

MODEL CADRU PENTRU PROIECTAREA, IMPLEMENTAREA ȘI SECURIZAREA ACCESULUI ÎN CADRUL UNUI SISTEM eLEARNING

Mihai Jitaru

Mihai.Jitaru@computerland.ro

MBL Computers, București

Dragoș Ioniță

Dragos.Ionita@training.computerland.ro

MBL Computers, București

Nicoleta Iacob

Nicoleta.Iacob@training.computerland.ro

MBL Computers, București

George Manea

George.Manea@computerland.ro

MBL Computers, București

Rezumat: În această lucrare se prezintă câteva din rezultatele proiectului de cercetare MEDSCEN-“Cercetări aprofundate pentru crearea unui sistem educațional pilot în spațiul virtual pentru simularea scenariilor privind dezastrea naturale și modulul de acțiune a cetățenilor și instituțiilor în situații de criză”, în curs de realizare de către un consorțiu condus de Universitatea Națională de Apărare „Carol I” (UNAp) și finanțat de ANCS prin CNMP. Este prezentat un model cadru pentru proiectarea, implementarea și securizarea accesului în cadrul unui sistem eLearning, cu accent pe tehnologiile și echipamentele care asigură infrastructura IT a soluției eLearning.

Cuvinte cheie: eLearning, model cadru, portal

Abstract: This paper presents some results of the MEDSCEN research project “Thorough research for the creation of a pilot educational system within the virtual space in order to simulate scenarios concerning natural disasters and appropriate action planning procedures designed for citizens and institutions in crisis situations”- a project in progress, conducted by a consortium coordinated by the National Defense University of Romania “Carol I” (UNAP) and financed by ANCS (the National Authority for Scientific Research) through CNMP (the National Centre for Programme Management). The authors present a framework for the design, implementation and access security of an eLearning system, focusing on technologies and equipment that provide the IT infrastructure of the eLearning solution.

Keywords: eLearning, infrastructure, framework, portal.

1. Introducere

Progresele înregistrate de IT, alături de schimbările din societate, au creat noi paradigme pentru educație și instruire. Odată cu dezvoltarea rapidă a Internet-ului și a tehnologiilor digitale, Web-ul a devenit un mediu puternic, global, interactiv, democratic și economic de învățare și instruire la distanță [1]. Modelele de eLearning au evoluat de la replicarea unei săli de clasă spre modele care integrează abordări tehnologice și pedagogice. În timp ce primele modele de eLearning pun accent pe rolul tehnologiei pentru furnizarea conținutului, pe servicii electronice și de acces, modelele mai noi pun accent pe abordările pedagogice, pe proiectarea instruirii on-line și crearea unor comunități de învățare on-line [2]. Khan a dezvoltat un model cadru pentru eLearning, care conține opt dimensiuni: instituțională, pedagogică, tehnologică, de proiectare interfață, evaluare, management, resurse suport și etică [3]. Fiecare dimensiune are subdimensiuni, cu accent pe aspectele specifice unui mediu eLearning.

În cadrul proiectului de cercetare MEDSCEN -“Cercetări aprofundate pentru crearea unui sistem educațional pilot în spațiul virtual pentru simularea scenariilor privind dezastrea naturale și modulul de acțiune a cetățenilor și instituțiilor în situații de criză”, în curs de realizare de către un consorțiu condus de Universitatea Națională de Apărare „Carol I” (UNAp) și finanțat de

ANCS prin CNMP, a fost realizat un model cadru pentru proiectarea, implementarea și securizarea accesului în cadrul unui sistem eLearning. Obiectivul general al proiectului MEDSCEN este crearea unei rețele educaționale folosind mediul Virtual Educațional și a unui Portal de Cunoștințe în domeniul intervenției, protecției și reconstrucției zonelor afectate de dezastru, în scopul formării culturii civice în ceea ce privește reacția la dezastru la nivelul cetățeanului și societății [4],[5],[6],[7]. Portalul de cunoștințe înglobează instrumente pentru crearea și difuzarea de conținut digital standardizat din domeniul protecției și reconstrucției în caz de dezastru, care să ofere cetățenilor, instituțiilor publice și agenților economici acces la informații neclasificate asupra asistenței în caz de dezastru și practici bune de răspuns la situații de dezastru care amenință individul și societatea. Totodată, prin acest portal, vor fi create și distribuite cursuri în format digital care vor viza cunoașterea în domeniu, formarea culturii de protecție și reconstrucție, noi metode de instruire și evaluare pentru instituții implicate în managementul crizelor și intervenția la dezastru, atitudinea civică și modelarea comportamentului uman în situații de criză, pe timpul acestora și în perioada post-criză.

2. Model cadru pentru tehnologiile eLearning

Pentru a putea clasifica și evalua tehnologiile și produsele folosite în soluțiile eLearning a fost introdus un model cadru pentru sistemele eLearning. Un astfel de model a fost dezvoltat de eLearnity Ltd. din Anglia, o organizație care oferă companiilor private și instituțiilor publice consultanță în implementarea unor soluții de eLearning sub formă de portaluri. Acest model este numit “cadru pentru tehnologiile eLearning” (eLearning Technology Framework) [8],[9].

Pe baza modelului propus de **eLearnity**, prezentăm în figura 1, sub forma unei diagrame, o variantă modificată pentru acest model, adaptată obiectivelor proiectului nostru. Ea prezintă, într-un cadru unitar, componentele principale ale arhitecturii unui sistem eLearning, inclusiv infrastructura informatică necesară soluției, dar și conținutul și mediul în care se face instruirea și se termină cu managementul și administrarea instruirii și a resurselor instruirii. Este un model organizat pe niveluri (straturi), fiecare nivel oferind resursele necesare pentru procesele (serviciile) de pe nivelul următor. Într-o anumită măsură acesta este un model arhitectural similar cu cel folosit în mod curent pentru a descrie protocoalele de rețea în standardul ISO-OSI.

Acest model cadru a fost proiectat pentru a ne ajuta să înțelegem rolul unor produse, modele și tehnologii necesare satisfacerii cerințelor specifice proiectării unui sistem eLearning. În plus, acest model cadru a fost foarte util pentru:

- clasificarea produselor pe baza rolurilor jucate în sistem;
- evaluarea unor produse și soluții specifice;
- identificarea produselor necesare pentru a răspunde unor cerințe eLearning specifice;
- proiectarea unei arhitecturi de ansamblu pentru o soluție eLearning;
- proiectarea unui model cadru pentru o combinație de produse, modele și tehnologii;
- alegerea unei strategii de securizarea a accesului utilizatorilor la conținutul portalului.

Aplicarea acestui model cadru în proiectul curent ne-a permis să identificăm componentele hardware și software care ar putea fi incluse în infrastructura IT și apoi, printr-o evaluare comparativă, să selectăm și să achiziționăm componentele cele mai potrivite, dar și strategia de configurare a securității accesului. În această evaluare am corelat mai mulți parametri, dintre care amintim:

- costuri;
- caracteristici tehnice;
- disponibilitatea pentru achiziționare;
- pregătirea tehnică a echipei în instalarea și configurarea componentelor;
- cerințele pentru securitatea sistemului.

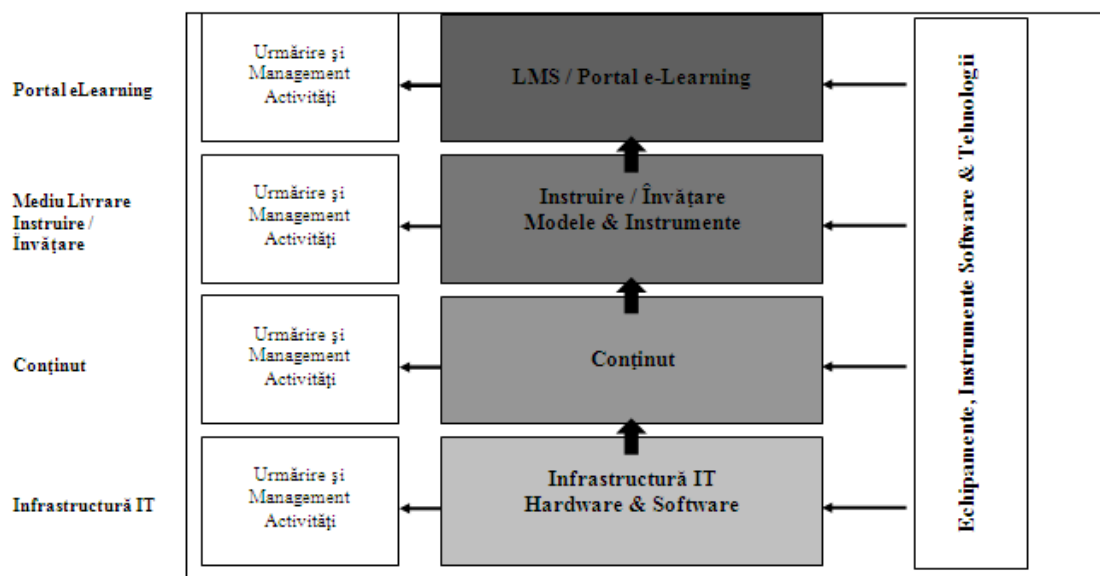


Figura 1. Model cadru tehnologic pentru soluții eLearning

La nivelul unu (nivelul cel mai de jos) sunt plasate procesele, tehnologiile și echipamentele care asigură infrastructura IT a soluției eLearning.

Cele 3 nivele superioare din modelul cadru au ca suport o infrastructură informatică (nivelul infrastructura IT în modelul cadru) compusă din calculatoare, echipamente de rețea, echipamente de stocare, software de bază (sisteme de operare), alte produse hardware și software specifice acestui nivel. În marea majoritate a situațiilor, în cazul portalurilor e-Learning pentru companii sau organizații, infrastructura IT pentru soluția eLearning este integrată în infrastructura IT a acestora. Aceasta include de asemenea accesul, utilizarea serviciilor de rețea, a bazelor de date, dar și a altor sisteme informatice existente (inclusiv a infrastructurii folosite pentru accesul la Internet). În cazul portalurilor publice, cum este și cazul proiectului nostru, infrastructura IT este dedicată și separată de cea a organizației gazdă, din diverse motive, inclusiv cele legate de securitatea și integritatea accesului la informații. Cât privește accesul la Internet în cadrul proiectului nostru, infrastructura IT este complet separată de cea a organizației ce găzduiește portalul (Universitatea Națională de Apărare). Soluția tehnică aleasă pentru implementarea infrastructurii IT este asemănătoare cu cea folosită de unele companii sub conceptul de centru de date (Data Center). Accesul la serviciile oferite se va face însă numai din rețeaua Internet.

3. Infrastructura IT

3.1 Aspecte de bază privind infrastructura IT

Nivelele 2, 3 și 4 din modelul cadru includ componente care pentru funcționare au nevoie de o infrastructură IT suport plasată în același model la nivelul 1.

Infrastructura IT include, printre altele, mai multe categorii de componente (Figura 2) pe care le-am grupat generic pe trei subnivele (straturi):

- hardware (echipamente fizice),
- sisteme de operare (software de bază) și
- servicii suport pentru aplicațiile de la nivelele 2, 3 și 4.

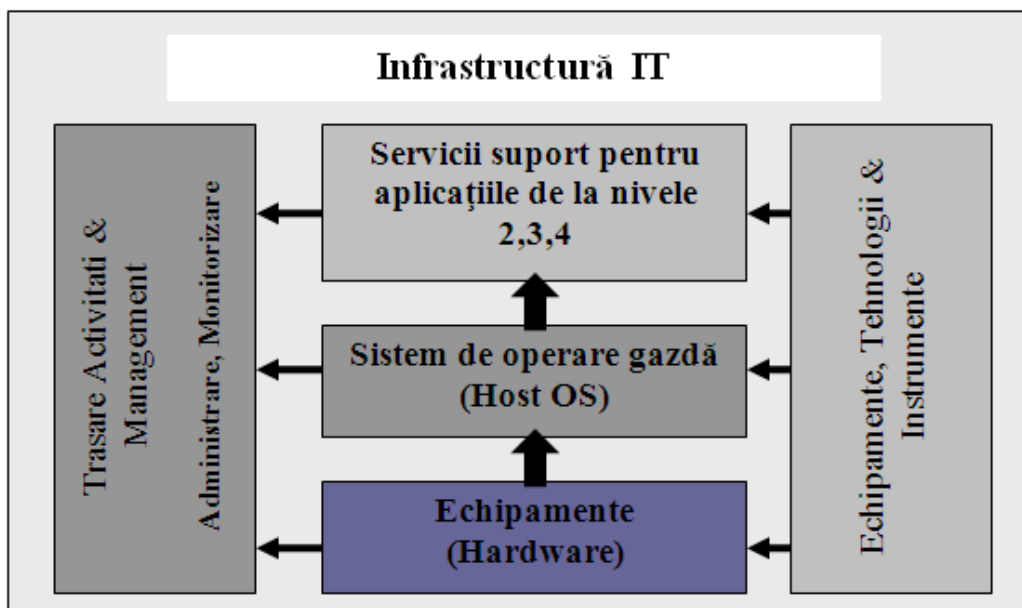


Figura 2. Model cadru tehnologii eLearning – Infrastructura IT (nivel 1)

Subnivelul **Hardware** include următoarele categorii de componente:

- calculatoare;
- echipamente de stocare date;
- echipamente de rețea.

Subnivelul **serviciilor suport** include:

- server Web;
- server proxy;
- server firewall;
- server DNS;
- server DHCP;
- server de poștă electronică;
- server pentru mesagerie instant;
- server pentru comunicații unificate;
- server Media streaming;
- server de baze de date;
- biblioteci suport.

Aceste servicii suport pot fi oferite pe mașini separate și atunci suprafața expusă atacurilor externe se reduce la mașina suport sau pot fi oferite pe aceeași mașină fizică și atunci suprafața expusă atacurilor crește semnificativ.

3.2 Categoriile de cerințe pentru infrastructura IT

În proiectarea și implementarea infrastructurii IT am ținut cont de o serie de cerințe care vin de la aplicațiile care în modelul cadru sunt plasate la nivelele 2, 3 și 4. Astfel de cerințe includ [10]:

- funcționalitatea;
- disponibilitatea;
- scalabilitatea;
- performanța;
- securitatea.

Funcționalitatea reprezintă o cerință minimală asupra infrastructurii IT. Aceasta trebuie gândită în așa fel încât să asigure funcționarea corectă a aplicațiilor atâta timp cât echipamentele, sistemul de operare și serviciile suport funcționează corect. Dacă una dintre aceste componente cade, atunci funcționalitatea aplicațiilor poate fi afectată pe o perioadă de timp mai scurtă sau mai lungă.

Disponibilitatea este o cerință care se referă la una dintre componentele din infrastructura IT, sau la un grup de componente din infrastructura IT. Ea cere ca funcționalitatea aplicației să nu fie afectată de funcționalitatea unei componente sau a unui grup de componente. De exemplu, dacă componenta referită este calculatorul, atunci cerința de disponibilitate cere să alegem o soluție care să ne asigure că aplicația funcționează, chiar dacă calculatorul suport la un moment dat devine neoperațional. În acest caz, în infrastructura IT trebuie să folosim o soluție tehnică care să garanteze disponibilitatea aplicației la căderea unui calculator. Ca soluție tehnică în acest caz va trebui să alegem tehnologia de tip “cluster de calculatoare”, adică un grup de minimum două calculatoare interconectate într-un cluster. În acest fel, dacă mașina pe care se execută aplicația la un moment dat cade și ea face parte dintr-un cluster, atunci aplicația va fi repornită automat (după un timp minim de nefuncționare) pe un alt calculator membru în cluster. Astfel de cerințe de disponibilitate pot fi formulate și în legătură cu alte componente din infrastructură, cum ar fi: procesoare, echipamente de stocare, interfețe de rețea, mediile de comunicare în rețeaua locală, componente din sistemul de operare gazdă, serviciile suport, conexiunea la Internet, etc. Aceste cerințe presupun soluții tehnice specifice, dar și costuri suplimentare. Concret, în cazul proiectului nostru pentru a răspunde acestei cerințe pe de o parte am inclus în infrastructura IT două calculatoare care vor oferi serviciile portalului către clienți, iar pe de altă parte, baza de date a portalului va fi stocată pe volume disc ce oferă disponibilitate avansată (RAID 5), iar sistemele de operare pentru cele două calculatoare sunt stocate pe volume în oglindă (RAID 1).

Scalabilitatea este legată de nevoia de a adapta un serviciu oferit unor consumatori în mod transparent pentru aceștia. De exemplu, dacă am proiectat o infrastructură IT scalabilă pentru un serviciu eLearning public pentru o cerere care astăzi înseamnă în medie 100 consumatori simultan și mâine cererea crește la 1000 consumatori simultan atunci, cu ajustări adecvate la nivelul echipamentelor, sistemului de operare, serviciilor suport sau al conexiunii la Internet, sistemul va putea fi adaptat să răspundă noilor cerințe fără ca cei care-l folosesc să simtă acest lucru. Modificările făcute nu trebuie să întrerupă funcționarea aplicației. Ca și în cazul disponibilității, cerința de scalabilitate trebuie să refere una sau mai multe dintre componentele din infrastructura IT. În cadrul proiectului nostru această cerință poate fi implementată simplu prin adăugarea transparentă pentru clienți a unor calculatoare suplimentare care să ofere aceleași servicii (inclusiv sub formă de mașini virtuale).

Performanța este o cerință care în general referă timpul necesar pentru a oferi un răspuns la un serviciu solicitat. De exemplu, în cazul nostru, dacă un consumator extern cere acces la un curs în format eLearning și interacțiunea cu sistemul este lentă (intervalul de timp scurs în trimiterea unei cereri și primirea răspunsului sistemului este mare) atunci putem spune că performanța cu care este oferit serviciul este redusă (deși serviciul funcționează corect și este disponibil permanent). În acest caz în infrastructura IT trebuie incluse componente, dar și tehnologii, care oferă performanțe suficient de mari pentru ca serviciul oferit să fie oferit în parametri de performanță acceptabili pentru consumator. De exemplu, într-o astfel de situație, viteza cu care informația este transmisă pe canalul care asigură legătura la Internet, viteza de procesare a informației în procesoarele calculatoarelor, viteza de acces la echipamentele de stocare pot fi parametri critici pentru performanța unui sistem. Cum serviciile portalului din proiectul nostru vor fi oferite pe două calculatoare, avem în vedere implementarea unui mecanism de tip “load balancing” prin care cererile clienților care vin din Internet să fie distribuite uniform pe cele două servere din infrastructura IT. În prima fază acest mecanism va fi implementat pe Firewall.

Securitatea este o cerință critică având în vedere faptul ca portalul creat ca produs final în cadrul acestei cercetări va oferi servicii eLearning publice. Expunerea la Internet înseamnă și

posibilitatea de a ne confrunta cu cea mai mare gamă de tipuri de atacuri posibile. Soluția aleasă de noi pentru a implementa “firewall-ul” ne permite să configurăm restricții de acces la serviciile portalului folosind reguli de filtrare pentru accesesele neautorizate.

3.3 Infrastructura fizică și infrastructură virtuală

În mod normal termenul **infrastructură fizică** este folosit pentru a desemna echipamentele fizice din infrastructura IT care sunt folosite de aplicații în cursul execuției acestora. Infrastructura fizică oferă resursele necesare aplicațiilor. Sistemul de operare este interfața care oferă infrastructura fizică aplicațiilor la cererea acestora. În plus, sistemul de operare joacă și rolul de arbitru în cazul în care mai multe aplicații cer acces în același timp la unele resurse din infrastructura fizică. Indiferent de caz, sistemul de operare oferă direct aplicațiilor resursele din infrastructura fizică.

În timp, unele resurse din infrastructura fizică au trecut dincolo de nevoile aplicațiilor sau au rămas sub cerințele unor aplicații. De exemplu, dacă în infrastructura fizică există un hard disc cu capacitatea de 100GB și o aplicație are nevoie doar de 10GB spațiu de stocare, a oferi aplicației această resursă în întregime nu este soluția corectă. Într-o astfel de situație, sistemul de operare transformă o resursă fizică în **resurse logice**, iar aplicațiilor li se oferă **resursele logice** și nu direct resursele fizice. În exemplul de mai sus, hard discul fizic este împărțit în mai multe volume logice de mărimi (sub 100GB) care sunt compatibile cu cerințele aplicațiilor. Aceeași metodă se poate aplica și în cazul în care aplicațiile au nevoie de resurse mai mari decât cele oferite de infrastructura fizică. De exemplu, dacă avem o aplicație care are nevoie de 200GB spațiu de stocare pentru un sistem de fișiere, atunci putem crea un volum logic de 200GB din spațiul disponibil pe două hard discuri fizice de câte 100GB disponibile în infrastructura fizică.

Aceasta este abordarea tradițională pentru infrastructura IT și ea se mulează perfect pe modelul cadru cu trei niveluri prezentat mai sus.

O abordare mai sistematică a procesului de transformare a resurselor din infrastructura fizică în resurse logice pentru aplicații este oferită de **virtualizare**. În industria IT, **virtualizarea** este văzută ca un mecanism prin care un set de resurse fizice disponibile în infrastructura fizică este prezentat ca un set coerent de resurse de calcul logice, astfel încât aceste resurse logice de calcul pot fi accesate de aplicații în același mod ca și resursele din infrastructura fizică. Un set de resurse logice de calcul include procesoare logice de calcul, memorie, rețea, alte periferice logice, adică tot ceea ce este necesar să oferim ca suport (platformă logică) pentru sistemul de operare și apoi aplicațiilor, sau direct pentru aplicații.

Virtualizarea înlocuiește astfel infrastructura fizică cu noțiunea de **infrastructură virtuală**. Infrastructura virtuală modifică modelul pe trei niveluri pentru infrastructura IT prezentat mai sus, introducând un nivel suplimentar între aplicații și infrastructura fizică. Infrastructura virtuală are marele avantaj că poate să armonizeze mai bine resursele disponibile în infrastructura fizică cu resursele necesare efectiv aplicațiilor. Mai mult, această asociere se poate face dinamic, pe măsură ce aplicațiile își ajustează cerințele de resurse de calcul, de memorie și de rețea, de la o execuție la alta sau chiar în cursul aceleiași execuții.

3.4 Virtualizarea și infrastructura IT

Resursele fizice care pot fi virtualizate includ: sistemele de calcul, echipamentele de stocare și rețeaua. Consolidarea serverelor prin virtualizare se poate realiza prin faptul că pe aceeași mașină fizică putem implementa roluri multiple folosind mașini virtuale separate pentru fiecare dintre acestea. În acest fel putem maximiza utilizarea resurselor fizice ale mașinii concomitent cu creșterea securității și simplificarea administrării prin faptul că fiecare rol (de fapt fiecare serviciu) va rula într-un mediu virtual izolat (mașina virtuală).

Virtualizarea infrastructurii fizice (inclusiv a serverelor unei companii) poate fi implementată la oricare dintre cele 3 subniveluri: hardware, sistem de operare sau servicii suport pentru aplicații.

4. Infrastructura Hardware

4.1 Descrierea soluției

În accepțiunea de față infrastructura IT hardware propusă pentru centrul pilot a fost compusă din următoarele categorii de componente fizice:

- calculatoare (într-o configurație de tip server);
- echipamente de stocare a datelor (storage devices);
- echipamentele de rețea (interfețe de rețea, medii de comunicație, echipamente de interconectare în rețea: switch, rutor).

În esență, infrastructura hardware implementată este de fapt o rețea locală fizică care interconectează echipamentele de tip server cu echipamentele de stocare a datelor. Această rețea a fost conectată la rețeaua Internet printr-un canal de comunicație dimensionat adecvat cerințelor de utilizare a serviciile oferite de centrul pilot către consumatori. Separarea între Internet și rețeaua fizică a centrului pilot este asigurată de un server dedicat, configurat ca “firewall”.

O soluție de implementare pentru infrastructura fizică, spre care ne-am orientat este prezentată în figura 3.

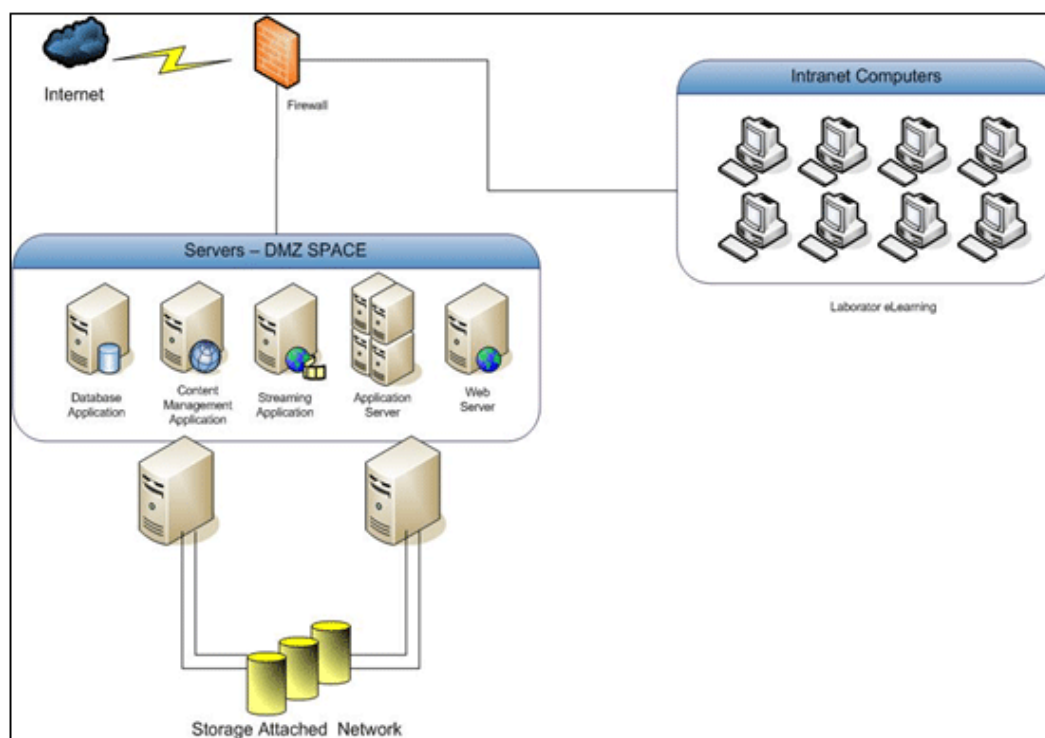


Figura 3. Soluție conceptuală de implementare pentru infrastructura IT hardware

La alegerea acestei soluții am luat ca bază soluțiile de organizare de tip “centru de date” (DataCenter) pe care le folosesc o mare parte dintre companiile din lume. Soluția este compactă, accesul se poate realiza strict controlat din Internet și din Intranet, monitorizarea echipamentelor și a serviciilor oferite se poate face remote, la limită tot ansamblul poate fi mutat dacă este nevoie într-o altă locație cu implicații minime etc.

4.2 Soluția implementată pentru infrastructura IT hardware

Schematic soluția propusă și implementată pentru infrastructura IT hardware a fost prezentată în figura 3. În figura 4 este prezentată o schemă ce redă soluția tehnică implementată.

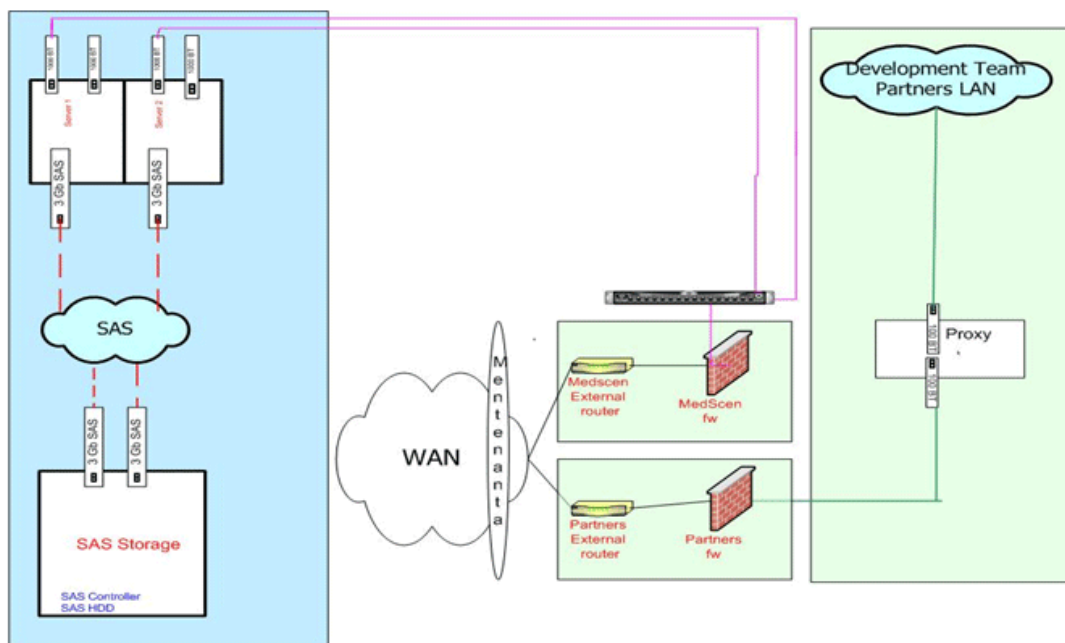


Figura 4. Schema tehnică de implementare pentru infrastructura IT hardware

Aceasta include următoarele componente:

- o două servere CISC (IBM x3650) cu arhitectura pe 64 biți care oferă resursele de procesare, stocare și acces în rețea pentru serviciile ce vor fi oferite prin portalul e-Learning consumatorilor.
- o un server CISC (IBM x3650) cu arhitectură pe 64 biți pe care va rula serviciul de tip firewall. Acest calculator se va situa la granița dintre Internet și rețeaua internă a Centrului Pilot.
- o un echipament de stocare în rețea de tip DAS (SAS Storage – IBM DS3200), care oferă spațiul de stocare necesar aplicațiilor care vor rula în portal, dar și pentru operațiile de salvare / restaurare curente.
- o o rețea locală pentru interconectarea celor două servere pentru portal și a serverului firewall (switch, medii de comunicație, interfețe de rețea).
- o o rețea locală specializată pentru transferul de date între servere și echipamentul de stocare (SAS cabling).
- o o conexiune la Internet pentru accesul utilizatorilor la serviciile oferite de portalul eLearning, dar și pentru administrarea remote a sistemelor din Centrul Pilot.

5. Infrastructura Software

5.1 Soluția propusă pentru infrastructura IT software

Pentru a identifica cât mai exact componentele care pot intra în infrastructura IT, am identificat și folosit un model pe niveluri, care ne-a permis alegerea soluțiilor ce vor fi implementate pentru serverele portalului, cât și pentru serverul de tip firewall care permite accesul din Internet la portal și securitatea necesară. Soluția propusă pentru infrastructura software este prezentată în figura 5. Componentele software posibil a fi folosite au fost

organizate într-un model pe mai multe niveluri, fiecare dintre aceste niveluri având propriul rol în crearea mediului virtual al portalului.

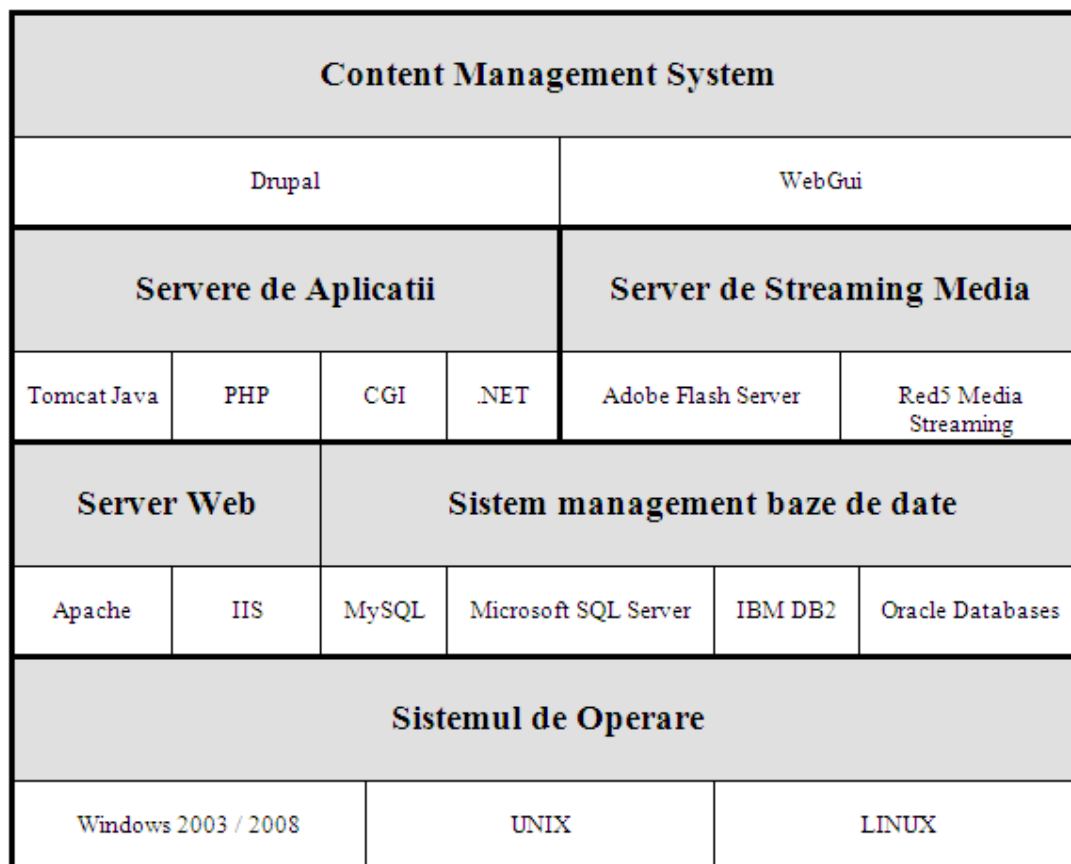


Figura 5. Soluții posibile în infrastructura IT subnivel software

Primul subnivel, de jos în sus, este cel al sistemului de operare, care se instalează pe infrastructura fizică sau virtuală selectată. Alegerea sistemului de operare va ține cont de rolul serverului în cadrul portalului: server web, server de aplicație, server streaming, server bază de date sau firewall.

5.2 Soluția implementată pentru infrastructura IT software pe serverele portalului

Ținând cont de analiza făcută anterior în legătură cu diversele soluții posibile, soluția implementată pentru infrastructura IT a portalului include componentele software specificate în figura 6. Am folosit pentru prezentare o stivă compatibilă cu modelul cadru.

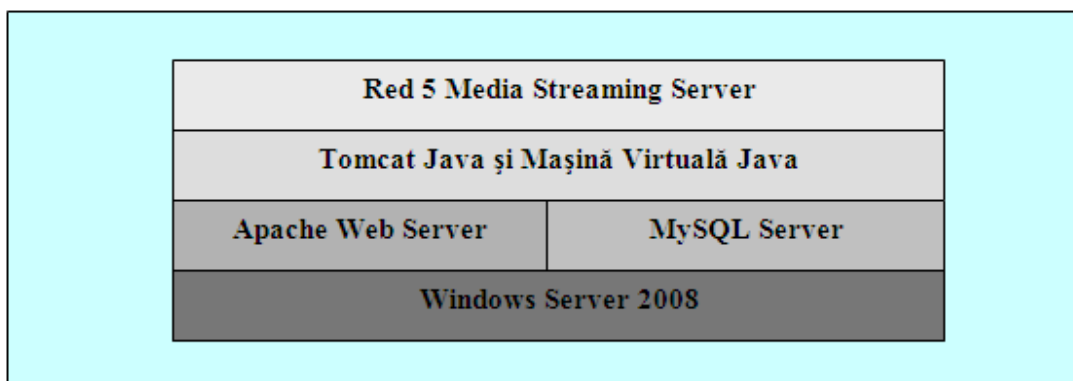


Figura 6. Infrastructura IT software implementată pe server portal

Componentele propuse ca parte a soluției software au fost implementate în acest moment pe infrastructura hardware fizică (figura 7). Ulterior este posibil să revenim asupra acestei soluții folosind o soluție bazată pe mașini virtuale (care va include un set adecvat de mașini virtuale) (figura 8). În primul caz, serviciile necesare portalului au fost distribuite pe cele două servere fizice în funcție de modul de conectare dintre acestea, dar și de resursele necesare acestora.

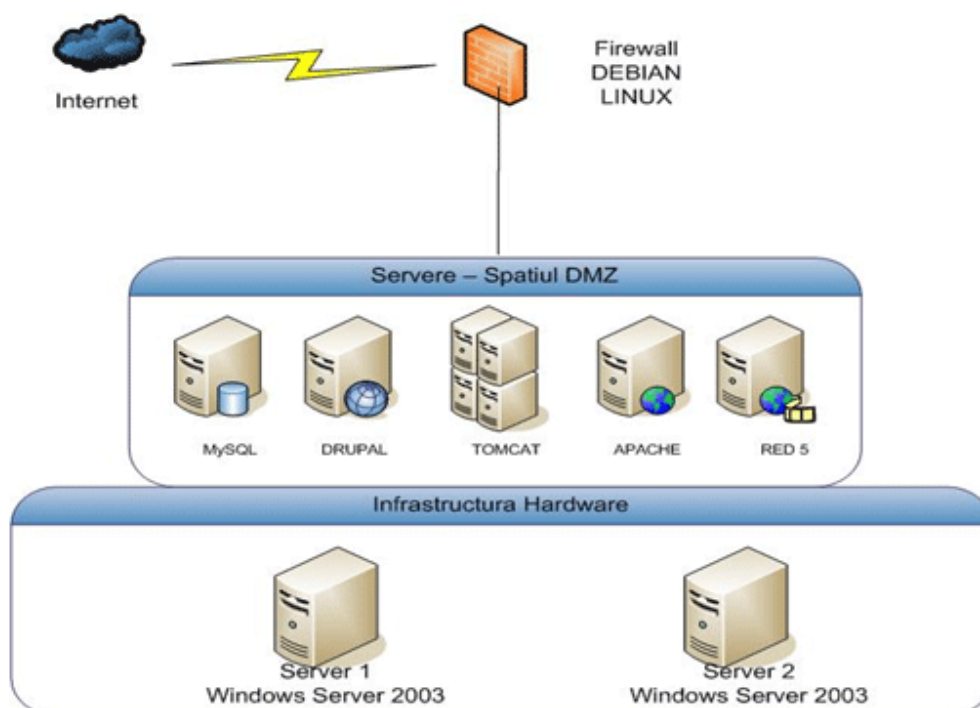


Figura 7. Schema de conectare în infrastructura fizica

În infrastructura virtuală, fiecare serviciu poate fi instalat pe o mașină virtuală, fiind astfel virtual din punct de vedere software.

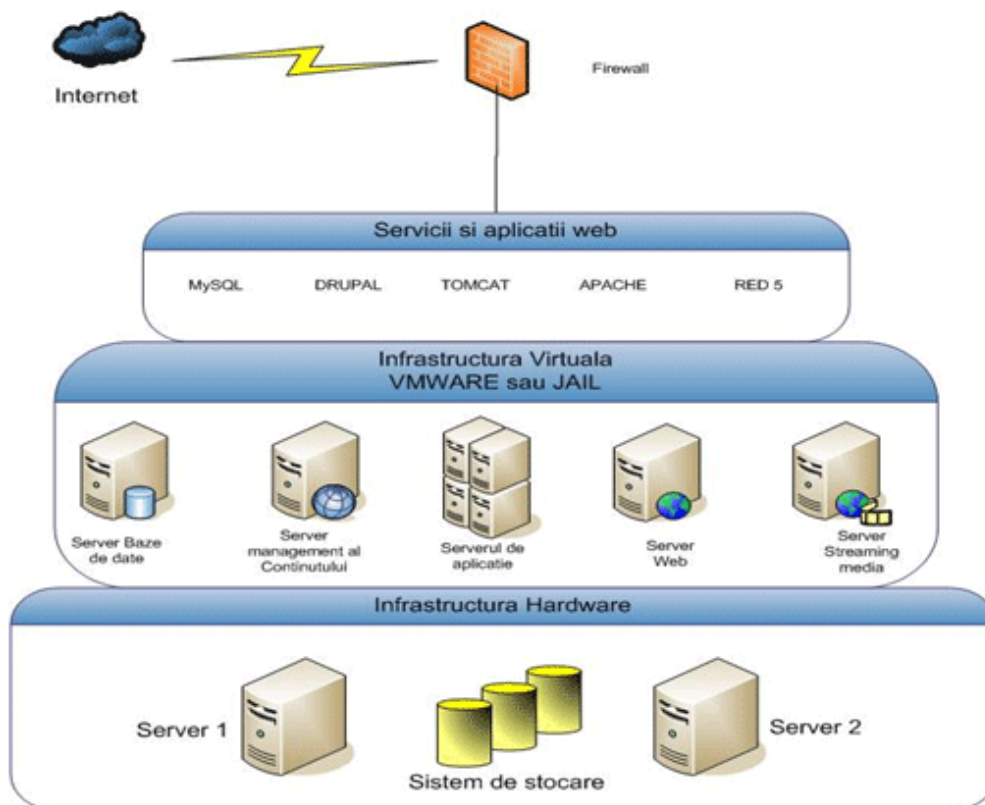


Figura 8. Schema de conectare în infrastructura virtuală

5.3 Soluția implementată pentru infrastructura IT software pe server-ul “firewall”

Pentru firewall infrastructura IT implementată are la bază una din distribuțiile de Linux consacrate pentru acest gen de utilizare. Este vorba de sistemul de operare Linux -Debian. Sistemul conține servicii incluse care ne permit să implementăm funcțiile standard pe un astfel de server:

- filtrare pachete pe bază de reguli;
- optimizarea accesului folosind un server proxy;
- protecție la viruși;
- distribuirea uniformă a cererilor din Internet pentru acces la portal pe cele două server-e suport
- rezolvarea numelor.

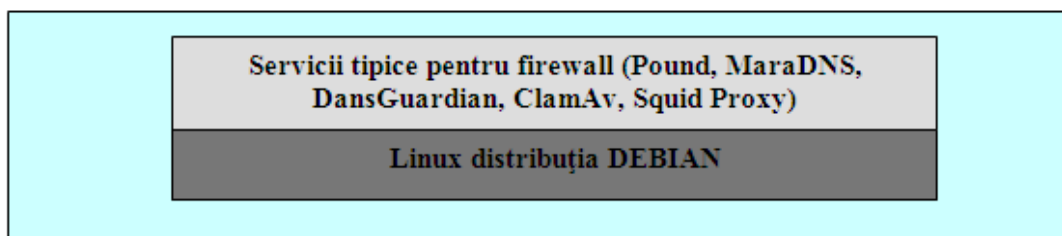


Figura 9. Infrastructura IT software implementată pe firewall

6. Concluzii

Modelul cadru pentru tehnologiile și componentele unei soluții eLearning, identificat în cadrul proiectului MEDSCEN, ne-a permis o abordare arhitecturală a unui sistem eLearning, inclusiv a portalului ce trebuie proiectat și realizat prin acest proiect. Același model cadru a fost folosit pentru aplicarea unei strategii globale de securizare a accesului utilizatorilor la serviciile oferite de portalul MEDUCA.

Modelul pentru designul, accesul, implementarea infrastructurii IT dar și pentru implementarea strategiei de securizare a fost cel al unui Centru de Date (Data Center), model folosit curent de companiile actuale. Acest model ne-a oferit maximum de flexibilitate, scalabilitate, securitate și chiar performanță în condițiile unor costuri mai reduse.

Infrastructura IT, în soluția propusă pentru centrul pilot, a fost implementată ca entitate de sine stătătoare, cu propria soluție de acces la Internet (obiectiv ce a fost implementat în faza actuală a proiectului). Nu există nici o interferență cu Intranet-ul organizației gazdă (UNAp). Portalul este în acest moment funcțional și este accesibil din Internet prin adresa <http://www.meduca.ro>.

BIBLIOGRAFIE

1. **KHAN, B. H.**, *Managing e-learning: design, delivery, implementation, and evaluation*, Information Science Publishing, 2005.
2. **KHAN, B. H.**, *A Framework for E-learning*, 2001, Disponibil la: [<http://www.bookstoread.com/framework/>]
3. **ENGELBRECHT, E.**, A look at e-learning models: investigating their value for developing an e-learning strategy, *Progressio*, Vol. 25 No.2, pp.38-47, 2003.
4. **ROCEANU, I.** coord., *Dezastrele naturale și efectele asupra populației*, Editura Universitară, București, 2008.
5. **ROCEANU, I.** coord., *Proiectarea și realizarea sistemului integrat eLearning pentru servicii educaționale on-line*, Editura Universitară, București, 2008.
6. <http://medscen.expert.org.ro/>
7. <http://www.meduca.ro/>
8. *** - "e-Learning The Feature of Learning", White Paper, eLearnity Ltd, UK, 2000.
9. *** - "Learning Management and Portals", White Paper, eLearnity Ltd, UK, 2001.
10. **ABBAS, Z., M. UMER, M. ODEH, R. MCCLATCHEY, A. ALI, F. AHMAD**, A semantic grid-based e-learning framework (SELF), Fifth IEEE International Symposium on Cluster Computing and the Grid (CCGrid'05) - Volume 1, 2005, pp. 11-18.