# “Αξιοποίηση παλαιού εξοπλισμού - εγκατάσταση-παραμετροποίηση Ubuntu Server σε σχολικό εργαστήριο σε ρόλο internet gateway / router – transparent Proxy server”

**Ρίτας Ιωάννης** [1]

[1]Καθηγητής Πληροφορικής ΠΕ 20 - Τεχνικός Υπεύθυνος ΚΕ.ΠΛΗ.ΝΕΤ ΣΕΡΡΩΝ
jritas@sch.gr

## Περίληψη

*Στη σημερινή εποχή το διαδίκτυο είναι το κυριότερο μέσο επικοινωνίας και ανταλλαγής πληροφοριών. Αποτελεί ισχυρό εργαλείο το οποίο μετατρέπει ένα σχολείο σε ένα χώρο με απεριόριστη πληροφορία και επικοινωνία. Εκτός από τα προφανή οφέλη, υποβόσκουν αρκετοί κίνδυνοι, όπως η έκθεση σε υλικό πορνογραφικό, βίαιο, ρατσιστικό ή γενικά προσβλητικό. Τα παιδιά και οι έφηβοι αποτελούν την πιο δυναμική ομάδα στο διαδίκτυο. Γι’ αυτό είναι απαραίτητο να εγκαταστήσουμε και να εφαρμόσουμε όχι μόνο αντι-ικά προγράμματα και firewalls αλλά και φιλτράρισμα περιεχομένου (content filtering) πέρα από τον έλεγχο που εφαρμόζει το Πανελλήνιο Σχολικό Δίκτυο.*

*Στην παρούσα εργασία παρουσιάζεται ο τρόπος με τον οποίο θα δημιουργήσουμε ένα σύστημα το οποίο θα επιτελεί ρόλο Gateway-Router, Firewall και Transparent-Proxy αξιοποιώντας παλαιό εξοπλισμό και ελεύθερο λογισμικό που θα βοηθά στην απρόσκοπτη λειτουργία του δικτύου με αξιοπιστία, ασφάλεια, διαφανή λειτουργία, μηδενικό κόστος εγκατάστασης, μηδαμινές απαιτήσεις συντήρησης, να μην απαιτεί εξειδικευμένο hardware-software και να μπορεί να χρησιμοποιηθεί για εξαγωγή χρήσιμων συμπερασμάτων για τη λειτουργία του σχολικού εργαστηρίου μέσω ανάλυσης logs για περαιτέρω βελτιστοποίηση.*

**Λέξεις κλειδιά:** Firewall, Transparent-Proxy, Router/gateway, content -filtering ,ελεύθερο λογισμικό.

## Abstract

I*n our time the internet is the major mean at communication and exchange. It is a powerful tool which is possible to turn a school into a place where information and communication will be available. Although the above benefits the underlie quite a few dangers, like exposure to material as pornographic, violent, racistic or generally insulting and which fosters hatred and aggression. The children and teenagers make up the most dynamic internet groups. Therefore, it is necessary not only to install antivirus programs and firewalls but content filtering except of the of the services of content filtering of Greek School Network.*

*In the present work, is presentated the way for creating a pc-system to act as Gateway-Route, Firewall and Transparent Proxy with utilisation old hardware and open source-free software that helps network operation without problems with reliability, security, zero cost and to able after log analysis to exact useful conjectural for further optimization.*

## *1. Εισαγωγή*

Είναι αδιαμφισβήτητη η χρησιμότητα του διαδικτύου σε ένα σχολικό περιβάλλον τόσο στην εκπαιδευτική όσο και στην διοικητική λειτουργία. Σήμερα η διείσδυση των ευρυζωνικών συνδέσεων και υπηρεσιών στα σχολεία έχει αγγίξει το 100%. Σημαντικοί κίνδυνοι προκύπτουν από τη διαθεσιμότητα και διακίνηση ακατάλληλου ή και παράνομου περιεχομένου (πορνογραφία, κανάλια συνομιλιών, δίκτυα κοινωνικής δικτύωσης, διακίνηση μουσικής βίντεο, άσεμνο περιεχόμενο, τυχερά παιχνίδια ανεπιθύμητη αλληλογραφία και τόσα άλλα). Το Πανελλήνιο Σχολικό Δίκτυο, (Π.Σ.Δ.) για προστασία των μαθητών και της εκπαιδευτικής κοινότητας εφαρμόζει την υπηρεσία ελεγχόμενης πρόσβασης (web filtering) και απαγορεύει την πρόσβαση σε σελίδες με παράνομο ή ακατάλληλο περιεχόμενο. Η μέθοδος φιλτραρίσματος παρόλο που είναι «διαφανής» μερικές φορές οι χρήστες μπορούν να την παρακάμψουν (με χρήση anonymous proxies). Υπάρχουν όμως και ιστοσελίδες που δεν «κόβονται» από το Π.Σ.Δ. όπως και προγράμματα P2P διακίνησης περιεχομένου, τα οποία δημιουργούν σοβαρά προβλήματα στη λειτουργία της σχολικής μονάδας.

Θα δούμε λοιπόν τον τρόπο με τον οποίο θα δημιουργήσουμε ένα σύστημα το οποίο θα επιτελεί ρόλο Gateway-Router, Firewall και Transparent-Proxy αξιοποιώντας παλαιό και μόνο εξοπλισμό και ελεύθερο λογισμικό που θα βοηθά στην απρόσκοπτη λειτουργία του δικτύου με αξιοπιστία, ασφάλεια, διαφανή λειτουργία, μηδενικό κόστος εγκατάστασης, μηδαμινές απαιτήσεις συντήρησης, να μην απαιτεί εξειδικευμένο hardware-software και να μπορεί να χρησιμοποιηθεί για εξαγωγή χρήσιμων συμπερασμάτων για τη λειτουργία του σχολικού εργαστηρίου μέσω ανάλυσης logs για περαιτέρω βελτιστοποίηση.

## *2. Περιγραφή - δίκτυο*

Hardware: Χρησιμοποιήθηκε ένα παλιό σύστημα Η/Υ με τα παρακάτω χαρακτηριστικά

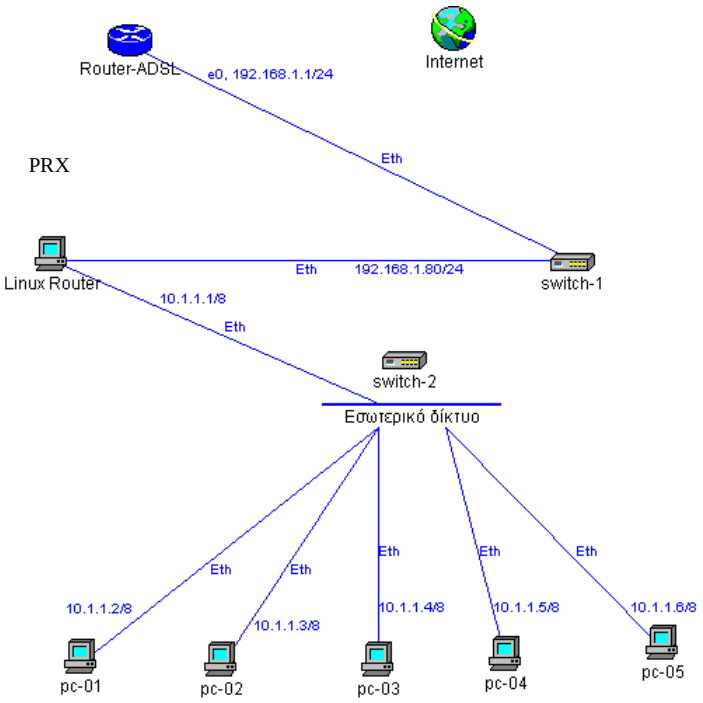
Η/Υ Pentium II 350 Mhz
Μνήμη RAM 128 MB
2 κάρτες δικτύου
Σκληρός δίσκος 20 GB

Λειτουργικό σύστημα: Linux Ubuntu server 7.10 (kernel 2.6.22-14-server)

Στον Η/Υ τοποθετήθηκαν δύο κάρτες δικτύου (μια για σύνδεση με το ιντερνέτ – με τον router του ΠΣΔ μέσω του ήδη υπάρχοντος switch και μία για την σύνδεση με το εσωτερικό δίκτυο – δηλαδή τους Η/Υ του σχολικού εργαστηρίου) Από νέο υλικό το μόνο που θα χρειαστεί είναι ένα νέο switch 5 ports για να συνδέσουμε τον Linux

server με το router. Εγκαθιστώντας και παραμετροποιώντας το linux μαζί και με όλες τις άλλες υπηρεσίες (squid, dhcp, ip-tables, webmin κλπ) μας δίνεται η δυνατότητα να ρυθμίσουμε πολύ εύκολα την διαδικτυακή κίνηση του εργαστηρίου (απαγόρευση πρόσβασης σε ορισμένες διευθύνσεις που δεν αποκλείει το ΠΣΔ, να σταματήσουμε εντελώς προγράμματα chatting, social networking, ανταλλαγής αρχείων p2p, να ξεχωρίσουμε το ή τα δίκτυα του σχολικού εργαστηρίου από το υπόλοιπο δίκτυο του σχολείου (υπολογιστές γραμματείας, e-school κλπ), να απαγορεύσουμε το κατέβασμα συγκεκριμένων τύπων αρχείων σε μερικούς ή σε όλους τους Η/Υ (πχ .mp3, .exe, .zip, .avi κλπ), να επιταχύνουμε την πρόσβαση σε ιστοσελίδες μέσω του proxy server και γενικά να αξιοποιήσουμε πολύ παλιό εξοπλισμό (πρακτικά άχρηστο) φτιάχνοντας ένα router, κατανοώντας τον τρόπο λειτουργίας-δρομολόγησης- επικοινωνία πακέτων σε διαφορετικά δίκτυα. Επίσης με τη χρήση του εργαλείου Webmin γίνεται πολύ εύκολα η παραμετροποίηση, η διαχείριση και οι όποιες αλλαγές στον τρόπο λειτουργίας, Αξίζει να σημειωθεί ότι με το εργαλείο Calamaris (add-on πακέτο στον proxy server) αλλά και του darkstat, μας δίνεται η δυνατότητα να δούμε με γραφικό και όχι μόνο τρόπο την κίνηση του δικτύου μας, τις πιο συχνές σελίδες που επισκέπτονται οι μαθητές και μέσω αυτών των log καταγραφής να αποφασίσουμε για περεταίρω βελτιστοποίηση. Η όλη εγκατάσταση βασίστηκε σε παλιά έκδοση Linux server και αυτό γιατί δεν είναι απαραίτητες οι νέες δυνατότητες των νέων εκδόσεων που ίσως απαιτούν και περισσότερους υπολογιστικούς πόρους.

Το όλο εγχείρημα μπορεί να στηθεί – παραμετροποιηθεί και να λειτουργήσει σε λιγότερο από 2 ώρες και το πιο σημαντικό είναι ότι δεν απαιτεί άδειες χρήσης – εξειδικευμένο λογισμό ή υλικό αφού τα πάντα βασίζονται σε ελεύθερο – ανοικτό λογισμικό και πολύ παλιό εξοπλισμό. Τέλος για μελλοντικές επεκτάσεις του συστήματος αξίζει να σημειωθεί ότι πολύ εύκολα μπορεί να προστεθεί ασύρματη κάρτα στο μηχάνημα και να γίνει εκτός από wired και wireless router-server-gateway, εξυπηρετώντας ασύρματα το εργαστήριο (με μικρή τοπική εμβέλεια) βάζοντας έτσι στην εκπαιδευτική διαδικασία τα netbook των μαθητών.




**Σχήμα 1:** διάγραμμα δικτύου

## 2. *Εγκατάσταση – παραμετροποίηση*

Έγινε εγκατάσταση της έκδοσης ubuntu 7.10 server. Από τα επιπλέον πακέτα λογισμικού εγκαταστάθηκε μόνο το πακέτο ssh-server και αυτό γιατί δεν χρειάζεται οθόνη στον server (παρά μόνο κατά την εγκατάσταση) και απλά να έχουμε πρόσβαση από άλλο τερματικό μέσω ssh console.

Μετά το πέρας της εγκατάστασης έγινε update και upgrade του λειτουργικού συστήματος με την μόνη ιδιαιτερότητα ότι μέσα στο αρχείο /etc/apt/sources.list αντικαταστάθηκαν οι πηγές λογισμικού με τις παλιές (old-ubuntu archives) ως εξής: προσθήκη στα sources list, των repositories από old releases για να προχωρήσουμε σε αναβάθμιση πακέτων ως εξής:

```
user@prx:~$ sudo sed -ie 's|//security|//old-releases|' /etc/apt/sources.list && sudo sed -ie 's|//us.archive|//old-releases|' /etc/apt/sources.list
```

Αναβάθμιση συστήματος και έλεγχος για νέες ενημερώσεις

```
user@prx:~$ sudo apt-get update || sudo apt-get upgrade
```

Ελέγχος και παραμετροποίηση των network interfaces

```
user@prx:~$ sudo nano /etc/network/interfaces
# The loopback network interface
auto lo
```

```
iface lo inet loopback
# Το πρώτο network interface σύνδεση με τον “έξω κόσμο” -internet-1η κάρτα
#δικτύου
auto eth0
iface eth0 inet static
        address 192.168.1.81
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        gateway 192.168.1.1
        dns-nameservers 192.168.1.1
        post-up iptables-restore < /etc/iptables.up.rules
# Το δεύτερο network interface σύνδεση με τον “έσωτερικό δίκτυο” -internal 2η
#κάρτα δικτύου  - αποδίδουμε δικές μας διευθύνσεις
auto eth1
iface eth1 inet static
address 10.1.1.1
netmask 255.255.255.0
broadcast 10.1.1.255
network 10.1.1.0
```

Εγκατάσταση του πακέτου squid (proxy server)

```
user@prx:~$ sudo apt-get install squid squid-common
```

Ενεργοποίηση του IP-FORWARDING ως εξής

```
user@prx:~$ sudo nano /etc/sysctl.conf
```

ενεργοποιούμε την γραμμή *net.ipv4.conf.default.forwarding=1*

και στη συνέχεια τροποποιούμε το αρχείο ip_forward

```
user@prx:~$ sudo nano /proc/sys/net/ipv4/ip_forward
```

και  αλλάζουμε την τιμή 0 σε 1

Εγκαθιστούμε τον dhcp Server (για απόδοση διευθύνσεων στο εσωτερικό δίκτυο)

```
user@prx:~$ sudo apt-get install dhcp3-server
```

και τροποποιούμε το αρχείο dhcpd.conf

```
user@prx:~$ sudo nano /etc/dhcpd.conf
```

```
option domain-name-servers 192.168.1.1;
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 10.1.1.0 netmask 255.255.255.0 {
  range 10.1.1.100 10.1.1.200;
  option subnet-mask 255.255.255.0;
  option broadcast-address 10.1.1.255;
  option routers 10.1.1.1;
}
```

Πολύ σύντομα αναφέρουμε ότι με την εντολή authoritative δηλώνουμε ότι ο linux server θα είναι ο πρωτεύων – κύριος DHCP Server και θα μοιράζει αυτός IP παρόλο που υπάρχει και ο dhcp server (router) του σχολικού εργαστηρίου. Επίσης στο εσωτερικό μας δίκτυο μοιράζουμε IP από 10.1.1.100 έως 10.1.1.200

Τέλος στο αρχείο /etc/default/dhcp3-server ορίζουμε σε πιο interface θα «ακούει» ο dhcp server

```
user@prx:~$ sudo nano /etc/default/dhcp3-server
```

και μέσα βάζουμε την κάρτα του εσωτερικού δικτύου πχ eth1ενώ στη συνέχεια επανεκκινούμε τον dhcp και τον squid server

```
user@prx:~$ sudo  /etc/init.d/dhcp3-server restart
user@prx:~$ sudo /etc/init.d/squid restart
```

Εγκατάσταση νέων πακέτων λογισμικού που χρειαζόμαστε

```
user@prx:~$ sudo apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl libmd5-perl
user@prx:~$ wget http://prdownloads.sourceforge.net/webadmin/webmin_1.500_all.deb
```

Εγκαθιστούμε το πακέτο webmin για έλεγχο του μηχανήματος μέσω web interface

```
user@prx:~$ sudo dpkg -i webmin_1.500_all.deb
```

Παραμετροποίηση του squid

```
user@prx:~$ sudo nano /etc/squid/squid.conf
```

Παρατίθεται το αρχείο για ανάλυση του configuration (http://www.squidcache.org/Doc/FAQ/, 2004)

```
http_port 3128 transparent  #η πόρτα σύνδεσης στον proxy server σε διαφανή λειτ.
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
access_log /var/log/squid/access.log squid
hosts_file /etc/hosts
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320
acl esoteriko src 20.1.1.0/24
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443          # https
acl SSL_ports port 563          # snews
acl SSL_ports port 873          # rsync
```

```
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl Safe_ports port 631         # cups
acl Safe_ports port 873         # rsync
acl Safe_ports port 901         # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
acl bad url_regex -i "/etc/squid/squid-block.acl"
acl malware url_regex -i "/etc/squid/malware.txt"
deny_info http://malware.hiperlinks.com.br/denied.shtml malware
deny_info ERR_BLOCKED_FILES bad
http_access deny bad
http_access deny malware
http_access allow esoteriko
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
icp_access allow all
visible_hostname prx
always_direct allow all
coredump_dir /var/spool/squid
extension_methods REPORT MERGE MKACTIVITY CHECKOUT
```

Αυτά που αξίζει να σημειώσουμε είναι τα εξής:

http_port 3128 transparent, η πόρτα στην οποία ακούει ο proxy server και ο τρόπος λειτουργίας (διαφανής λειτουργία – οι χρήστες δεν χρειάζεται να κάνουν καμιά ρύθμιση στους browsers των τερματικών), acl esoteriko src 20.1.1.0/24 δημιουργούμε μια access list με όνομα πχ esoteriko για τις IP του εσωτερικού δικτύου και με την εντολή http_access allow esoteriko επιτρέπουμε την πρόσβαση στο Internet για αυτές τις IP.

Ορίζουμε μέσα στο αρχείο /etc/squid/squid-block.acl κάποιες διευθύνσεις που θέλουμε να αποκλείσουμε από τους χρήστες μας (και οι οποίες ίσως ΔΕΝ ΑΠΟΚΛΕΙΟΝΤΑΙ ΑΠΟ ΤΟ ΣΧΟΛΙΚΟ ΔΙΚΤΥΟ)ως εξής

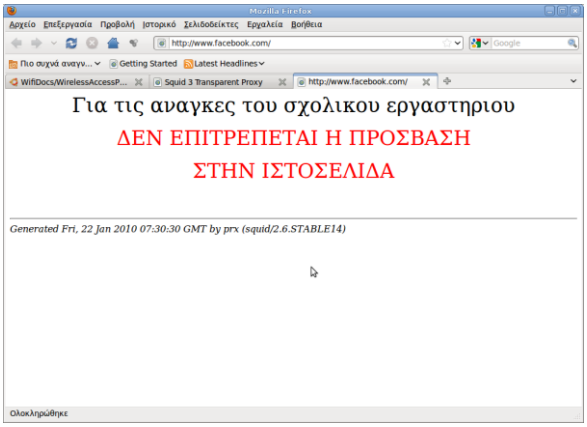
.facebook.com
.hi5.com
.zoo.com κλπ

acl bad url_regex -i "/etc/squid/squid-block.acl"

ορίζοντας αυτή τη λίστα με το όνομα bad και με την σημείωση url_regex αποτρέπουμε την πρόσβαση σε όλες τις διευθύνσεις που εισάγαμε στο παραπάνω αρχείο με την εντολή http_access deny bad απαγορεύουμε την πρόσβαση, ενώ με την εντολή deny_info ERR_BLOCKED_FILES bad εμφανίζουμε στην οθόνη του browser το μήνυμα που θέλουμε να εμφανίζεται όταν κάποιος χρήστης επισκέπτεται κάποια απαγορευμένη σελίδα π.χ.

user@prx:~$ sudo nano /usr/share/squid/errors/English/ERR_BLOCKED_FILES

και μέσα γράφουμε κώδικα html.




**Σχήμα 2** :Αποτέλεσμα πρόσβασης σε απαγορευμένη σελίδα

Εγκαθιστούμε το πακέτο calamaris που χρησιμοποιείται για ανάλυση των log του proxy server μας για στατιστική ανάλυση και επεξεργασία

user@prx:~$ sudo apt-get install calamaris

Δημιουργούμε το αρχείο tr.sh (αρχείο script) και μέσα γράφουμε τα παρακάτω (http://www.yolinux.com/TUTORIALS/LinuxTutorialIptablesNetworkGateway.html)

```
# Squid server IP
SQUID_SERVER="192.168.1.81"
# καρτα δικτύου συνδεμένη στο Internet
INTERNET="eth0"
# διευθύνσεις εσωτερικού δικτύου LAN
LOCAL="20.1.1.0/24"
LOCAL2="192.168.1.0/24"
SQUID_PORT="3128"
```

```
# καθαρισμός παλιών roules firewal
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
# Ενεργοποίηση ip_forwarding
echo ‘‘1’’ > /proc/sys/net/ipv4/ip_forward
# default  policy γενικά
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# Επιτρέπουμε κυκλοφορία πακέτων UDP, DNS και FTP
iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
# ορισμός του συστήματός μας ως  router για όλο το  LAN
iptables -t nat -A POSTROUTING -o $INTERNET -j MASQUERADE
iptables -A FORWARD -s $LOCAL -j ACCEPT
#απεριόριστη πρόσβαση στο εσωτερικό LAN
iptables -A INPUT -s $LOCAL -j ACCEPT
iptables -A OUTPUT -s $LOCAL -j ACCEPT
# Οι αιτήσεις στην πόρτα 80 από το εσωτ. Δίκτυο θα πηγαίνουν στην 3128
iptables -t nat -A PREROUTING -s $LOCAL -p tcp --dport 80 -j DNAT --to
SQUID_SERVER:SQUID_PORT
iptables -t nat -A PREROUTING -s $LOCAL2 -p tcp --dport 80 -j DNAT --to
SQUID_SERVER:SQUID_PORT
iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j REDIRECT --to-port
$SQUID_PORT
iptables -A INPUT -i $INTERNET -j ACCEPT
iptables -A OUTPUT -o $INTERNET  -j ACCEPT
iptables -A INPUT -j LOG
iptables -A INPUT -j DROP
```

το κάνουμε εκτελέσιμο

user@prx:~$ sudo chmod +x tr.sh
και το εκτελούμε user@prx:~$ sudo ./tr.sh

Με τον τρόπο αυτό γίνεται το NAT και η δρομολόγηση πακέτων ανάμεσα στα δυο Interfaces μέσω του Linux firewall (IP-tables)

## *Συμπεράσματα*

Η πρόσβαση στο INTEPNTET παρά την αδιαμφισβήτητη χρησιμότητά της υποκρύπτει και κινδύνους. Η εξέλιξη των τεχνολογιών της πληροφορικής και των επικοινωνιών μπορεί να αυξήσει την παραβατικότητα των ανήλικων μαθητών. Δεν υπάρχει απόλυτη ασφάλεια όσον αφορά τον έλεγχο περιεχομένου στο διαδίκτυο για το Π.Σ.Δ.. Είναι εφικτό χρησιμοποιώντας παλαιό εξοπλισμό και ελεύθερο λογισμικό να απαγορεύσουμε την πρόσβαση σε συγκεκριμένες σελίδες και με τη χρήση

κατάλληλου λογισμικού να εξάγουμε χρήσιμα συμπεράσματα για τη λειτουργία του σχολικού εργαστηρίου μέσω ανάλυσης logs για περαιτέρω βελτιστοποίηση.

## *Βιβλιογραφία*


*Using Linux iptables or ipchains to set up an internet gateway / firewall / router for home or office from* http://www.yolinux.com/TUTORIALS/LinuxTutorialIptablesNetworkGateway.html

*Iptables Tutorial 1.2.2 by Oskar Andreasson Copyright © 2001-2006 Oskar Andreasson from* http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html

Squid cache from http://wiki.squid-cache.org/

*Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort written by Michael Rash and published by No Starch Press in September, 2007* from http://cipherdyne.org/LinuxFirewalls/

Squid Team, "*SQUID Frequently Asked Questions*", http://www.squidcache.org/Doc/FAQ/, 2004.

http://ubuntuforums.org/index.php

http://old-releases.ubuntu.com/ubuntu/dists/gutsy/

http://www.webmin.com/docs.html

http://cord.de/tools/squid/calamaris/

The Perfect Server - Ubuntu Gutsy Gibbon (Ubuntu 7.10) from http://www.howtoforge.com/perfect_server_ubuntu7.10

http://ubuntuguide.org/wiki/Ubuntu:Gutsy