarządzanie hierarchicznym dostępem dla użytkowników do monitorowanych zasobów sieciowych
- Personalizacja kreowanych raportów i widoków dla poszczególnych użytkowników
- Korelacja danych z TVF
- Konfiguracja systemu z jednego centralnego miejsca
- Rozbudowane raportowanie w oparciu o dane zgromadzone w kolektorze TVF

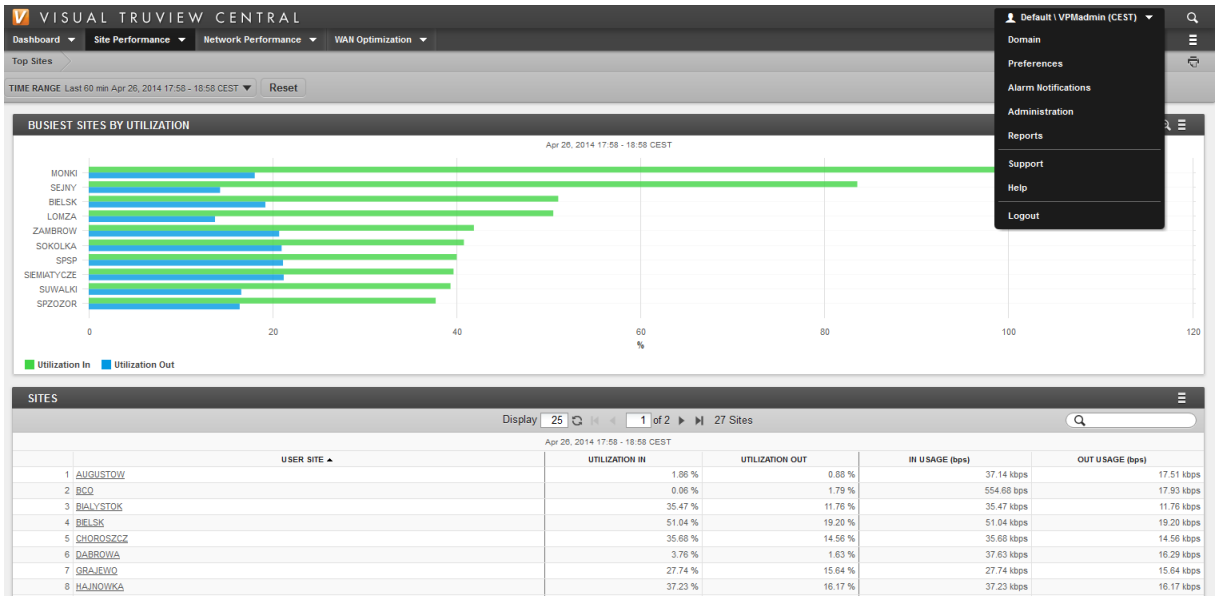
Funkcjonalność rozwiązania TVF przydatna w pracy departamentów IT:

- Zarządzanie wykorzystaniem zasobów
- Badanie profilów ruchu według
    - Aplikacji
    - Urządzeń
    - Interfejsów
- Weryfikacja prawidłowości priorytetyzacji ruchu - przydziału QoS
- Identyfikacja najaktywniejszych hostów, które w największym stopniu utylizują pasmo
- Identyfikacja wszystkich konwersacji z każdej placówki zdalnej
- Zarządzanie w sytuacjach awaryjnych
- Dostępność informacji o stanie sieci w czasie rzeczywistym z dokładnością do pojedynczych konwersacji
- Lokalizowanie użytkowników (konwersacji) powodujących przeciążenia w sieci
- Wykrywanie anomalii lub stanów nietypowych
- Zarządzanie wydajnością sieci
- Określenie tzw. *stanu normalnego* (baselinning) działania sieci

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

- Prognozowanie zapotrzebowania na pasmo i łącza na podstawie danych historycznych
- Planowanie rozwoju (zmian) sieci w oparciu o rzeczywiste, bieżące dane i parametry ruchu
- Prowadzenie polityki zgodności z uregulowaniami prawnymi i korporacyjnymi
- Wykrywanie przypadków nielegalnego wykorzystywania zasobów firmowych
- Pojawienie się nieautoryzowanych
    - Aplikacji (Recognized Applications)
    - Użytkowników (adresy IP/porty TCP)

5.2. Interfejs portalu TVC



Rysunek 7 Interfejs systemu TruView Central

Interfejs systemu posiada 4 główne zakładki:

- Zakładka Dashboard – umożliwia wyświetlanie predefiniowanych przez administratorów raportów zawierających wybrane treści
- Zakładka Site Performance – umożliwia dostęp do szczegółowych informacji o ruchu sieciowym w ramach zdefiniowanych Site'ów
- Zakładka Network Performance – umożliwia dostęp do informacji zawartych w eksportach NetFlow, które nie mieszczą się w definicjach Site'ów (np. dla interfejsów urządzeń sieciowych nie przypisanych do żadnego Site'u)
- Zakładka WAAN Optimization – zakładka prezentująca dane pochodzące z Central Manager'a Cisco WAAS na temat optymalizacji ruchu na łączach WAN

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

W prawym górnym rogu interfejsu znajduje się nazwa zalogowanego użytkownika, która po kliknięciu umożliwia przejście do panelu Administratora.

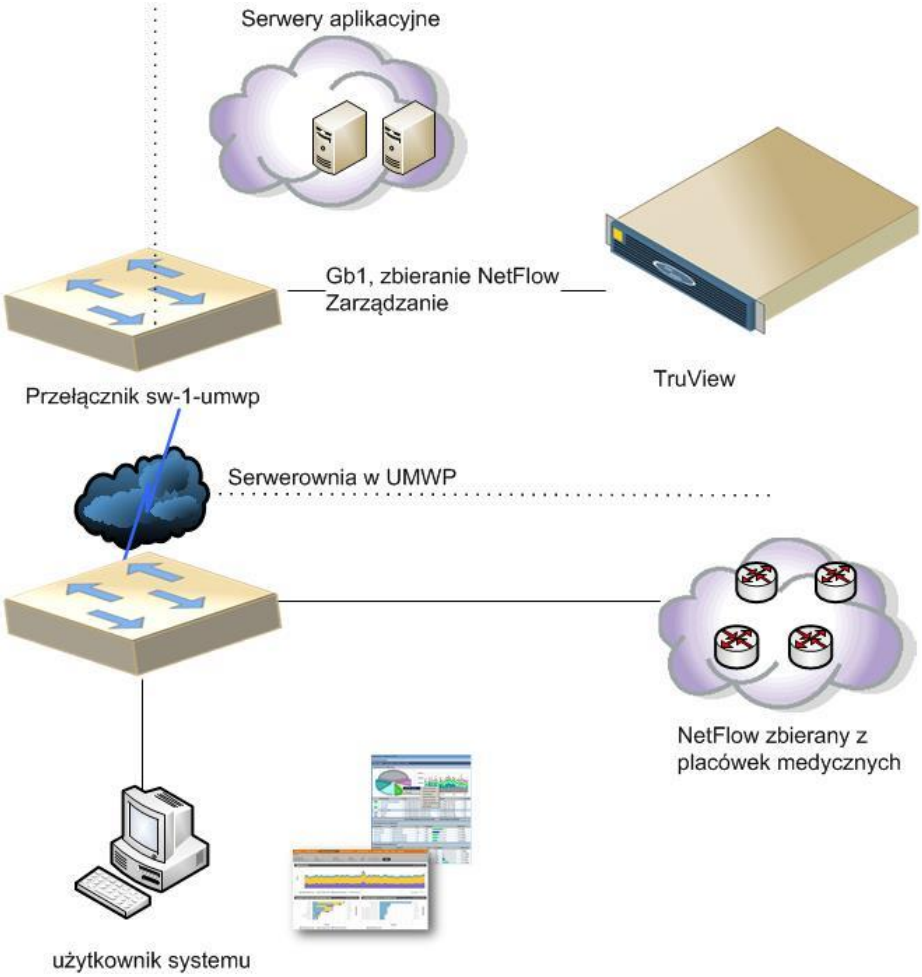
5.3. Opis faz i zadań podczas wdrożenia systemu monitoringu

Przeprowadzone wdrożenie przebiegało w kilku odrębnych fazach:

- Część I - Fizyczna instalacja serwera oraz nadanie adresacji
- Część II - Konfiguracja monitoringu sieci
- Część III - Integracja z Cisco WAAS

5.3.1. Cześć I – fizyczna instalacja serwera oraz nadanie adresacji

Serwer będący platformą dla systemu TruView został zainstalowany w serwerowni UMWP. Adresacja IP uwzględnia potrzebę zbierania eksportów NetFlow ze wszystkich routerów dostarczonych w ramach projektu E-zdrowie. Schemat logiczny podłączenia serwera do sieci UMWP przedstawia rysunek nr 1.



Rysunek 8 Schemat logiczny podłączenia serwera w UMWP

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

5.3.2. Część II – konfiguracja monitoringu sieci

System wymaga skonfigurowania minimum jednego adresu IP, na który routery będą wysyłać eksporty NetFlow oraz jednego adresu IP dla portalu dostępowego TVC. Pomiędzy routerami a serwerem musi być możliwa komunikacja po IP. Routery do wysyłania pakietów NetFlow wykorzystują protokół UDP i port 2055 (numer portu może być zmieniony w dowolnym momencie). Ewentualne zapory, access listy muszą umożliwiać przesłanie tych pakietów. Ponieważ adres kolektora NetFlow zawiera się w adresacji VLAN-u MGMT, komunikacja pomiędzy routerami oraz kolektorem jest zapewniona poprzez odpowiednie reguły na Firewallach.

Serwer vTVF komunikuje się z routerami wykorzystując protokół SNMP (protokół UDP, port 161) w celu odczytania podstawowych informacji o routerze: nazwie, dostępnych interfejsach i ich parametrach. W tym celu na routerach aktywowano usługę SNMP server w wersji 2.

Serwer vTVF posiada funkcjonalność powiadamiania użytkowników o alarmach. Powiadamianie realizowane jest przez wysyłania SNMP trap (protokół UDP, port 162) na adres IP systemu zarządzania. Do skonfigurowania tej usługi w przyszłości potrzebny będzie adres IP systemu zarządzania.

5.3.3. Konfiguracja eksportów NetFlow na urządzeniach sieciowych

W celu skonfigurowania eksportów protokołu NetFlow na routerach Cisco zainstalowanych w placówkach medycznych wykorzystano polecenia konfiguracyjne[3].

Aby zweryfikować poprawność konfiguracji oraz skuteczność zbierania otrzymywanych eksportów należy zalogować się do interfejsu vTVF poprzez przeglądarkę WWW, następnie przejść do Main menu->Settings->**Device Settings**.

Wszelkie problemy z przyjmowaniem eksportów sygnalizowane są czerwonym wykrzyknikiem przy nazwie/adresie IP urządzenia generującego eksporty.

5.3.4. Konfiguracja lokalizacji zdalnych, tzw. Site'ów

W celu łatwiejszej interpretacji informacji o ruchu, zawartych w otrzymywanych eksportach NetFlow, system TVC umożliwia skonfigurowanie definicji lokalizacji zdalnych, czyli tzw. Site'ów. Site może w tym wypadku oznaczać każdą placówkę medyczną połączoną z UMWP poprzez sieć WAN MPLS. Monitorowanie wykorzystania łączy WAN jest kluczowe z punktu widzenia administratora sieci. Z jednej strony łącza WAN są łączami o stosunkowo niewielkich przepustowościach (rzędu kilku Mbps), w związku z czym łatwo doprowadzić do ich wysycenia. Ponadto każdy administrator powinien być w

[3] X w nazwie routera oznacza nr placówki medycznej zgodnie z przyjętym w projekcie schematem

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

stanie szybko zidentyfikować skład ruchu na poszczególnych łączach WAN do każdej lokalizacji zdalnej wraz z informacjami, jakiego rodzaju ruch utylizuje te łącza.

Konfiguracja Site'ów odbywa się w panelu Administratora TVC. Korzystając z przeglądarki logujemy się na adres TVC www i przechodzimy do zakładki Sites->Add new site. W nowym oknie uzupełniamy informacje o nowej lokalizacji podając jej nazwę, opis, współrzędne geograficzne oraz prędkości łączy w kierunku IN/OUT. Na koniec wybieramy interfejs NetFlow, który oznacza interfejs urządzenia sieciowego, przez który dana placówka połączona jest z siecią WAN. Eksporty z tego interfejsu będą zawierać opis całego ruchu generowanego/odbieranego w tej lokalizacji.

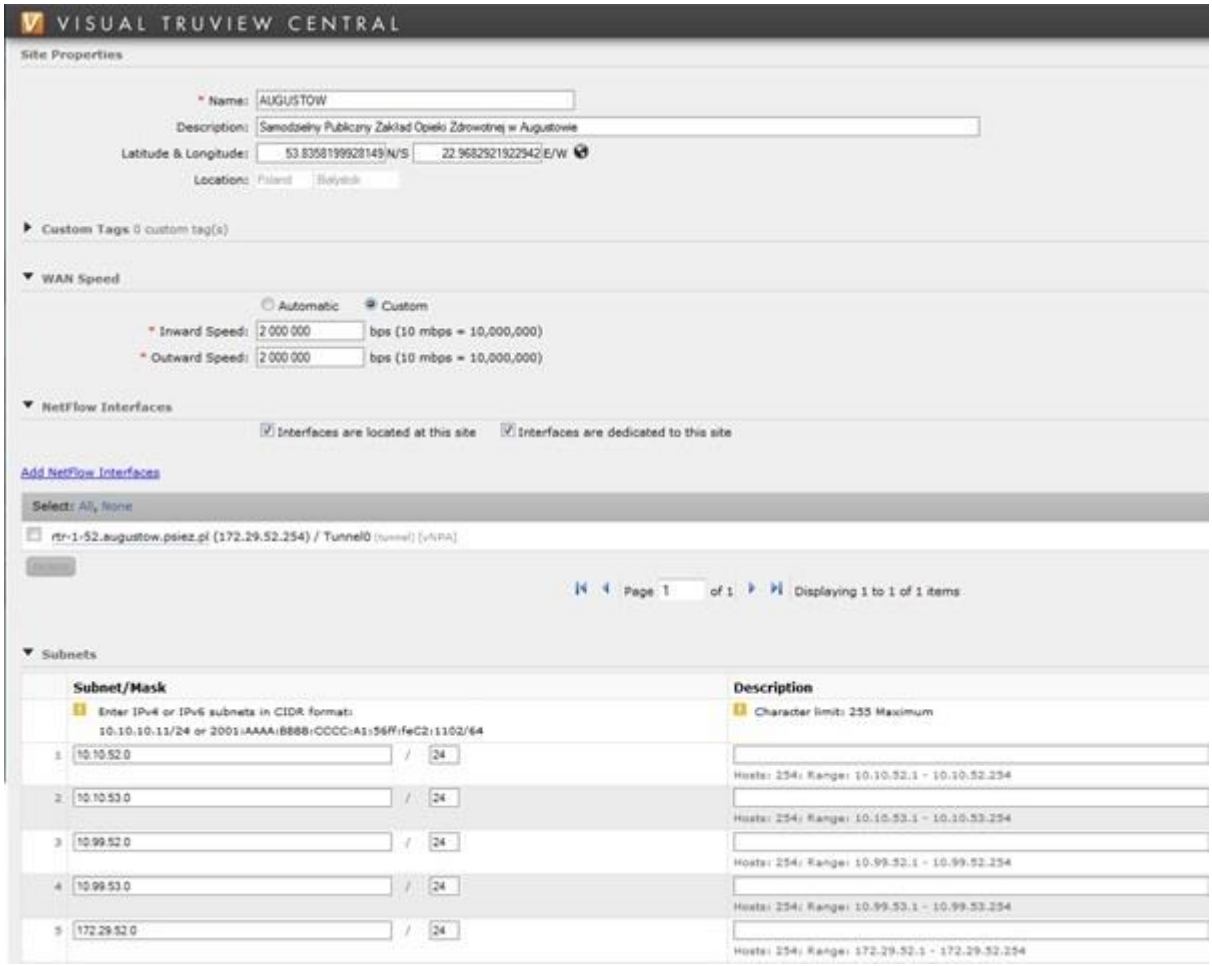
Administrator ma także możliwość podania podsieci IP, z których korzystają użytkownicy w danej lokalizacji[4]. Poniżej zaprezentowano przykładową konfigurację dla placówki medycznej. W ramach wdrożenia wykonano konfigurację dla 25 placówek oraz UMWP.

[4] Administrator ma możliwość wyboru dwóch dodatkowych opcji, których opis znajduje się poniżej:

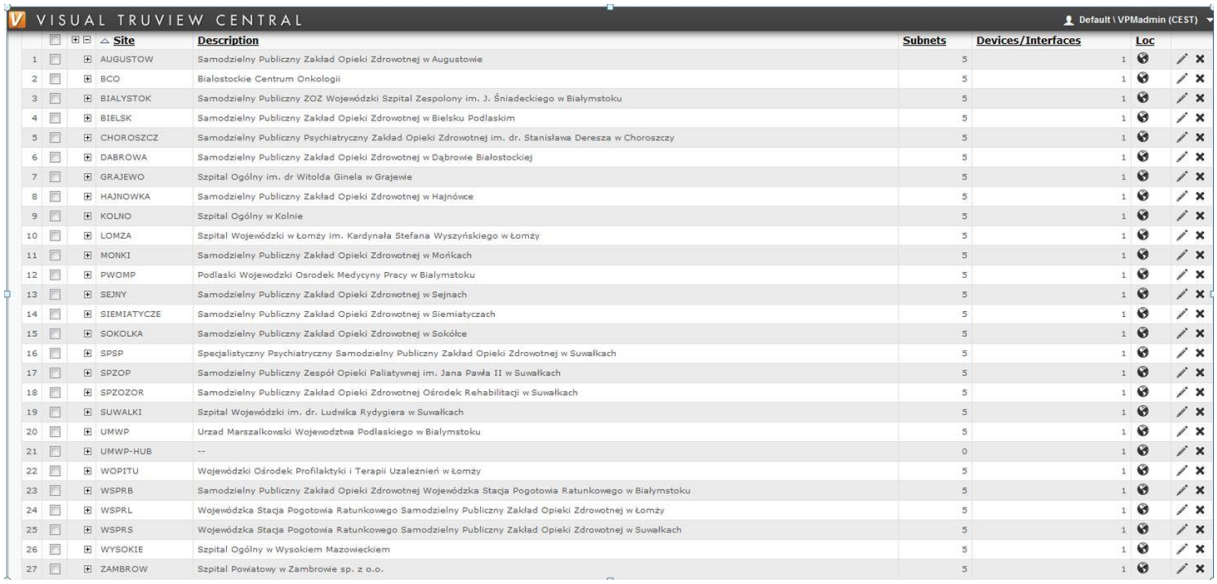
Interfaces are located at this site – opcję tę należy wybrać w momencie posiadania dedykowanego urządzenia (np. routera), z którego generowane są eksporty, bezpośrednio w lokalizacji zdalnej; w przeciwnym razie należy odznaczyć pole wyboru

Interfaces are dedicated for this site – opcję tę należy wybrać w przypadku generowania eksportów NetFlow z interfejsu sieciowego, przez który przechodzi ruch tylko i wyłącznie w ramach konfigurowanej lokalizacji; jeżeli eksportujemy NetFlow z interfejsu współdzielonego, na którym widoczny jest ruch także z innych lokalizacji, należy odznaczyć to pole i uzupełnić dane o podsieciach w konfigurowanej placówce (posłuży ona do filtrowania danych z interfejsu współdzielonego)

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 9 Przykładowa konfiguracja Site'u Augustów



	Site	Description	Subnets	Devices/Interfaces	Loc
1	AUGUSTOW	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie	5	1	
2	BCO	Bialostockie Centrum Onkologii	5	1	
3	BIALYSTOK	Samodzielny Publiczny ZOZ Wojewódzki Szpital Zespolony im. J. Śniadeckiego w Białymstoku	5	1	
4	BIELSK	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Bielsku Podlaskim	5	1	
5	CHOROSZCZ	Samodzielny Publiczny Psychiatryczny Zakład Opieki Zdrowotnej im. dr. Stanisława Deresza w Choroszczy	5	1	
6	DABROWA	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Dąbrowie Białostockiej	5	1	
7	GRAJEWO	Szpital Ogólny im. dr Witolda Ginela w Grajewie	5	1	
8	HAJNOWKA	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Hajnówce	5	1	
9	KOLNO	Szpital Ogólny w Kolnie	5	1	
10	LOMZA	Szpital Wojewódzki w Łomży im. Kardynała Stefana Wyszyńskiego w Łomży	5	1	
11	MONKI	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Mońkach	5	1	
12	PWOMP	Podlaski Wojewodzki Osrodek Medycyny Pracy w Bialymstoku	5	1	
13	SEJNY	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach	5	1	
14	SIEMIATYCZE	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Siemiatyczach	5	1	
15	SOKOLKA	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sokółce	5	1	
16	SPSP	Specjalistyczny Psychiatryczny Samodzielny Publiczny Zakład Opieki Zdrowotnej w Suwałkach	5	1	
17	SPZOP	Samodzielny Publiczny Zespół Opieki Paliatywnej im. Jana Pawła II w Suwałkach	5	1	
18	SPZOZOR	Samodzielny Publiczny Zakład Opieki Zdrowotnej Ośrodek Rehabilitacji w Suwałkach	5	1	
19	SUWALKI	Szpital Wojewódzki im. dr. Ludwika Rydygiera w Suwałkach	5	1	
20	UMWP	Urzad Marszalkowski Wojewodztwa Podlaskiego w Bialymstoku	5	1	
21	UMWP-HUB	--	0	1	
22	WOPITU	Wojewódzki Ośrodek Profilaktyki i Terapii Uzależnień w Łomży	5	1	
23	WSPRB	Samodzielny Publiczny Zakład Opieki Zdrowotnej Wojewódzka Stacja Pogotowia Ratunkowego w Białymstoku	5	1	
24	WSPRL	Wojewódzka Stacja Pogotowia Ratunkowego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Łomży	5	1	
25	WSPRS	Wojewódzka Stacja Pogotowia Ratunkowego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Suwałkach	5	1	
26	WYSOKIE	Szpital Ogólny w Wysokiem Mazowieckiem	5	1	
27	ZAMBROW	Szpital Powiatowy w Zambrowie sp. z o.o.	5	1	

Rysunek 10 Lista skonfigurowanych Site'ów

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

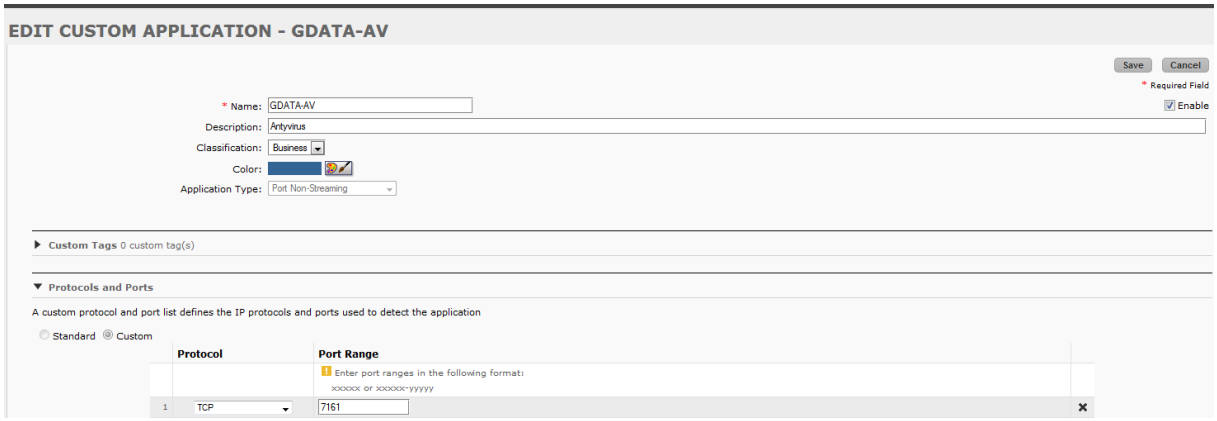
Konfiguracja Site'ów pozwoliła generować raporty typu Top Sites z informacjami o utylizacji poszczególnych łączy WAN oraz z możliwością dotarcia do pojedynczych konwersacji w ramach każdego łącza.

5.3.5. Sieciowa definicja aplikacji

Eksporty NetFlow na podstawie informacji warstwy 3 oraz 4 (adres IP oraz numery portów L4) umożliwiają identyfikację aplikacji, w ramach których generowany jest ruch sieciowy. System TVC posiada definicję około 150 tzw. dobrze znanych aplikacji. Oprócz tego możliwe jest konfigurowanie własnych definicji aplikacji w celu identyfikacji aplikacji niestandardowych.

Aby przejść do konfiguracji nowych aplikacji bądź edycji istniejących aplikacji należy wybrać panel Administratora, a następnie zakładkę Applications. Pozwoli to przenieść się do listy obecnie skonfigurowanych aplikacji (obok każdej z nich widnieje ikona ołówka, która daje możliwość edycji definicji) bądź też dodania nowej aplikacji (Add new Custom App). Definicje własnych aplikacji znajdują się w panelu Custom App. Panel Standard App zawiera definicje wspomnianych wcześniej popularnych, tzw. „dobrze znanych aplikacji", jak chociażby bazy danych MS SQL, Oracle itd. Dzięki aplikacjom standardowym system jest w stanie rozpoznać w sposób automatyczny ruch w ramach tych aplikacji. Warto jednak stworzyć własne definicje uzupełniając numery portów o adresy IP serwerów, tak aby system prezentował dane przy wykorzystaniu nazewnictwa intuicyjnego dla użytkowników systemu.

Poniżej zamieszczono przykład definicji aplikacji oraz listę wszystkich zdefiniowanych podczas wdrożenia aplikacji.

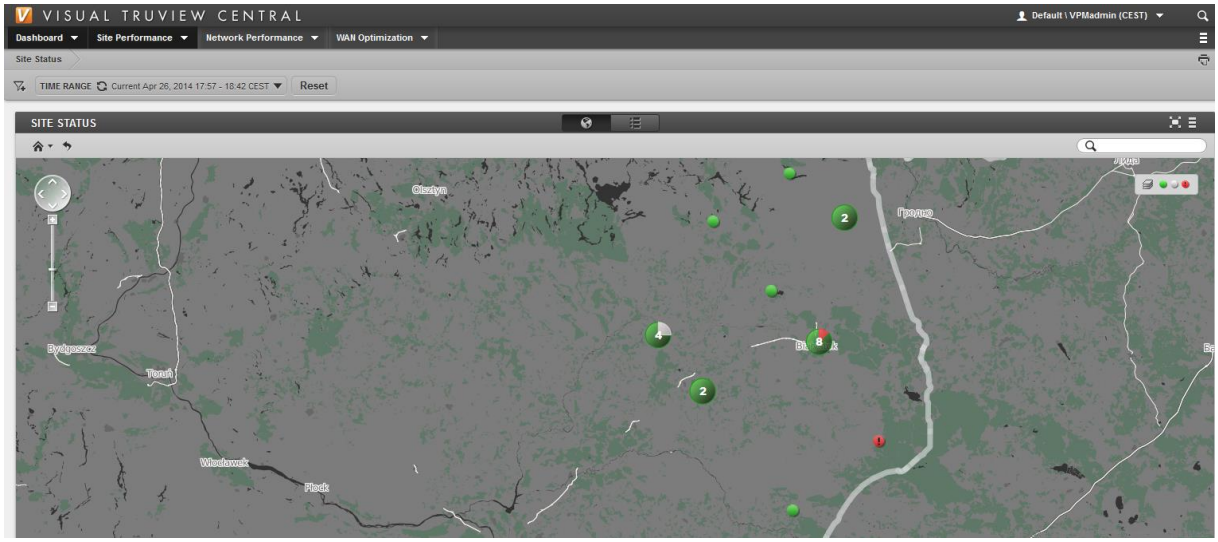


Rysunek 11 Przykładowa definicja aplikacji sieciowej

5.3.6. Wykorzystanie mapy do monitorowania dostępności lokalizacji

Skonfigurowanie lokalizacji użytkowników umożliwia podgląd dostępności placówek zdalnych w postaci mapy zawierającej informacje o wszystkich lokalizacjach, z których napływają eksporty NetFlow.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 12 Dostępność placówek medycznych zaprezentowana w postaci mapy

5.3.7. Część III – Integracja z Cisco WAAS

System TVC umożliwia integrację z technologią optymalizacji łącz WAN Cisco WAAS. W ramach projektu każda placówka medyczna została wyposażona w moduł akceleracji Cisco WAE, w związku z czym możliwe było zmapowanie danych z Central Managera na poszczególne Site'y skonfigurowane w TVC.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

6. Systemy Microsoft wdrożone w ramach projektu

Niniejszy rozdział przedstawia koncepcję wdrożenia systemów z rodziny Microsoft, opis poszczególnych modułów wraz z ich konfiguracją.

Zgodnie z wymaganiami SIWZ przyjmuje się ogólne wstępne zagadnienia technologiczne:

- Projekt realizowany jest w środowisku hybrydowym opartym o serwery fizyczne jak i maszyny wirtualne.
- Jako platforma wirtualizacja zastosowany zostanie system Windows Server 2012 R2 Datacenter. Jako system operacyjny przeznaczony pod systemy bazodanowe wykorzystany zostanie Windows Server 2008 R2.
- Środowisko zostanie zbudowane w oparciu o model domeny Windows – o strukturze jeden las z wieloma poddomenami, rozproszony geograficznie.
- Ze względu na konieczność zapewnienia wysokiej dostępności maszyn wirtualnych (klaster fail-over) roli Hyper-V, oraz wymóg, iż węzły klastra Hyper-V muszą być członkami domeny, w lokalizacji centralnej UMWP zostanie dodany dodatkowy sprzętowy kontroler domeny. Wymóg takiej konfiguracji spowodowany jest koniecznością dostępu do kontrolera domeny w przypadku startu węzłów klastra.

6.1. Opis projektu

Projekt składać się będzie z architektury fizycznej i logicznej. Jednakże ze względu na zagadnienia integracyjne z innymi systemami w wielu elementach dodawane będą uwagi odnośnie sprzętu czy infrastruktury sieciowej.

6.2. Architektura logiczna Active Directory

Ze względu na przyjęty model konfiguracji sprzętowej oraz ogólny model bezpieczeństwa wybrany został model środowiska Active Directory składający się z jednego lasu / jednego drzewa /wielu poddomen. Uprawnienia do poszczególnych jednostek leczniczych delegowane są na podstawie członkostwa w danej domenie oraz odpowiednich jednostek organizacyjnych.

Ilość lokalizacji – centrala + 25 lokalizacji zdalnych, poszczególne lokalizacje wraz z centralą traktowane są jako site (lokacje) Active Directory

Dla wygody wdrożeń późniejszych systemów typu poczta elektroniczna czy komunikacja VOIP lub wideokonferecje lub konferencje multimedialne, które potencjalnie będą mogły realizować dostęp od strony Internetu najwygodniejszym wydaje się przyjęcie tej samej domeny w zakresie Active Directory jak i domeny internetowej związanej z portalami lub usługami zewnętrznymi.

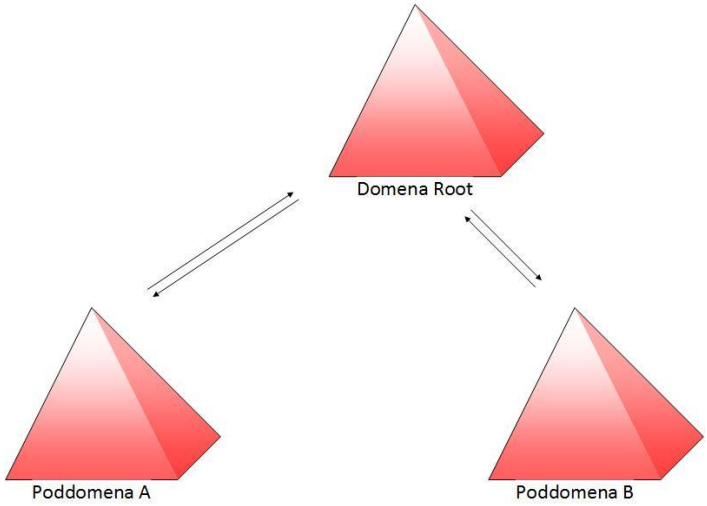
Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Przyjęcie modelu jednego lasu jest najbardziej polecane przez Microsoft ze względu na możliwą w przyszłości elastyczną integrację usług typu Exchange (poczta/unified messaging), Lync (Unified Communication) czy rodziny System Center (w zakresie zarządzania i monitorowania) środowiskiem.

Środowisko będzie instalowane/ konfigurowane zaczynając od centrali - potem będą podłączane poszczególne lokalizacje zdalne.

Nazwa DNS domeny **psiez.pl.** Nazwy poddomen zebrano w tabeli 12.

Nazwa NETBIOS domeny: **PSIEZ**



Rysunek 13 Architektura ogólna AD

6.2.1. Struktura nazw domen

Nazwa domeny najwyższego poziomu: psiez.pl

Struktura poddomen w konwencji: xxxxx.psiez.pl

Lokalizacja / Nazwa – Podmiot leczniczy	Nazwa domeny Active Directory (DNS)	Nazwa domeny Active Directory (NETBIOS)	Zakresy podsieci (trzeci oktet)
Urząd Marszałkowski Województwa Podlaskiego w Białymstoku	PSIEZ.pl	PSIEZ	0
Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku,	BCO.psiez.pl	BCO	8

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Szpital Wojewódzki w Łomży im. Kardynała Stefana Wyszyńskiego,	LOMZA.psiez.pl	LOMZA	22
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sokółce,	SOKOLKA.psiez.pl	SOKOLKA	24
Szpital Ogólny im. dr Witolda Ginela w Grajewie,	GRAJEWO.psiez.pl	GRAJEWO	40
Szpital Ogólny w Kolnie,	KOLNO.psiez.pl	KOLNO	42
Szpital Ogólny w Wysokiem Mazowieckiem,	WYSOKIE.psiez.pl	WYSOKIE	44
Samodzielny Publiczny Zakład Opieki Zdrowotnej - Wojewódzki Szpital Zespolony im. Jędrzeja Śniadeckiego w Białymstoku,	BIALYSTOK.psiez.pl	BIALYSTOK	36
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Hajnówce,	HAJNOWKA.psiez.pl	HAJNOWKA	6
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Mońkach,	MONKI.psiez.pl	MONKI	16
Samodzielny Publiczny Psychiatryczny Zakład Opieki Zdrowotnej im. dr. Stanisława Deresza w Choroszczy,	CHOROSZCZ.psiez.pl	CHOROSZCZ	12
Szpital Wojewódzki im. dr. Ludwika Rydygiera w Suwałkach,	SUWALKI.psiez.pl	SUWALKI	50
Specjalistyczny Psychiatryczny Samodzielny Publiczny Zakład Opieki Zdrowotnej w Suwałkach,	SPSP.psiez.pl	SPSP	38
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Bielsku Podlaskim,	BIELSK.psiez.pl	BIELSK	4
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Siemiatyczach,	SIEMATYCZE.psiez.pl	SIEMATYCZE	20
Szpital Powiatowy w Zambrowie Sp. z o.o.,	ZAMBROW.psiez.pl	ZAMBROW	46

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Samodzielny Publiczny Zakład Opieki Zdrowotnej Ośrodek Rehabilitacji w Suwałkach,	SPZOZOR.psiez.pl	SPZOZOR	34
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie,	AUGUSTOW.psiez.pl	AUGUSTOW	52
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Dąbrowie Białostockiej,	DABROWA.psiez.pl	DABROWA	14
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach,	SEJNY.psiez.pl	SEJNY	18
Samodzielnym Publicznym Zakładem Opieki Paliatywnej im. Jana Pawła II w Suwałkach,	SPZOP.psiez.pl	SPZOP	32
Wojewódzki Ośrodek Profilaktyki i Terapii Uzależnień w Łomży,	WOPITU.psiez.pl	WOPITU	48
Podlaski Wojewódzki Ośrodek Medycyny Pracy w Białymstoku,	PWOMP.psiez.pl	PWOMP	10
Samodzielny Publiczny Zakład Opieki Zdrowotnej - Wojewódzka Stacja Pogotowia Ratunkowego w Białymstoku,	WSPRB.psiez.pl	WSPRB	26
Samodzielny Publiczny Zakład Opieki Zdrowotnej - Wojewódzka Stacja Pogotowia Ratunkowego - w Łomży,	WSPRL.psiez.pl	WSPRL	28
Wojewódzką Stacją Pogotowia Ratunkowego Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Suwałkach,	WSPRS.psiez.pl	WSPRS	30

Tabela 11 Informacje w zakresie domen/poddomen

Wszystkie kontrolery domeny będą pełnić rolę Global Catalog

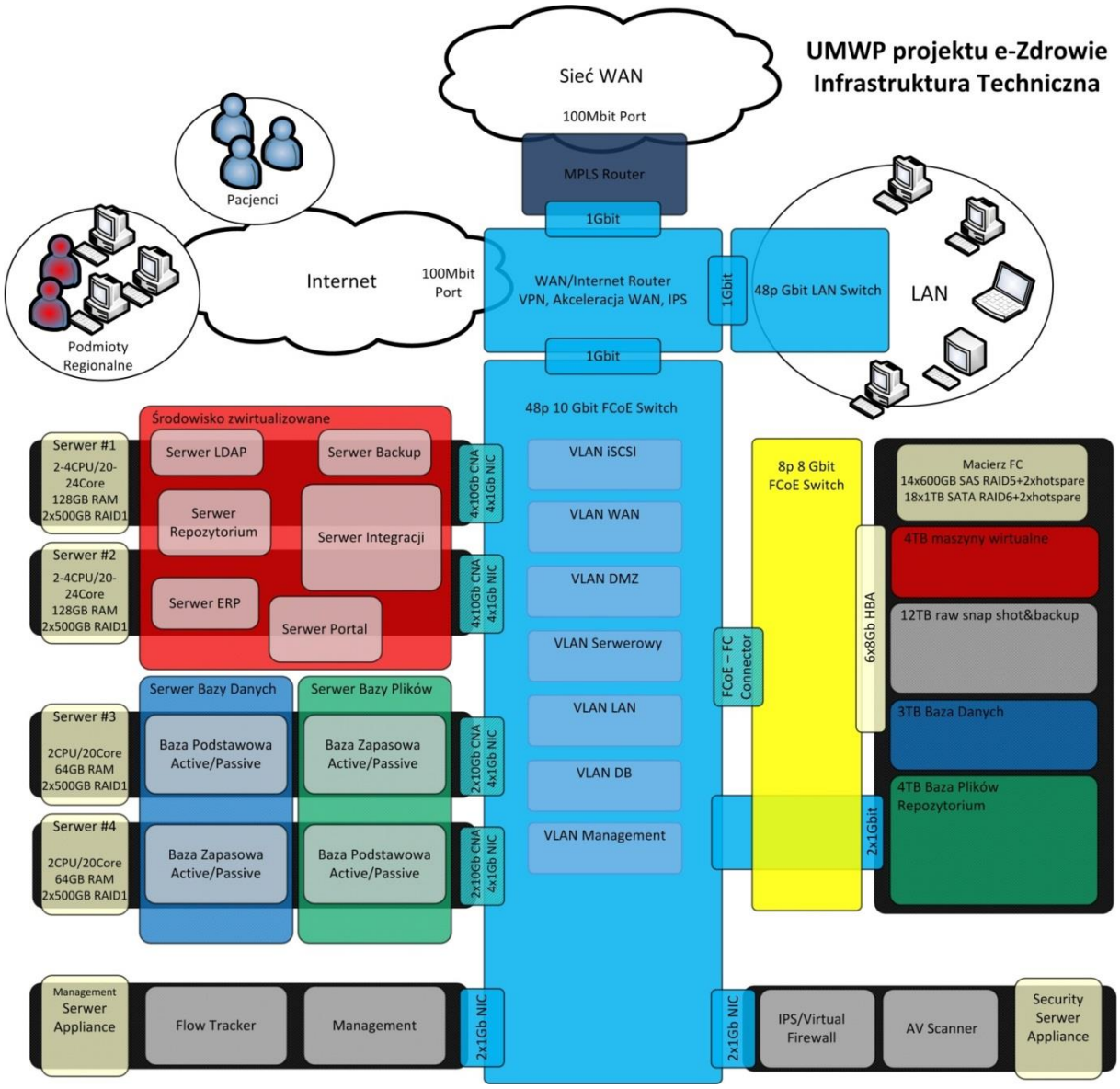
Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

6.3. Architektura fizyczna

Infrastruktura sieciowa bazuje na wydzielonej sieci WAN w technologii MPLS.

Całość operacji poza domeną najwyższego poziomu będzie można przeprowadzić zdalnie. Zakładamy, iż serwery będą posiadały interfejsy zdalnego zarządzani (ILO, DRAC).

6.3.1. UMWP



Rysunek 14 Architektura UMWP

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Zgodnie z wymaganiami dla zapewniania minimalnego poziomu odporności na awarie dla każdej domeny przeznaczone są po dwa serwery wirtualne przeznaczone na rolę kontrolera domeny (serwer LDAP).

Procedura instalacji środowiska dla UMWP

1. Instalacja sprzętowego kontrolera domeny DC0-PSIEZ
2. Instalacja systemu operacyjnego Windows Server 2012 R2 Datacenter na serwerze Server #1
3. Instalacja systemu operacyjnego Windows Server 2012 R2 Datacenter na serwerze Server #2
4. Instalacja systemu operacyjnego Windows Server 2008 R2 Datacenter na serwerze Server #3
5. Instalacja systemu operacyjnego Windows Server 2008 R2 Datacenter na serwerze Server #4
6. Instalacja roli Hyper-V na serwerze Server #1
7. Instalacja roli Hyper-V na serwerze Server #2
8. Podpięcie serwerów Server #1 i Server #2 do domeny Psiez.pl
9. Instalacja roli klastra Hyper-V Fail-Over na serwerach Server #1 i Server #2
10. Instalacja maszyny wirtualnej pod kontroler domeny DC1-PSIEZ (serwer LDAP) na serwerze Server #1. Wypromowanie kontrolera domeny dla domeny Psiez.pl. Kontrolery domeny nie są instalowane jako maszyny wysoko dostępne.
11. Instalacja maszyny wirtualnej pod kontroler domeny DC2-PSIEZ (serwer LDAP) na serwerze Server #2. Wypromowanie kontrolera domeny dla domeny Psiez.pl. Kontrolery domeny nie są instalowane jako maszyny wysoko dostępne.
12. Podpięcie serwerów Server #3 i Server #4 do domeny Psiez.pl
13. Instalacja roli klastra Fail-Over na serwerach Server #3 i Server #4

Uwagi instalacyjne

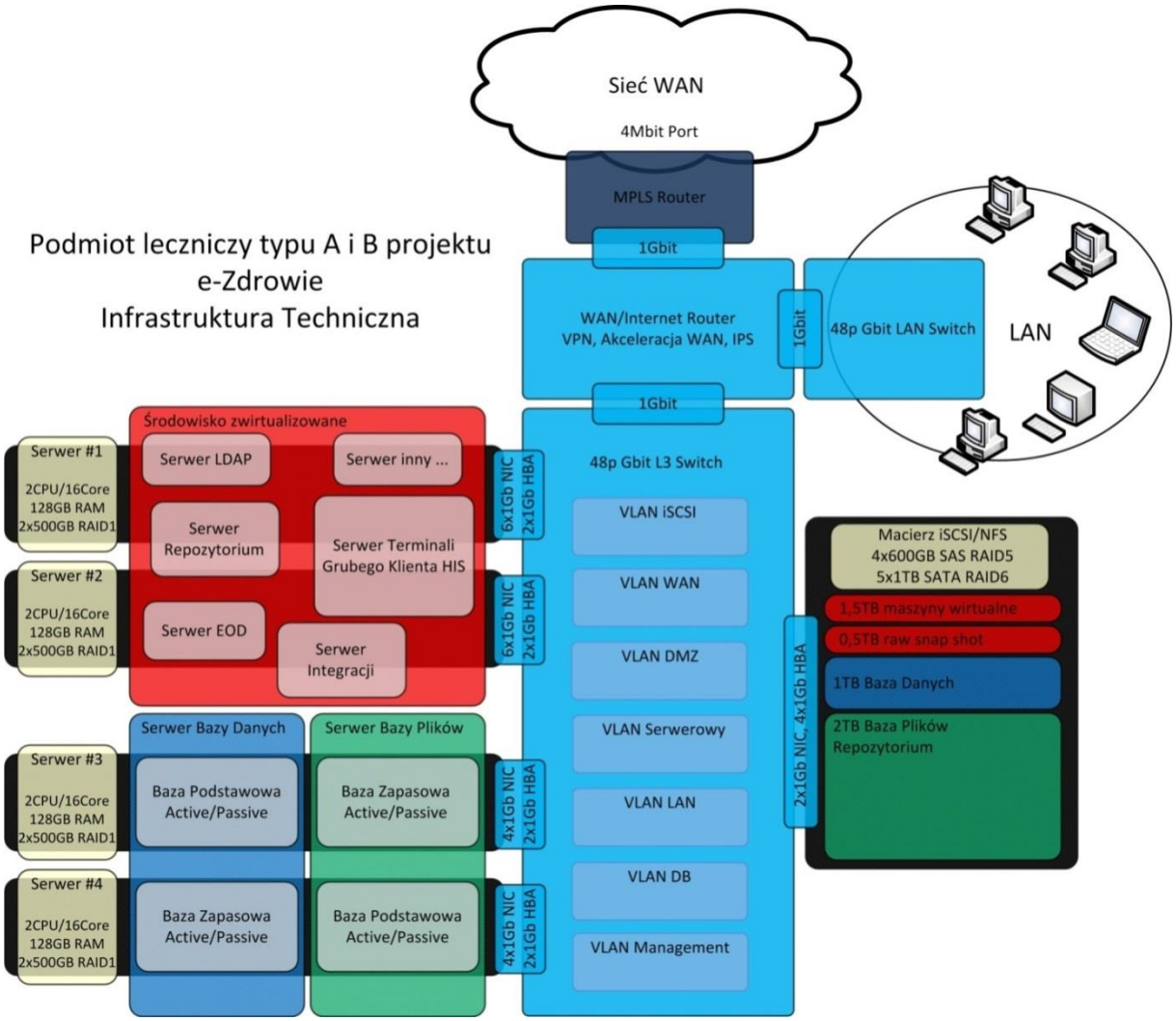
1. Każdy z kontrolerów domeny pełnić będzie rolę serwera DNS.
2. Adresacja podana jest w tabeli 15
3. Kontroler domeny DC0-PSIEZ jest wzorcem czasu dla lasu AD

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Wymagania sprzętowe na kontroler domeny

1. 1 procesor wirtualny
2. 4 GB RAM
3. Dysk (pojedynczy) o wielkości 40 GB – dysk dynamicznie rozszerzający się
4. Wersja systemu operacyjnego kontrolera domeny 2k12 R2
5. Poziom funkcjonalności domeny i lasu 2k8R2

6.3.2. Podmioty lecznicze A i B



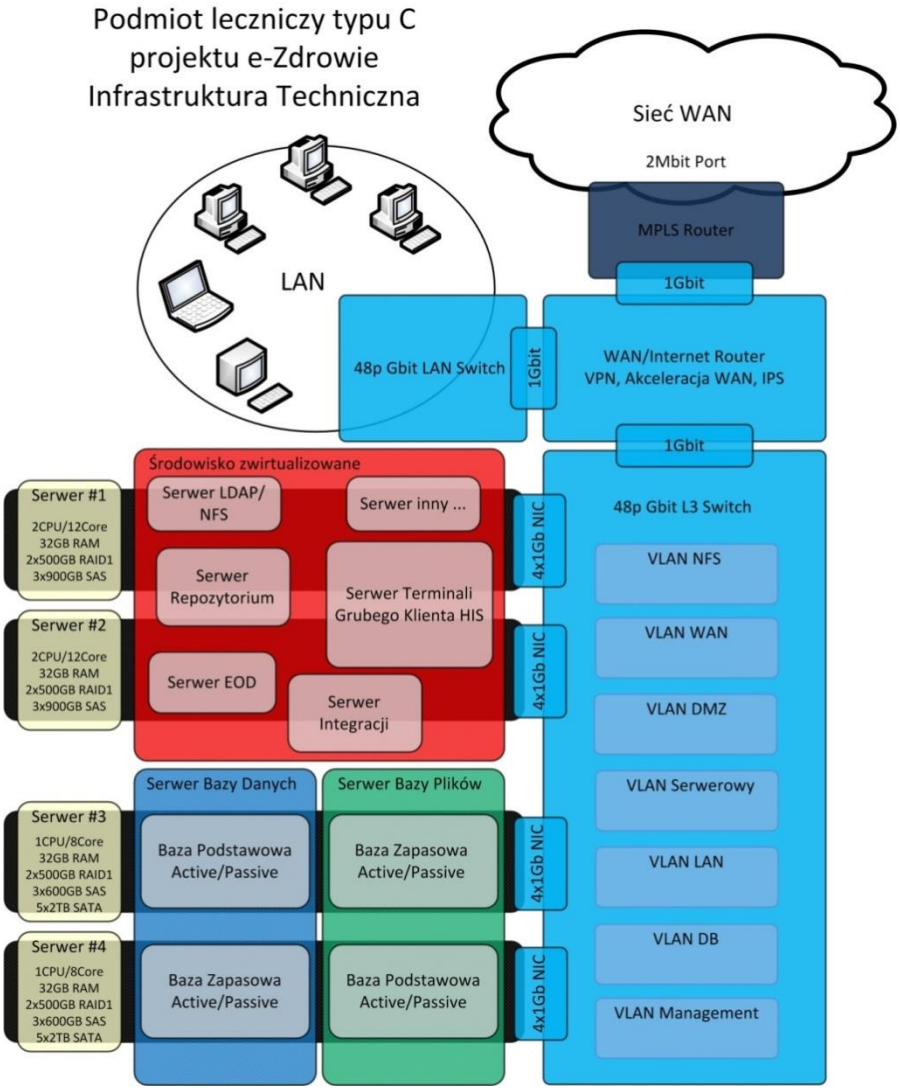
Rysunek 15 Architektura podmiotu leczniczego A i B

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Procedura instalacyjna i konfiguracyjna analogiczna jak dla UMWP. Poza brakiem sprzętowego kontrolera domeny.

6.3.3. Podmioty lecznicze C

Lokalizacje bez fizycznego storage. Storage dla klastra SQL będzie emulowany z wykorzystaniem funkcjonalności iSCSI Target serwera 2012 R2 pracującego jako maszyna wirtualna. Jej zabezpieczeniem będzie replica odnawiana co 5 minut. Takie podejście zapewni nam możliwość przywrócenia pracy w przypadku awarii serwera z utratą co najwyżej 5 ostatnich minut pracy.



Rysunek 16 Architektura podmiotu leczniczego C

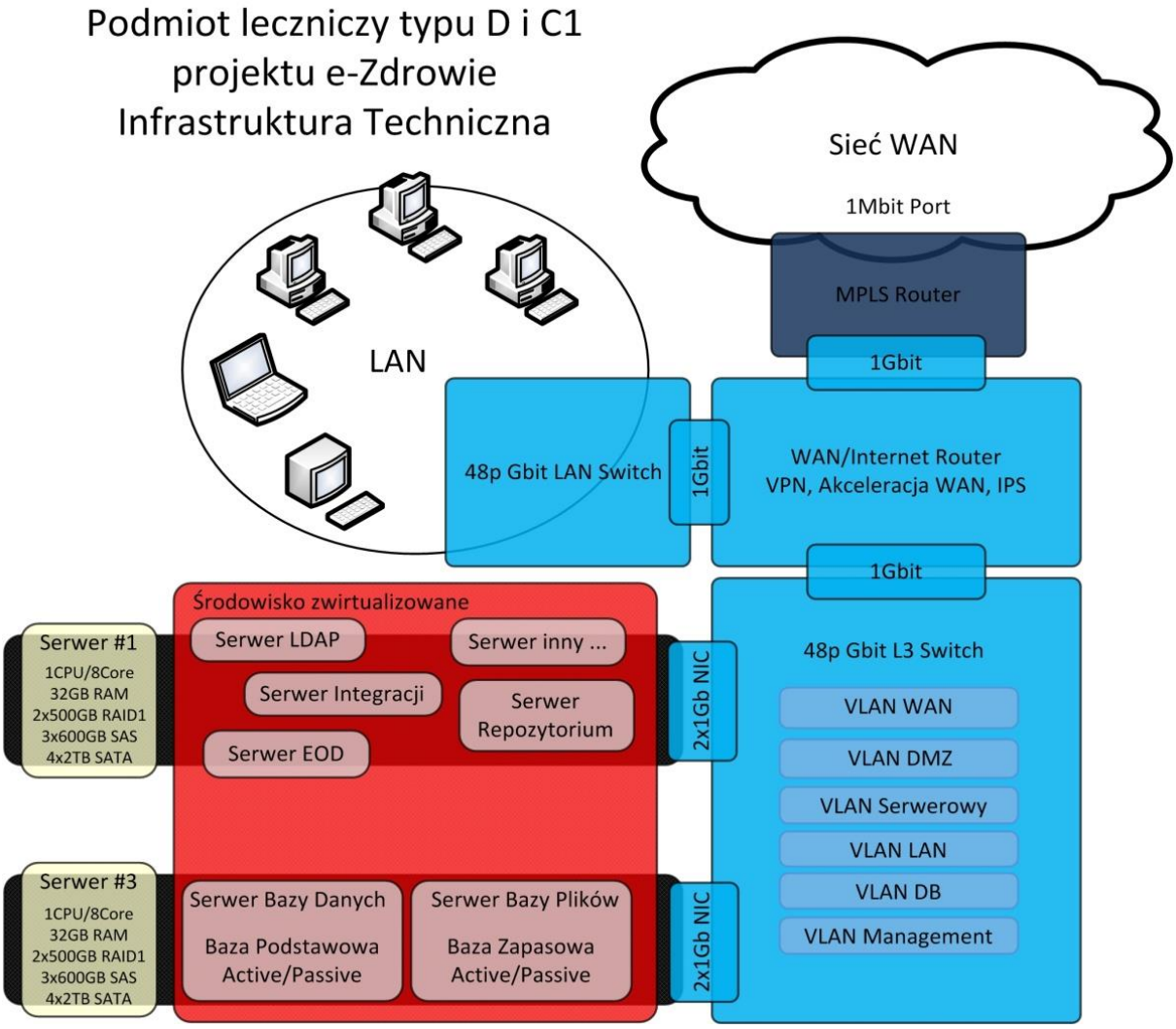
Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

1. Instalacja systemu operacyjnego Windows Server 2012 R2 Datacenter na serwerze Server #1
2. Instalacja systemu operacyjnego Windows Server 2012 R2 Datacenter na serwerze Server #2
3. Instalacja systemu operacyjnego Windows Server 2008 R2 Datacenter na serwerze Server #3
4. Instalacja systemu operacyjnego Windows Server 2008 R2 Datacenter na serwerze Server #4
5. Instalacja roli Hyper-V na serwerze Server #1
6. Instalacja roli Hyper-V na serwerze Server #2
7. Podpięcie serwerów Server #1 i Server #2 do domeny Psiez.pl
8. Instalacja maszyny wirtualnej pod kontroler domeny DC1-PSIEZ (serwer LDAP) na serwerze Server #1. Wypromowanie kontrolera domeny dla domeny Psiez.pl. Kontrolery domeny nie są instalowane jako maszyny wysoko dostępne.
9. Instalacja maszyny wirtualnej pod kontroler domeny DC2-PSIEZ (serwer LDAP) na serwerze Server #2. Wypromowanie kontrolera domeny dla domeny Psiez.pl. Kontrolery domeny nie są instalowane jako maszyny wysoko dostępne.
10. Podpięcie serwerów Server #3 i Server #4 do domeny Psiez.pl
11. Instalacja maszyny wirtualnej na Server #1 pełniącej rolę ISCSI TARGET dla klastra SQL (Server #3 i Server #4)
12. Instalacja roli klastra Fail-Over na serwerach Server #3 i Server #4

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

6.3.4. Podmioty lecznicze C1 i D

W podmiotach leczniczych C1 i D nie ma środowiska wysokiej dostępności. Na obu serwerach zainstalowana zostanie rola Hyper-V (z włączoną funkcjonalnością Hyper-V Replica). Oba serwery pracować będą w oparciu o Windows Server 2012 R2 Datacenter.



Rysunek 17 Architektura podmiotów leczniczych D i C1

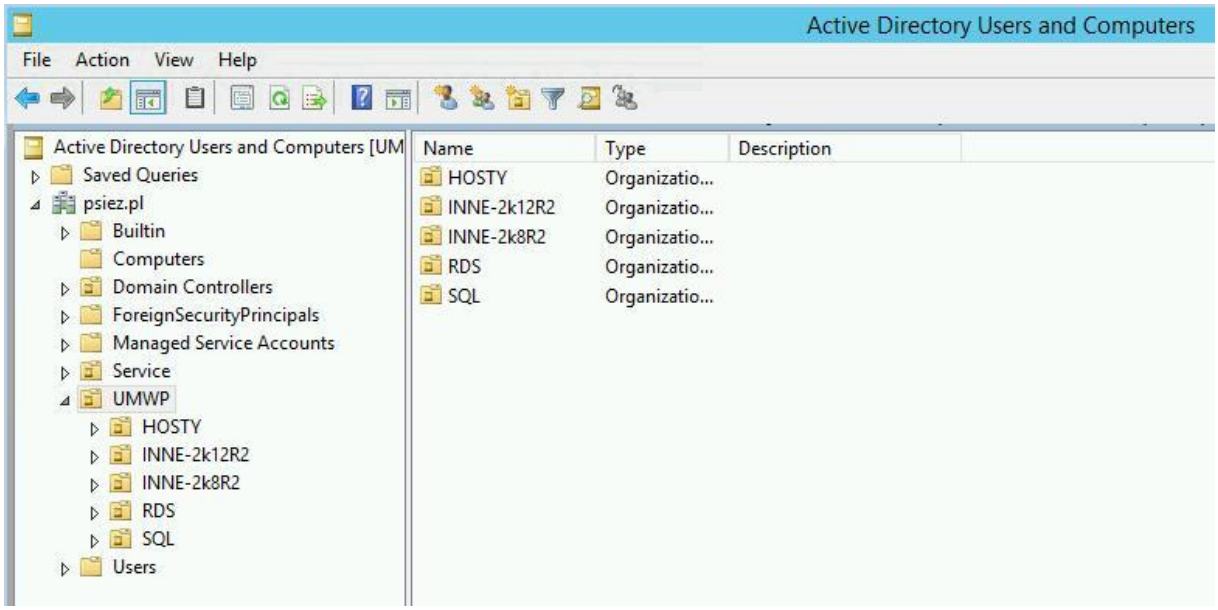
Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

6.4. Active Directory w UMWP

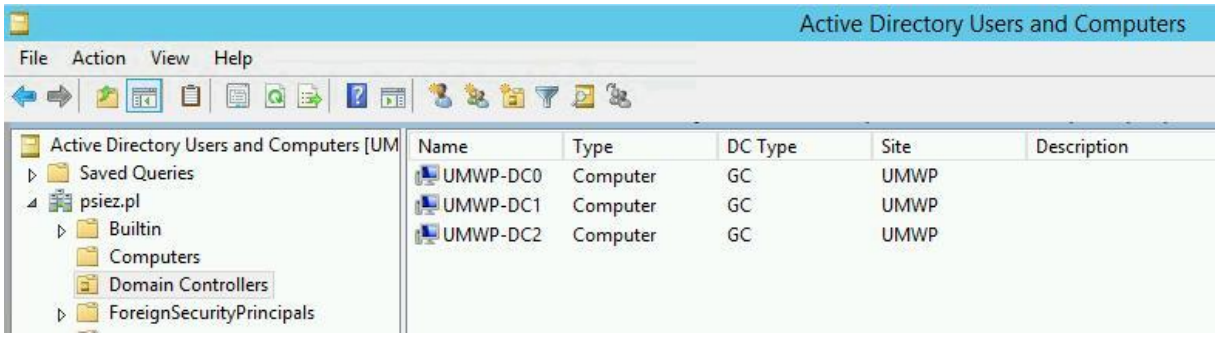
Konfiguracja AD domeny root: PSIEZ.PL

6.4.1. Struktura jednostek organizacyjnych

W każdej domenie struktura jednostek organizacyjnych będzie praktycznie identyczna.

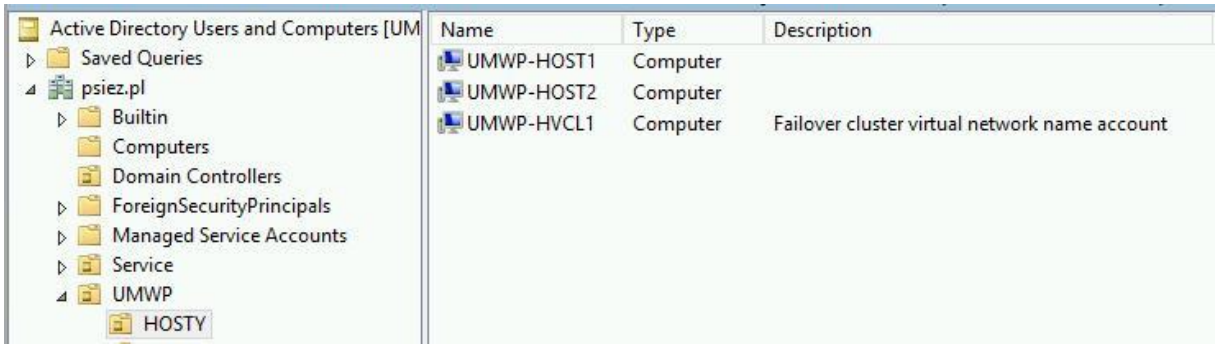


Kontrolery domeny

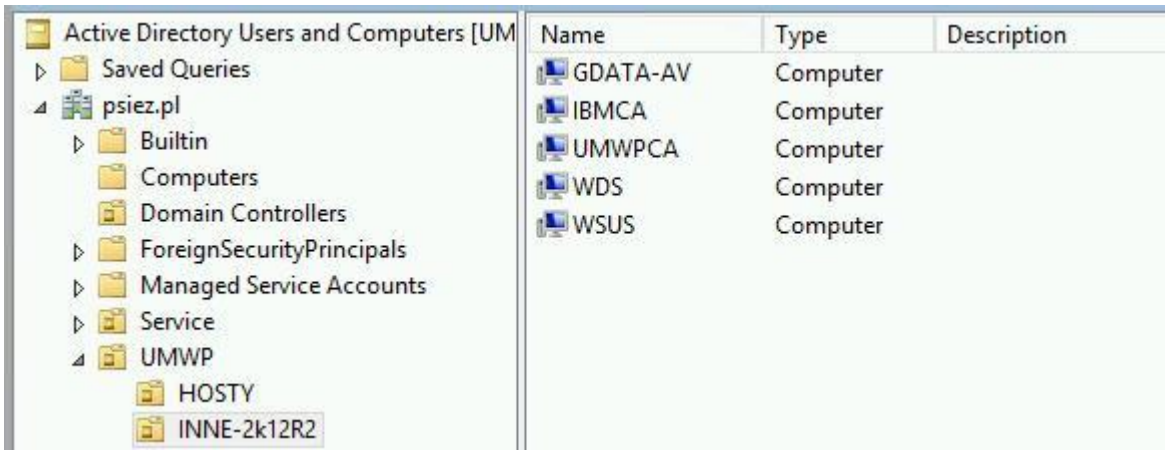


Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Jednostka organizacyjna – hostów Hyper-V



Jednostka organizacyjna innych serwerów – pracujących z Windows Server 2012 R2

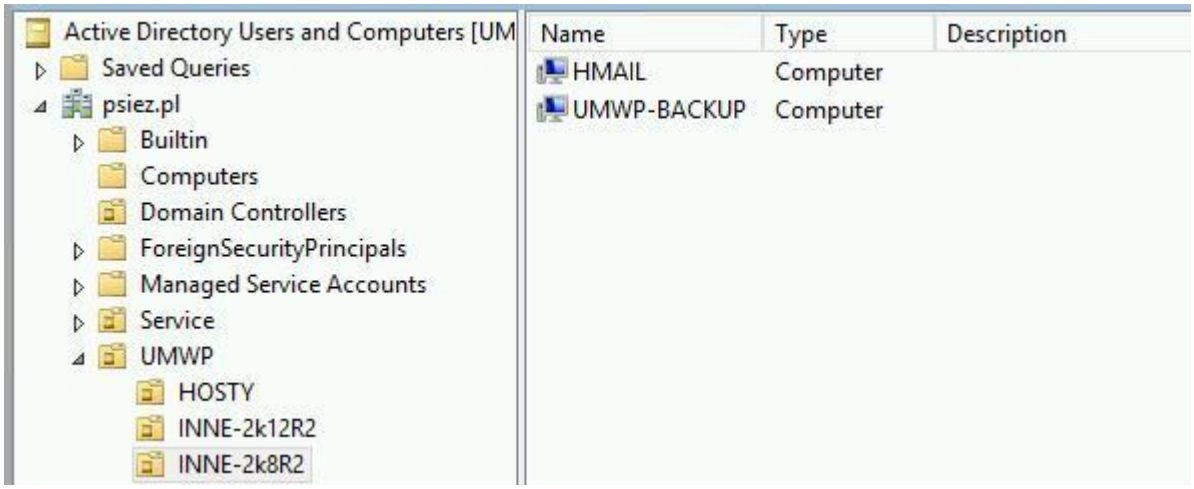


Przeznaczenie serwerów

Nazwa	Przeznaczenie
IBMCA	Jednostka certyfikująca dla półki dyskowej szyfrowanej
GDATA-AV	Serwer zarządzający oprogramowaniem antywirusowym wszystkich serwerów całego projektu
UMWPCA	Jednostka certyfikująca dla serwerów usług terminalowych wszystkich lokalizacji
WSUS	Centralny serwer zarządzający aktualizacji wszystkich serwerów projektu

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

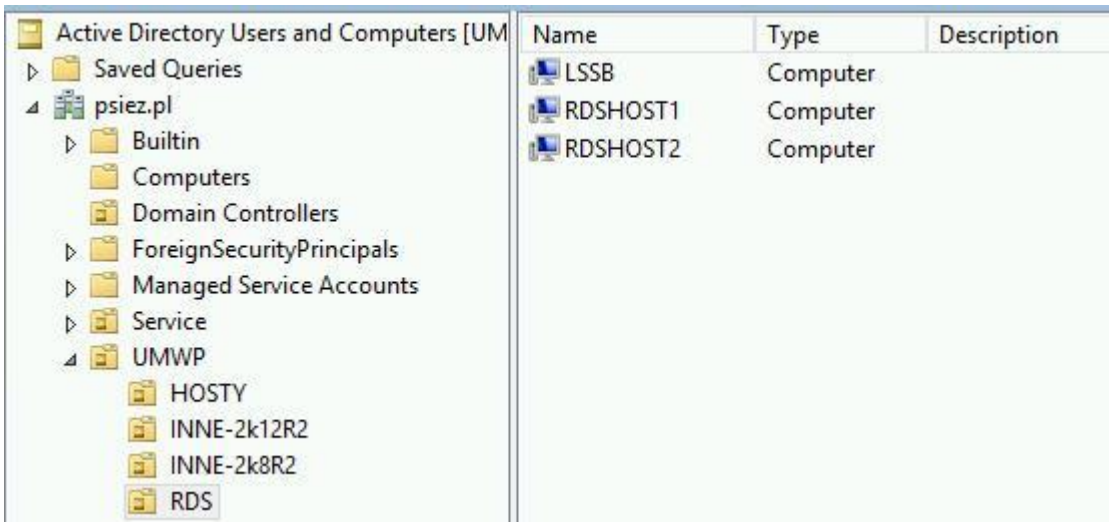
Inne serwery pracujące na Windows Server 2008 R2



Przeznaczenie serwerów

Nazwa	Przeznaczenie
HMAIL	Serwer pocztowy
UMWP-BACKUP	Serwer zarządzający oprogramowaniem archiwizującym

Jednostka organizacyjna dla serwerów usług terminalowych



Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Przeznaczenie serwerów

Nazwa	Przeznaczenie
LSSB	Serwer licencjonowania – na wszystkie serwery terminalowe projektu Session Broker, RD Web Access
RDHOST1, RDHOST2	2 serwery usług terminalowych – session hosty

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

7. Serwer antywirusowy GDATA-AV

W ramach projektu E-Zdrowie dostarczone serwery zostały wyposażone w dedykowane oprogramowanie antywirusowe G Data Antyvirus. Oprogramowanie to zostało zainstalowane na wszystkich hostach, a także na maszynach wirtualnych utworzonych w ramach prac wdrożeniowych.

Jednym z głównych wymagań stawianych systemowi antywirusowemu było działanie w scentralizowanej architekturze, w której występuje serwer zarządzający. Z tego względu w na serwerach w Urzędzie Marszałkowskim utworzono maszynę wirtualną z systemem operacyjnym Windows Server 2012 R2, na którym zainstalowano oprogramowanie G Data Management Server.

Maszyna ta ma posiada dostęp do Internetu, w związku z czym do jej głównych zadań należy pobieranie aktualnych baz sygnatur oraz szczepionek antywirusowych, a następnie ich dystrybucja do wszystkich stacji końcowych. W konsoli zarządzającej do dyspozycji administratorów zostały oddane takie funkcjonalności jak:

- Możliwość zdalnego zarządzania serwerami z zainstalowanym oprogramowaniem G Data Antyvirus
- Możliwość zdalnej instalacji klienta antywirusowego na nowych serwerach/maszynach wirtualnych, a także zdalnego inicjalizowania skanowania antywirusowego na wybranych stacjach
- Kontrolowanie aktualności posiadanych sygnatur oraz szczepionek
- Kontrolowanie oprogramowania instalowanego na stacjach posiadających klienta antywirusowego

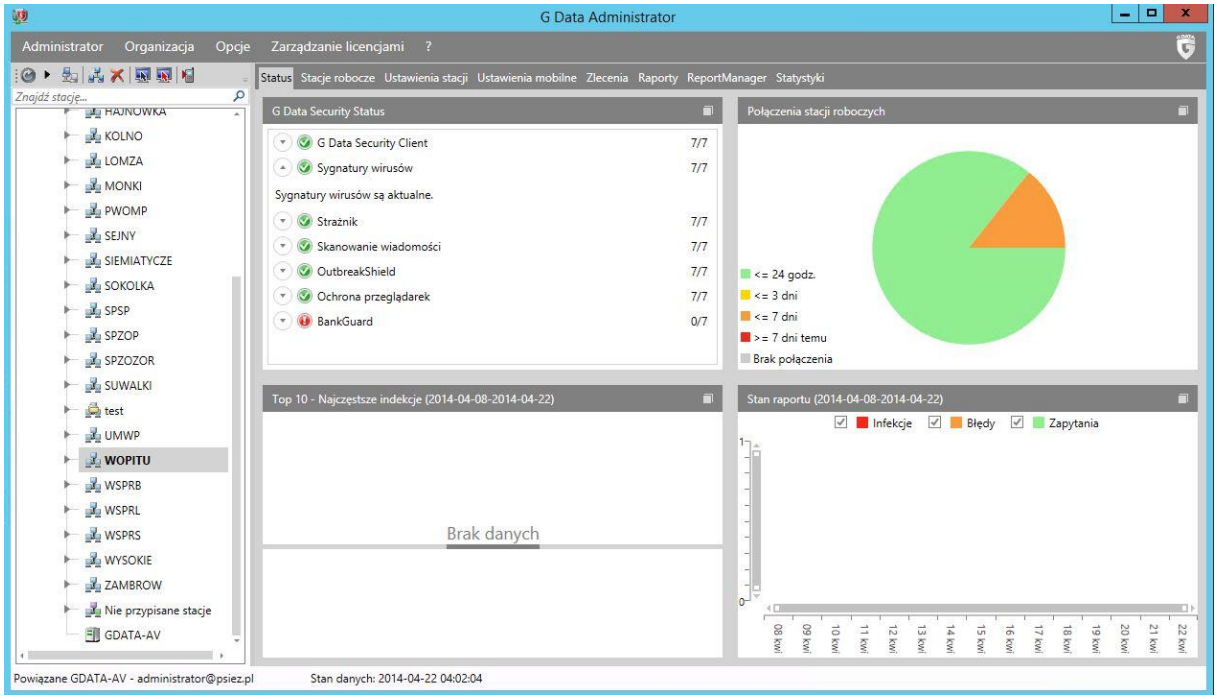
7.1. Dostęp do serwera zarządzającego

Baza danych systemu antywirusowego została zainstalowana na maszynie wirtualnej dostępnej pod adresem IP:

Na pulpicie znajduje się skrót do konsoli serwera zarządzającego umożliwiającej dostęp do konfiguracji ochrony antywirusowej.

Widok konsoli zarządzającej systemu G Data Antyvirus:

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 18 Serwer zarządzający systemu antywirusowego

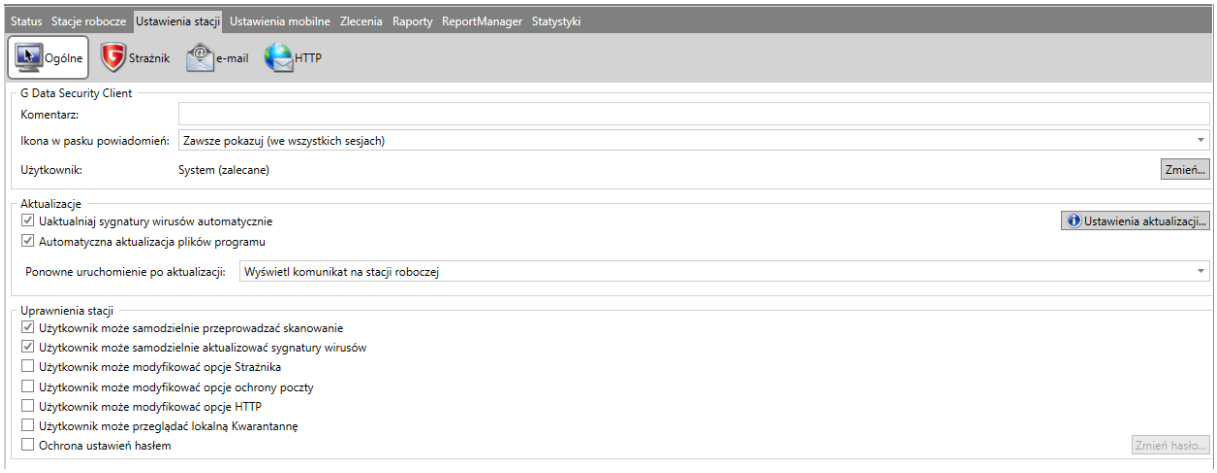
Obecnie konfiguracja serwera zarządzającego zakłada wykonywanie aktualizacji posiadanych sygnatur cyklicznie w odstępach jednogodzinnych. Po ukończeniu tego procesu, serwer rozpoczyna dystrybucję najnowszych wersji baz sygnatur do wszystkich stacji końcowych. Istnieje możliwość rekonfiguracji serwera w celu ograniczenia częstotliwości pobierania aktualizacji.

W konsoli zarządzania utworzono 26 jednostek organizacyjnych, w których pogrupowano stacje serwerowe objęte ochroną G Data Antyvirus. Dzięki temu można w łatwy sposób dokonywać przeglądu aktualności oprogramowania, szczepionek itd. per placówka.

Przyjęto następujące globalne ustawienia dla stacji roboczych:

- Automatyczne aktualizowanie baz wirusów
- Automatyczne aktualizowanie plików programu G Data
- Udostępnienie każdej ze stacji możliwości przeprowadzania skanowania

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 19 Ustawienia klientów antywirusowych na stacjach roboczych

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

8. System kopii zapasowych z wykorzystaniem bibliotek taśmowych

W niniejszej rozdziale zostały przedstawione aspekty techniczne wdrożenia systemu tworzenia kopii zapasowych (backupów) w ramach „Podlaskiego Systemu Informacyjnego e-Zdrowie". Dokumentacja obejmuje opis systemu backup w lokalizacji centralnej UMWP (Urząd Marszałkowski Województwa Podlaskiego).

System ma na celu wykonywanie kopii zapasowych danych z serwerów fizycznych oraz wirtualnych. Kopie zapasowe są wykonywane na każdym z serwerów za pomocą systemowego narzędzia Windows Server Backup i umieszczane na specjalnie do tego celu przeznaczonej przestrzeni na macierzy dyskowej. Następnie kopie zapasowe są kopiowane na biblioteki taśmowe za pomocą oprogramowania Symantec Backup Exec.

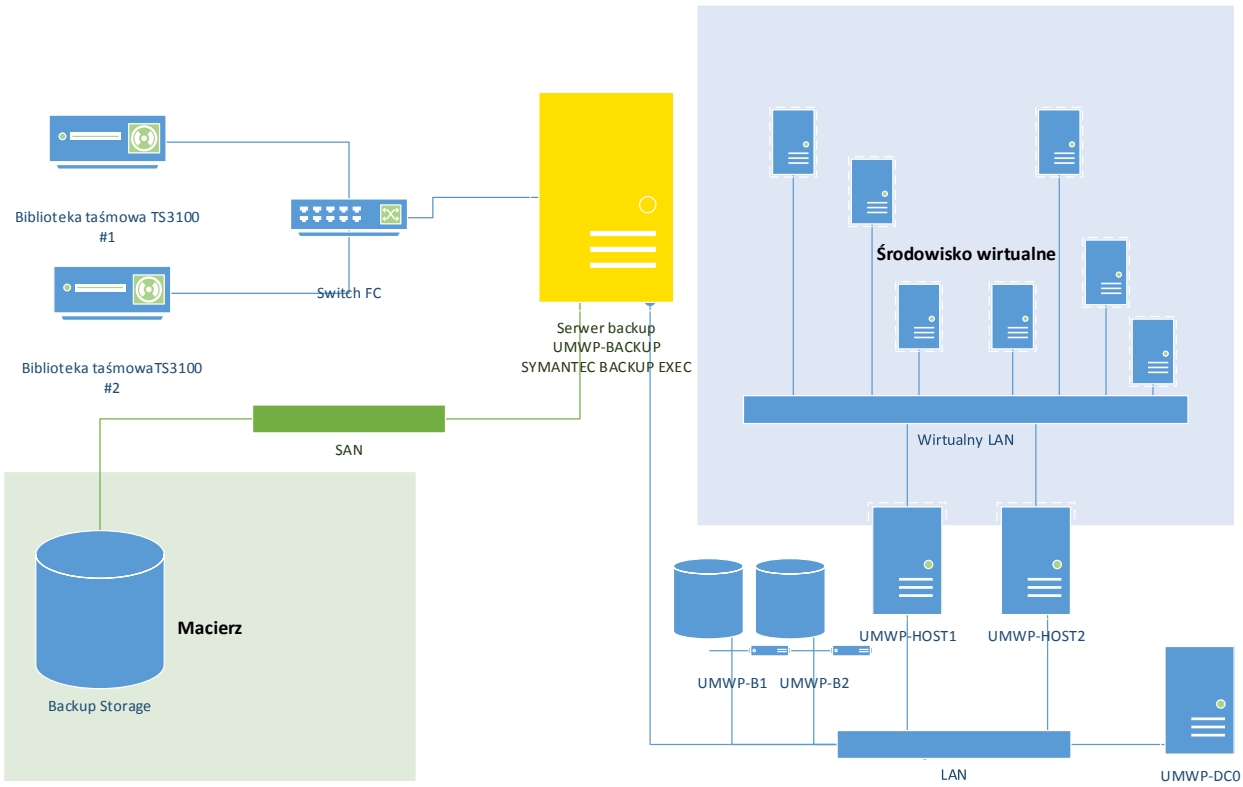
8.1. Architektura rozwiązania

Architektura systemu backupowego „Podlaskiego Systemu Informacyjnego e-Zdrowie" w centralnej lokalizacji UMWP (Urząd Marszałkowski Województwa Podlaskiego) składa się z następujących komponentów:

- Serwer backupowy – serwer fizyczny IBM Express x3650 M4, do którego został podmontowany LUN macierzy przeznaczony na dane backupowe serwerów. Na serwerze zostało zainstalowane oprogramowanie Symantec Backup Exec 2012, które wykonuje cykliczne kopiowanie backupów z podmontowanego LUN-a na dwie biblioteki taśmowe IBM TS3100. Serwer wykonuje również backup samego siebie na podmontowany LUN.
- Biblioteki taśmowe IBM TL3100 – dwie biblioteki taśmowe. Każda zawiera jeden napęd taśmowy Ultrium LTO 6. Biblioteki są podłączone do media serwera Backup Exec za pośrednictwem sieci Fibre Channel.
- Macierz dyskowa NetApp – Na dane backupowe został stworzony wolumen o pojemności 12 TB, który został podmontowany, jako LUN do serwera backupowego. Połączenie macierzy z serwerem backupowym jest realizowane w sieci SAN za pomocą infrastruktury Cisco Nexus. Serwer backupowy udostępnia zasoby z podłączonego LUN-a, jako zasoby sieciowe (SMB/CIFS).
- Serwery baz danych – dwa serwery fizyczne przeznaczone pod bazy danych, na których metodą systemowego backupu będą wykonywane kopie zapasowe baz danych i umieszczane w repozytorium backupów – przestrzeni macierzowej podłączonej, jako LUN do serwera backupowego.
- Serwery pozostałe – serwery fizyczne (hosty Hyper-V, kontroler domeny DC0) oraz wszystkie serwery wirtualne, na których metodą systemowego backupu będą wykonywane kopie zapasowe danych i umieszczane w repozytorium backupów – przestrzeni macierzowej podłączonej, jako LUN do serwera backupowego.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Poniższy rysunek przedstawia architekturę systemu backupowego „Podlaskiego Systemu Informacyjnego e-Zdrowie" w UMWP.



Rysunek 20 Schemat systemu backup w UMWP

8.2. Backupy systemowe serwerów

Dane przeznaczone do backupu na serwerach baz danych oraz na pozostałych serwerach są cyklicznie backupowane na LUN macierzy przeznaczony specjalnie do backupu. Serwery mają udostępnione następujące zasoby w sieci.

Serwery wykonują backupy na powyższe zasoby metodą systemową – za pomocą wbudowanego narzędzia Windows Server Backup.

Każde kolejne zadanie backupowe będzie nadpisuje poprzednio zbackupowane dane. Zbackupowane dane są dalej cyklicznie kopiowane na taśmy za pomocą oprogramowania Symantec Backup Exec na serwerze backupowym.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

8.3. Serwer backupowy

Serwer backupu jest fizycznym serwerem IBM Express x3650 M4 z systemem operacyjnym Windows Server 2008 R2 Standard SP1. Na serwerze zostało zainstalowane oprogramowanie do tworzenia kopii zapasowych Symantec Backup Exec w wersji 2012 SP3.

Poniższa tabela przedstawia parametry serwera backupowego.

Obiekt	Parametry
Hardware	IBM Express x3650 M4, CPU: Xeon 6C E5-2620 95W RAM: 8 GB Dyski: 2x500 GB 7.2K 6Gbps NL SAS (RAID1)
Nazwa hosta	UMWP-BACKUP
Adres IP	X.X.X.X
System operacyjny	Windows Server 2008 R2 SP1 Standard
Zainstalowane oprogramowanie do tworzenia kopii zapasowych	Symantec Backup Exec 2012 SP3
Dyski w systemie	C:\ - System 500 GB (lokalne dyski w RAID1) E:\ - Backup 12 TB (podmontowany LUN macierzy)

Tabela 12 Parametry serwera backupowego

8.4. Biblioteki taśmowe

Do serwera backupowego są podłączone 2 biblioteki taśmowe IBM TS3100. Każda z bibliotek została wyposażona w napęd taśmowy LTO6 z interfejsem FC, który jest połączony z kartą HBA w serwerze backupowym. W każdej bibliotece zastosowano 20 taśm LTO6 na dane backupowe + po jednej taśmie czyszczącej (maksymalna pojemność każdej z bibliotek: 23 sloty).

Biblioteki posiadają interfejsy zarządzające wpięte w sieć LAN. Zarządzanie odbywa się za pośrednictwem przeglądarki internetowej po zalogowaniu na adres IP interfejsu zarządzającego danej biblioteki i podaniu następujących poświadczeń:

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

9. Pamięć masowa na macierzach dyskowych

9.1. Opis konfiguracji macierzy FAS3220

9.1.1. Spis komponentów

System macierzowy FAS3220HA z IOXM składa się dwóch osobny kontrolerów umieszczonych w osobnych obudowach wraz z dodatkowym modułem IO. Do kontrolerów zostały dodane dodatkowe karty: 1 szt. 4 porty SAS, 2 szt. 2 porty 10 GB.

Do obu kontrolerów są podłączone półki dyskowe SAS oraz SATA. Zapewnienie możliwości kontroli półek jest realizowane przez okablowanie ACP (Alternative Control Path).

Dla celów zarządzania oraz komunikacji po sieci LAN przydzielono adresy IP odpowiednim interfejsom sieciowym: zarządzanie, Sieć ACP (adresacja wewnętrzna), sieć Gigabit Ethernet (VIF) oraz 10 Gigabit Ethernet. Lista adresów IP została przedstawiona w osobnej tabeli adresacji.

Na każdym kontrolerze zostanie ustanowione hasło dla użytkownika root, dające dostęp administracyjny oraz możliwość zarządzania poprzez karty zarządzania.

Interfejsy ethernetowe e0a i e0b mogą być zgrupowane w wirtualne interfejsy vif0 z wykorzystanie funkcji LACP dla celów dodatkowego udostępnia plików lub dysków po protokole iSCSI.

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

Nazwa	Funkcjonalność
Data ONTAP Essentials	System operacyjny macierzy razem z podstawowymi funkcjonalnościami
FC,CIFS	Obsługiwane protokoły
RAID DP	Obsługa RAID 4 oraz RAID DP
FlexVol	Dynamiczne wolumeny, którymi można zarządzać i dynamicznie zmieniać ich wielkość niezależnie do fizycznego położenia
FlexShare	Priorytetyzacja wolumenów
Snapshot	Możliwość wykonywania migawek danego stanu wolumenu bez wpływu na wydajność
Data Deduplication	Deduplikacja identycznych bloków danych
Data Compression	Kompresja bloków danych
Thin Provisioning	Efektywne wykorzystanie nieużytkowanej przestrzeni wolumenu, wolna przestrzeń nieużytkowana wolumenu jest do dyspozycji innych wolumenów.
Disk Sanitization	Czyszczenie dysków uniemożliwiające odczyt wcześniej zapisanych na nich danych
SyncMirror	Wykonywanie kopi lustrzanych wewnątrz macierzy
MetroCluster	Możliwosć tworzenia klastrów geograficznych
System Management	Zarządzanie politykami w macierzy, snapshotami oraz replikacją danych
Provisioning Manager	Rozwiązanie do automatycznej alokacji przestrzeni dyskowej w środowiskach NAS I SAN
Host Utilities	Narzędzia dla iSCSI i FCP służace do poprawnej konfiguracji kart HBA
MultiStore	MultiStore tworzy wiele wirtualnych systemów pamięci masowej w ramach jednej fizycznej macierzy

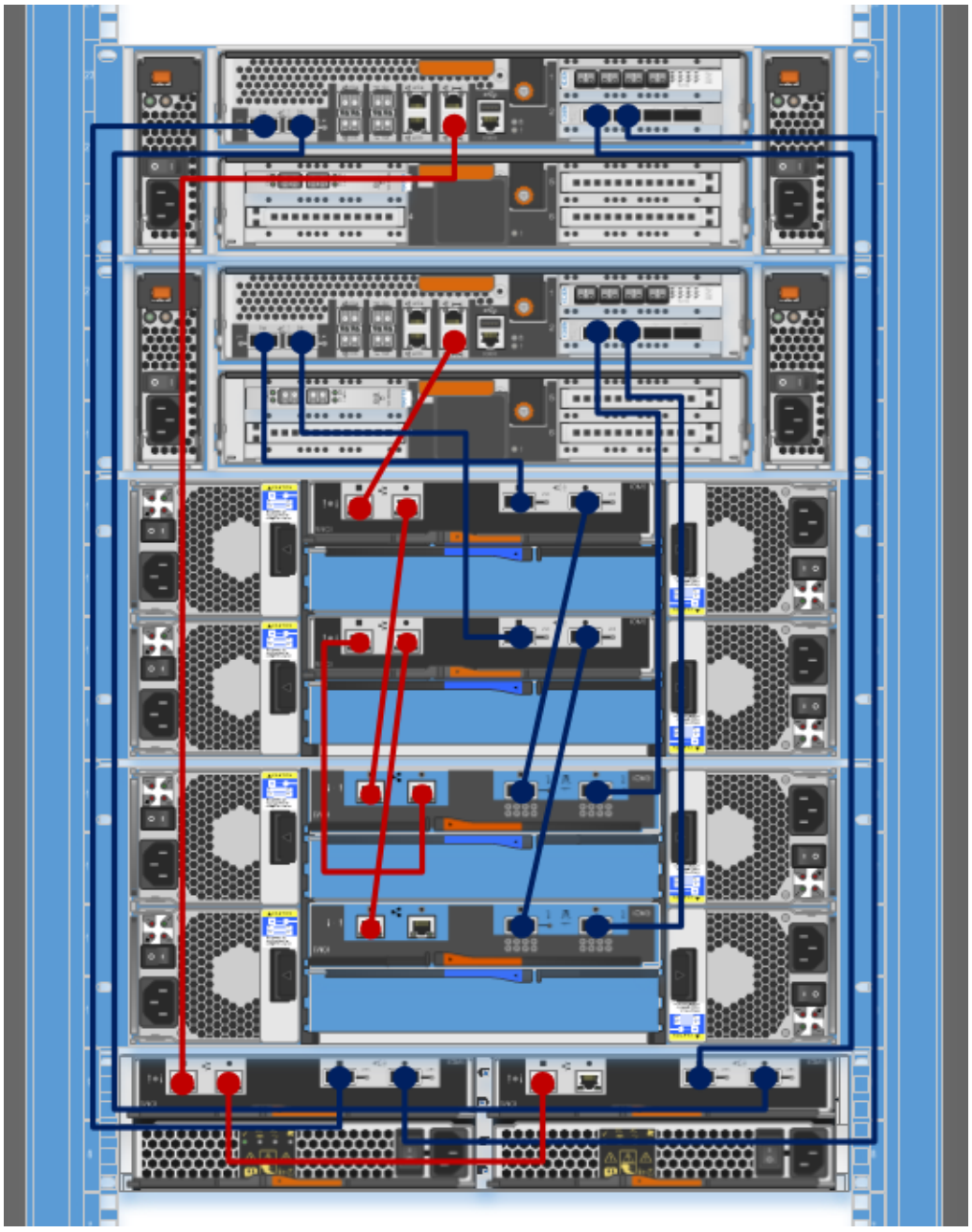
Tabela 13 Funkcjonalność oprogramowania dostarczanego z macierzą

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

9.1.2. Opis i schemat połączeń

Połączenia pomiędzy komponentami macierzy FAS3220 są w pełni redundantne. Poniżej zostały zaprezentowany sposób połączenia kontrolerów oraz półek (Kable ACP - kolor czerwony oraz Kable SAS - kolor niebieski). Ze względu na różny rodzaj półek i dysków zostały wykonane dwie pętle dyskowe. Wymaga to użycia dodatkowych kart z portami SAS.

Schemat połączeń komponentów macierzowych

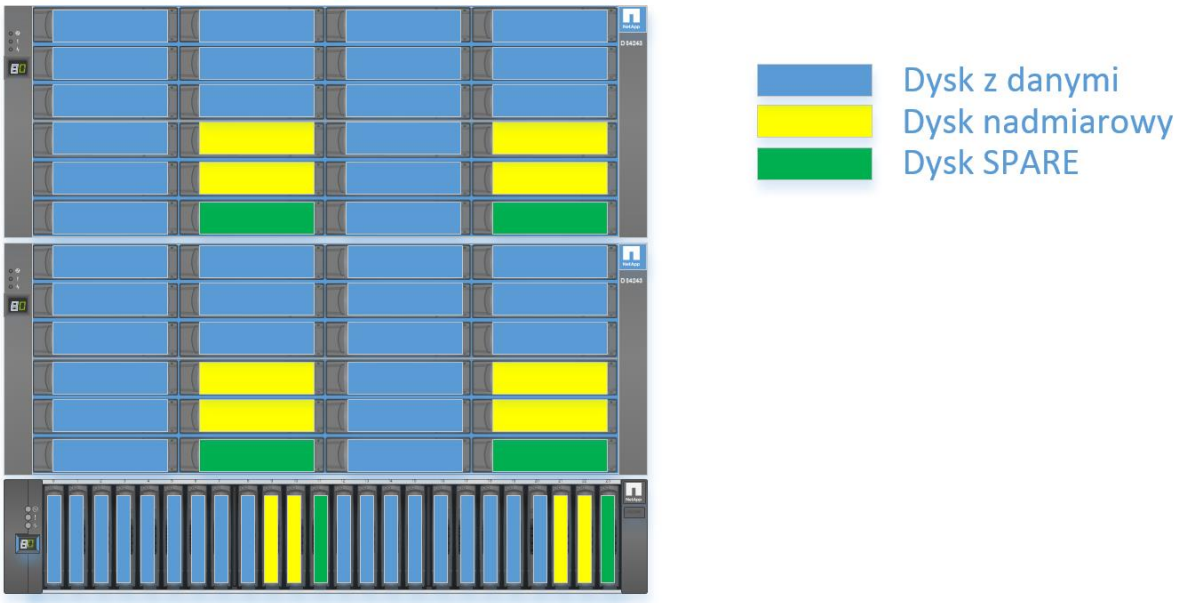


Rysunek 21 Schemat połączeń pomiędzy poszczególnymi portami macierzy

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

9.1.2.1. Grupy RAID

Dyski zostały zgrupowane w następujące grupy RAID:



- Grupa dyskowa SAS 12x 600 GB przypisana do kontrolera 2 – zasoby Baza danych
- Grupa dyskowa SAS 12x 600 GB przypisana do kontrolera 2 – zasoby Maszyny wirtualne
- Grupa dyskowa SATA 12x 1 TB przypisana do kontrolera 2 – zasoby Backup
- Grupa dyskowa SATA 12x 1 TB przypisana do kontrolera 2 – zasoby Backup
- Grupa dyskowa SAS 12x 600 GB E przypisana do kontrolera 1 – zasoby Baza plików
- Grupa dyskowa SAS 12x 600 GB E przypisana do kontrolera 1 – zasoby Baza plików

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl

10. Dostęp do serwerów out off band (CIMC)

W ramach projektu dostarczono platformę serwerową Cisco C240-M3L. Serwery te wyposażone są w niezależny interfejs przeznaczony do dostępu zdalnego do serwera oraz do zarządzania nim. Jest to szczególnie przydatne w przypadku awarii/niedostępności systemów operacyjnych zainstalowanych na serwerach – CIMC (Cisco Integrated Management Controller) umożliwia uruchomienie wirtualnego dostępu KVM. Dostęp do CIMC odbywa się za pośrednictwem przeglądarki internetowej WWW (adresacja oraz dane dostępowe umieszczono w rozdziale 11 - Zarządzanie).

10.1. Podstawowe funkcje CIMC

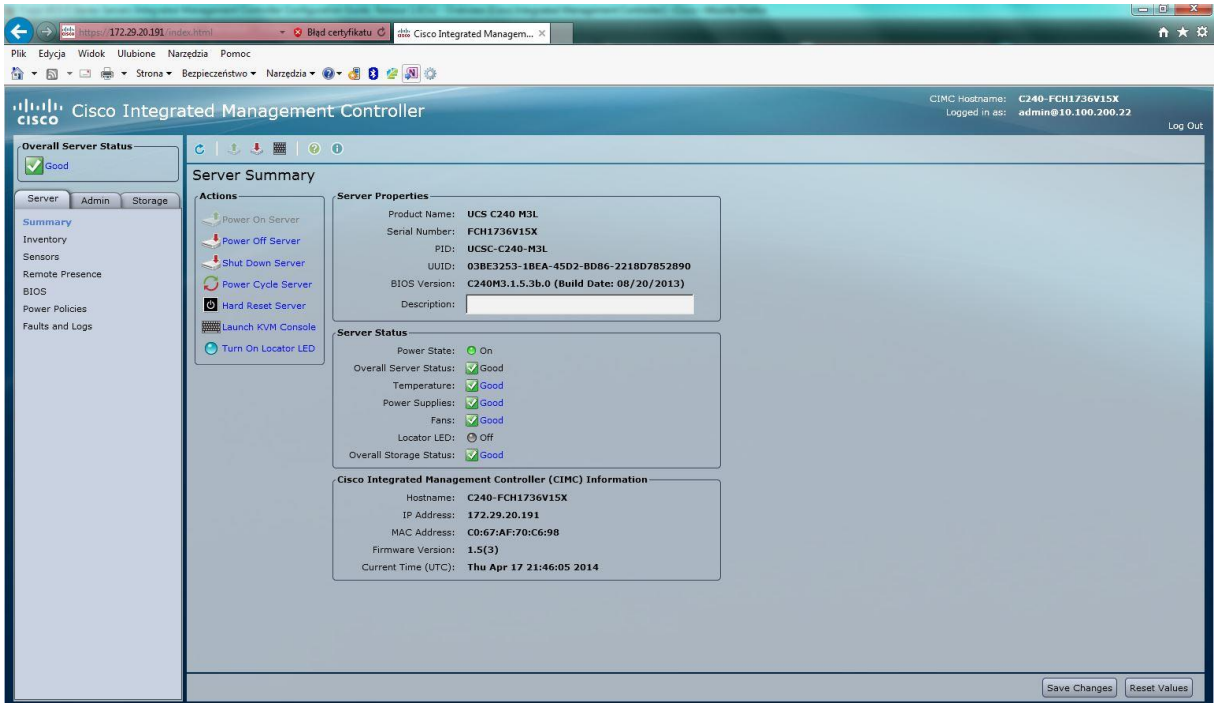
Przy wykorzystaniu CIMC możemy przeprowadzić następujące czynności:

- Zdalne uruchomienie, wyłączenie, zrestartowanie, resetowanie serwera
- Zlokalizowanie serwera przy pomocy diody LED
- Konfiguracja kolejności bootowania serwera
- Konfiguracja grup RAID
- Weryfikacja wskazań sensorów serwera
- Dostęp zdalny przez vKVM
- Konfiguracja sieciowa CIMC
- Konfiguracja dostępu zdalnego przez SSH, http IPMI over LAN
- Zarządzanie certyfikatami
- Dostęp do logów systemowych oraz dziennika zdarzeń
- Aktualizacja firmware'u CIMC
- Monitorowanie awarii, alarmów oraz statusu serwera

10.2. Elementy interfejsu

Poniższy rysunek przedstawia interfejs CIMC:

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl



Rysunek 22 Interfejs CIMC umożliwiający zdalne zarządzanie serwerami Cisco

Pełna dokumentacja CIMC wraz z opisem poszczególnych zakładek znajduje się pod adresem:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/1-5/b_Cisco_UCS_C-series_GUI_Configuration_Guide_151.pdf

Projekt współfinansowany przez Unię Europejską w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013
www.rpowp.wrotapodlasia.pl