



UNIVERSITY  
OF THE AEGEAN

## ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

### 2η Εργαστηριακή Αναφορά

κ. ΣΤΕΦΑΝΟΣ ΓΚΡΙΤΖΑΛΗΣ

κα. ΑΝΑΣΤΑΣΙΑ ΔΟΥΜΑ

κ. ΔΗΜΗΤΡΗΣ ΠΑΠΑΜΑΡΤΖΙΒΑΝΟΣ

### ΣΤΟΙΧΕΙΑ ΦΟΙΤΗΤΩΝ:

ΙΩΑΝΝΗΣ ΡΟΥΣΣΟΣ icsd08125

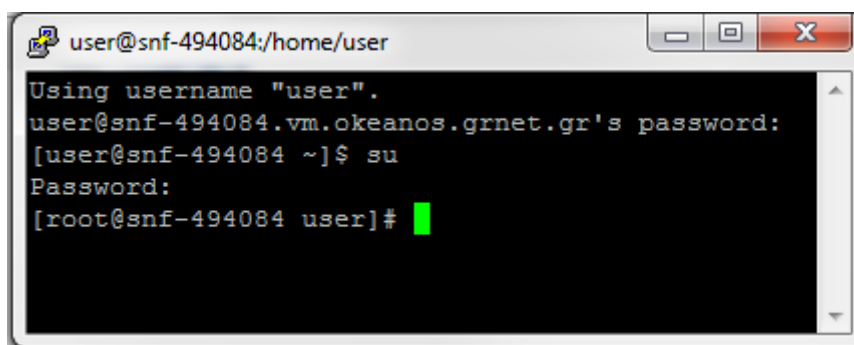
ΔΗΜΗΤΡΑ ΑΓΓΕΛΙΚΗ ΤΑΛΕΚΟΓΛΟΥ icsd09137

## Part 1: Linux Server

### Αρχική εγκατάσταση και παραμετροποίηση του λειτουργικού συστήματος

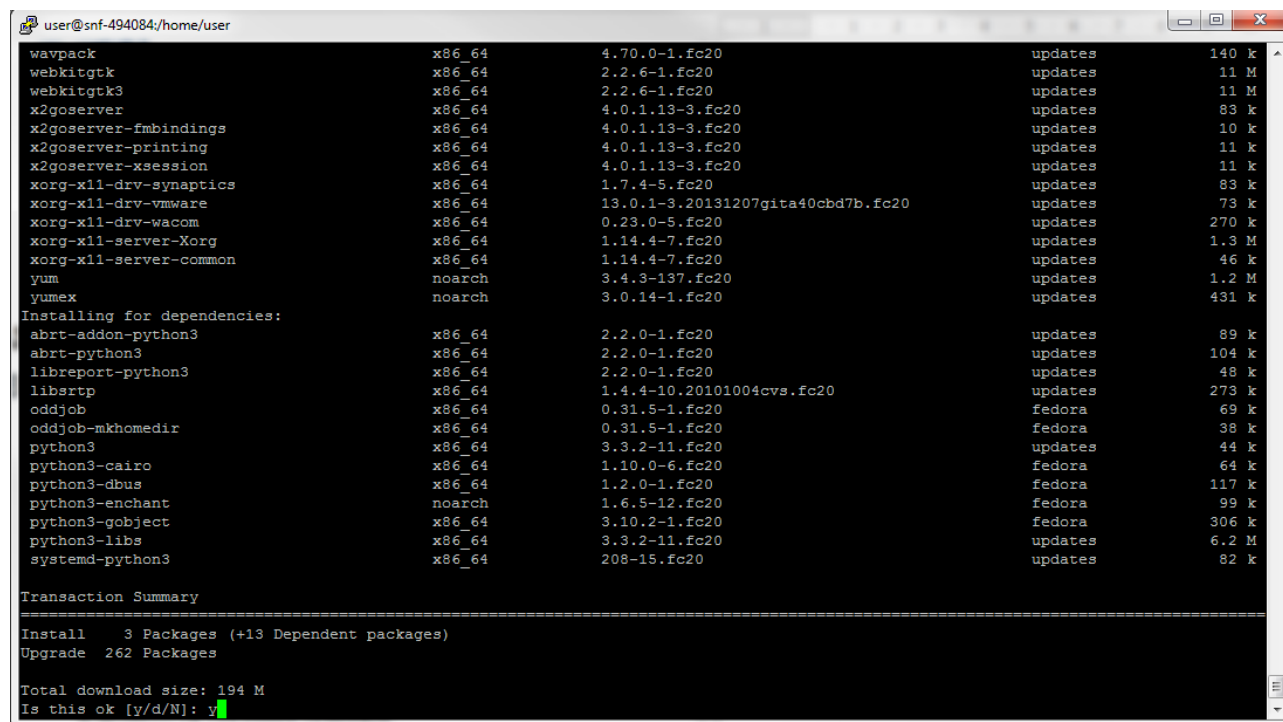
Ξεκινάμε με την εγκατάσταση του λειτουργικού συστήματος Linux , Fedora 20 64-bit. Την τρέχουμε ως Virtual Machine στον Οκεανο.

Αρχικό Login μας ως admin με την εντολή su.



```
user@snf-494084:/home/user
Using username "user".
user@snf-494084.vm.okeanos.grnet.gr's password:
[user@snf-494084 ~]$ su
Password:
[root@snf-494084 user]#
```

Εκτελούμε την εντολή **yum update** για να κάνουμε update τις υπηρεσίες που προϋπάρχουν στην έκδοσή μας.



```
user@snf-494084:/home/user
wavpack                x86_64                4.70.0-1.fc20          updates              140 k
webkitgtk               x86_64                2.2.6-1.fc20           updates              11 M
webkitgtk3              x86_64                2.2.6-1.fc20           updates              11 M
x2goserver              x86_64                4.0.1.13-3.fc20        updates              83 k
x2goserver-fmbindings  x86_64                4.0.1.13-3.fc20        updates              10 k
x2goserver-printing     x86_64                4.0.1.13-3.fc20        updates              11 k
x2goserver-xsession     x86_64                4.0.1.13-3.fc20        updates              11 k
xorg-x11-drv-synaptics  x86_64                1.7.4-5.fc20           updates              83 k
xorg-x11-drv-vmware     x86_64                13.0.1-3.20131207gita40cbd7b.fc20 updates              73 k
xorg-x11-drv-wacom      x86_64                0.23.0-5.fc20          updates              270 k
xorg-x11-server-Xorg    x86_64                1.14.4-7.fc20          updates              1.3 M
xorg-x11-server-common  x86_64                1.14.4-7.fc20          updates              46 k
yum                     noarch                3.4.3-137.fc20         updates              1.2 M
yumex                   noarch                3.0.14-1.fc20          updates              431 k
Installing for dependencies:
abrt-addon-python3      x86_64                2.2.0-1.fc20           updates              89 k
abrt-python3            x86_64                2.2.0-1.fc20           updates              104 k
libreport-python3       x86_64                2.2.0-1.fc20           updates              48 k
librtpt                  x86_64                1.4.4-10.20101004cvs.fc20 updates              273 k
oddjob                   x86_64                0.31.5-1.fc20          fedora               69 k
oddjob-mkhomedir        x86_64                0.31.5-1.fc20          fedora               38 k
python3                  x86_64                3.3.2-11.fc20          updates              44 k
python3-cairo            x86_64                1.10.0-6.fc20          fedora               64 k
python3-dbus             x86_64                1.2.0-1.fc20           fedora              117 k
python3-enchanted        noarch                1.6.5-12.fc20          fedora               99 k
python3-gobject           x86_64                3.10.2-1.fc20          fedora              306 k
python3-libs              x86_64                3.3.2-11.fc20          updates              6.2 M
systemd-python3          x86_64                208-15.fc20            updates              82 k

Transaction Summary
-----
Install    3 Packages (+13 Dependent packages)
Upgrade   262 Packages

Total download size: 194 M
Is this ok [y/d/N]: y
```

Εγκαθιστούμε την υπηρεσία **iptables**, την οποία χρειαζόμαστε, με την εντολή **yum install iptables-services**.

```
user@snf-494084:/home/user
[root@snf-494084 user]# yum install iptables-services
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
---> Package iptables-services.x86_64 0:1.4.19.1-1.fc20 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                        Arch          Version           Size              Repository
=====
Installing:
iptables-services             x86_64        1.4.19.1-1.fc20   43 k              fedora
Transaction Summary
-----
Install 1 Package

Total download size: 43 k
Installed size: 18 k
Is this ok [y/d/N]: y
```

```
user@snf-494084:/home/user
Transaction Summary
-----
Install 1 Package

Total download size: 43 k
Installed size: 18 k
Is this ok [y/d/N]: y
Downloading packages:
iptables-services-1.4.19.1-1.fc20.x86_64.rpm | 43 kB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : iptables-services-1.4.19.1-1.fc20.x86_64 1/1
  Verifying   : iptables-services-1.4.19.1-1.fc20.x86_64 1/1

Installed:
iptables-services.x86_64 0:1.4.19.1-1.fc20

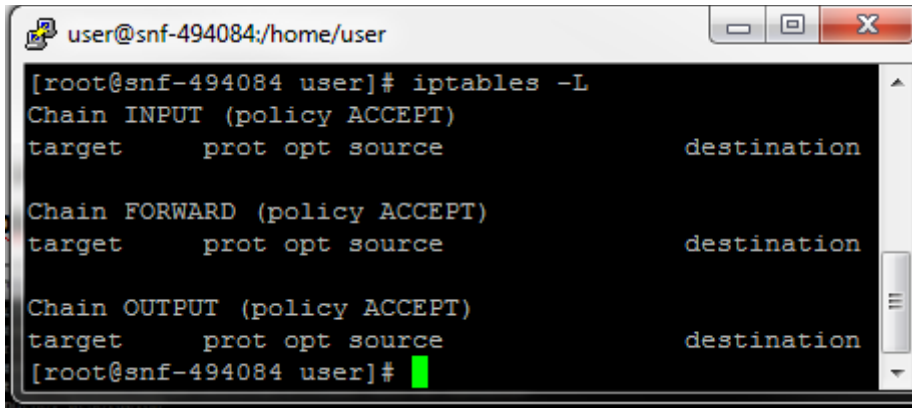
Complete!
[root@snf-494084 user]#
```

Για να ξεκινάνε αυτόματα τα **iptables** όταν ξεκινάει το σύστημα, χρησιμοποιούμε την εντολή **chkconfig --level 345 iptables on**.

```
user@snf-494084:/home/user
[root@snf-494084 user]# chkconfig --level 345 iptables on
Note: Forwarding request to 'systemctl enable iptables.service'.
ln -s '/usr/lib/systemd/system/iptables.service' '/etc/systemd/system/basic.target.wants/iptables.service'
[root@snf-494084 user]#
```

Για να δέχεται το σύστημά μας **μόνο** συνδέσεις SSH, πρέπει να θέσουμε τους δικούς μας κανόνες.

Με την εντολή **iptables -L** βλέπουμε την λίστα των κανόνων των **iptables**.



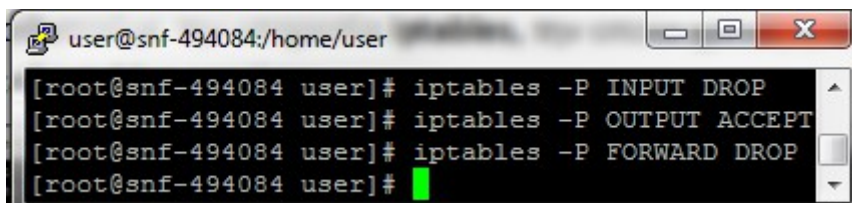
```
user@snf-494084:/home/user
[root@snf-494084 user]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source      destination

Chain FORWARD (policy ACCEPT)
target     prot opt source      destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source      destination
[root@snf-494084 user]#
```

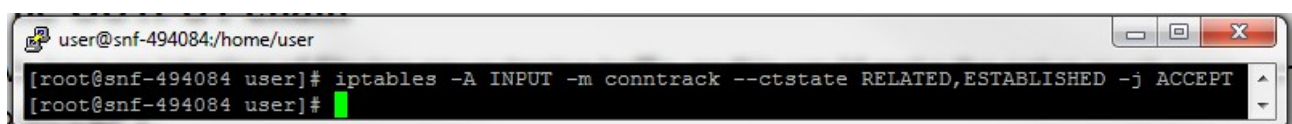
Βλέπουμε ότι μέχρι στιγμής, δεν υπάρχει κανένας κανόνας.

Για να ρυθμίσουμε την πολιτική φίλτρων ώστε να επιτρέπει μόνο εξωστρεφή κίνηση δεδομένων, χρησιμοποιούμε τις εντολές **iptables -P INPUT DROP**, **iptables -P OUTPUT ACCEPT** και **iptables -P FORWARD DROP**.



```
user@snf-494084:/home/user
[root@snf-494084 user]# iptables -P INPUT DROP
[root@snf-494084 user]# iptables -P OUTPUT ACCEPT
[root@snf-494084 user]# iptables -P FORWARD DROP
[root@snf-494084 user]#
```

Χρησιμοποιούμε την εντολή **iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT** για να επιτρέψουμε στην ήδη καθιερωμένη κίνηση να συνεχίσει.



```
user@snf-494084:/home/user
[root@snf-494084 user]# iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
[root@snf-494084 user]#
```

Για να επιτρέψουμε **ΜΟΝΟ** συνδέσεις SSH, εκτελούμε τις εντολές **iptables -A INPUT -p tcp --dport ssh -i eth0 -j ACCEPT** και **iptables -A INPUT -p udp --dport ssh -i eth0 -j ACCEPT**.

```
user@snf-494084:/home/user
[root@snf-494084 user]# iptables -A INPUT -p tcp --dport ssh -i eth0 -j ACCEPT
[root@snf-494084 user]# iptables -A INPUT -p udp --dport ssh -i eth0 -j ACCEPT
[root@snf-494084 user]#
```

Επίσης, με την εντολή **iptables -A INPUT -i lo -j ACCEPT** επιτρέπουμε **loopbacks** σε κινήσεις τοπικού δικτύου.

```
[root@snf-494084 user]# iptables -A INPUT -i lo -j ACCEPT
[root@snf-494084 user]#
```

Για να αποθηκεύσουμε τους κανόνες που δημιουργήσαμε, εκτελούμε την εντολή **iptables-save > servertables**. Η τελική μορφή των **iptables** είναι η παρακάτω:

```
[root@snf-494084 user]# iptables-save > servertables
[root@snf-494084 user]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            ctstate RELATED,ESTABLISHED
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
INPUT_direct all  --  anywhere              anywhere
INPUT_ZONES_SOURCE all  --  anywhere              anywhere
INPUT_ZONES all  --  anywhere              anywhere
ACCEPT    icmp --  anywhere              anywhere
REJECT    all  --  anywhere              anywhere          reject-with icmp-host-prohibited
ACCEPT    all  --  anywhere              anywhere          ctstate RELATED,ESTABLISHED
ACCEPT    tcp  --  anywhere              anywhere          tcp dpt:ssh
ACCEPT    udp  --  anywhere              anywhere          udp dpt:ssh
ACCEPT    all  --  anywhere              anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination            ctstate RELATED,ESTABLISHED
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
FORWARD_direct all  --  anywhere              anywhere
FORWARD_IN_ZONES_SOURCE all  --  anywhere              anywhere
FORWARD_IN_ZONES all  --  anywhere              anywhere
FORWARD_OUT_ZONES_SOURCE all  --  anywhere              anywhere
FORWARD_OUT_ZONES all  --  anywhere              anywhere
ACCEPT    icmp --  anywhere              anywhere
REJECT    all  --  anywhere              anywhere          reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
OUTPUT_direct all  --  anywhere              anywhere

Chain FORWARD_IN_ZONES (1 references)
target     prot opt source                destination
FWDI_public all  --  anywhere              anywhere          [goto]
FWDI_public all  --  anywhere              anywhere          [goto]
FWDI_public all  --  anywhere              anywhere          [goto]

Chain FORWARD_IN_ZONES_SOURCE (1 references)
target     prot opt source                destination

Chain FORWARD_OUT_ZONES (1 references)
target     prot opt source                destination
FWDO_public all  --  anywhere              anywhere          [goto]
FWDO_public all  --  anywhere              anywhere          [goto]
FWDO_public all  --  anywhere              anywhere          [goto]

Chain FORWARD_OUT_ZONES_SOURCE (1 references)
target     prot opt source                destination

Chain FORWARD_direct (1 references)
target     prot opt source                destination

Chain FWDI_public (3 references)
target     prot opt source                destination
FWDI_public_log all  --  anywhere              anywhere
FWDI_public_deny all  --  anywhere              anywhere
FWDI_public_allow all  --  anywhere              anywhere
```

```

Chain FWDI_public (3 references)
target      prot opt source      destination
FWDI_public_log  all  --  anywhere      anywhere
FWDI_public_deny all  --  anywhere      anywhere
FWDI_public_allow all  --  anywhere      anywhere

Chain FWDI_public_allow (1 references)
target      prot opt source      destination

Chain FWDI_public_deny (1 references)
target      prot opt source      destination

Chain FWDI_public_log (1 references)
target      prot opt source      destination

Chain FWDO_public (3 references)
target      prot opt source      destination
FWDO_public_log  all  --  anywhere      anywhere
FWDO_public_deny all  --  anywhere      anywhere
FWDO_public_allow all  --  anywhere      anywhere

Chain FWDO_public_allow (1 references)
target      prot opt source      destination

Chain FWDO_public_deny (1 references)
target      prot opt source      destination

Chain FWDO_public_log (1 references)
target      prot opt source      destination

Chain INPUT_ZONES (1 references)
target      prot opt source      destination
IN_public   all  --  anywhere      anywhere      [goto]
IN_public   all  --  anywhere      anywhere      [goto]
IN_public   all  --  anywhere      anywhere      [goto]

Chain INPUT_ZONES_SOURCE (1 references)
target      prot opt source      destination

Chain INPUT_direct (1 references)
target      prot opt source      destination

Chain IN_public (3 references)
target      prot opt source      destination
IN_public_log  all  --  anywhere      anywhere
IN_public_deny all  --  anywhere      anywhere
IN_public_allow all  --  anywhere      anywhere

Chain IN_public_allow (1 references)
target      prot opt source      destination
ACCEPT      udp  --  anywhere      224.0.0.251      udp dpt:mdns ctstate NEW
ACCEPT      tcp  --  anywhere      anywhere          tcp dpt:ssh ctstate NEW

Chain IN_public_deny (1 references)
target      prot opt source      destination

Chain IN_public_log (1 references)
target      prot opt source      destination

Chain OUTPUT_direct (1 references)
target      prot opt source      destination
[root@snf-494084 user]# █

```

## Εγκατάσταση Web Server, DNS Server, FTP Server και Database Server

### Web Server

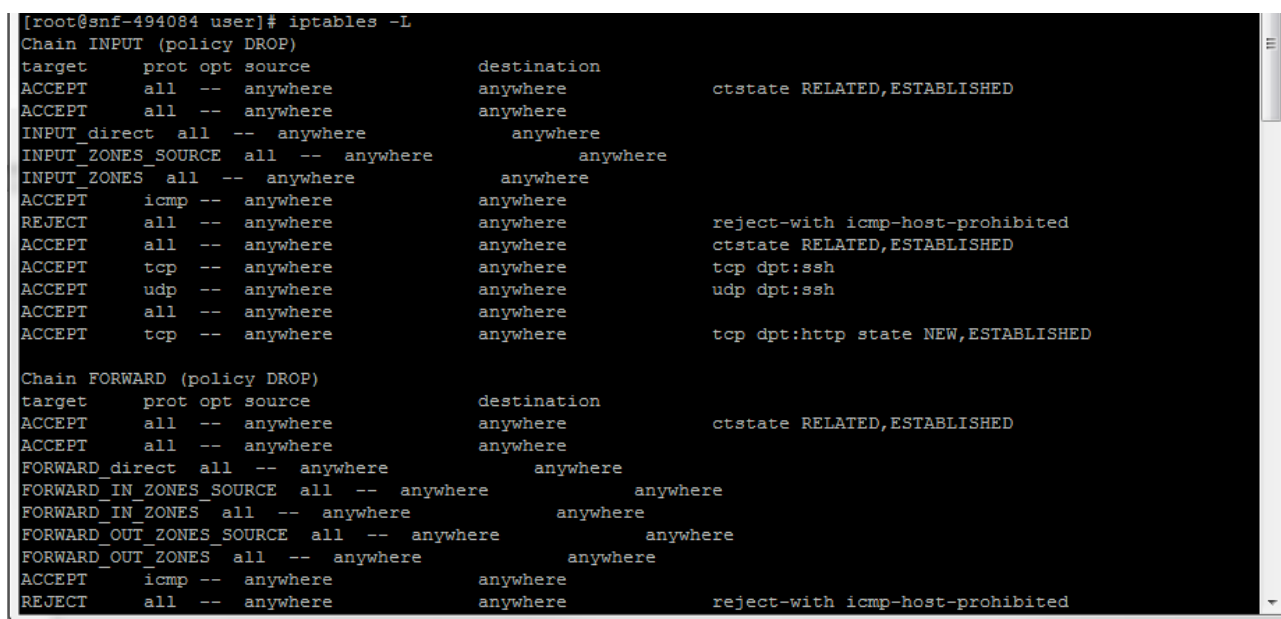
Για τον Web Server, θα χρησιμοποιήσουμε το πρόγραμμα Apache.

Αρχικά, αλλάζουμε τα iptables, έτσι ώστε να δώσουμε πρόσβαση στην θύρα 80 για το πρωτόκολλο http, με τις εντολές **iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT** και **iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT**



```
user@snf-494084:/home/user
[root@snf-494084 user]# iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
[root@snf-494084 user]# iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
[root@snf-494084 user]#
```

Παρατηρούμε ότι:



```
[root@snf-494084 user]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
INPUT_direct all  --  anywhere              anywhere
INPUT_ZONES_SOURCE all  --  anywhere              anywhere
INPUT_ZONES all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere
REJECT     all  --  anywhere              anywhere          reject-with icmp-host-prohibited
ACCEPT     all  --  anywhere              anywhere          ctstate RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere          tcp dpt:ssh
ACCEPT     udp  --  anywhere              anywhere          udp dpt:ssh
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              anywhere          tcp dpt:http state NEW,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source                destination            ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
FORWARD_direct all  --  anywhere              anywhere
FORWARD_IN_ZONES_SOURCE all  --  anywhere              anywhere
FORWARD_IN_ZONES all  --  anywhere              anywhere
FORWARD_OUT_ZONES_SOURCE all  --  anywhere              anywhere
FORWARD_OUT_ZONES all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere
REJECT     all  --  anywhere              anywhere          reject-with icmp-host-prohibited
```



## Εγκατάσταση του Apache(με την εντολή yum install httpd)

```
user@snf-494084:/home/user
--> Processing Dependency: system-logos-httpd for package: httpd-2.4.9-2.fc20.x86_64
--> Processing Dependency: libaprutil-1.so.0()(64bit) for package: httpd-2.4.9-2.fc20.x86_64
--> Processing Dependency: libapr-1.so.0()(64bit) for package: httpd-2.4.9-2.fc20.x86_64
--> Running transaction check
---> Package apr.x86_64 0:1.5.0-2.fc20 will be installed
---> Package apr-util.x86_64 0:1.5.3-1.fc20 will be installed
---> Package fedora-logos-httpd.noarch 0:21.0.1-1.fc20 will be installed
---> Package httpd-tools.x86_64 0:2.4.9-2.fc20 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                               Arch              Version            Repository          Size
=====
Installing:
httpd                                 x86_64            2.4.9-2.fc20       updates             1.2 M
Installing for dependencies:
apr                                   x86_64            1.5.0-2.fc20       updates             106 k
apr-util                             x86_64            1.5.3-1.fc20       updates             91 k
fedora-logos-httpd                   noarch            21.0.1-1.fc20      fedora              28 k
httpd-tools                           x86_64            2.4.9-2.fc20       updates             78 k
=====

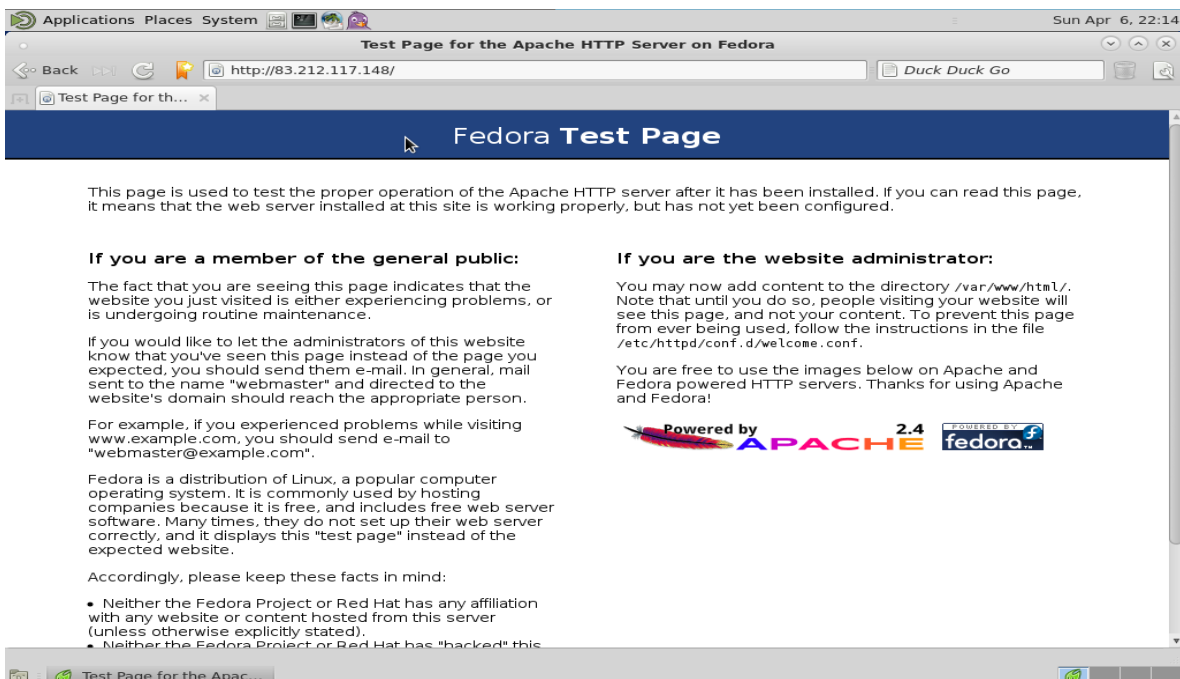
Transaction Summary
-----
Install 1 Package (+4 Dependent packages)

Total download size: 1.5 M
Installed size: 4.3 M
Is this ok [y/d/N]:
```

Για να ξεκινάει αυτόματα το Apache στο boot, εκτελούμε την εντολή  
**/sbin/chkconfig httpd on**

```
user@snf-494084:/home/user
[root@snf-494084 user]# /sbin/chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-user.target.wants/httpd.service'
[root@snf-494084 user]#
```

Ξεκινάμε τον Apache με την εντολή **/sbin/service httpd start** και ελέγχουμε αν δουλεύει σωστά, πληκτρολογώντας την IP του server μας στον browser μας.

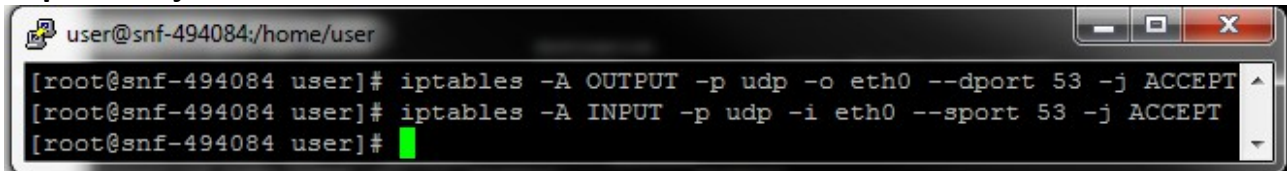




## DNS Server

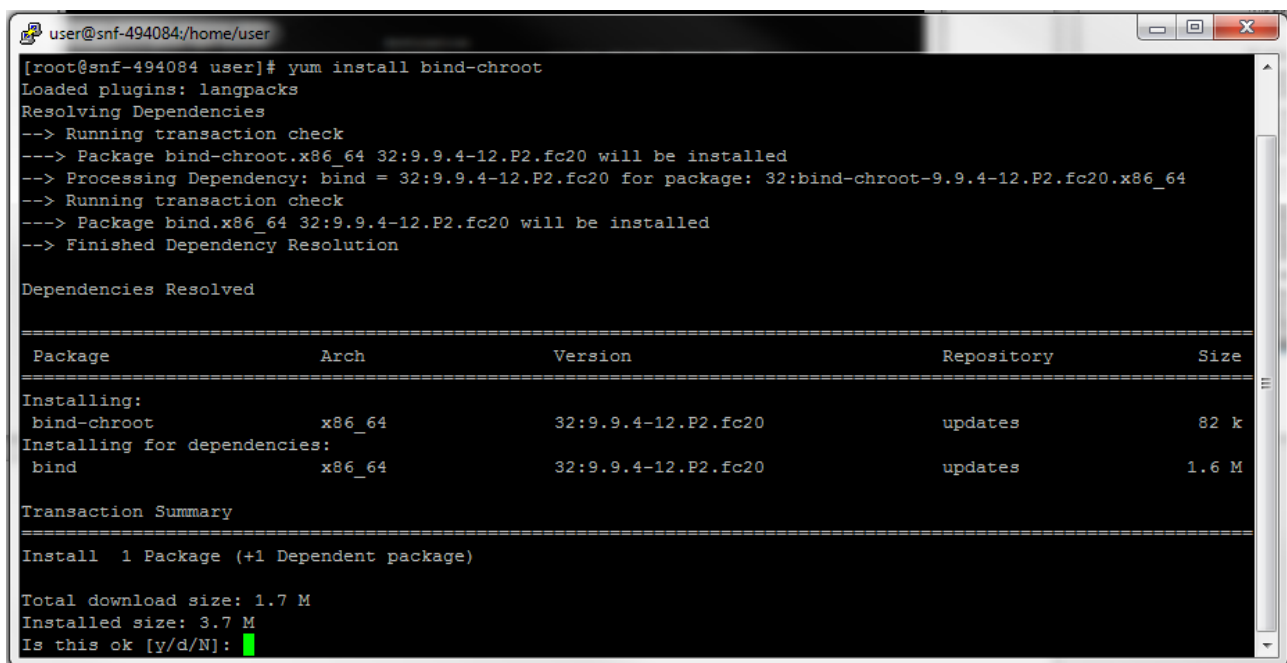
Για τον DNS Server, θα χρησιμοποιήσουμε τον BIND

Αρχικά, ανοίγουμε τις κατάλληλες θύρες για DNS, με τις εντολές **iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT** και **iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT**.

A terminal window with a dark background and light text. The title bar shows 'user@snf-494084:/home/user'. The terminal contains three lines of commands entered by the root user. The first two lines are successful, and the third line is partially visible.

```
[root@snf-494084 user]# iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
[root@snf-494084 user]# iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT
[root@snf-494084 user]#
```

Εγκαθιστούμε τον BIND με την εντολή **yum install bind-chroot**

A terminal window with a dark background and light text. The title bar shows 'user@snf-494084:/home/user'. The terminal shows the output of the 'yum install bind-chroot' command, including dependency resolution and a transaction summary table.

```
[root@snf-494084 user]# yum install bind-chroot
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
--> Package bind-chroot.x86_64 32:9.9.4-12.P2.fc20 will be installed
--> Processing Dependency: bind = 32:9.9.4-12.P2.fc20 for package: 32:bind-chroot-9.9.4-12.P2.fc20.x86_64
--> Running transaction check
--> Package bind.x86_64 32:9.9.4-12.P2.fc20 will be installed
--> Finished Dependency Resolution

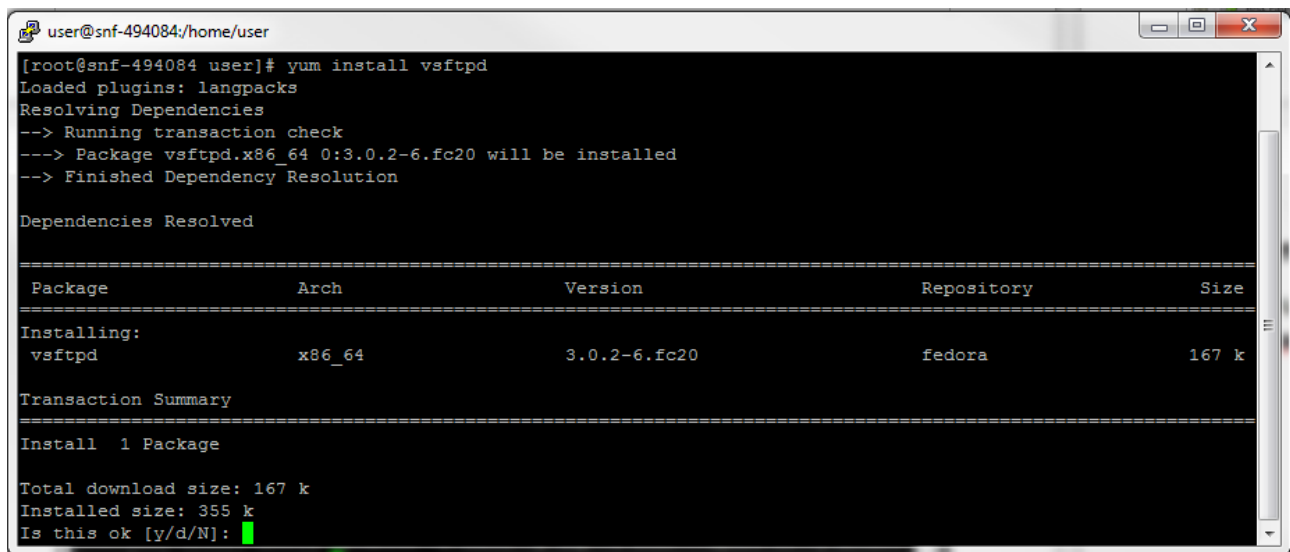
Dependencies Resolved

=====
Package                        Arch          Version              Repository           Size
=====
Installing:
bind-chroot                    x86_64        32:9.9.4-12.P2.fc20  updates             82 k
Installing for dependencies:
bind                           x86_64        32:9.9.4-12.P2.fc20  updates             1.6 M
Transaction Summary
=====
Install 1 Package (+1 Dependent package)

Total download size: 1.7 M
Installed size: 3.7 M
Is this ok [y/d/N]:
```

## FTP Server

Θα χρησιμοποιήσουμε το Very Secure FTP Daemon, χρησιμοποιώντας την εντολή **yum install vsftpd**.



```
user@snf-494084:/home/user
[root@snf-494084 user]# yum install vsftpd
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.x86_64 0:3.0.2-6.fc20 will be installed
--> Finished Dependency Resolution

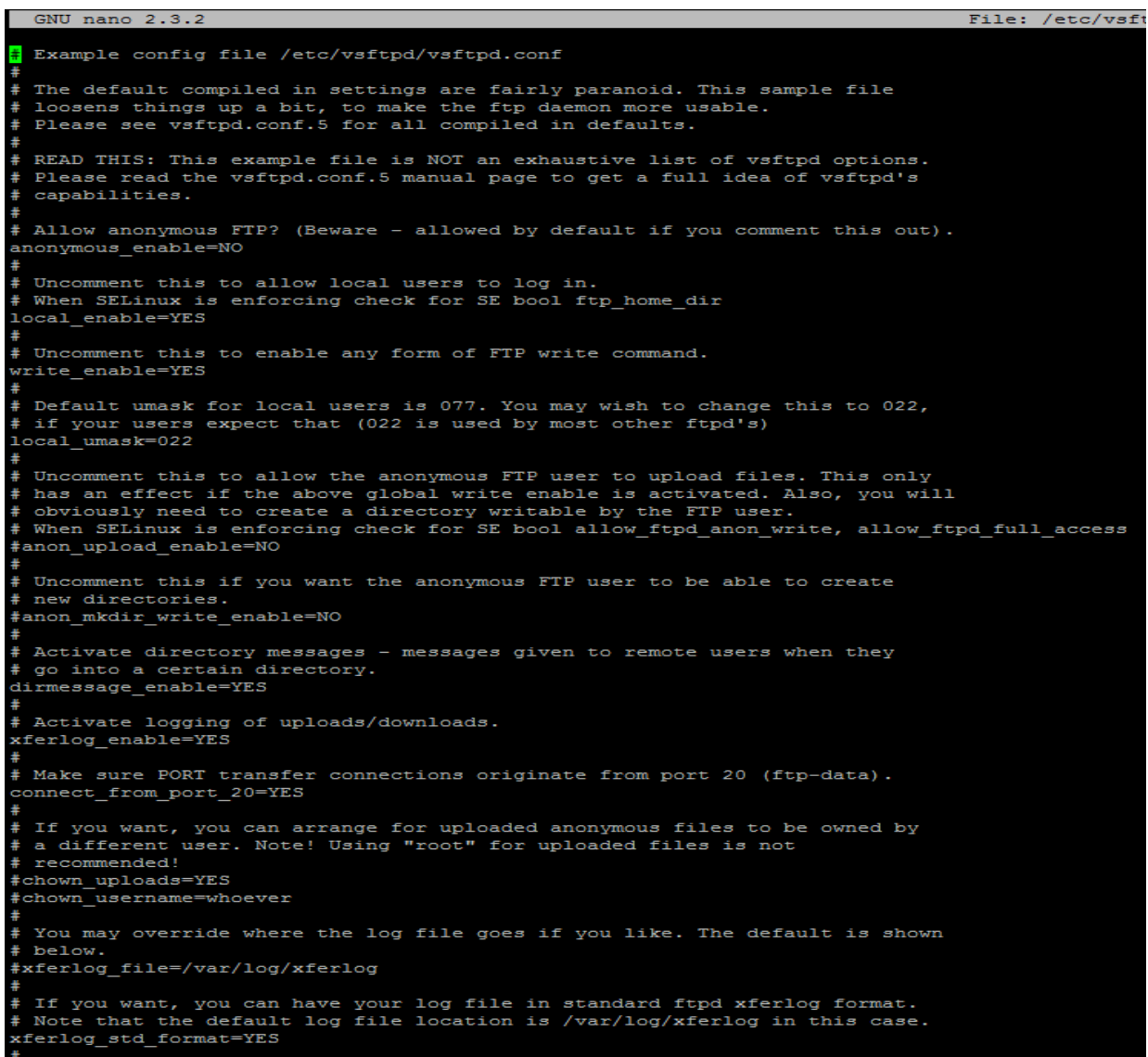
Dependencies Resolved

=====
Package                Arch             Version           Repository        Size
=====
Installing:
vsftpd                  x86_64           3.0.2-6.fc20      fedora            167 k
=====

Transaction Summary
=====
Install 1 Package

Total download size: 167 k
Installed size: 355 k
Is this ok [y/d/N]:
```

Για να ρυθμίσουμε τον server, τρέχουμε την εντολή **nano /etc/vsftpd/vsftpd.conf** και κάνουμε τις αλλαγές που βλέπουμε παρακάτω:



```
GNU nano 2.3.2                                File: /etc/vsftpd
Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
# When SELinux is enforcing check for SE bool ftp_home_dir
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
# When SELinux is enforcing check for SE bool allow_ftpd_anon_write, allow_ftpd_full_access
anon_upload_enable=NO
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=NO
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
chown_uploads=YES
chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
xferlog_file=/var/log/xferlog
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
```

Κάναμε τις εξής αλλαγές:

anonymous\_enable=YES → NO

anon\_upload\_enable=YES → NO

anon\_mkdir\_write\_enable=YES → NO

ascii\_upload\_enable=YES → uncomment

ascii\_download\_enable=YES → uncomment

chroot\_local\_user=YES → uncomment

chroot\_list\_enable=YES → uncomment

ls\_recurse\_enable=YES → uncomment

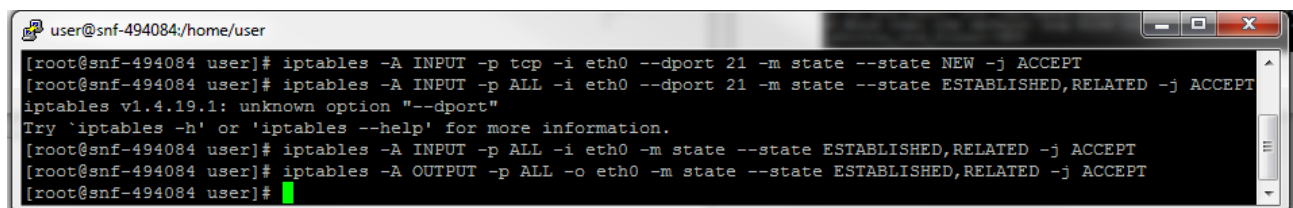
listen=NO → YES

listen\_ipv6=YES → NO

seccomp\_sandbox=YES → NO

Έπειτα, ανοίγουμε τις θύρες για τον FTP, με τις εντολές:

- `iptables -A INPUT -p tcp -i eth0 --dport 21 -m state --state NEW -j ACCEPT`
- `iptables -A INPUT -p ALL -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT`
- `iptables -A OUTPUT -p ALL -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT`



```
user@snf-494084:/home/user
[root@snf-494084 user]# iptables -A INPUT -p tcp -i eth0 --dport 21 -m state --state NEW -j ACCEPT
[root@snf-494084 user]# iptables -A INPUT -p ALL -i eth0 --dport 21 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables v1.4.19.1: unknown option "--dport"
Try 'iptables -h' or 'iptables --help' for more information.
[root@snf-494084 user]# iptables -A INPUT -p ALL -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
[root@snf-494084 user]# iptables -A OUTPUT -p ALL -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
[root@snf-494084 user]#
```

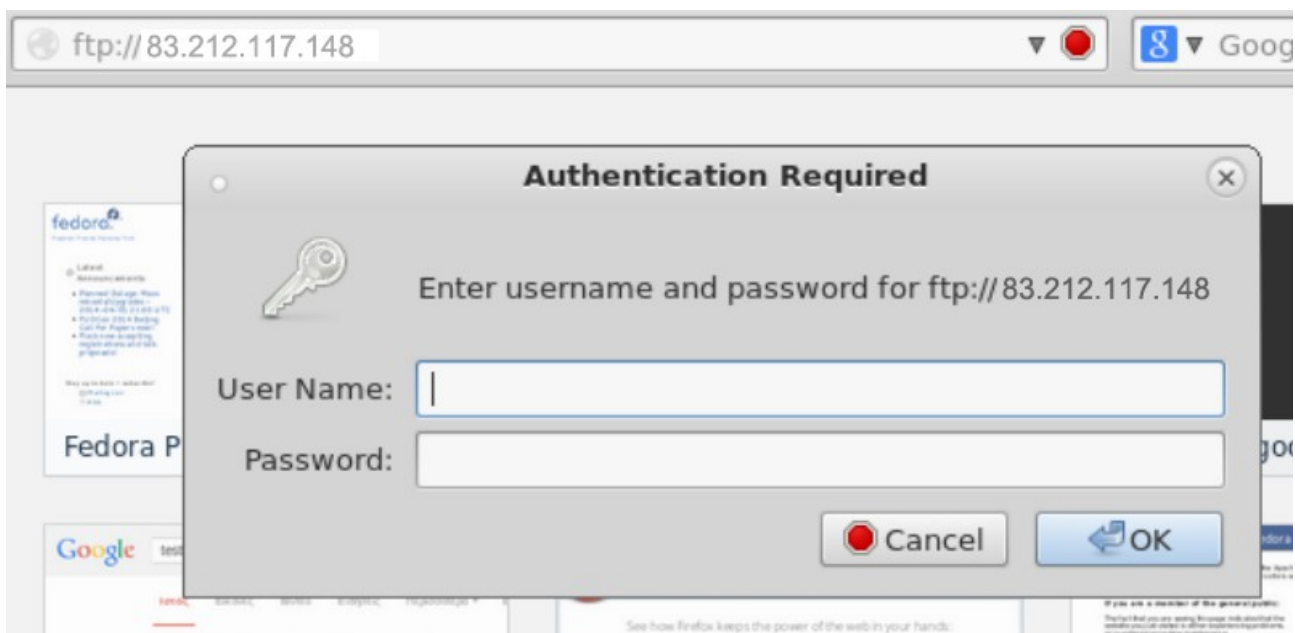
Τελειώνοντας, ξαναρυθμίζουμε τα iptables(προσθέτοντας τα ports του FTP) και, στη συνέχεια, εκτελούμε την εντολή **service vsftpd start**.

- `iptables -A INPUT -p tcp --dport ftp -i eth0 -j ACCEPT`
- `iptables -A INPUT -p udp --dport ftp -i eth0 -j ACCEPT`
- `iptables -A INPUT -p tcp --dport ftp-data -i eth0 -j ACCEPT`
- `iptables -A INPUT -p udp --dport ftp-data -i eth0 -j ACCEPT`

```
user@snf-494084:/home/user
[root@snf-494084 user]# iptables -A INPUT -p tcp --dport ftp -i eth0 -j ACCEPT
[root@snf-494084 user]# iptables -A INPUT -p udp --dport ftp -i eth0 -j ACCEPT
[root@snf-494084 user]# iptables -A INPUT -p udp --dport ftp-data -i eth0 -j ACCEPT
[root@snf-494084 user]# iptables -A INPUT -p tcp --dport ftp-data -i eth0 -j ACCEPT
[root@snf-494084 user]#
```

```
user@snf-494084:/home/user
[root@snf-494084 user]# service vsftpd start
Redirecting to /bin/systemctl start vsftpd.service
[root@snf-494084 user]#
```

Ελέγχουμε αν λειτουργεί σωστά ο FTP Server μας, γράφοντας στο url bar του browser μας `ftp://83.212.117.148`.

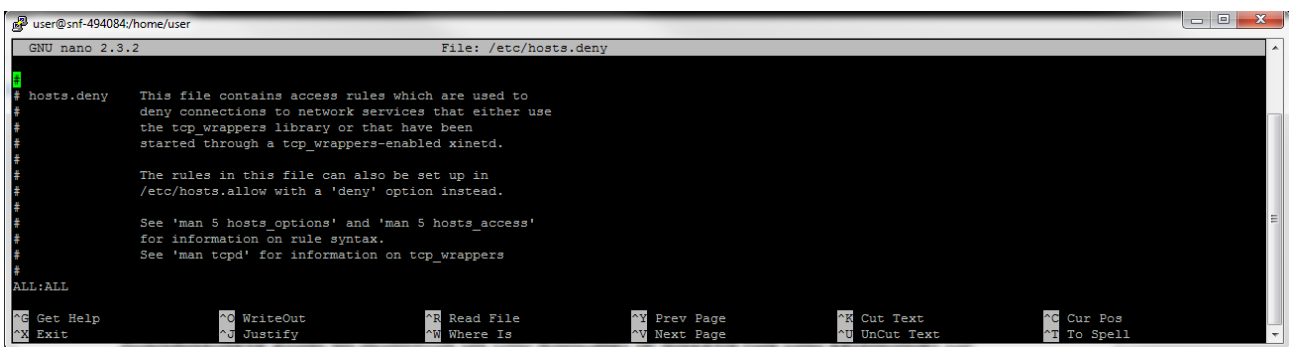


Μας ζητήθηκε μετά να κάνουμε το εξής:

Ρυθμίστε τις παραμέτρους ασφάλειας του πυρήνα. Αυτό που πρέπει σίγουρα να διασφαλίσετε είναι το σύστημα να μην προωθεί IP πακέτα (να μην λειτουργεί ως δρομολογητής).

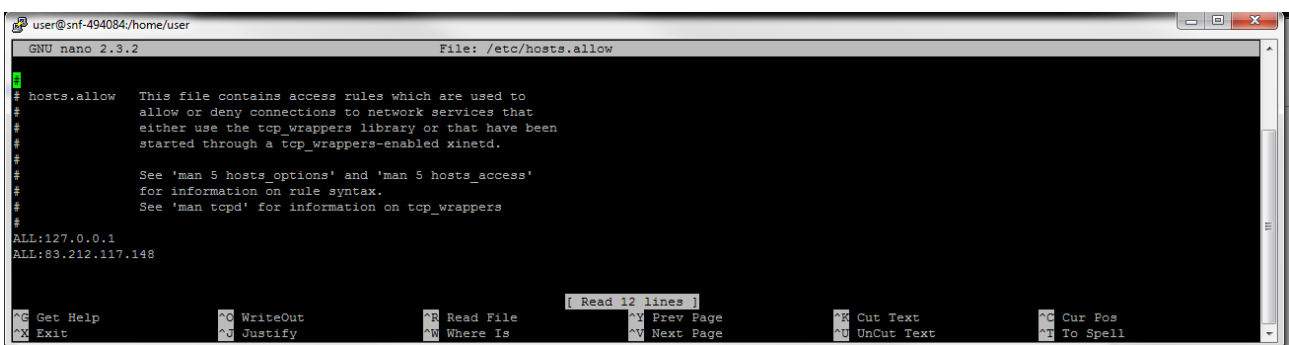
Για να το κάνουμε αυτό, πρέπει να αλλάξουμε(σύμφωνα με το ζητούμενο) τα αρχεία **/etc/hosts.allow** και **/etc/hosts.deny**, έτσι ώστε να επιτρέπονται ή να απαγορεύονται συνδέσεις από συγκεκριμένες IP ή δίκτυα.

Στο αρχείο **/etc/hosts.deny**, προσθέτουμε την γραμμή **ALL:ALL**, ώστε να μην δεχόμαστε τίποτα.



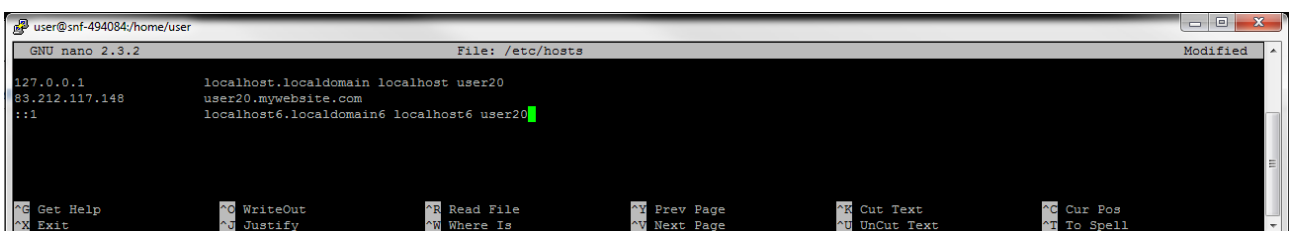
```
GNU nano 2.3.2 File: /etc/hosts.deny
# hosts.deny This file contains access rules which are used to
# deny connections to network services that either use
# the tcp_wrappers library or that have been
# started through a tcp_wrappers-enabled xinetd.
#
# The rules in this file can also be set up in
# /etc/hosts.allow with a 'deny' option instead.
#
# See 'man 5 hosts_options' and 'man 5 hosts_access'
# for information on rule syntax.
# See 'man tcpd' for information on tcp_wrappers
#
ALL:ALL
```

Στο αρχείο **/etc/hosts.allow**, προσθέτουμε τις γραμμές **ALL:127.0.0.1** και **ALL:83.212.117.148**(η δικιά μας IP).



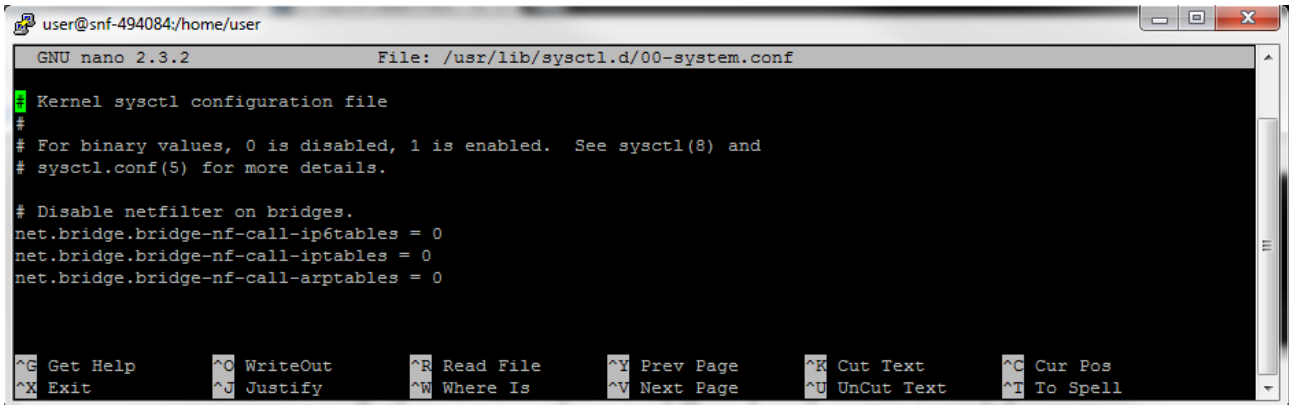
```
GNU nano 2.3.2 File: /etc/hosts.allow
# hosts.allow This file contains access rules which are used to
# allow or deny connections to network services that
# either use the tcp_wrappers library or that have been
# started through a tcp_wrappers-enabled xinetd.
#
# See 'man 5 hosts_options' and 'man 5 hosts_access'
# for information on rule syntax.
# See 'man tcpd' for information on tcp_wrappers
#
ALL:127.0.0.1
ALL:83.212.117.148
```

Τελειώνοντας, τροποποιούμε το αρχείο **/etc/hosts** όπως φαίνεται:



```
GNU nano 2.3.2 File: /etc/hosts Modified
127.0.0.1 localhost localhost6.localdomain6 localhost user20
83.212.117.148 user20.mywebsite.com
::1 localhost6.localdomain6 localhost6 user20
```

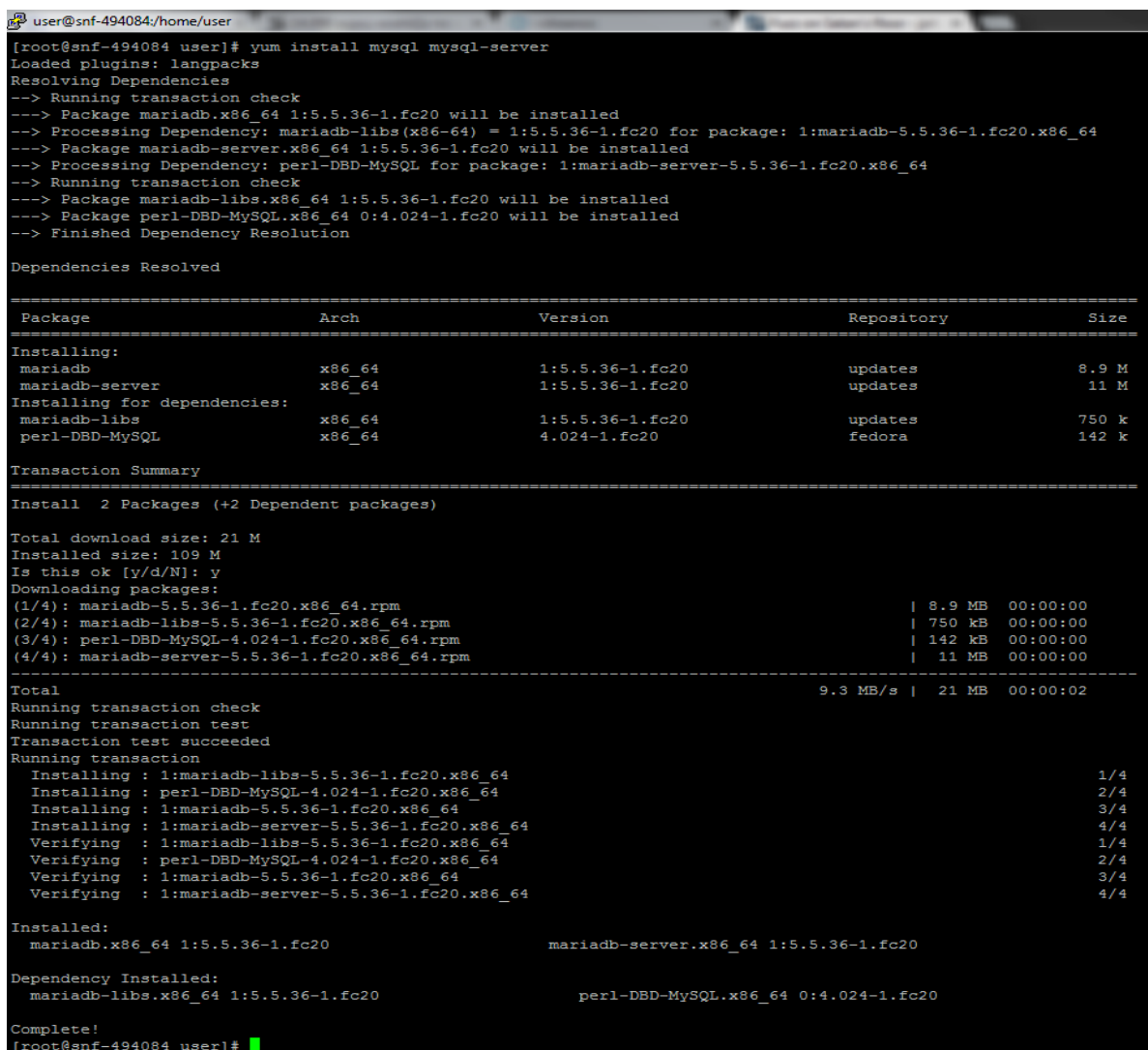
Βλέπουμε ότι η προώθηση πακέτων είναι απενεργοποιημένη(κοιτώντας το αρχείο `/usr/lib/sysctl.d/00-system.conf`)



```
user@snf-494084:/home/user
GNU nano 2.3.2 File: /usr/lib/sysctl.d/00-system.conf
Kernel sysctl configuration file
#
# For binary values, 0 is disabled, 1 is enabled. See sysctl(8) and
# sysctl.conf(5) for more details.
# Disable netfilter on bridges.
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0
^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is    ^V Next Page    ^U UnCut Text   ^T To Spell
```

## Database Server

Εγκαθιστούμε τον MySQL-Server(με την εντολή `yum install mysql mysql-server`)



```
user@snf-494084:/home/user
[root@snf-494084 user]# yum install mysql mysql-server
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
--> Package mariadb.x86_64 1:5.5.36-1.fc20 will be installed
--> Processing Dependency: mariadb-libs(x86-64) = 1:5.5.36-1.fc20 for package: 1:mariadb-5.5.36-1.fc20.x86_64
--> Package mariadb-server.x86_64 1:5.5.36-1.fc20 will be installed
--> Processing Dependency: perl-DBD-MySQL for package: 1:mariadb-server-5.5.36-1.fc20.x86_64
--> Running transaction check
--> Package mariadb-libs.x86_64 1:5.5.36-1.fc20 will be installed
--> Package perl-DBD-MySQL.x86_64 0:4.024-1.fc20 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                                Arch              Version            Repository         Size
=====
Installing:
mariadb                                x86_64            1:5.5.36-1.fc20    updates            8.9 M
mariadb-server                         x86_64            1:5.5.36-1.fc20    updates            11 M
Installing for dependencies:
mariadb-libs                           x86_64            1:5.5.36-1.fc20    updates            750 k
perl-DBD-MySQL                         x86_64            4.024-1.fc20       fedora             142 k
=====

Transaction Summary
-----
Install 2 Packages (+2 Dependent packages)

Total download size: 21 M
Installed size: 109 M
Is this ok [y/d/N]: y
Downloading packages:
(1/4): mariadb-5.5.36-1.fc20.x86_64.rpm | 8.9 MB 00:00:00
(2/4): mariadb-libs-5.5.36-1.fc20.x86_64.rpm | 750 kB 00:00:00
(3/4): perl-DBD-MySQL-4.024-1.fc20.x86_64.rpm | 142 kB 00:00:00
(4/4): mariadb-server-5.5.36-1.fc20.x86_64.rpm | 11 MB 00:00:00
-----
Total                                     9.3 MB/s | 21 MB 00:00:02
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mariadb-libs-5.5.36-1.fc20.x86_64 1/4
  Installing : perl-DBD-MySQL-4.024-1.fc20.x86_64 2/4
  Installing : 1:mariadb-5.5.36-1.fc20.x86_64 3/4
  Installing : 1:mariadb-server-5.5.36-1.fc20.x86_64 4/4
  Verifying : 1:mariadb-libs-5.5.36-1.fc20.x86_64 1/4
  Verifying : perl-DBD-MySQL-4.024-1.fc20.x86_64 2/4
  Verifying : 1:mariadb-5.5.36-1.fc20.x86_64 3/4
  Verifying : 1:mariadb-server-5.5.36-1.fc20.x86_64 4/4

Installed:
  mariadb.x86_64 1:5.5.36-1.fc20                mariadb-server.x86_64 1:5.5.36-1.fc20

Dependency Installed:
  mariadb-libs.x86_64 1:5.5.36-1.fc20          perl-DBD-MySQL.x86_64 0:4.024-1.fc20

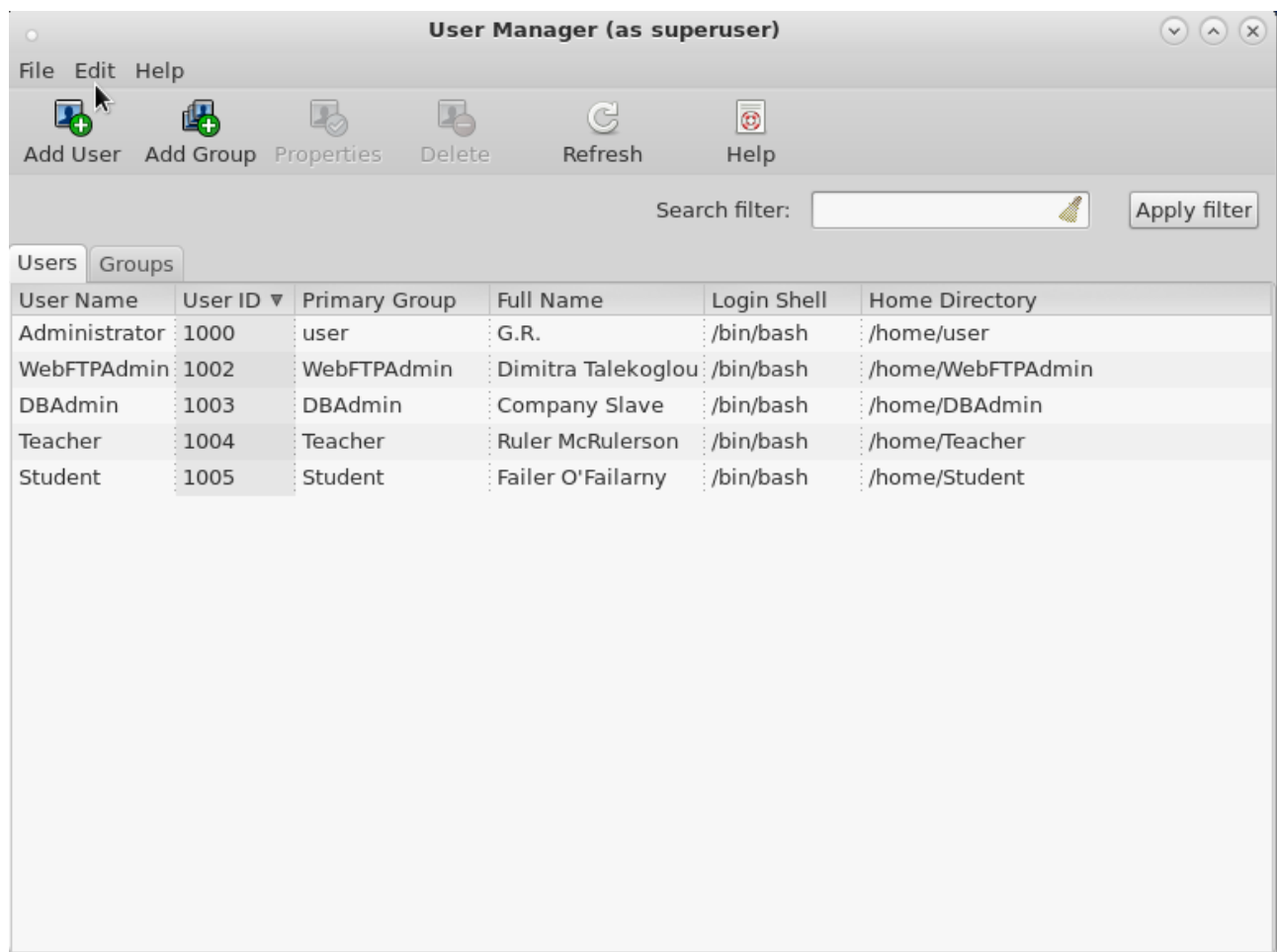
Complete!
[root@snf-494084 user]#
```

## Δημιουργία Χρηστών

### Χρήστες

- System Admin(different than root) – θα τον δημιουργήσω μέσω του Terminal
- Web/FTP Admin
- DB Admin
- Teacher
- Student

Ανοίγουμε το **User Manager**(με την εντολή **system-config-users**) και δημιουργούμε τους 5 χρήστες μας.





Για να δημιουργήσω τον διαχειριστή του συστήματος(**System Admin**), εκτελώ την εντολή **adduser -u 1 -o -g 0 -M SystemAdmin**.

1: User ID

SystemAdmin: username

-M: δεν δημιουργεί κατάλογο /home



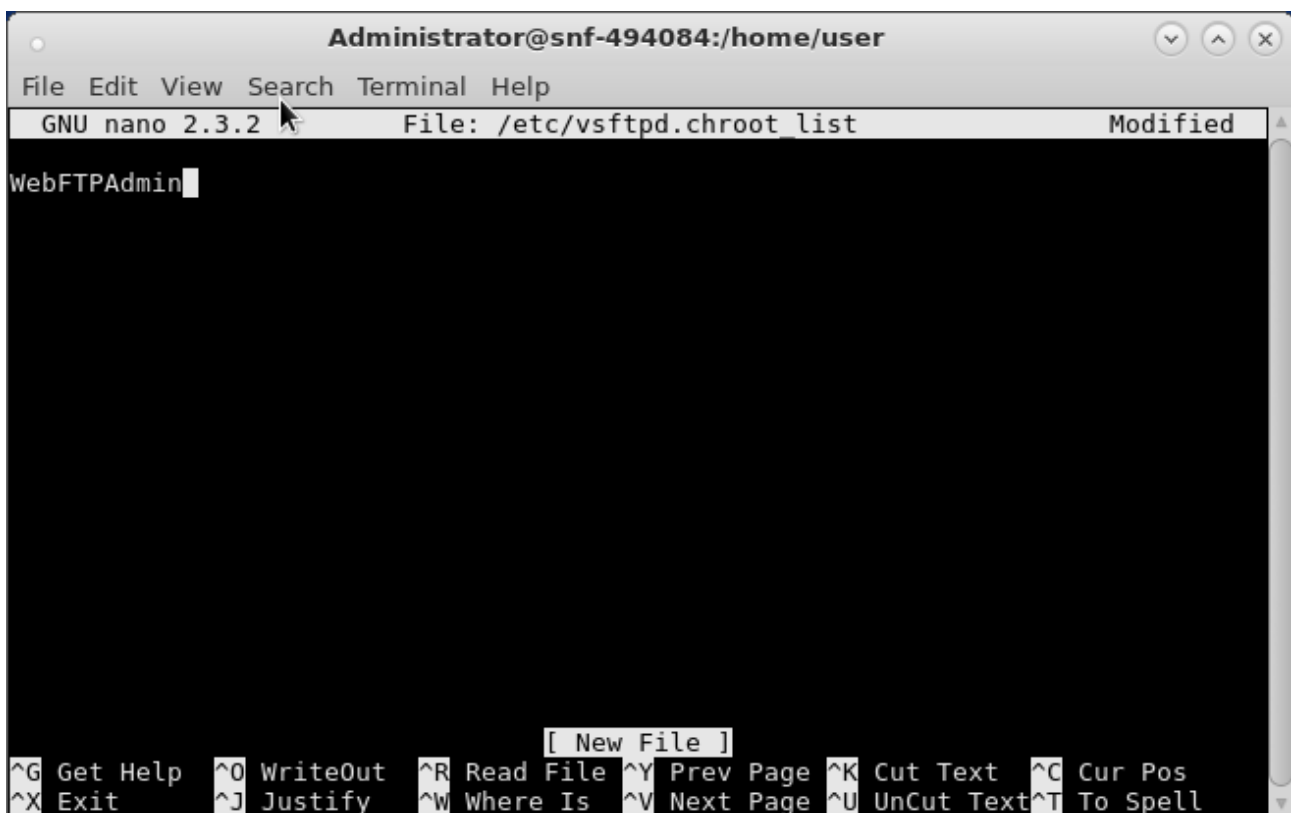
```
Administrator@snf-494084:/home/user
File Edit View Search Terminal Help
[root@snf-494084 user]# adduser -u 1 -o -g 0 -M SystemAdmin
[root@snf-494084 user]#
```

Για να κάνω διαχειριστή του Web/FTP ο χρήστης με username **WebFTPAdmin**, εκτελώ την εντολή **usermod -a -G apache WebFTPAdmin**



```
Administrator@snf-494084:/home/user
File Edit View Search Terminal Help
[root@snf-494084 user]# adduser -u 1 -o -g 0 -M SystemAdmin
[root@snf-494084 user]# usermod -a -G apache WebFTPAdmin
[root@snf-494084 user]#
```

και προσθέτουμε το username του στο αρχείο **/etc/vsftpd.chroot\_list**



```
Administrator@snf-494084:/home/user
File Edit View Search Terminal Help
GNU nano 2.3.2 File: /etc/vsftpd.chroot_list Modified
WebFTPAdmin

[ New File ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

Ζήτημα: Ρυθμίστε το επιτρεπτό όριο αποθηκευτικού χώρου για κάθε

χρήστη(quotas) και ότι άλλους περιορισμούς προτείνετε(επεξεργαστή, μνήμη κλπ.), όπως για παράδειγμα ποιοι χρήστες επιτρέπεται να έχουν απομακρυσμένη πρόσβαση μέσω SSH.

Αρχικά, εγκαθιστώ το quota με την εντολή **yum install quota**.

```
Administrator@snf-494084:/home/user
File Edit View Search Terminal Help
[root@snf-494084 user]# yum install quota
Loaded plugins: langpacks
Package 1:quota-4.01-11.fc20.x86_64 already installed and latest version
Nothing to do
[root@snf-494084 user]#
```

Τροποποιούμε το αρχείο **/etc/fstab** ως εξής:

```
Administrator@snf-494084:/home/user
GNU nano 2.3.2 File: /etc/fstab Modified
#
# /etc/fstab
# Created by anaconda on Tue Feb  4 11:25:28 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=c9390f72-bd00-4139-a3bf-a443d76cc497 / ext4 defaults 1 1
UUID=15665ff6-ad43-430b-bc8a-9ae45b24c1ea /boot ext4 defaults,usrquota,grpquota 1 2
```

Για την ενεργοποίηση των quotas, τρέχουμε τις εξής εντολές:

- **touch /aquota.user /aquota.group**
- **chmod 600 /aquota.\***
- **mount -o remount /**
- **quotacheck -avugm**
- **quotaon -avug**

```
Administrator@snf-494084:/home/user
File Edit View Search Terminal Help
[root@snf-494084 user]# yum install quota
Loaded plugins: langpacks
Package 1:quota-4.01-11.fc20.x86_64 already installed and latest version
Nothing to do
[root@snf-494084 user]# nano /etc/fstab
[root@snf-494084 user]# touch /aquota.user /aquota.group
[root@snf-494084 user]# chmod 600 /aquota.*
[root@snf-494084 user]# mount -o remount /
[root@snf-494084 user]# quotacheck -avugm
bash: quotacheck: command not found
[root@snf-494084 user]# quotachk -avugm
bash: quotachk: command not found
[root@snf-494084 user]# quotacheck -avugm
quotacheck: Cannot find filesystem to check or filesystem not mounted with quota option.
[root@snf-494084 user]# quotaon -avug
[root@snf-494084 user]#
```

Για να δηλώσουμε το ξεχωριστό όριο δίσκου μνήμης για τον κάθε χρήστη, εκτελούμε την εντολή **edquota** “...” (Όπου “...” το username του χρήστη που θέλουμε, π.χ. **edquota WebFTPAdmin**)

Για να απαγορεύσουμε την απομακρυσμένη πρόσβαση στο σύστημά μας στους χρήστες μέσω SSH, ανοίγουμε το αρχείο **/etc/ssh/sshd\_config**, και αλλάζουμε τα εξής:

```
Administrator@snf-494084:/home/user
File Edit View Search Terminal Help
GNU nano 2.3.2 File: /etc/ssh/sshd_config Modified
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 3m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 4
#MaxSessions 10

#RSAAuthentication yes
PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

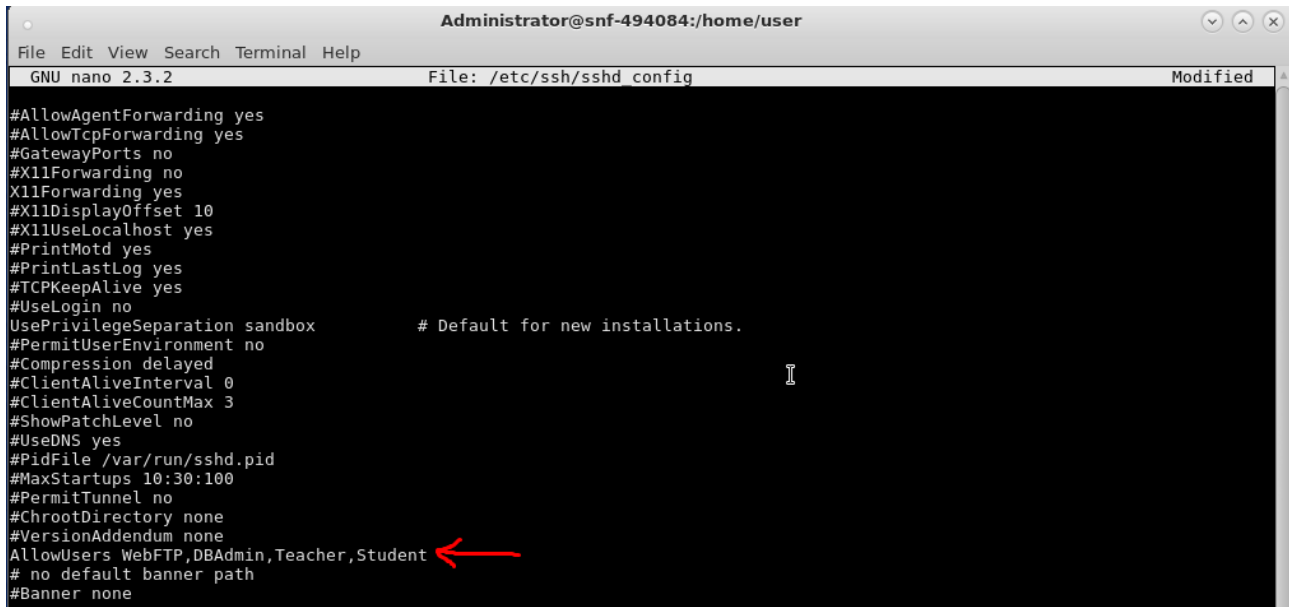
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
```

Έτσι λοιπόν μειώσαμε τις προσπάθειες σύνδεσης από 6 σε 4 φορές, και μπορούμε να έχουμε ταυτόχρονα μέχρι και 10 χρήστες συνδεδεμένους. Επίσης, αποκλείσαμε την σύνδεση από τον root. Παρακάτω βλέπουμε τους χρήστες που αφήνουμε να

χρησιμοποιούν το σύστημά μας με απομακρυσμένη πρόσβαση:



```
Administrator@snf-494084:/home/user
File Edit View Search Terminal Help
GNU nano 2.3.2 File: /etc/ssh/sshd_config Modified
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
UsePrivilegeSeparation sandbox # Default for new installations.
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
AllowUsers WebFTP,DBAdmin,Teacher,Student
# no default banner path
#Banner none
```

Αφού κάνουμε save, ενεργοποιούμε την υπηρεσία με τις εντολές:

- **systemctl start sshd.service**
- **systemctl enable sshd.service**

**Ζήτημα: Ρυθμίστε ποιες πληροφορίες θα καταγράφονται στα αρχεία καταγραφής του συστήματος και πόσο συχνά θα επανεγγράφονται τα αρχεία αυτά(log rotation). Προτείνετε και ρυθμίστε πολιτικές ασφαλεία στο λειτουργικό σύστημα. Περιγράψτε τα εργαλεία/εντολές που χρησιμοποιήσατε για να εφαρμόσετε τις πολιτικές αυτές.**

Τρέχουμε το πρόγραμμα **logrotate**, ανοίγουμε τα αρχεία **/etc/logrotate.conf**(για τα logs του συστήματος) και **/etc/logrotate.d/httpd**(για τα logs του Web Server, αντίστοιχα), και γράφουμε μέσα ποιές πληροφορίες θέλουμε να καταγράφονται και πόσο συχνά.

```
user@snf-494084:~  
File Edit View Search Terminal Help  
GNU nano 2.3.2 File: /etc/logrotate.conf  
  
# see "man logrotate" for details  
# rotate log files weekly  
weekly  
  
# keep 4 weeks worth of backlogs  
rotate 4  
  
# create new (empty) log files after rotating old ones  
create  
  
# use date as a suffix of the rotated file  
dateext  
  
# uncomment this if you want your log files compressed  
#compress  
  
# RPM packages drop log rotation information into this directory  
include /etc/logrotate.d  
  
[ Read 35 lines (Warning: No write permission) ]  
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

```
user@snf-494084:~  
File Edit View Search Terminal Help  
GNU nano 2.3.2 File: /etc/logrotate.d/httpd  
  
/var/log/httpd/*log {  
    missingok  
    notifempty  
    sharedscripts  
    delaycompress  
    postrotate  
        /bin/systemctl reload httpd.service > /dev/null 2>/dev/null || true  
    endscript  
}
```

Τελειώνοντας, εκτελούμε τα rotations με την εντολή **logrotate** **/etc/logrotare.conf**(για το σύστημά μας) και την εντολή **logrotate** **/etc/logrotate.d/http**(για τον Web Server, αντίστοιχα).

### **Βιβλιογραφία-Βοηθητικοί Σύνδεσμοι**

-[http://www.howtoforge.com/perfect-server-fedora-15-x86\\_64-ispconfig-3](http://www.howtoforge.com/perfect-server-fedora-15-x86_64-ispconfig-3)

-<http://www.howtoforge.com/> ← Πολύ καλό website, με πολύ καλά tutorials και καλό community γενικά.

-Google. ← Πολύ, πάρα πολύ, απίστευτα πάρα πολύ Googlάρισμα!

-Διάφορα Linux Forums