ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

Υπολογιστικό Κέντρο
Σχολή Θετικών & Τεχνολογικών Επιστημών

ΤΑΧΥΔΡ. ΘΥΡ. 2208, 71003 ΗΡΑΚΛΕΙΟ, ΚΡΗΤΗ Τηλ: +30-2810-394155/3352 Fax: +30-2810-394171 e-mail: info@cc.uoc.gr

26/09/2012

Προτάσεις υλοποίησης Κεντρικών Υπηρεσιών του Π.Κ.

Μέσα στα πλαίσια των δραστηριοτήτων της, η Ομάδα Συστημάτων & Δικτύων / Μηχανογράφηση Γραμματειών του ΕΕΔ (Εργαστήριο Επεξεργασίας Δεδομένων) παρέχει υπηρεσίες στα τμήματα Βιολογία, Ιατρική, ΕΤΥ και Φυσικό.

Σε μία προσπάθεια συνδυασμού αφενός μεν της απρόσκοπτης παροχής των υπηρεσιών που ήδη προσφέρονται στα παραπάνω τμήματα και αφετέρου της εύλογης επιθυμίας της διοίκησης για την υλοποίηση κεντρικά παρεχόμενων υπηρεσιών προς όλο το Ίδρυμα, θα θέλαμε να προτείνουμε την υλοποίηση και διαχείριση των ακόλουθων κεντρικά παρεχόμενων υπηρεσιών. Οι προτεινόμενες προς υλοποίηση Κεντρικές Υπηρεσίες θα είναι βασισμένες κύρια σε Open Source λογισμικό:

1. Κεντρική Υπηρεσία Single Sign-On (SSO)

Προτείνεται η ανάληψη υλοποίησης και διαχείρισης Κεντρικής Υπηρεσίας Single Sign-On (SSO). Πρόκειται για μια σύγχρονη Κεντρική Υπηρεσία με αρκετά οφέλη για το Ίδρυμα.

Οι χρήστες κατά την απόπειρα τους να πιστοποιηθούν σε Web υπηρεσίες, οι οποίες είναι διασυνδεδεμένες με την Υπηρεσία SSO, ανακατευθύνονται αυτόματα σε μια μοναδική σελίδα πιστοποίησης. Εκεί εισαγάγουν για μια μόνο φορά τα προσωπικά στοιχεία του Ιδρυματικού τους λογαριασμού (LDAP username/password) και στην συνέχεια αποκτούν αυτόματα πρόσβαση σε όλες τις υποστηριζόμενες υπηρεσίες χωρίς να χρειαστεί να πιστοποιηθούν ξανά.

Οφέλη για το Ίδρυμα:

1. Δωρεάν υλοποίηση βασισμένη σε Open Source λογισμικό
2. Ασφάλεια χρηστών γιατί τα στοιχεία τους εισάγονται σε μία μόνο υπηρεσία και όχι σε κάθε υπηρεσία που απαιτεί πιστοποίηση. Αυτό βοηθά και στην αντιμετώπιση επιθέσεων τύπου fishing γιατί οι χρήστες μαθαίνουν ότι βάζουν τα στοιχεία τους μόνο σε αυτήν τη σελίδα
3. Ευκολία για τους χρήστες γιατί δεν χρειάζεται να βάζουν τα στοιχεία τους πολλές φορές

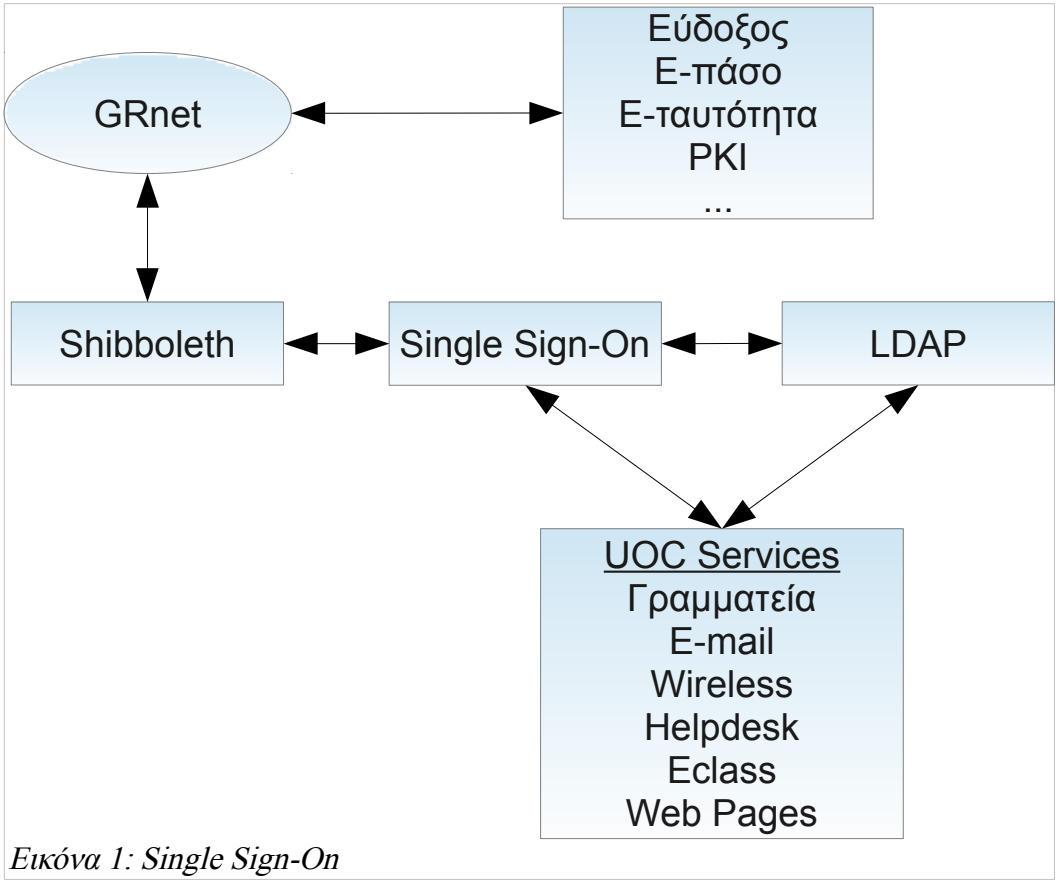
Η υλοποίηση της μπορεί να γίνει άμεσα μιας και υπάρχει η κατάλληλη τεχνογνωσία από την εφαρμογή της στο ΤΕΙ Κρήτης. Έγινε από προσωπικό της Ομάδας μας και λειτουργεί εδώ και τρία χρόνια με απόλυτη επιτυχία.

Η υπηρεσία θα λειτουργεί με Open Source λογισμικό σε περιβάλλον High Availability στο Datacenter και μπορούν άμεσα να διασυνδεθούν οι παρακάτω υπηρεσίες οι οποίες υποστηρίζουν SSO:

1. Πιστοποίηση σε υπηρεσίες Shibboleth Ε.Δ.Ε.Τ.
    - Εύδοξος
    - Ηλεκτρονικό Πάσο
    - Ακαδημαϊκή Ταυτότητα
    - Υπηρεσία Έκδοσης Προσωπικών Ψηφιακών Πιστοποιητικών (PKI)
    - MSDNAA
    - Pithos
    - IPTV
    - DreamSpark
    - RTS
    - Scopus
    - Forrester
    - myNetLab
2. Πιστοποίηση σε Web υπηρεσίες Γραμματείας
    - StudentsWeb
    - ClassWeb
3. Πιστοποίηση σε κεντρικό WebMail χρηστών που υποστηρίζει SSO

4. Πιστοποίηση σε ασύρματα δίκτυα
5. Πιστοποίηση σε σελίδες μαθημάτων (eClass, Moodle κτλ)
6. Πιστοποίηση σε κεντρικό HelpDesk εξυπηρέτησης χρηστών
7. Πιστοποίηση σε κεντρικές Mailing Lists
8. Πιστοποίηση σε άλλες Web σελίδες (πχ. ανακοινώσεις, Blogs, Forums κτλ.)

Η υλοποίηση αυτή μπορεί να βοηθήσει στην επιτάχυνση δημιουργίας ενός Portal χρηστών τύπου **my.uoc.gr** όπου οι χρήστες από εκεί θα έχουν πρόσβαση σε όλες τις προσφερόμενες προς αυτούς υπηρεσίες. Στην εικόνα 1 βλέπετε την προτεινόμενη υλοποίηση.



Εικόνα 1: Single Sign-On

2. Active Directory

Πολλά τμήματα και επιμέρους υπηρεσίες του Ιδρύματος διατηρούν υποδομή Windows Active Directory για τις εκπαιδευτικές και διαχειριστικές τους δραστηριότητες. (ΕΛΚΕ?). Εξάλλου, διατηρούνται επιμέρους εγκαταστάσεις λειτουργικού συστήματος Microsoft Windows που δεν είναι διασυνδεδεμένες με καμία κεντρική υποδομή ταυτοποίησης και διαχείρισης.

Η ανάγκη διατήρησης εμπορικών λειτουργικών συστημάτων έχει καταγραφεί για τη χρήση

συγκεκριμένου λογισμικού τόσο για εκπαιδευτικές όσο και διοικητικές ανάγκες, όταν η πλήρης μετάβαση σε λογισμικό ανοιχτού κώδικα δεν είναι εφικτή. Επίσης, τοπικοί διαχειριστές αξιοποιούν το Active Directory για διαχείριση κοινόχρηστων αρχείων και εκτυπωτών, αλλά και για κεντρική επίβλεψη ενημερώσεων και προσθαφαίρεση λογισμικού σε σταθμούς εργασίας.

Προτείνουμε την υλοποίηση και διαχείριση κεντρικής υποδομής Active Directory κατ΄αντιστοιχία με άλλες κεντρικές υπολογιστικές υπηρεσίες, που θα παρέχει τη δυνατότητα συγκέντρωσης όλων των υπαρχουσών δομών. Αυτές συμπεριλαμβάνουν όλους τους

επιμέρους τομείς (domains), αλλά και επιλεγμένους υπολογιστές που δεν ανήκουν ήδη σε κεντρικές διαχειριστικές δομές.

Με αυτόν τον τρόπο θα ενσωματωθεί στο κεντρικό σχήμα διαχείρισης οι δυνατότητα πιστοποίησης Kerberos, ενώ τα δεδομένα χρηστών θα συγχρονιστούν αυτόματα με την Κεντρική Υπηρεσία Καταλόγου. Η ύπαρξη και υψηλή διαθεσιμότητα της κεντρικής υποδομής σημαίνει ότι τοπικοί διαχειριστές μπορούν να επιλέξουν να μην διατηρούν επιπλέον εξυπηρετητές, χωρίς απώλεια λειτουργικότητας.

Αυτό επιτυγχάνεται με τη δημιουργία υποτομέων (subdomains) σε ένα δάσος (forest), στους οποίους θα εκχωρηθούν πλήρη διαχειριστικά δικαιώματα στους τοπικούς διαχειριστές. Εναλλακτικά, υπάρχει η δυνατότητα δημιουργίας και εκχώρησης απλών διαχειριστικών ομάδων (organizational units), ή συνδυασμός των παραπάνω.

Ταυτόχρονα με τη διαχειριστική ανεξαρτησία της, η προτεινόμενη υποδομή επιτρέπει την εξασφάλιση κεντρικα διαχειριζόμενου σχήματος, δεδομένων χρηστών και πολιτικών χρήσης (όπως καθορίζονται από AD Group Policy).

Άμεσα οφέλη της πρότασης είναι:

- ο περιορισμός του αριθμού εξυπηρετητών Active Directory που διατηρούνται στο Ίδρυμα
- η εξάλειψη του αντίστοιχου διαχειριστικού κόστους
- η ενοποίηση διαχείρισης χρηστών με την Κεντρική Υπηρεσία Καταλόγου θα ελαττώσει τόσο το φόρτο διαχείρισης, όσο και την πολυπλοκότητα για χρήστες και διαχειριστές τοπικών υπηρεσιών.

Η παρούσα πρόταση θα έχει άμεσα οφέλη και στην ασφάλεια δεδομένων, καθώς η κεντρική διαχείριση θα εξασφαλίζει ότι όλοι οι συμμετέχοντες υπολογιστές τηρούν τις προδιαγραφές ασφαλείας και είναι έγκαιρα ενημερωμένοι με τις τελευταίες διορθώσεις λογισμικού (patches). Το σχήμα που προτείνεται διευκολύνει εξάλλου την κεντρική διαχείριση κοινόχρηστου λογισμικού – ενδεικτικά για προστασία από κακόβουλο λογισμικό (antivirus) ή εκπαιδευτικό λογισμικό για το οποίο απαιτούνται μαζικές εγκαταστάσεις.

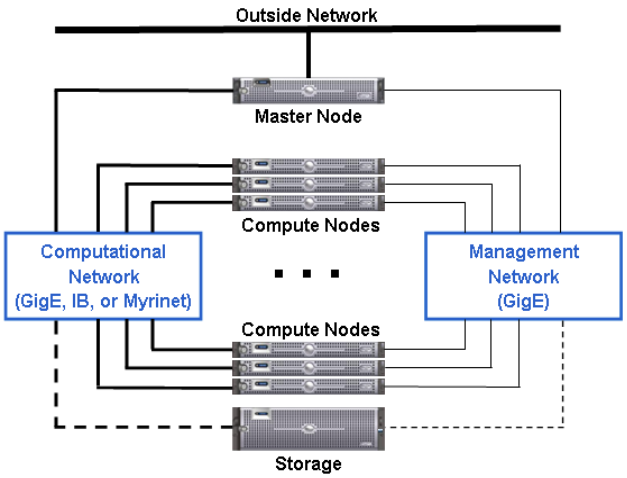
Τέλος, η πρότασή μας μπορεί να συνδυαστεί μελλοντικά χωρίς τροποποίηση με τη δυνατότητα υποστήριξης εικονικής επιφάνειας εργασίας (Virtual Desktop Infrastructure-VDI).

3. Κεντρική Υπηρεσία HPC

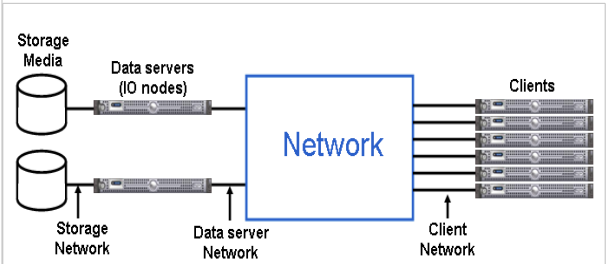
Προτείνουμε το σχεδιασμό και την υλοποίηση σε μεγάλη κλίμακα HPC υποδομής, βασιζόμενοι στην αντίστοιχη υλοποίηση των τμημάτων Επιστήμης & Τεχνολογίας Υλικών και Φυσικής, η οποία λειτουργεί παραγωγικά από το 2005 και έχει γίνει στα πρότυπα αντίστοιχων HPC υποδομών των Lawrence Berkeley National Laboratory (LBL http://scs.lbl.gov/html/Lawrencium.html), Niflheim cluster του NORDGRID (https://wiki.fysik.dtu.dk/niflheim) και Princeton University High Performance Computing Systems (http://www.princeton.edu/researchcomputing).

Αρχιτεκτονική της υπηρεσίας

Η συγκεκριμένη αρχιτεκτονική βασίζεται στην ύπαρξη ενός ή περισσότερων (redundant) *master node* που αναλαμβάνει τη διαχείριση των *compute nodes* και τη δρομολόγηση/ροή εργασιών σε μορφή *batch jobs* (Εικόνα 2). Η δομή συμπληρώνεται με το *storage* (Εικόνα 3) το οποίο μπορεί να είναι οποιαδήποτε μορφής από συστοιχία *NFS ή AFS servers* ή *cloud storage.*



Εικόνα 2: HPC Architecture



Εικόνα 3: HPC Storage

Η υπηρεσία θα παρέχει τη δυνατότητα στους χρήστες του Ιδρύματος να εκτελούν εργασίες με τη μορφή *batch jobs* οι οποίες θα δρομολογούνται μέσω ενός συστήματος ουρών (*queueing system*). Η δρομολόγηση θα γίνεται με κριτήρια, μερικά από τα οποία είναι και τα ακόλουθα:

- Modular περιβάλλον εργασίας ανάλογα με το λογισμικό που απαιτείται ανά χρήστη ή ομάδα χρηστών, πλήρως παραμετροποιήσιμο

- Προτεραιότητες εργασιών ανά χρήστη ή ομάδα χρηστών
- Επίπεδα πρόσβασης σε *compute nodes* και θέσπιση ορίων στη χρήση υπολογιστικών πόρων
- Profiling εργασιών ανάλογα με το μέγεθος και τις απαιτήσεις τους σε CPU time ή μνήμη
- Διαθεσιμότητα nodes
- Αρχιτεκτονική nodes
- Ερευνητικό ή διδακτικό έργο
- Load balancing / QOS

Η υλοποίηση θα περιλαμβάνει επιπλέον ένα *portal* χρηστών με την περιγραφή της υπηρεσίας και δυνατότητες ενεργοποίησης πρόσβασης και διαμόρφωσης του περιβάλλοντος εργασίας τους με την ενεργοποίηση / απενεργοποίηση των αντίστοιχων modules (πχ MPI module, MPICH2 module, MATLAB module, Compilers module κλπ) όπως επίσης *job profiling* και *job monitoring*. Επιπλέον, θα υπάρξει διασύνδεση με το κεντρικό HelpDesk προκειμένου να διευθετούνται άμεσα τα αιτήματα των χρηστών και τέλος η υποδομή θα συμπληρωθεί από διαδραστικά εργαλεία παρακολούθησης, αποτύπωσης λειτουργίας και καταγραφής ιστορικών δεδομένων του cluster.

Λογισμικό

Υπάρχει πληθώρα OpenSource λογισμικού που είναι διαθέσιμο για την υλοποίηση της υποδομής, τόσο για την υλοποίηση του queuing system όσο και για την διαχείρισή της. **Δεν απαιτείται σε καμία περίπτωση η αγορά λογισμικού για την δημιουργία και διάθεση της υπηρεσίας**.

Επίσης, μπορεί να εγκατασταθεί και να παραμετροποιηθεί μέσω του portal χρηστών από τους ίδιους τους χρήστες όλο το OpenSource επιστημονικό λογισμικό που θα είναι εγκατεστημένο.

Ωστόσο, εάν απαιτείται από μερίδα χρηστών η χρήση εμπορικού λογισμικού τότε θα παρέχεται η δυνατότητα σε αυτούς να εγκαταστήσουν, είτε μόνοι τους είτε με την συμβολή του προσωπικού του Εργαστηρίου, το λογισμικό που απαιτείται και κατόπιν μέσω του υποσυστήματος profiling και αδειοδότησης της HPC υποδομής να είναι διαθέσιμο σε αυτούς αποκλειστικά ή σε άτομα της επιλογής τους.

4. Κεντρική Υπηρεσία E-mail

Προτείνεται η ανάληψη υλοποίησης και διαχείρισης Κεντρικής Υπηρεσίας E-mail. Η υπηρεσία θα αφορά σε όλους τους χρήστες του Πανεπιστημίου Κρήτης (προπτυχιακούς φοιτητές, μεταπτυχιακούς φοιτητές, διδακτικό προσωπικό και διοικητικό προσωπικό).

Λόγω της μέχρι τώρα κατανομής του Π.Κ. σε τρεις παν/πόλεις (Κνωσός, Βούτες και Ρέθυμνο) και συχνά λόγω έλλειψης και του απαραίτητου προσωπικού, παρουσιάζεται διαφορετική ποιότητα παροχής υπηρεσίας στα διάφορα τμήματα και υπηρεσίες του Ιδρύματος. Προτείνουμε την ενοποίηση όλων των E-mail Υπηρεσιών σε μία, με ενιαία μορφή και υψηλής ποιότητας υπηρεσία και για όλους.

Η ομάδα μας έχει την αρτιότερη και πλέον μακρόχρονη τεχνογνωσία στην παροχή τέτοιου είδους υπηρεσία σε μεγάλη κλίμακα (~5500 χρήστες - Τμήματα Βιολογία, Ιατρική, ΕΤΥ, Φυσικό).

Η Κεντρική Υπηρεσία θα λειτουργεί με Open Source λογισμικό σε περιβάλλον High Availability στο Datacenter και θα περιλαμβάνει:

- Κεντρικό WebMail (ανάγνωση ηλεκτρονικής αλληλογραφίας από το Web)
- Κεντρική Υπηρεσία SMTP (παραλαβή και αποστολή ηλεκτρονικής αλληλογραφίας)
- Κεντρική Υπηρεσία IMAP/POP3 (ανάγνωση ηλεκτρονικής αλληλογραφίας από προσωπικούς υπολογιστές)
- Κεντρική Υπηρεσία AntiSpam (έλεγχος μη επιθυμητών μηνυμάτων ηλεκτρονικής αλληλογραφίας)
- Κεντρική Υπηρεσία AntiVirus (έλεγχος κακόβουλων μηνυμάτων ηλεκτρονικής αλληλογραφίας)
- Κεντρική Υπηρεσία Mailing Lists (λίστες ηλεκτρονικής αλληλογραφίας)

5. Κεντρική Υπηρεσία Firewall

Η ομάδα μας προτείνει να αναλάβει την υλοποίηση και την διαχείριση Κεντρικής Υπηρεσίας Firewall (Statefull, High Available). Η υπηρεσία θα αφορά σε όλο το δίκτυο και τις δικτυακές συσκευές του Πανεπιστημίου Κρήτης. Η υλοποίηση θα είναι βασισμένη σε Open Source

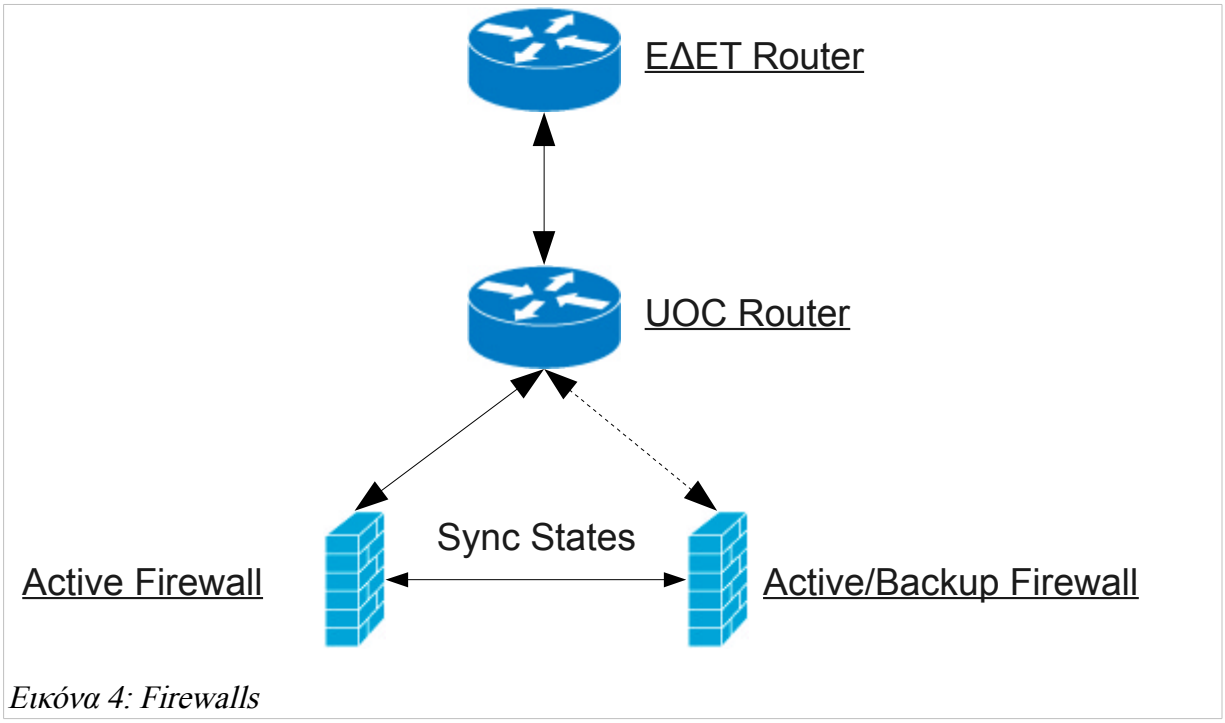
λογισμικό και θα λειτουργεί σε περιβάλλον High Availability.

Εδώ και ένα χρόνο η ομάδα μας λειτουργεί Υπηρεσία Firewall για τα τμήματα Φυσικής, Βιολογία και ΕΤΥ. Τα τμήματα αυτά διακινούν τον μισό όγκο δεδομένων από το σύνολο του Π.Κ. οπότε κάλλιστα η υποδομή μπορεί να υλοποιηθεί και στο σημείο διασύνδεσης με το Ε.Δ.Ε.Τ. κάτι που μέχρι τώρα δεν έχει εφαρμοστεί.

Με την Υπηρεσία Firewall το Π.Κ. θα έχει τα εξής οφέλη:

- Ασφάλεια και προστασία Κεντρικών Εξυπηρετητών (servers)
- Ασφάλεια και προστασία προσωπικών υπολογιστών
- Κεντρική εφαρμογή πολιτικής Ασφαλείας του ιδρύματος
- Οικονομία και απεμπλοκή από άδειες χρήσης και υλικό αντίστοιχων εταιρικών προϊόντων (π.χ. Cisco)
- Statefull Firewalling: Οι Access Lists (ACLs) που εφαρμόζονται τώρα παρακάμπτονται αρκετά εύκολα

Στην Εικόνα 4 φαίνεται η προτεινόμενη υλοποίηση. Εναλλακτικά τα Firewalls μπορούν να συνδεθούν απευθείας με το ΕΔΕΤ ώστε να παρέχεται προστασία και στον κεντρικό δρομολογητή του Π.Κ.



Εικόνα 4: Firewalls

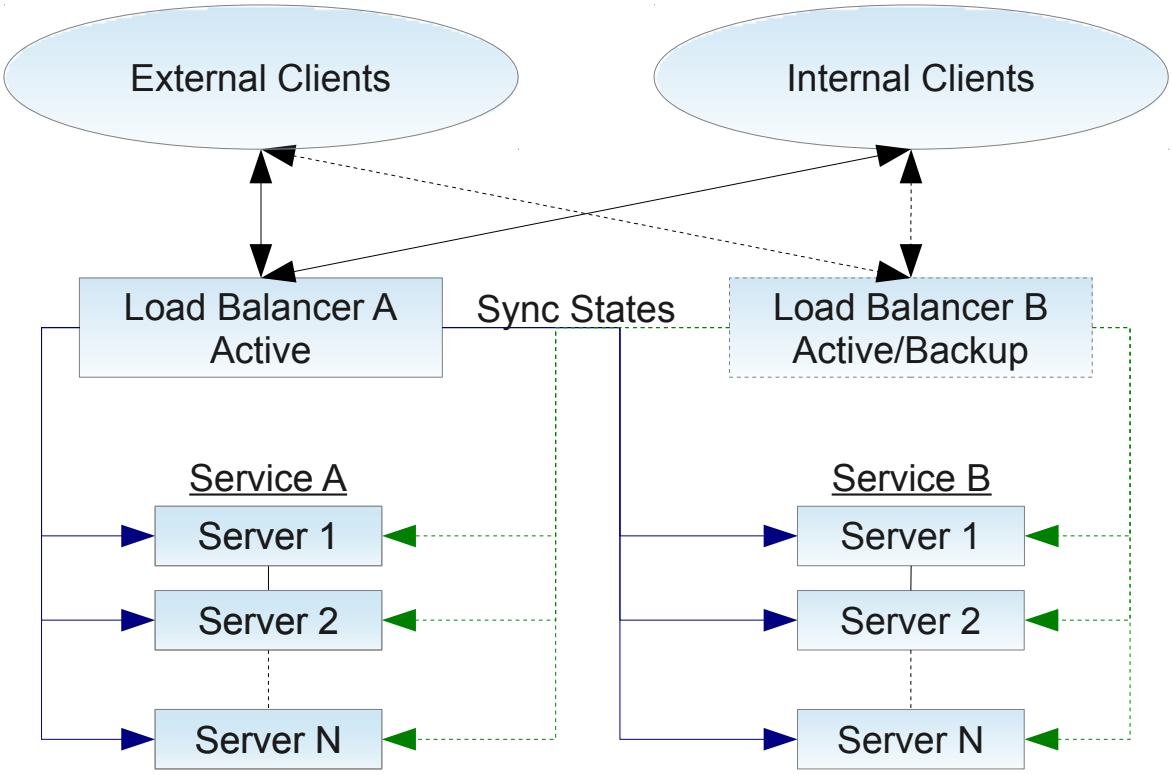
6. Κεντρική Υπηρεσία Load Balancing

Προτείνεται η ανάληψη υλοποίησης και διαχείρισης Κεντρικής Υπηρεσίας Load Balancing με σκοπό την επίτευξη High Availability σε αρκετές δικτυακές υπηρεσίες όπως Web, E-mail, DNS κτλ. Η υλοποίηση θα είναι βασισμένη σε Open Source λογισμικό και θα λειτουργεί σε περιβάλλον High Availability.

Ένας Load Balancer έχει ρόλο στο να διαμοιράζει τον δικτυακό φόρτο που δέχεται μια υπηρεσία σε πολλούς servers ελέγχοντας συγχρόνως ποιοι από τους servers αυτούς είναι ενεργοί. Αν κάποιος server δεν αποκρίνεται είτε για λόγους διαχείρισης είτε λόγω κάποιου τεχνικού προβλήματος ο φόρτος ανακατευθύνεται μόνο στους υπόλοιπους ενεργούς.

Έτσι επιτυγχάνεται καλύτερη απόκριση υπηρεσίας ενώ παράλληλα ελαχιστοποιώντας τον χρόνο που μια υπηρεσία είναι ανενεργή.

Στην παρακάτω εικόνα φαίνεται παράδειγμα της προτεινόμενης υλοποίησης.



Υλοποίηση

Η υλοποίηση των παραπάνω υπηρεσιών θα μπορούσε να αρχίσει άμεσα με ορίζοντα ολοκλήρωσης τους 6 μήνες.

Η Ομάδα υλοποίησης είναι η ακόλουθη:

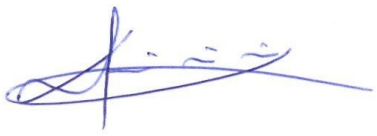
- Χαρά Τομαρά (συντονισμός)
- Μηνάς Θεοδωράκης
- Γιάννης Καπετανάκης
- Δημήτρης Κουναλάκης.

Αξιολόγηση

Στα πλαίσια του έργου της ΜΟΔΙΠ είναι και η αξιολόγηση των υπηρεσιών που προσφέρονται στο Ίδρυμα.

Προτείνουμε λοιπόν με τη βοήθεια της διοίκησης, της Δ/νσης Σχεδιασμού Προγραμματισμού, της ΜΟΔΙΠ του Π.Κ, του Δ/ντή του ΕΕΔ και αντιπροσωπευτικών χρηστών να σχεδιαστεί σχετικό ερωτηματολόγιο για την αξιολόγηση του παραχθέντος έργου.

Η αξιολόγηση αυτή θα μπορούσε να παίξει και το ρόλο της pilot αξιολόγησης των υπηρεσιών του Ιδρύματος.



Χαρά Τομαρά

Ομάδα Συστημάτων & Δικτύων /

Συντονισμός Μηχανογράφησης Γραμματειών

Εργαστήριο Επεξεργασίας Δεδομένων