

APACHE  
HTTP SERVER



10/16/2012

---

---

# Αναδιάρθρωση υπηρεσιών ιστού

*Project proposal*

---

---

Άντρη Μιχαηλίδου

Έκδοση 3<sup>η</sup>

## Περιεχόμενα

Σκοπός του έργου .....	2
ΔΙΚΤΥΟ.....	3
Τοπολογία μηχανών στο δίκτυο .....	3
Χρήση DMZ - Τι κερδίζουμε; .....	4
Firewall .....	4
ΠΕΡΙΕΧΟΜΕΝΟ ΙΣΤΟΥ και ΥΠΗΡΕΣΙΕΣ.....	5
Κατηγορίες περιεχομένου ιστού .....	5
Υπηρεσίες.....	6
Υπάρχουσα δομή .....	12
ΑΝΑΔΙΑΡΘΡΩΣΗ.....	14
Γενική περιγραφή/στόχοι έργου.....	15
Φάσεις έργου.....	16
Νέες πρακτικές .....	17
ΧΡΗΣΗ ΥΛΙΚΟΥ .....	17
Μελλοντική εργασία.....	18
Comments: .....	19

# Αναδιάρθρωση υπηρεσιών ιστού

*Project proposal*

## Σκοπός του έργου

---

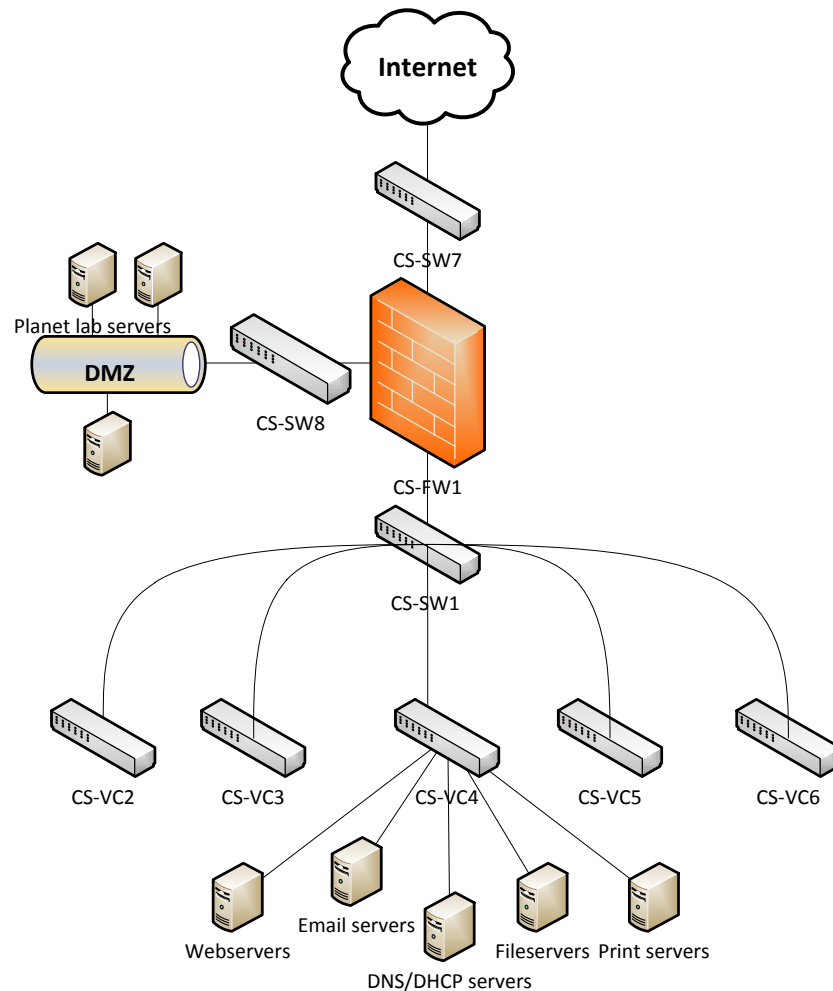
Σκοπός του έργου είναι η αναδιάρθρωση των εξυπηρετητών ιστού του τμήματος με στόχο την ασφάλεια των συστημάτων και της υποδομής του τμήματος. Επιπλέον πρέπει να διασφαλίζεται η αδιάλειπτη παροχή υπηρεσιών ιστού που εξυπηρετούν κρίσιμες υπηρεσίες όπως τη σελίδα του τμήματος και το webmail.

Σε γενικές γραμμές πρέπει να γίνουν τα πιο κάτω:

- Προστασία των εξυπηρετητών ιστού από 'εισβολείς', αλλά και προστασία της υποδομής του τμήματος από τους web servers
- Αλληλοκάλυψη των υπηρεσιών που παρέχονται από της μηχανές σε περιόδους αναβάθμισης, χωρίς downtime
- Απαγόρευση της απευθείας πρόσβασης από τα μέλη του τμήματος, αλλά χρήση ενός login server, για την ανανέωση και αλλαγή των σελίδων
- Διαχωρισμός των web application των φοιτητών (short term/non secure) από τα web applications του τμήματος
- Καλύτερος διαμοιρασμός του φόρτου στις μηχανές
- Καθορισμός της μηχανής www5 καθαρά ως testing μηχανήμα για την ΟΤΥ
- Πολιτική τοποθέτησης web servers/web applications στο δίκτυο

## ΔΙΚΤΥΟ

### Τοπολογία μηχανών στο δίκτυο



**Εικόνα 1: Τοπολογία μηχανών**

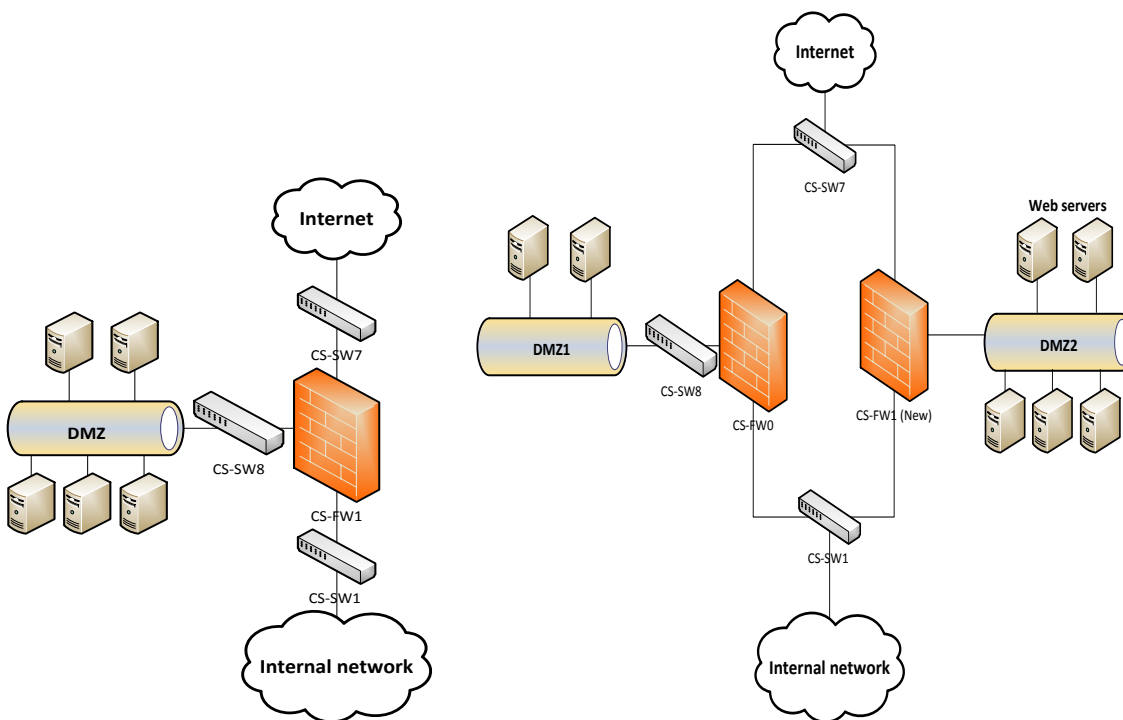
Μέχρι σήμερα χρησιμοποιείται η πιο πάνω τοπολογία των μηχανών στο δίκτυο του τμήματος. Για την προστασία της υποδομής του τμήματος και παρεμπόδιση των 'εισβολών' να διεισδύσουν στο εσωτερικό δίκτυο του τμήματος όλοι οι «ορατοί» (public) web servers του τμήματος θα τοποθετηθούν στην DMZ (περιλαμβανομένων και όλων των web pages/servers των ερευνητικών προγραμμάτων)

## Χρήση DMZ - Τι κερδίζουμε;

- Καλύτερη προστασία του δικτύου του Τμήματος, αφού οι public web servers δεν θα έχουν πρόσβαση προς το εσωτερικό δίκτυο
- Προστασία του internal δικτύου, αφού σε περίπτωση που ένας εξυπηρετητής γίνει compromise δεν κινδυνεύουν άλλα συστήματα.
- DoS attacks με στόχο κάποιο web server δεν μπορεί να έχει αντίκτυπο σε σύστημα που βρίσκεται στο εσωτερικό δίκτυο

## Firewall

Ακολουθεί η εικονική αναπαράσταση της τοπολογίας της DMZ χωρίς τη χρήση και με τη χρήση του νέου firewall που είναι ήδη σε λειτουργία.



Εικόνα 2: DMZ without or with the use of the new firewall.

## ΠΕΡΙΕΧΟΜΕΝΟ ΙΣΤΟΥ και ΥΠΗΡΕΣΙΕΣ

### Κατηγορίες περιεχομένου ιστού

Ακολουθεί πίνακας με τις κατηγορίες του περιεχομένου ιστού σύμφωνα με το πόσο critical θεωρείται το κάθε ένα, αλλά και με τη περίοδο που πρέπει να γίνονται Host.

Category 1 <b>Highest Availability</b>	Category 2 <b>High Availability</b>	Category 3 <b>Lower Availability</b>
<b>LONG TERM HOSTING</b>		<b>SHORT TERM HOSTING</b>
www site	Research Labs (ie. <a href="http://graphics.cs.ucy.ac.cy">http://graphics.cs.ucy.ac.cy</a> <a href="http://grid.ucy.ac.cy/">http://grid.ucy.ac.cy/</a> )	Student projects
Webmail	Courses (ie. <a href="http://www.cs.ucy.ac.cy/courses/EPL131/">http://www.cs.ucy.ac.cy/courses/EPL131/</a> )	Student thesis
	Conferences (ie. <a href="http://www.icsoc2011.cs.ucy.ac.cy">www.icsoc2011.cs.ucy.ac.cy</a> <a href="http://www.discotec07.cs.ucy.ac.cy/">http://www.discotec07.cs.ucy.ac.cy/</a> )	PhpMyAdmin
	Research projects (ie. <a href="http://www.cs.ucy.ac.cy/Projects/DYXTYS/">http://www.cs.ucy.ac.cy/Projects/DYXTYS/</a> <a href="http://www.cs.ucy.ac.cy/Projects/smartnet/">http://www.cs.ucy.ac.cy/Projects/smartnet/</a> )	
	Moodle	
	Mailing Lists	
	PhpMyAdmin	
	Public_html (~username) Personal pages	
	OTY pages (ie. <a href="http://its.cs.ucy.ac.cy/">http://its.cs.ucy.ac.cy/</a> <a href="http://helpdesk.cs.ucy.ac.cy/">http://helpdesk.cs.ucy.ac.cy/</a> <a href="http://www5.cs.ucy.ac.cy/OATS">http://www5.cs.ucy.ac.cy/OATS</a> )	

**Πίνακας 1: Κατηγοριοποίηση των υπηρεσιών**

Το περιεχόμενο έχει χωριστεί σε 3 κατηγορίες. Η πρώτη κατηγορία περιλαμβάνει τις critical εφαρμογές, οι οποίες πρέπει να είναι ζωντανές συνεχώς. Περιλαμβάνει τη σελίδα του τμήματος και το webmail.

Η δεύτερη κατηγορία περιλαμβάνει τις σελίδες της ΟΤΥ, τις προσωπικές σελίδες, τις σελίδες των συνεδρίων, των μαθημάτων και των ερευνητικών εργαστηρίων.

Η τρίτη κατηγορία περιλαμβάνει τις σελίδες που γίνονται develop από τους φοιτητές για σκοπούς εργασιών. Οι σελίδες αυτές πρέπει να είναι πιο ελεγχόμενες με πολύ μικρή διάρκεια ζωής.

## Υπηρεσίες

Ακολουθεί λίστα με τις υπηρεσίες που παρέχει κάθε εξυπηρετητής:

Εξυπηρετητής	Υπηρεσίες	Εφαρμογές
<b>www (evterpi)</b>	<ul style="list-style-type: none"> <li>• Apache</li> <li>• PHP</li> <li>• Tomcat</li> <li>• Squid</li> <li>• Sazeides SVN port 4213</li> </ul>	Πίνακας 3
<b>www5 (melpomene)</b>	<ul style="list-style-type: none"> <li>• Apache</li> <li>• PHP</li> <li>• Testing Mysql</li> </ul>	Πίνακας 3
<b>www6 (ariadne)</b>	<ul style="list-style-type: none"> <li>• Apache</li> <li>• PHP</li> <li>• Mailman</li> <li>• Postfix</li> </ul>	Πίνακας 3
<b>nemesis</b>	<ul style="list-style-type: none"> <li>• Apache</li> <li>• PHP</li> <li>• Mysql</li> </ul>	KnowledgeTree (ktdms.cs.ucy.ac.cy)
<b>museum</b>	<ul style="list-style-type: none"> <li>• Apache</li> <li>• PHP</li> <li>• Mysql</li> <li>• jdk</li> </ul>	Foodmuseum.cs.ucy.ac.cy
<b>www3 (poseidon)</b>	<ul style="list-style-type: none"> <li>• ISS 7.5 (ASP.NET 2.0 -4.0)</li> </ul>	Πίνακας 2

Πιο κάτω επισυνάπτεται λεπτομερείς πίνακας με όλες τις σελίδες που γίνονται host από τον IIS (poseidon) και τον Apache (evterpi, ariadne, melpomene).

IIS				
A/A	Website	Scope	Where	Info
1	<a href="http://www3.cs.ucy.ac.cy/socialwater/">http://www3.cs.ucy.ac.cy/socialwater/</a>	Student project	IN	Empty
2	<a href="http://www3.cs.ucy.ac.cy/armes/">http://www3.cs.ucy.ac.cy/armes/</a>	Student project	IN	Empty /έληξε
3	<a href="http://www3.cs.ucy.ac.cy/ecoactnow/">http://www3.cs.ucy.ac.cy/ecoactnow/</a>	Student project	IN	Empty/ έληξε
4	<a href="http://www3.cs.ucy.ac.cy/bankdata/">http://www3.cs.ucy.ac.cy/bankdata/</a>	Student project	IN	έληξε
5	<a href="http://www3.cs.ucy.ac.cy/csresearchprograms/Login.aspx">http://www3.cs.ucy.ac.cy/csresearchprograms/Login.aspx</a>	Student project	IN	έληξε
6	<a href="http://www3.cs.ucy.ac.cy/gymnasialikeia">http://www3.cs.ucy.ac.cy/gymnasialikeia</a>	Student project	IN	έληξε
7	<a href="http://philotimo.cs.ucy.ac.cy/">http://philotimo.cs.ucy.ac.cy/</a>	Student project	IN	έληξε
8	<a href="http://www3.cs.ucy.ac.cy/socialelectricitytest">http://www3.cs.ucy.ac.cy/socialelectricitytest</a>	Student project	IN	έληξε
9	<a href="http://www3.cs.ucy.ac.cy/task/">http://www3.cs.ucy.ac.cy/task/</a>	Student project	IN	έληξε
10	<a href="http://www3.cs.ucy.ac.cy/energycompetition/">http://www3.cs.ucy.ac.cy/energycompetition/</a>	Student project	IN	έληξε
11	<a href="http://www3.cs.ucy.ac.cy/adaptiveweb">http://www3.cs.ucy.ac.cy/adaptiveweb</a>	Research	DMZ	
12	<a href="http://www3.cs.ucy.ac.cy/adaptivewebmobile/">http://www3.cs.ucy.ac.cy/adaptivewebmobile/</a>	Research	DMZ	
13	<a href="http://www3.cs.ucy.ac.cy/adaptivewebplus/">http://www3.cs.ucy.ac.cy/adaptivewebplus/</a>	Research	DMZ	
14	<a href="http://www3.cs.ucy.ac.cy/adaptivewebsystem">http://www3.cs.ucy.ac.cy/adaptivewebsystem</a>	Research	DMZ	
15	<a href="http://cardiacm.cs.ucy.ac.cy/">http://cardiacm.cs.ucy.ac.cy/</a>	Research	DMZ	
16	<a href="http://www3.cs.ucy.ac.cy/ditis3/">http://www3.cs.ucy.ac.cy/ditis3/</a>	Research	DMZ	
17	<a href="http://www3.cs.ucy.ac.cy/ekpaideion/Site/index.html">http://www3.cs.ucy.ac.cy/ekpaideion/Site/index.html</a>	Research	DMZ	
18	<a href="http://www3.cs.ucy.ac.cy/ema/">http://www3.cs.ucy.ac.cy/ema/</a>	Research	DMZ	
19	<a href="http://www.eumas09.cs.ucy.ac.cy/index.html">http://www.eumas09.cs.ucy.ac.cy/index.html</a>	Conference	DMZ	
20	<a href="http://firewatch.cs.ucy.ac.cy/">http://firewatch.cs.ucy.ac.cy/</a>	Research	DMZ	
21	<a href="http://www.ict2011.cs.ucy.ac.cy/index.html">http://www.ict2011.cs.ucy.ac.cy/index.html</a>	Conference	DMZ	
22	<a href="http://www.melco.cs.ucy.ac.cy/">http://www.melco.cs.ucy.ac.cy/</a>	Research	DMZ	
23	<a href="http://mesarch.cs.ucy.ac.cy/">http://mesarch.cs.ucy.ac.cy/</a>	Research	DMZ	
24	<a href="http://www3.cs.ucy.ac.cy/pads/">http://www3.cs.ucy.ac.cy/pads/</a>	Student project	IN	
25	<a href="http://scrat.cs.ucy.ac.cy/">http://scrat.cs.ucy.ac.cy/</a>	Research	DMZ	
26	<a href="http://smartag.cs.ucy.ac.cy/">http://smartag.cs.ucy.ac.cy/</a>	Research	DMZ	
27	<a href="http://socialelectricity.cs.ucy.ac.cy/">http://socialelectricity.cs.ucy.ac.cy/</a>	Research	DMZ	
28	<a href="http://www3.cs.ucy.ac.cy/vpnfiles/">http://www3.cs.ucy.ac.cy/vpnfiles/</a>	OTY	DMZ	

Πίνακας 2: Εφαρμογές/σελίδες που εξυπηρετούνται από τον IIS



Apache				
A/A	Server	Website	Scope	Where
1	www	aiai2010	conference	DMZ
2	www	ayia-napa06	conference	DMZ
3	www	bibe2012	conference	DMZ
4	www	ccic12	conference	DMZ
5	www	CIT2011	conference	DMZ
6	www	cn2011	conference	DMZ
7	www	colloquium	conference	DMZ
8	www	cp2001	conference	DMZ
9	www	cse2012	conference	DMZ
10	www	cwspi2011	conference	DMZ
11	www	cwspi2012	conference	DMZ
12	www	dfmworkshop	conference	DMZ
13	www	disotec07	conference	DMZ
14	www	dmsn10	conference	DMZ
15	www	ecoop08	conference	DMZ
16	www	ecows10	conference	DMZ
17	www	ecsa2008	conference	DMZ
18	www	ecscw2013	conference	DMZ
19	www	ectel2013	conference	DMZ
20	www	egsr2006	conference	DMZ
21	www	eHealthForum	conference	DMZ
22	www	epy8	conference	DMZ
23	www	etaps10	conference	DMZ
24	www	euc2012	conference	DMZ
25	www	hdms2010	conference	DMZ
26	www	ica3pp08	conference	DMZ
27	www	iclp2001	conference	DMZ
28	www	icsoc2011	conference	DMZ
29	www	icwe2011	conference	DMZ
30	www	idc2009	conference	DMZ
31	www	isd2008	conference	DMZ
32	www	ISYC06	conference	DMZ
33	www	itab2009	conference	DMZ
34	www	mdm05	conference	DMZ
35	www	med98	conference	DMZ
36	www	medhocnet2012	conference	DMZ
37	www	melecon2000	conference	DMZ

38	www	mobide08	conference	DMZ
39	www	mobiwis2013	conference	DMZ
40	www	nc2010	conference	DMZ
41	www	pdp2011	conference	DMZ
42	www	profes2013	conference	DMZ
43	www	SAC2000	conference	DMZ
44	www	SCALCOM2011	conference	DMZ
45	www	sums	conference	DMZ
46	www	symp1	conference	DMZ
47	www	symposium	conference	DMZ
48	www	vsmm2008	conference	DMZ
49	www	wise2012	conference	DMZ
50	www	AnnualAssessment	assignment	Internal
51	www	foodATfingerprints	assignment	Internal
52	www	ResearchProjects	assignment	Internal
53	www	WebMinutes	assignment	Internal
54	www	archives	list archives	DMZ
55	www	archives_2007_03_08	list archives	DMZ
56	www	carch	Rlabs	DMZ
57	www	ecl	Rlabs	DMZ
58	www	graphics	Rlabs	DMZ
59	www	grid	Rlabs	DMZ
60	www	carch.old	Rlabs	DMZ
61	www	cin	Rlabs	DMZ
62	www	medinfo	Rlabs	DMZ
63	www	mrld	Rlabs	DMZ
64	www	netrl	Rlabs	DMZ
65	www	EPL001	courses	DMZ
66	www	EPL002	courses	DMZ
67	www	EPL003	courses	DMZ
68	www	EPL011	courses	DMZ
69	www	EPL012	courses	DMZ
70	www	EPL031	courses	DMZ

71	www	EPL032	courses	DMZ
72	www	EPL032-2	courses	DMZ
73	www	EPL033	courses	DMZ
74	www	EPL034	courses	DMZ
75	www	EPL035	courses	DMZ
76	www	EPL111	courses	DMZ
77	www	EPL131	courses	DMZ
78	www	EPL132	courses	DMZ
79	www	EPL202	courses	DMZ
80	www	EPL211	courses	DMZ
81	www	EPL221	courses	DMZ
82	www	EPL222	courses	DMZ
83	www	EPL231	courses	DMZ
84	www	EPL232	courses	DMZ
85	www	EPL233	courses	DMZ
86	www	EPL241	courses	DMZ
87	www	EPL324	courses	DMZ
88	www	EPL341	courses	DMZ
89	www	EPL342	courses	DMZ
90	www	EPL345	courses	DMZ
91	www	EPL361	courses	DMZ
92	www	EPL370	courses	DMZ
93	www	EPL371	courses	DMZ
94	www	EPL375	courses	DMZ
95	www	EPL420	courses	DMZ
96	www	EPL422	courses	DMZ
97	www	EPL425	courses	DMZ
98	www	EPL426	courses	DMZ
99	www	EPL428	courses	DMZ
100	www	EPL429	courses	DMZ
101	www	EPL433	courses	DMZ
102	www	EPL434	courses	DMZ
103	www	EPL435	courses	DMZ
104	www	EPL441	courses	DMZ
105	www	EPL442	courses	DMZ
106	www	EPL445	courses	DMZ
107	www	EPL446	courses	DMZ
108	www	EPL447	courses	DMZ
109	www	EPL450	courses	DMZ
110	www	EPL451	courses	DMZ

111	www	EPL470	courses	DMZ
112	www	EPL475	courses	DMZ
113	www	EPL476	courses	DMZ
114	www	EPL495	courses	DMZ
115	www	EPL496	courses	DMZ
116	www	EPL497	courses	DMZ
117	www	EPL498	courses	DMZ
118	www	EPL499	courses	DMZ
119	www	EPL602	courses	DMZ
120	www	EPL603	courses	DMZ
121	www	EPL604	courses	DMZ
122	www	EPL606	courses	DMZ
123	www	EPL625	courses	DMZ
124	www	EPL646	courses	DMZ
125	www	EPL651	courses	DMZ
126	www	EPL653	courses	DMZ
127	www	EPL656	courses	DMZ
128	www	EPL657	courses	DMZ
129	www	EPL658	courses	DMZ
130	www	EPL660	courses	DMZ
131	www	EPL662	courses	DMZ
132	www	EPL663	courses	DMZ
133	www	EPL671	courses	DMZ
134	www	EPL672	courses	DMZ
135	www	EPL674	courses	DMZ
136	www	EPL698	courses	DMZ
137	www	MscGames	courses	DMZ
138	www	acip	projects	DMZ
139	www	aeras	projects	DMZ
140	www	Athena	projects	DMZ
141	www	AthenaQTI	projects	DMZ
142	www	ci	projects	DMZ
143	www	ci.old	projects	DMZ
144	www	cjis	projects	DMZ
145	www	cjis.old	projects	DMZ
146	www	colognet	projects	DMZ
147	www	compulog	projects	DMZ
148	www	ConLoad	projects	DMZ
149	www	create	projects	DMZ

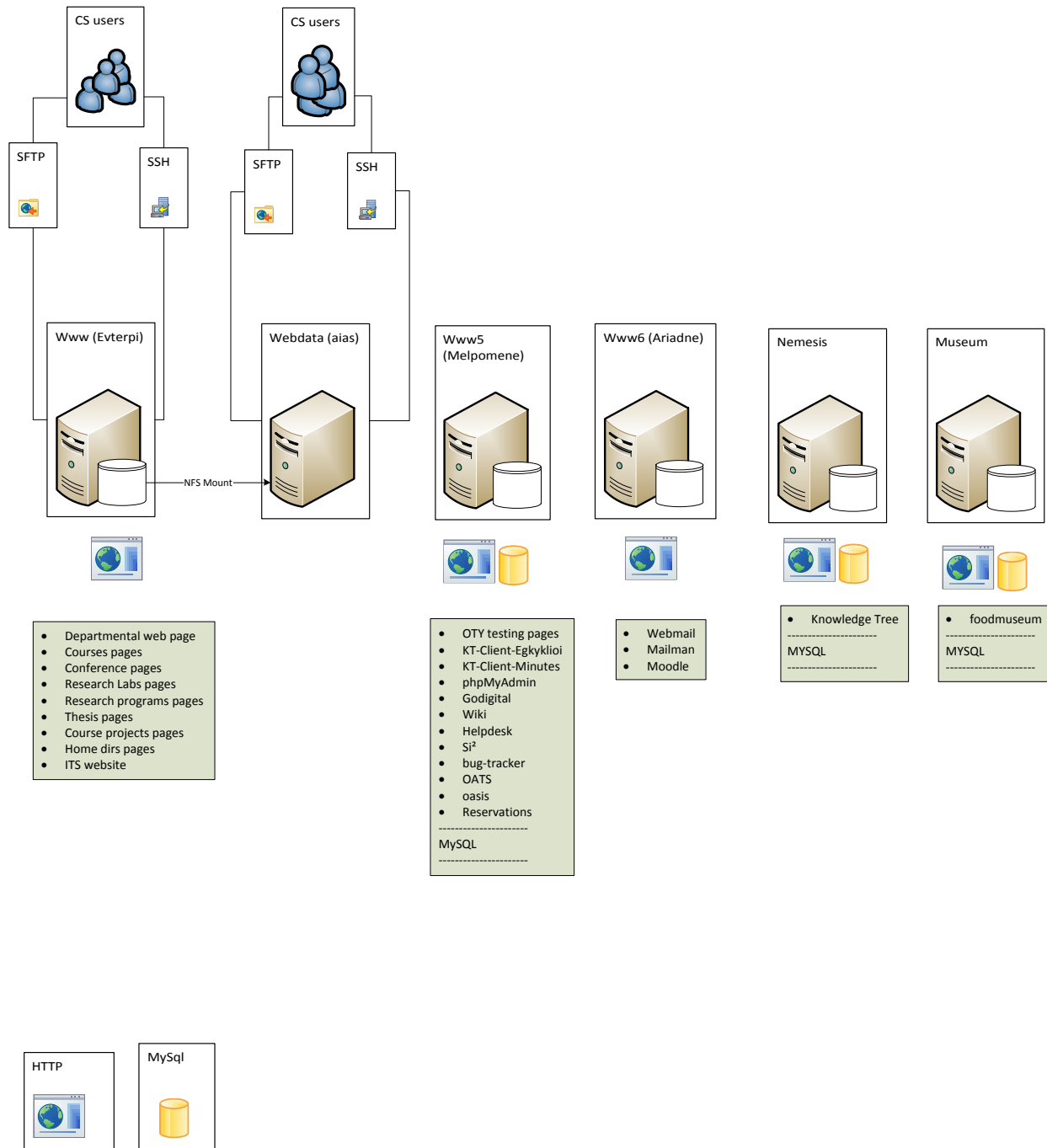
150	www	crossgrid	projects	DMZ
151	www	crowdcast	projects	DMZ
152	www	cs01ka	projects	DMZ
153	www	cyec	projects	DMZ
154	www	cyec_phase1	projects	DMZ
155	www	cyec_testing	projects	DMZ
156	www	cyec06	projects	DMZ
157	www	cyec07	projects	DMZ
158	www	cyehr	projects	DMZ
159	www	cygrid	projects	DMZ
160	www	cygrid-ca	projects	DMZ
161	www	dancedb	projects	DMZ
162	www	ddmgroup	projects	DMZ
163	www	DYXTYS	projects	DMZ
164	www	emispher	projects	DMZ
165	www	endiktis	projects	DMZ
166	www	eRACE	projects	DMZ
167	www	eris	projects	DMZ
168	www	eunomia	projects	DMZ
169	www	fastmwmr	projects	DMZ
170	www	fcmdss	projects	DMZ
171	www	folk	projects	DMZ
172	www	gorgias	projects	DMZ
173	www	healthnet	projects	DMZ
174	www	hpcl	projects	DMZ
175	www	icoper	projects	DMZ
176	www	ideal-ist	projects	DMZ
177	www	IntraMEDnet	projects	DMZ
178	www	intuition	projects	DMZ
179	www	isccsp	projects	DMZ
180	www	ist	projects	DMZ
181	www	locationaware internet	projects	DMZ
182	www	MarketMaker	projects	DMZ
183	www	melco	projects	DMZ
184	www	M-HealthBook	projects	DMZ
185	www	mi	projects	DMZ
186	www	mi.old	projects	DMZ
187	www	mind2c	Projects	DMZ

188	www	mrdl	projects	DMZ
189	www	museums	projects	DMZ
190	www	museumst	projects	DMZ
191	www	NetworksGroup	projects	DMZ
192	www	newcswweb	projects	DMZ
193	www	newCSwebsite	projects	DMZ
194	www	OFTL	projects	DMZ
195	www	pls4	projects	DMZ
196	www	PPproject	projects	DMZ
197	www	proodos	projects	DMZ
198	www	reading	projects	DMZ
199	www	Rehab	projects	DMZ
200	www	ric	projects	DMZ
201	www	safeweb	projects	DMZ
202	www	seiisrl	projects	DMZ
203	www	seit	projects	DMZ
204	www	SensorsGroup	projects	DMZ
205	www	sic	projects	DMZ
206	www	smartlab	projects	DMZ
207	www	smartLib	projects	DMZ
208	www	smartp2p	projects	DMZ
209	www	smarttrace	projects	DMZ
210	www	SMIL	projects	DMZ
211	www	tac	projects	DMZ
212	www	tonemap	projects	DMZ
213	www	Treasure	projects	DMZ
214	www	Treasure.old	projects	DMZ
215	www	video	projects	DMZ
216	www	webeng	projects	DMZ
217	www	widemednet	projects	DMZ
218	www	contextprivacy scenario	thesis	Internal
219	www	Digitalcy	thesis	Internal
220	www	isdegree	thesis	Internal
221	www	jobgames	thesis	Internal
222	www	MasterApplication	thesis	Internal

223	www	si2	thesis	Internal
224	www	smartscan	thesis	Internal
225	www	support	thesis	Internal
226	www	www	department website	DMZ
227	www	its	oty website	DMZ
228	melpomene	bug-tracker		Internal
229	melpomene	cswiki		?
230	melpomene	goDigital		DMZ
231	melpomene	KT-Client-Egkyklioι		DMZ
232	melpomene	KT-Client-Minutes		DMZ
233	melpomene	oasis		Internal
234	melpomene	OATS-1.0		DMZ
235	melpomene	phpHelpDesk		DMZ
236	melpomene	reservations		Internal
237	melpomene	rooms		Internal
238	melpomene	si2		Internal
239	melpomene	testing ...		Internal
240	melpomene	phpMyAdmin		Internal
241	ariadne	horde		DMZ
242	ariadne	moodle		DMZ
243	ariadne	listserver		DMZ

**Πίνακας 3: Εφαρμογές/σελίδες που εξυπηρετούνται από Apache server**

## Υπάρχουσα δομή



Εικόνα 3: Υπάρχουσα δομή υπηρεσιών ιστού

Πιο πάνω φαίνεται η υπάρχουσα δομή των υπηρεσιών που παρέχονται σήμερα στο τμήμα. Το μεγαλύτερο μέρος των εφαρμογών ιστού εξυπηρετούνται από τον εξυπηρετητή **evterpi** (**www**), όπου όλοι οι χρήστες του τμήματος έχουν απευθείας πρόσβαση με ssh και sftp. Επιπλέον τα WebData γίνονται share με NFS και στον εξυπηρετητή **aias** (**webdata**).

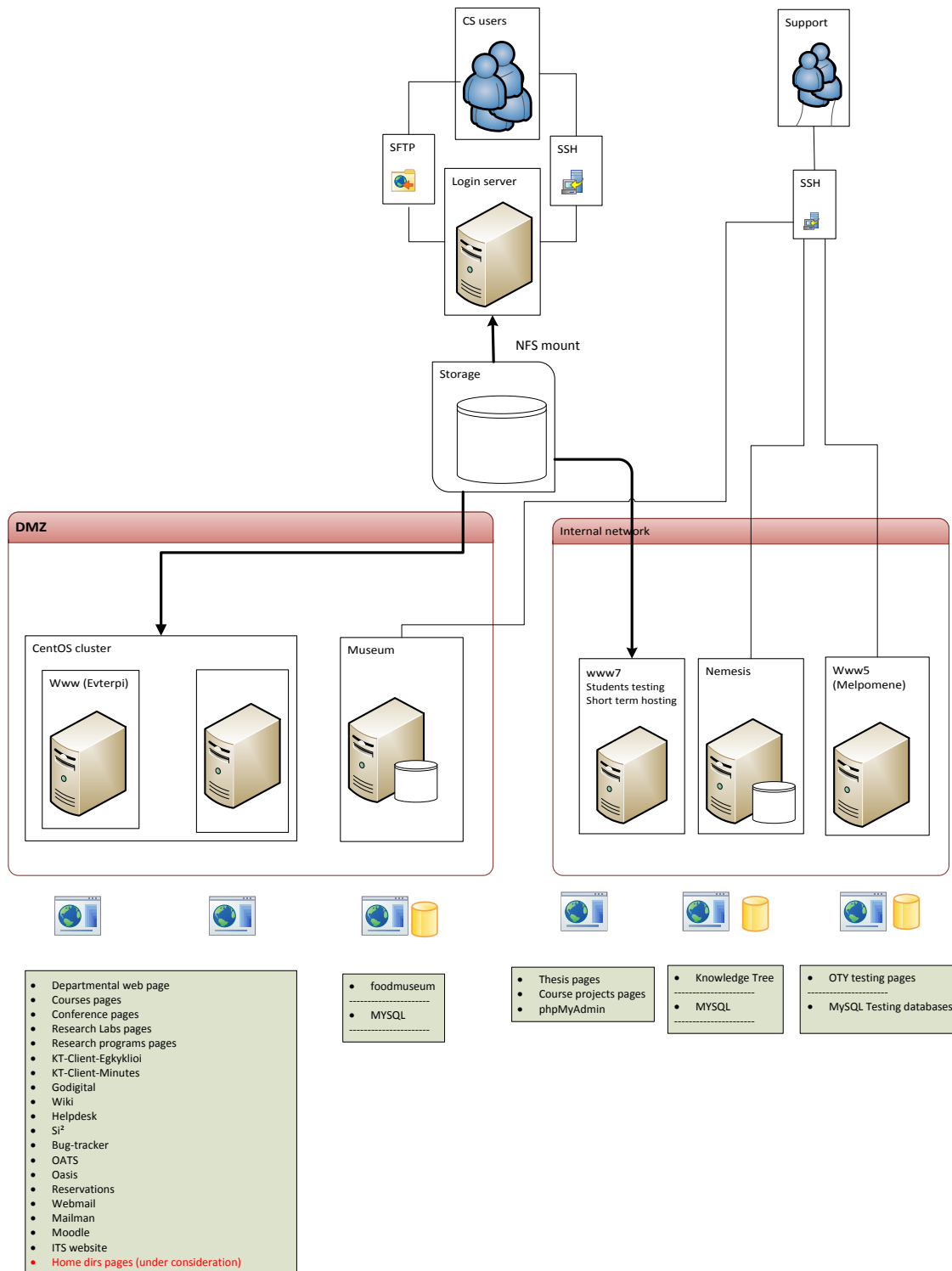
Η μηχανή **Ariadne** (**www6**), είναι περιορισμένης πρόσβασης και εξυπηρετεί 3 υπηρεσίες μεγάλου φόρτου, το webmail, moodle και mailman.

Η μηχανή **melpomene** (**www5**) εξυπηρετεί τις ιστοσελίδες της ΟΤΥ, το PhpMyAdmin, καθώς και όλες τις testing σελίδες της ΟΤΥ. Το πιο πάνω αποτέλεσε πρόβλημα στο παρελθόν, αφού λόγω του ότι είναι production και testing εξυπηρετητής μαζί, περιορίζει την χρήση των δυνατοτήτων του ως εξυπηρετητής δοκιμών, αφού δεν μας δίνεται η δυνατότητα αλλαγών.

Τέλος οι εξυπηρετητές **nemesis** και **museum** είναι εξυπηρετητές dedicated σε συγκεκριμένη δουλειά, ο πρώτος στο KnowledgeTree και ο δεύτερος στο foodmuseum application (Γ. Χρυσάνθου)

# ΑΝΑΔΙΑΡΘΡΩΣΗ

## Προτεινόμενη δομή



Εικόνα 4: Προτεινόμενη δομή των υπηρεσιών

Πιο πάνω φαίνεται η προτεινόμενη δομή των υπηρεσιών ιστού, σύμφωνα με τον σκοπό του έργου που αναφέρθηκε στην εισαγωγή.

## Γενική περιγραφή/στόχοι έργου

Πιο κάτω ακολουθούν οι στόχοι του έργου με μια μικρή περιγραφή.

1. Μεταφορά των μηχανών σε εικονικές μηχανές (virtualization) καθότι αυτό θα προσφέρει ευελιξία στην αναβάθμιση και διαχείριση των συστημάτων.
2. Προτείνεται η δημιουργία ενός CentOS cluster με τη χρήση του πακέτου heartbeat (virtual IP) και δύο μηχανών. Αυτό θα εξασφαλίσει για το μεγαλύτερο μέρος των υπηρεσιών ιστού του τμήματος high availability και better performance.
3. Θα γίνει διαχωρισμός των less secure και short term hosting εφαρμογών των φοιτητών από τις εφαρμογές του τμήματος.
4. Για την υλοποίηση του πιο πάνω θα προστεθεί ένας νέος εξυπηρετητής (**www7**) για την εξυπηρέτηση των φοιτητών σε εργασίες και διπλωματικές. Ο εξυπηρετητής αυτός θα τοποθετηθεί σε κλειστό δίκτυο και θα είναι προσβάσιμος με VPN. [Ίσως καλό να ήταν στη συγκεκριμένη μηχανή να τρέχει το MySQL για την εξυπηρέτηση μόνο των φοιτητών, ούτως ώστε να περιοριστεί η πρόσβαση στον dbserver (MySQL) από τους φοιτητές. (Σάββας)]
5. Η πρόσβαση των χρηστών απευθείας στους εξυπηρετητές δεν θα επιτρέπεται, και θα χρησιμοποιηθεί ένας login server (Μαρία), ο οποίος θα κάνει mount τα webdata των εξυπηρετητών. Η αλλαγή του περιεχομένου θα γίνεται μέσω του Login server.
6. Θα γίνει διαχωρισμός του production με το testing περιβάλλον εργασίας της ΟΤΥ, διατηρώντας την μηχανή www5 ως καθαρά testing περιβάλλον.
7. Στο επόμενο στάδιο αναδιάρθρωσης των υπηρεσιών ιστού θα μελετηθεί η αυτοματοποίηση και η αυτοεξυπηρέτηση των φοιτητών, σε συνάρτηση με τον εξυπηρετητή αυτό, αλλά έχει διαχωριστεί από το Project αυτό. Θα μελετηθεί η χρήση κάποιου πακέτου από τα: Webmin, CPANEL και Plesk Panel.



## Φάσεις έργου

Για την ολοκλήρωση του έργου απαιτούνται οι πιο κάτω εργασίες:

### Φάση 1<sup>η</sup>:

Ετοιμασία της μηχανής που θα τρέχει τους virtual servers. Μεταφορά του Knowledge Tree σε virtual περιβάλλον (έχει ήδη γίνει)

### Φάση 2<sup>η</sup>:

Μεταφορά της μηχανής Melromene σε virtual περιβάλλον σε εσωτερικό κλειστό δίκτυο διαθέσιμο μόνο από το 10.16.16.χ (OTY Network)

### Φάση 3<sup>η</sup>:

Ετοιμασία του cluster με χρήση δύο εικονικών μηχανών. Έλεγχος και διαμόρφωση των εξυπηρετητών, μεταφορά στην DMZ και σταδιακή μεταφορά των εφαρμογών.

### Φάση 4<sup>η</sup>:

Ετοιμασία και εγκατάσταση της νέας εικονικής μηχανής **www7 για την εξυπηρέτηση των φοιτητών**. Μεταφορά σε εσωτερικό κλειστό δίκτυο, ασφαλής διαμόρφωση του εξυπηρετητή και μεταφορά των εφαρμογών των φοιτητών.

### Φάση 5<sup>η</sup>:

Μεταφορά των εφαρμογών από τον www5 (production) , ούτως ώστε να σερβίρονται από το cluster και μεταφορά των υπηρεσιών του εξυπηρετητή ariadne στο cluster.

Τέλος αναφέρεται ότι η μεταφορά του Museum στη DMZ μπορεί να γίνει ανεξάρτητα από τα πιο πάνω.

Σημειώνεται ότι στο παρόν στάδιο το nfs mount μπορεί να γίνεται στον aias μέχρι την ετοιμασία του login server

## Νέες πρακτικές

Για να διασφαλιστούν οι στόχοι που θέσαμε στην αρχή, δηλαδή η ασφάλεια των εξυπηρετητών αλλά και της υποδομής του τμήματος θα πρέπει να αλλάξει εντελώς ο τρόπος με τον οποίο ήταν διαμορφωμένοι οι εξυπηρετητές μέχρι τώρα, αλλά και ολόκληρη η οργάνωσή τους στο δίκτυο.

Σε γενικές γραμμές θα πρέπει:

1. Οι εφαρμογές που πρέπει να είναι προσβάσιμες από έξω, πρέπει πάντα να τοποθετούνται πάντα μέσα στη DMZ.
2. Ο server που εξυπηρετεί τις εργασίες των φοιτητών ΔΕΝ πρέπει να είναι προσβάσιμος από έξω, άρα θα τοποθετείται σε εσωτερικό κλειστό δίκτυο.
3. Θα απαγορεύεται η απευθείας πρόσβαση στους webserver από τα μέλη του τμήματος, αλλά θα χρησιμοποιείται ενός login server, για την ανανέωση και αλλαγή των σελίδων.
4. Οι webserver δεν θα πρέπει να τρέχουν άσχετα services (πχ SVN)
5. Θα μελετηθεί ολοκληρωτικά από την αρχή η εγκατάσταση και διαμόρφωση των υπηρεσιών, ούτως ώστε να διασφαλιστεί η ασφάλεια των δεδομένων των εξυπηρετητών αλλά και του εσωτερικού δικτύου.

## Χρήση υλικού

Μετά την ολοκλήρωση του πιο πάνω έργου προτείνεται όπως η μηχανή cs910 (Melromene) γίνει retire, ενώ θα περισσέψουν 3 physical μηχανές τις οποίες μπορούμε να επανάχρησιμοποιήσουμε σε άλλες υπηρεσίες (cs5386 IBM x3455, cs5387 IBM x3455, cs5389 IBM x3455 )

## Μελλοντική εργασία

Θα μελετηθεί η διαμόρφωση των webservers, ούτως ώστε να γίνουν όσο το δυνατόν ασφαλέστεροι για το περιβάλλον μας. Θα μελετηθούν τα πιο κάτω:

- apache mod\_security (application firewall)
- apache mod\_suphp & mod\_suexec (allow php scripts to run under a predefined user)
- apache mod\_httpbl (block IP with proven malicious activity)
- run Apache in a chroot jail
- mpm-itk (or other Multi Processing Module)
- run different virtual hosts under different userids using a reverse proxy
- change how public\_html pages are treated
- Joomla multisites control
- Joomla sh404

---

### Under consideration

- Τα Home directories θα σερβίρουν σελίδες από το cluster ?? Φοιτητές;
- Τα data του εξυπηρετητή www7 θα γίνονται export στον login server?
- Κάποιες σελίδες που γίνονται develop από φοιτητές και μένουν στάσιμες για πολλά χρόνια ίσως δεν είναι καλή τακτική να τοποθετηθούν στο cluster? (πχ conferences, projects)