

## Εργαστηριακή Άσκηση 10

### Τείχη προστασίας (Firewalls) και NAT

#### Άσκηση 1

1

```
root@PC:~ # sysrc ifconfig_em0="192.168.1.1/24"
ifconfig_em0: -> 192.168.1.1/24
root@PC:~ # sysrc ifconfig_em1="192.0.2.1/30"
ifconfig_em1: -> 192.0.2.1/30
root@PC:~ # defaultrouter="192.0.2.2"
defaultrouter=192.0.2.2: Command not found.
root@PC:~ # sysrc defaultrouter="192.0.2.2"
defaultrouter: NO -> 192.0.2.2
root@PC:~ # sysrc gateway_enable="YES"
gateway_enable: NO -> YES
root@PC:~ # sysrc firewall_enable="YES"
firewall_enable: NO -> YES
root@PC:~ # sysrc firewall_nat_enable="YES"
sysrc: unknown variable 'firewall'
nat_enable: -> YES
root@PC:~ # sysrc firewall_logif="YES"
firewall_logif: NO -> YES
root@PC:~ # █
```

1.1 ifconfig em0 192.168.1.2/24 και ifconfig em0 192.168.1.3/24 στα pc1 και pc2 αντίστοιχα.

1.2 Εκτελούμε στο PC1 "kldload ipfw".

1.3 service ipfw onestatus

1.4 Όχι δε μπορούμε

1.5

```
root@PC:~ # ipfw list
65535 deny ip from any to any
```

1.6 Ο παραπάνω κανόνας είναι ο προκαθορισμένος, ο οποίος απορρίπτει σιωπηλά όλα τα πακέτα. Επιπλέον, με "ipfw show" βλέπουμε και τις τιμές των μετρητών.

1.7 Με "ipfw zero".

1.8

```
root@PC:~ # ipfw add 00100 allow all from any to any via lo0
00100 allow ip from any to any via lo0
root@PC:~ # ipfw show
00100 0 0 allow ip from any to any via lo0
65535 18 1512 deny ip from any to any
```

1.9 Ναι.

1.10 Όχι, παίρνουμε το ίδιο μήνυμα λάθους με πριν.

```
root@PC:~ # ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3): 56 data bytes
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
```

1.11

```
root@PC:~ # ipfw add allow icmp from any to any
00200 allow icmp from any to any
```

1.12 00200, 100 δηλαδή παραπάνω από το προηγούμενο, αφού δε το ορίσαμε ρητά α/α.

1.13 Πετυχαίνουν

1.14 Δε μπορούμε καθώς το traceroute by default χρησιμοποιεί UDP Datagrams, τα οποία και δεν επιτρέπονται να περάσουν από το firewall μας. Αν ωστόσο εκτελέσουμε “traceroute -I 192.168.1.3”, ώστε να στείλουμε ICMP Echo αντ’ αυτών, τότε πετυχαίνει.

1.15 Εκτελούμε “ipfw add allow udp from me to any 33434-33534”.

1.16

```
root@PC:~ # ssh 192.168.1.3
ssh: connect to host 192.168.1.3 port 22: Permission denied
```

1.17 Εκτελούμε “ipfw add allow tcp from any to any established” και “ipfw add allow tcp from me to any setup”.

1.18 Στη συνέχεια “ipfw zero” → “ssh lab@192.168.1.3” → “ls” → “exit”.

1.19

```
root@PC:~ # ipfw show
00100 0 0 allow ip from any to any via lo0
00200 0 0 allow icmp from any to any
00300 0 0 allow udp from me to any 33434-33534
00400 91 12620 allow tcp from any to any established
00500 1 60 allow tcp from me to any setup
65535 49 3384 deny ip from any to any
```

Η πρώτη στήλη μετά τον αριθμό του κανόνα (και εξαιρουμένου του τελευταίου κανόνα, του οποίου οι μετρητές δε μηδενίζονται) δείχνει πόσες φορές εφαρμόστηκε ο κάθε κανόνας στην παραπάνω διαδικασία. Άρα εφαρμόστηκε μία φορά ο κανόνας 00500 (στην τριμερή χειραψία) και 91 φορές ο κανόνας 00400 (κατά τη μεταφορά δεδομένων στη σύνδεση ssh).

**1.20** Δε μπορούμε, καθώς έχουμε επιτρέψει μόνο απερχόμενες tcp συνδέσεις από τον PC1. (00500)

**1.21** Εκτελούμε “service ftpd onestart”.

**1.22** Εκτελούμε στον PC1 “ftp lab@192.168.1.3”, εισάγουμε κωδικό “ntua”, όντας στο FTP prompt εκτελούμε “cd /usr/bin” → “get whatis”. Βλέπουμε πως το αρχείο κατέβηκε κανονικά:

```
ftp> exit
221 Goodbye.
root@PC:~ # ls
.cshrc          .login          .ssh
.k5login        .profile        whatis
```

## Άσκηση 2

**2.1** Στο PC2 “kldload ipfw”

**2.2** Όχι. (Permission denied)

**2.3**

```
root@PC:~ # ipfw add allow all from any to any via lo0
00100 allow ip from any to any via lo0
```

**2.4**

```
root@PC:~ # ipfw add allow icmp from me to any icmp types 8
00200 allow icmp from me to any icmp types 8
```

**2.5** Όχι, αλλά δε λαμβάνουμε Permission Denied αυτή τη φορά.

**2.6** Για να παρατηρήσουμε το φαινόμενο, αρχικά καθαρίζουμε τους μετρητές (“ipfw zero”), στη συνέχεια στέλνουμε ένα ICMP Echo request (“ping -c 1 192.168.1.2”) και μετά εκτελούμε “ipfw show” και βλέπουμε πως ο κανόνας 00200 χρησιμοποιείται μία φορά, επομένως τα πακέτα ICMP όταν είναι εξερχόμενα περνούν το τείχος προστασίας του PC2.

```

root@PC:~ # ping -c 1 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
^C
--- 192.168.1.2 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
root@PC:~ # ipfw show
00100 0 0 allow ip from any to any via lo0
00200 1 84 allow icmp from me to any icmp types 8
65535 104 8736 deny ip from any to any

```

2.7 Ναι, πλέον μπορούμε.

```

root@PC:~ # ipfw delete 00200
root@PC:~ # ipfw add allow icmp from me to any icmp types 8 keep-state
00000 allow icmp from me to any icmp types 8 keep-state :default

```

2.8 Ναι

2.9 Όχι, πλέον δεν επιτυγχάνει. Το Ping πέτυχε προηγουμένως, καθώς η επιλογή keep-state που είχαμε προσθέσει έκανε τη σύνδεση PC1-PC2 stateful με αποτέλεσμα τα Ping του PC1 να περνάνε όσο ο PC2 έστελνε ping.

2.10

```

root@PC:~ # ipfw add allow icmp from any to me icmp types 8 keep-state
00000 allow icmp from any to me icmp types 8 keep-state :default

```

2.11 Βλέπουμε τη χρήση ενός δυναμικού κανόνα κατά την επικοινωνία.

```

root@PC:~ # ipfw -d show
00100 224 54718 allow ip from any to any via lo0
00200 424 35616 allow icmp from me to any icmp types 8 keep-state :default
00300 14 1176 allow icmp from any to me icmp types 8 keep-state :default
65535 110 9240 deny ip from any to any
## Dynamic rules (1 136):
00300 14 1176 (5s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 :default

```

2.12 Πλέον βλέπουμε μόνο του στατικούς κανόνες:

```

root@PC:~ # ipfw -d show
00100 224 54718 allow ip from any to any via lo0
00200 424 35616 allow icmp from me to any icmp types 8 keep-state :default
00300 216 18144 allow icmp from any to me icmp types 8 keep-state :default
65535 110 9240 deny ip from any to any

```

2.13

```

root@PC:~ # ipfw add allow udp from any to me 33434-33534
00400 allow udp from any to me 33434-33534
root@PC:~ # ipfw add allow icmp from me to any icmp types 3
00500 allow icmp from me to any icmp types 3

```

2.14

```
root@PC:~ # ipfw add allow udp from me to any 33434-33534
00600 allow udp from me to any 33434-33534
```

```
root@PC:~ # ipfw add allow icmp from any to me icmp types 3
00700 allow icmp from any to me icmp types 3
```

2.15

```
root@PC:~ # ipfw add allow udp from any to me 33434-33534
00600 allow udp from any to me 33434-33534
```

2.16

```
root@PC2:~ # ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state
00000 allow tcp from 192.168.1.0/24 to me 22 keep-state :default
```

2.17

```
root@PC:~ # ssh lab@192.168.1.3
Password for lab@PC2:
```

2.18

```
root@PC2:~ # ipfw add allow tcp from me to any 22 keep-state
00000 allow tcp from me to any 22 keep-state :default
```

2.19

```
root@PC:~ # ipfw add allow tcp from 192.168.1.3 to me 22
00700 allow tcp from 192.168.1.3 to me 22
```

2.20 Ναι, αφού το sftp τρέχει πάνω από ssh session.

2.21 Δε μπορούμε, οπότε εισάγουμε τον παρακάτω κανόνα:

```
root@PC2:~ # ipfw add allow tcp from any to me 21 setup keep-state
00000 allow tcp from any to me 21 setup keep-state :default
```

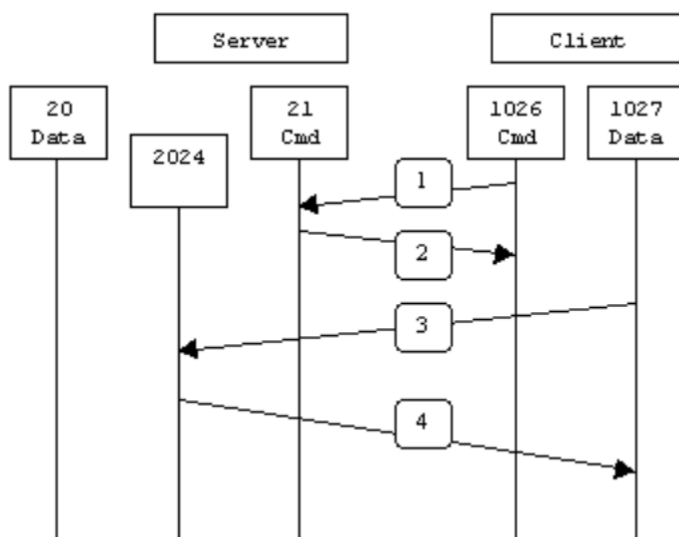
2.22 Έχουμε ενεργοποιήσει μόνο την θύρα 21, η οποία αφορά συνδέσεις Control FTP και όχι την 20 που αφορά FTP data transfer (το οποίο συμβαίνει με την εντολή ls).

```

root@PC:~ # ftp 192.168.1.3
Connected to 192.168.1.3.
220 PC2 FTP server (Version 6.00LS) ready.
Name (192.168.1.3:root): lab
331 Password required for lab.
Password:
230 User lab logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /usr
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||57959|)
ftp: Can't connect to `192.168.1.3:57959': Operation timed out
200 EPRT command successful.
425 Can't build data connection: Permission denied.

```

**2.23** Τον κανόνα “ipfw add allow tcp from any 1024-65535 to me 1024-65535 setup keep-state”, βάσει και του παρακάτω σχήματος.



**2.24** Ναι

**2.25** Εισάγουμε τα παρακάτω στα PC2 και PC1 αντίστοιχα και βλέπουμε πως επιτυγχάνει.

```
root@PC2:~ # ipfw add allow tcp from me 20 to any 1024-65535 setup keep-state
000000 allow tcp from me 20 to any 1024-65535 setup keep-state :default
```

```
root@PC:~ # ipfw add allow tcp from any 20 to me 1024-65535 setup
```

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /usr
250 CWD command successful.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> ls
200 EPRT command successful.
150 Opening ASCII mode data connection for '/bin/ls'.
total 160
drwxr-xr-x  2 root  wheel   8704 Jun 12  2020 bin
drwxr-xr-x  3 root  wheel    512 Mar  9 03:25 home
drwxr-xr-x 54 root  wheel   6656 Jun 12  2020 include
drwxr-xr-x 10 root  wheel  15872 Jun 12  2020 lib
drwxr-xr-x  4 root  wheel    512 Jun 12  2020 lib32
drwxr-xr-x  6 root  wheel    512 Jun 12  2020 libdata
drwxr-xr-x  9 root  wheel   1536 Jun 12  2020 libexec
drwxr-xr-x  2 root  wheel    512 Jun 12  2020 local
drwxr-xr-x  2 root  wheel    512 Jun 12  2020 obj
drwxr-xr-x  2 root  wheel   5632 Jun 12  2020 sbin
drwxr-xr-x 33 root  wheel   1024 Jun 12  2020 share
drwxr-xr-x  2 root  wheel    512 Jun 12  2020 src
drwxr-xr-x 15 root  wheel    512 Jun 12  2020 tests
226 Transfer complete.
```

**2.26** Βλέπουμε πως το ftp μπορεί να αξιοποιεί μεγάλο εύρος θυρών, με αποτέλεσμα εάν κάποιος θέλει να αφήνει ενεργή την υπηρεσία να εκτίθεται σε κίνδυνο λόγω των πολλών ανοιχτών θυρών. Για αυτό θα μπορούσαμε να αξιοποιήσουμε π.χ. δυναμικούς κανόνες, ώστε να επιτρέπεται ανταλλαγή δεδομένων μόνο αφού έχει εγκατασταθεί η σύνδεση.

**2.27** Εκτελούμε στα PC1, PC2 “service ipfw onestop”.

## Άσκηση 3

### 3.1

```
root@PC:~ # hostname PC1
root@PC:~ # ifconfig em0 192.168.1.2/24
root@PC:~ # route add default 192.168.1.1
add net default: gateway 192.168.1.1
```

```
root@PC:~ # hostname PC2
root@PC:~ # ifconfig em0 192.168.1.3/24
root@PC:~ # route add default 192.168.1.1
add net default: gateway 192.168.1.1
```

### 3.2

```

root@router1~# cli

Hello, this is Quagga (version 0.99.17.11).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

router.ntua.lab# configure terminal
router.ntua.lab(config)# hostname R1
R1(config)# interface em0
R1(config-if)# ip address 192.0.2.2/30
R1(config-if)# exit
R1(config)# interface em1
R1(config-if)# ip address 192.0.2.6/30

```

### 3.3

```

root@PC:~ # hostname SRV1
root@PC:~ # ifconfig em0 192.0.2.5/30
root@PC:~ # route add default 192.0.2.6
add net default: gateway 192.0.2.6

```

3.4 Εκτελούμε στα μηχανήματα “service ftpd onestart”.

### 3.5

```

root@FW1:~ # kldstat

```

| Id | Refs | Address    | Size    | Name        |
|----|------|------------|---------|-------------|
| 1  | 11   | 0x8000000  | 18593a0 | kernel      |
| 2  | 1    | 0x16000000 | 6000    | intpm.ko    |
| 3  | 1    | 0x16006000 | 4000    | smbus.ko    |
| 4  | 2    | 0x1600a000 | 30000   | ipfw.ko     |
| 5  | 1    | 0x1603a000 | 6000    | ipfw_nat.ko |
| 6  | 1    | 0x16040000 | 10000   | libalias.ko |

3.6 Το ipfw

### 3.7

```

root@FW1:~ # sysrc firewall_type
firewall_type: UNKNOWN

```

3.8 Βλέπουμε τους παρακάτω 11 κανόνες, με τον τελευταίο να αποτελεί τον default, ο οποίος απορρίπτει σιωπηλά όλα τα πακέτα:



```

root@FW1:~ # ipfw list
00100 allow ip from any to any via lo0
00200 deny ip from any to 127.0.0.0/8
00300 deny ip from 127.0.0.0/8 to any
00400 deny ip from any to ::1
00500 deny ip from ::1 to any
00600 allow ipv6-icmp from :: to ff02::/16
00700 allow ipv6-icmp from fe80::/10 to fe80::/10
00800 allow ipv6-icmp from fe80::/10 to ff02::/16
00900 allow ipv6-icmp from any to any icmp6types 1
01000 allow ipv6-icmp from any to any icmp6types 2,135,136
65535 deny ip from any to any

```

**3.9** Με την εντολή “ipfw nat show config” και βλέπουμε πως δεν υπάρχει κανένας πίνακας.

**3.10** Όχι, σε καμία από τις 2.

**3.11** Όχι.

**3.12**

```

root@FW1:~ # ipfw nat 123 config if em1 unreg_only reset
ipfw nat 123 config if em1 unreg_only reset

```

**3.13**

```

root@FW1:~ # ipfw add nat 123 all from any to any
01100 nat 123 ip from any to any

```

**3.14** Ναι, μπορούμε

**3.15** Εκτελούμε στο R1 “tcpdump -i em0”

**3.16**

```

root@FW1:~ # ipfw show
00100 60 13934 allow ip from any to any via lo0
00200 0 0 deny ip from any to 127.0.0.0/8
00300 0 0 deny ip from 127.0.0.0/8 to any
00400 0 0 deny ip from any to ::1
00500 0 0 deny ip from ::1 to any
00600 0 0 allow ipv6-icmp from :: to ff02::/16
00700 0 0 allow ipv6-icmp from fe80::/10 to fe80::/10
00800 0 0 allow ipv6-icmp from fe80::/10 to ff02::/16
00900 0 0 allow ipv6-icmp from any to any icmp6types 1
01000 0 0 allow ipv6-icmp from any to any icmp6types 2,135,136
01100 690 38556 nat 123 ip from any to any
65535 40 2400 deny ip from any to any
root@FW1:~ # ipfw zero
Accounting cleared.

```

**3.17** Πηγή των ICMP Echo requests εμφανίζεται να είναι η 192.0.2.1, δηλαδή η em1 του FW1.

```
[root@router1]~# tcpdump -i em0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 65535 bytes
03:11:31.218843 IP 192.0.2.1 > 192.0.2.2: ICMP echo request, id 57513, seq 0, length 64
03:11:31.219005 IP 192.0.2.2 > 192.0.2.1: ICMP echo reply, id 57513, seq 0, length 64
03:11:32.226406 IP 192.0.2.1 > 192.0.2.2: ICMP echo request, id 57513, seq 1, length 64
03:11:32.226477 IP 192.0.2.2 > 192.0.2.1: ICMP echo reply, id 57513, seq 1, length 64
03:11:33.238958 IP 192.0.2.1 > 192.0.2.2: ICMP echo request, id 57513, seq 2, length 64
03:11:33.239034 IP 192.0.2.2 > 192.0.2.1: ICMP echo reply, id 57513, seq 2, length 64
```

**3.18** Διεύθυνση προορισμού η 192.0.2.2 (em0 του R1).

**3.19** Υπεύθυνος είναι ο κανόνας “nat 123 ip from any to any”.

**3.20** Βλέπουμε πως εφαρμόστηκε 12 φορές. Συνολικά πέρασαν από το τείχος 6 πακέτα (3 requests και 3 reply), ωστόσο, το κάθε πακέτο μπήκε για μετάφραση κατά την είσοδο και κατά την έξοδό του από αυτό, οπότε και προκύπτει το 12.

```
01100 12 1008 nat 123 ip from any to any
```

**3.21** Ναι

**3.22** Είναι ο ίδιος κανόνας με παραπάνω, ο οποίος χρησιμοποιήθηκε 2 φορές αυτή τη φορά.

```
01100 14 1176 nat 123 ip from any to any
```

**3.23** Ωθείται για μετάφραση, αλλά δεν υπόκειται σε μετάφραση.

**3.24** Ναι

**3.25** Κάνοντας “tcpdump -i em1” βλέπουμε πως ο R1 απαντάει με “host 192.168.1.3 unreachable”, ενώ δε περνάει τίποτα από τον R1 στο WAN1, επομένως είναι πρόβλημα δρομολόγησης, καθώς βλέποντας και τον πίνακα δρομολόγησης του R1 παρατηρούμε πως δεν έχει κατάλληλη εγγραφή για να απαντήσει στο PC2.

```
04:07:09.485345 IP 192.0.2.6 > 192.0.2.5: ICMP host 192.168.1.3 unreachable, length 68
04:07:12.460687 IP 192.0.2.5.25245 > 192.168.1.3.ssh: Flags [S], seq 1734204315, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 3800327175 ecr 0], length 0
```

```

R1(config-if)# do show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo0
C>* 192.0.2.0/30 is directly connected, em0
C>* 192.0.2.4/30 is directly connected, em1

```

### 3.26

```

root@FW1:~ # ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1
.3 192.0.2.1
ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1

```

**3.27** Ναι είναι επιτυχής (“ssh lab@192.0.2.1” από το SRV1) και βλέπουμε από το prompt πως έχουμε συνδεθεί στο PC2.

```
lab@PC2:~ %
```

### 3.28

```

root@FW1:~ # ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1
.3 192.0.2.1 redirect_port tcp 192.168.1.2:22 192.0.2.1:22
ipfw nat 123 config if em1 unreg_only reset redirect_port tcp 192.168.1.2:22 192
.0.2.1:22 redirect_addr 192.168.1.3 192.0.2.1

```

**3.29** Τώρα συνδεθήκαμε στο PC1.

**3.30** ) Εκτελούμε στα PC1 και PC2 “netstat -a” και βλέπουμε στο PC2 πως έχει γίνει σύνδεση ftp, επομένως εκεί συνδέθηκε ο SRV1.

```

Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      0 192.168.1.3.ftp         192.0.2.5.48453        ESTABLISHED

```

**3.31** Ναι

**3.32** Το PC2.

**3.33** Στο PC1.

## Άσκηση 4

**4.1** Και τα 2 ping αποτυγχάνουν

**4.2** Ναι και τα 2 γίνονται αποδεκτά. Αποτυγχάνουν, ωστόσο, αφού απενεργοποιήσαμε το one-pass, οπότε και ελέγχθηκε ο επόμενος κανόνας, ο οποίος εν προκειμένω ήταν ο προκαθορισμένος που απέρριψε τα πακέτα.

#### 4.3

```
root@FW1:~ # ipfw add 1100 allow ip from any to any via em0
01100 allow ip from any to any via em0
```

4.4 Ναι, σε αμφότερες τις διεπαφές.

4.5 Στο FW1.

4.6 Ο κανόνας που εισάγαμε στο 4.3.

#### 4.7

```
root@FW1:~ # ipfw add 3000 nat 123 ip from any to any xmit em1
03000 nat 123 ip from any to any xmit em1
```

#### 4.8

```
root@FW1:~ # ipfw add 3001 allow ip from any to any
03001 allow ip from any to any
```

#### 4.9

```
root@FW1:~ # ipfw add 2000 nat 123 ip from any to any recv em1
02000 nat 123 ip from any to any recv em1
```

#### 4.10

```
root@FW1:~ # ipfw add 2001 check-state
02001 check-state :default
```

4.11 Το FW1.

4.12 Το PC2. Παρακάτω βλέπουμε το tcpdump στο PC2:

```
root@PC:~ # tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:18:59.654977 IP 192.0.2.5 > 192.168.1.3: ICMP echo request, id 23814, seq 0, length 64
06:18:59.655090 IP 192.168.1.3 > 192.0.2.5: ICMP echo reply, id 23814, seq 0, length 64
06:18:59.689893 IP 192.168.1.3.55796 > 62.217.126.164.domain: 5949+ PTR? 5.2.0.192.in-addr.arpa. (40)
06:18:59.691409 IP 192.0.2.2 > 192.168.1.3: ICMP host 62.217.126.164 unreachable, length 36
06:18:59.692005 IP 192.168.1.3.52958 > 194.177.210.210.domain: 5949+ PTR? 5.2.0.192.in-addr.arpa. (40)
06:18:59.693451 IP 192.0.2.2 > 192.168.1.3: ICMP host 194.177.210.210 unreachable, length 36
06:18:59.693879 IP 192.168.1.3.55080 > 62.217.126.164.domain: 5949+ PTR? 5.2.0.192.in-addr.arpa. (40)
06:18:59.695367 IP 192.0.2.2 > 192.168.1.3: ICMP host 62.217.126.164 unreachable, length 36
06:18:59.695785 IP 192.168.1.3.37816 > 194.177.210.210.domain: 5949+ PTR? 5.2.0.192.in-addr.arpa. (40)
06:18:59.697332 IP 192.0.2.2 > 192.168.1.3: ICMP host 194.177.210.210 unreachable, length 36
```

**4.13** Στο FW1.

**4.14** Στο PC1

**4.15** Στο PC2.

**4.16** Ναι.

**4.17** Ναι.

**4.18** Ναι.

**4.19**

```
root@FW1:~ # ipfw add 2999 deny ip from any to any via em1
02999 deny ip from any to any via em1
```

**4.20** Επιτυγχάνουν μόνο τα 4.11 και 4.13, καθώς όλα τα άλλα απαιτούν να εισέλθει κίνηση από το WAN1 μέσω του firewall, πράγμα που απαγορεύσαμε.

**4.21**

```
root@FW1:~ # ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
02500 skipto 3000 icmp from any to any xmit em1 keep-state :default
root@FW1:~ #
```

**4.22** Ναι

**4.23**

```
root@FW1:~ # ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-s
tate
02600 skipto 3000 tcp from any to any 22 out via em1 keep-state :default
```

**4.24** Ναι.

**4.25**

```
root@FW1:~ # ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-stat
e
02100 skipto 3000 icmp from any to any in via em1 keep-state :default
```

**4.26** Το PC2, όπως βλέπουμε με “tcpdump -i em0” στο FW1

```
07:30:12.297065 IP 192.0.2.5 > 192.168.1.3: ICMP echo request, id 60166, seq 40, l
length 64
07:30:12.297232 IP 192.168.1.3 > 192.0.2.5: ICMP echo reply, id 60166, seq 40, l
length 64
```

**4.27** Εκτελούμε “ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keepstate”.

**4.28** Στο PC1.

4.29 Όχι, καθώς απορρίπτεται από τον κανόνα 2999.

4.30 Εισάγουμε τους κανόνες “ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state” και “ipfw add 2700 skipto 3000 tcp from any 20 to any setup xmit em1 keep-state”.

## Άσκηση 5

5.1 192.168.1.1/24.

5.2 10.0.0.1/30.

5.3 67%.

5.4 Τις αναμενόμενες 4.

5.5 172.22.1.1/24.

5.6

|                 |   |
|-----------------|---|
| <b>Hostname</b> | <input type="text" value="fw"/><br>name of the firewall host, without domain part<br>e.g. <i>firewall</i> |
|-----------------|---|


5.7 Κάνουμε την αλλαγή.

5.8 Δεν υπάρχουν κανόνες που να έχουμε ορίσει, ωστόσο by default όλες οι εισερχόμενες συνδέσεις σε αυτή τη διεπαφή θα μπλοκάρονται μέχρι να βάλουμε pass rules.

5.9

| Static IP configuration |  |
|-------------------------|--|
| <b>IP address</b>       | <input type="text" value="192.0.2.1"/> / <input type="text" value="30"/> ▼ |
| <b>Gateway</b>          | <input type="text" value="192.0.2.2"/>                                     |

### 5.10

| Proto   | Source            | Port | Destination | Port | Description            |
|---|-------------------|------|-------------|------|------------------------|
| *   | RFC 1918 networks | *    | *           | *    | Block private networks |
| <p>No rules are currently defined for this interface.<br/>All incoming connections on this interface will be blocked until you add pass rules.</p> <p>Click the  button to add a new rule.</p> |                   |      |             |      |                        |

### 5.11 Όχι

### 5.12 Την ενεργοποιούμε.

### 5.13

|   |  |   |
|---|--|---|
| <b>Enable IPv4 DHCP server on LAN interface</b> |  | <input checked="" type="checkbox"/> <b>Enable</b> |
| <b>Deny unknown clients</b>                     | <input type="checkbox"/> Only respond to reserved clients listed below.              |   |
| <b>Subnet</b>                                   | 192.168.1.0  |   |
| <b>Subnet mask</b>                              | 255.255.255.0  |   |
| <b>Available range</b>                          | 192.168.1.1 - 192.168.1.254  |   |
| <b>Range</b>                                    | <input type="text" value="192.168.1.2"/> to <input type="text" value="192.168.1.3"/> |   |

### 5.14

IP: 192.168.1.2, Default Gateway: 192.168.1.1, DNS server: 192.168.1.1.

**5.15** Προκειμένου να χρησιμοποιηθεί η διεπαφή του FW1 στο LAN1 ως DNS για τους πελάτες DHCP.

**5.16** Στο “dhcp leases”.

**5.17** Τις παρακάτω 6:

## Diagnostics: ARP table

|                          | IP address   | MAC address       | Hostname | Interface |
|--------------------------|--------------|-------------------|----------|-----------|
| <input type="checkbox"/> | 172.22.1.1   | 08:00:27:51:62:02 |          | DMZ       |
| <input type="checkbox"/> | 192.168.56.1 | 0a:00:27:00:00:14 |          | MNG       |
| <input type="checkbox"/> | 192.168.56.2 | 08:00:27:a4:4d:90 |          | MNG       |
| <input type="checkbox"/> | 192.0.2.1    | 08:00:27:f9:b3:17 |          | WAN       |
| <input type="checkbox"/> | 192.168.1.1  | 08:00:27:2b:7e:31 |          | LAN       |
| <input type="checkbox"/> | 192.168.1.2  | 08:00:27:61:be:f7 | PC1      | LAN       |

5.18 Όχι

5.19 Βλέπουμε το αποτυχημένο ping.

### Last 50 firewall log entries

| Act | Time            | If  | Source      | Destination              | Proto |
|-----|-----------------|-----|-------------|--------------------------|-------|
| ✗   | 22:39:02.269073 | LAN | 192.168.1.2 | 192.168.1.1, type echo/0 | ICMP  |

5.20 Τα εξής 5 παρακάτω:

## Diagnostics: Firewall states

### Statistics snapshot control

[Start new](#)

Last statistics snapshot: Never

| Source                       | Port  | Destination                    | Port  | Protocol | Packets | Bytes | TTL     |
|------------------------------|-------|--------------------------------|-------|----------|---------|-------|---------|
| <a href="#">192.168.56.1</a> | 58724 | <a href="#">192.168.56.2</a>   | 80    | tcp      | 3       | 749   | 2:30:00 |
| <a href="#">192.168.56.1</a> | 57621 | <a href="#">192.168.56.255</a> | 57621 | udp      | 2       | 144   | 1:43    |
| <a href="#">192.168.56.1</a> | 57621 | <a href="#">192.168.56.255</a> | 57621 | udp      | 2       | 144   | 1:07    |
| <a href="#">192.168.56.1</a> | 57621 | <a href="#">192.168.56.255</a> | 57621 | udp      | 2       | 144   | 0:07    |
| <a href="#">192.168.56.1</a> | 58725 | <a href="#">192.168.56.2</a>   | 80    | tcp      | 2       | 92    | 2:30:00 |

Firewall connection states displayed: 5

5.21 Κανέναν

5.22



## Firewall: Rules: Edit

|                  |  |
|------------------|--|
| <b>Action</b>    | <div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below.<br/>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p> |
| <b>Disabled</b>  | <div><input type="checkbox"/> <b>Disable this rule</b></div> <p>Set this option to disable this rule without removing it from the list.</p>  |
| <b>Interface</b> | <div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>   |
| <b>Protocol</b>  | <div>any ▾</div> <p>Choose which IP protocol this rule should match.<br/>Hint: in most cases, you should specify <i>TCP</i> here.</p>  |

5.23 Ναι

5.24 Όχι

5.25 Ναι

```
[root@router]~# arp -a
? (192.0.2.2) at 08:00:27:65:a2:78 on em0 permanent [ethernet]
? (192.0.2.1) at 08:00:27:f9:b3:17 on em0 expires in 1186 seconds [ethernet]
```

5.26

## Firewall: Rules: Edit

|                  |  |
|------------------|--|
| <b>Action</b>    | <div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below.<br/>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p> |
| <b>Disabled</b>  | <div><input type="checkbox"/> <b>Disable this rule</b></div> <p>Set this option to disable this rule without removing it from the list.</p>  |
| <b>Interface</b> | <div>WAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>   |
| <b>Protocol</b>  | <div>ICMP ▾</div> <p>Choose which IP protocol this rule should match.<br/>Hint: in most cases, you should specify <i>TCP</i> here.</p>   |
| <b>ICMP type</b> | <div>any ▾</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>  |

5.27 Ναι

5.28 Όχι δε μπορούμε, καθώς ο R1 δεν έχει ούτε default gateway, ούτε κατάλληλη εγγραφή για το δίκτυο του PC1.

5.29 Ναι μπορούμε, αφού το PC1 έχει default gateway και επιπλέον το NAT είναι by default ενεργοποιημένο, επομένως λόγω των stateful κανόνων μπορεί το R1 να απαντήσει.

5.30 Όχι, καθώς ο SRV1 δε μπορεί να δρομολογήσει την απάντηση.

5.31


```
root@SRV1:~ # route add default 172.22.1.1
add net default: gateway 172.22.1.1
```

5.32 Ναι

5.33 Όχι. Δεδομένου πως δεν έχουμε προσθέσει κανόνες στο firewall για το DMZ, όλα τα πακέτα μπλοκάρονται, ενώ προηγουμένως στο 5.32 μπορούσαμε αφού οι κανόνες είναι stateful, οπότε αφού επιτρεπόταν κίνηση από το PC1 προς τον SRV1, επιτρεπόταν και η αντίστροφη.

## Firewall: Rules

**LAN** **WAN** **MNG** **DMZ**

| Proto  | Source | Port | Destination | Port | Description |
|--|--------|------|-------------|------|-------------|
| No rules are currently defined for this interface.<br>All incoming connections on this interface will be blocked until you add pass rules.<br>Click the  button to add a new rule. |        |      |             |      |             |

5.34 Όχι, για τον ίδιο λόγο με το 5.33

5.35

| Proto | Source  | Port | Destination | Port | Description |
|-------|---------|------|-------------|------|-------------|
| *     | DMZ net | *    | ! LAN net   | *    |             |

5.36 Ναι

5.37 Ναι

5.38 Όχι, καθώς δεν υπάρχει αντίστοιχη εγγραφή στον πίνακα δρομολόγησης του R1 αλλά και ούτε προεπιλεγμένη πύλη.

5.39 Ναι γιατί αφενός υπάρχει προεπιλεγμένη πύλη για το SRV1 και αφετέρου έχουν ορισθεί οι απαραίτητοι κανόνες για να επιτραπεί η κίνηση δια μέσου του FW1.

5.40 IP = 192.168.1.3, Default Gateway = 192.168.1.1, DNS = 192.168.1.1

5.41

## Firewall: Rules: Edit

|                   |   |
|-------------------|---|
| Action            | <div>Block ▾</div> <p>Choose what to do with packets that match the criteria specified below.<br/>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p> |
| Disabled          | <div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>  |
| Interface         | <div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>  |
| Protocol          | <div>any ▾</div> <p>Choose which IP protocol this rule should match.<br/>Hint: in most cases, you should specify <i>TCP</i> here.</p>   |
| ICMP type         | <div>any ▾</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>   |
| Source            | <div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>192.168.1.3</div> / <div>▾</div></p>   |
| Source port range | <p>from: <div>any ▾</div> <div></div></p> <p>to: <div>any ▾</div> <div></div></p> <p>Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any").<br/>Hint: you can leave the 'to' field empty if you only want to filter a single port</p>   |
| Destination       | <div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>172.22.1.2</div> / <div>▾</div></p>  |

|   |             |   |            |   |  |
|---|-------------|---|------------|---|--|
| * | 192.168.1.3 | * | 172.22.1.2 | * |  |
|---|-------------|---|------------|---|--|

**5.42** Πρέπει να τοποθετηθεί πριν από τον ήδη υπάρχοντα καθώς οι κανόνες ελέγχονται σειριακά και ο πρώτος κανόνας είναι πιο γενικός, συνεπώς θα περνάει όλη η κίνηση.

**5.43** Όχι

**5.44** Ναι, καθώς απαγορεύσαμε μόνο τη διέλευση από το PC2 προς το SRV1, όχι προς όλο το DMZ.

## Άσκηση 6

**6.1** route add 203.0.118.0/24 192.0.2.1

6.2 Firewall-> NAT -> Outbound -> Enable advanced outbound NAT -> Save

6.3

| Interface | Source         | Destination | Target       | Description |
|-----------|----------------|-------------|--------------|-------------|
| WAN       | 192.168.1.2/32 | *           | 203.0.118.14 |             |

6.4

|     |                |   |              |  |
|-----|----------------|---|--------------|--|
| WAN | 192.168.1.3/32 | * | 203.0.118.15 |  |
|-----|----------------|---|--------------|--|

6.5 tcpdump-iem0

6.6 Μπορούμε να κάνουμε ping από PC1, PC2 στον R1 και τα πακέτα φτάνουν με την διεύθυνση αντιστοίχησης.

6.7 Firewall -> NAT -> Server NAT -> ExternalIP address: 203.0.118.18.

6.8

### Firewall: NAT: Edit

|                     |  |
|---------------------|--|
| Interface           | <div>WAN ▾</div> <div>Choose which interface this rule applies to.<br/>Hint: in most cases, you'll want to use WAN here.</div>   |
| External address    | <div>203.0.118.18 () ▾</div> <div>If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define IP addresses on the <a href="#">Server NAT</a> page first).</div>   |
| Protocol            | <div>TCP ▾</div> <div>Choose which IP protocol this rule should match.<br/>Hint: in most cases, you should specify <i>TCP</i> here.</div>  |
| External port range | <div>from: SSH ▾ <input type="text"/></div> <div>to: SSH ▾ <input type="text"/></div> <div>Specify the port or port range on the firewall's external address for this mapping.<br/>Hint: you can leave the 'to' field empty if you only want to map a single port</div>                            |
| NAT IP              | <div>172.22.1.2 <input type="text"/></div> <div>Enter the internal IP address of the server on which you want to map the ports.<br/>e.g. 192.168.1.12</div>  |
| Local port          | <div>SSH ▾ <input type="text"/></div> <div>Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).<br/>Hint: this is usually identical to the 'from' port above</div> |
| Description         | <div><input type="text"/></div> <div>You may enter a description here for your reference (not parsed).</div>   |

☒ Auto-add a firewall rule to permit traffic through this NAT rule

Save

| If  | Proto | Ext. port range | NAT IP                                | Int. port range | Description |
|-----|-------|-----------------|---------------------------------------|-----------------|-------------|
| WAN | TCP   | 22 (SSH)        | 172.22.1.2<br>(ext.:<br>203.0.118.18) | 22 (SSH)        |             |

## 6.9

|     |   |   |            |             |     |
|-----|---|---|------------|-------------|-----|
| TCP | * | * | 172.22.1.2 | 22<br>(SSH) | NAT |
|-----|---|---|------------|-------------|-----|

**6.10** Ναι μπορούμε, συνδεόμαστε στο SRV1 λόγω του κανόνα NAT που δημιουργήσαμε προηγουμένως

**6.11** Όχι, καθώς ο κανόνας που προσθέσαμε αφορά μόνο για ssh σύνδεση (διαφορετική tcp θύρα)

**6.12** Μπορούμε να συνδεθούμε Για τα IP πακέτα ακολουθείται η παρακάτω διαδρομή: Το PC2 στέλνει τα IP πακέτα για το 203.0.118.18 στην προεπιλεγμένη πύλη του, δηλαδή το FW1, το οποίο με τη σειρά του, δεδομένου ότι δεν έχει εγγραφή στον ARP πίνακα για το 203.0.118.18, το προωθεί στη δική του προεπιλεγμένη πύλη, δηλαδή το R1. Ωστόσο, στον R1 προσθέσαμε στατική εγγραφή για το 203.0.118.0/24 μέσω του FW1, οπότε επαναλαμβάνεται αυτή η κίνηση μεταξύ FW1 και R1 μέχρι να μηδενιστεί το TTL.

```
root@PC2:~ # ssh lab@203.0.118.18
The authenticity of host '203.0.118.18 (203.0.118.18)' can't be established.
ECDSA key fingerprint is SHA256:JUpmw5WmgsBzQBplyYvDw01DobJBD/Ts2aysBLX5zqo.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '203.0.118.18' (ECDSA) to the list of known hosts.
Password for lab@SRV1:
```

```
root@PC2:~ # traceroute 203.0.118.18
traceroute to 203.0.118.18 (203.0.118.18), 64 hops max, 40 byte packets
 1 fw1.lab.ntua.gr (192.168.1.1) 1.205 ms 1.073 ms 0.921 ms
 2 192.0.2.2 (192.0.2.2) 2.514 ms 1.875 ms 2.102 ms
 3 * * *
```

**6.13** Όχι δεν μπορούμε να κάνουμε ping γιατί υπάρχει εγγραφή στο τείχος προστασίας που μπλοκάρει πακέτα από private addresses.

**6.14** Ναι, πλέον γίνεται η αντιστοίχιση με τη διεύθυνση της διεπαφής του FW1 στο WAN1 και τα πακέτα που φθάνουν στον R1 έχουν διεύθυνση 192.0.2.1.

**6.15** Από το PC2 δεν μπορούμε γιατί υπάρχει κανόνας που μπλοκάρει τη σχετική κίνηση.

**6.16** tcpdump -i em0 -e. ssh [lab@172.22.1.2](#)

Connection refused από το τείχος προστασίας

**6.17** Υπεύθυνος είναι ο κανόνας Block που θέσαμε στην ερώτηση 5.41 καθώς παρατηρούμε ότι δεν φθάνουν πακέτα στα μηχανήματα R1, SRV1. Συνεπώς μπλοκάρονται από το τείχος προστασίας.

## Άσκηση 7

**7.1** Αποσυνδέουμε το καλώδιο.

**7.2** Κάνουμε την αλλαγή και μετά πρέπει να συνδεθούμε στο “http://192.168.56.2”:

### Interfaces: Optional 1 (MNG)

|  |  |                      |
|--|--|----------------------|
| <b>Primary configuration</b>   |  | <b>Secondary IPs</b> |
| <input checked="" type="checkbox"/> <b>Enable Optional 1 interface</b>                 |  |                      |
| Description  | <input type="text" value="MNG"/><br>Enter a description (name) for the interface here. |                      |
| <b>IP configuration</b>  |  |                      |
| Bridge with  | <input type="text" value="none"/> ▼  |                      |
| IP address   | <input type="text" value="192.168.56.3"/> / <input type="text" value="24"/> ▼          |                      |
| <input type="button" value="Save"/>  |  |                      |
| <b>Note:</b><br>be sure to add firewall rules to permit traffic through the interface. |  |                      |

**7.3** Επανασυνδέουμε τις κάρτες.

**7.4** Ναι μπορούμε, στα “http://192.168.56.2” για το FW1 και στο “http://192.168.56.3” για το FW2.

**7.5**

### System: General setup

|                 |  |
|-----------------|--|
| <b>Hostname</b> | <input type="text" value="fw2"/><br>name of the firewall host, without domain part<br>e.g. <i>firewall</i> |
|-----------------|--|

**7.6** Κάνουμε τις αλλαγές.

7.7 Κάνουμε τις αλλαγές.

7.8 Κάνουμε reboot το FW2.

```
Copyright (C) 2002-2012 by Manuel Kasper. All rights reserved.
Visit http://m0n0.ch/wall for updates.

LAN IP address: 192.168.1.1
WAN IP address: 10.0.0.1

Port configuration:

LAN    -> em0
WAN    -> em1
OPT1   -> em2 (MNG)
OPT2   -> em3 (DMZ)

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 5
```

7.9 Προσθέτουμε τον κανόνα.

## Firewall: Rules: Edit

|           |  |
|-----------|--|
| Action    | <div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below.<br/>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p> |
| Disabled  | <div><input type="checkbox"/> <b>Disable this rule</b></div> <p>Set this option to disable this rule without removing it from the list.</p>  |
| Interface | <div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>   |
| Protocol  | <div>any ▾</div> <p>Choose which IP protocol this rule should match.<br/>Hint: in most cases, you should specify <i>TCP</i> here.</p>  |

7.10



## Firewall: Rules



The changes have been applied successfully.

LAN

WAN

MNG

DMZ



| Proto | Source | Port | Destination | Port | Description |
|-------|--------|------|-------------|------|-------------|
| ICMP  | *      | *    | *           | *    |             |



pass



block



reject



log



pass (disabled)



block (disabled)



reject (disabled)



log (disabled)

### 7.11

```
root@PC:~ # ifconfig em0 192.168.2.2/24
root@PC:~ # route add default 192.168.2.1
add net default: gateway 192.168.2.1
```

### 7.12 Ναι

### 7.13 Ναι

7.14 Η επικοινωνία αμφίδρομα είναι αδύνατη, καθώς ο R1 δε μπορεί να δρομολογήσει τα πακέτα. Παρουσιάζουμε τον πίνακα δρομολόγησής του:

```
R1(config)# do show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo0
C>* 192.0.2.0/30 is directly connected, em0
C>* 192.0.2.4/30 is directly connected, em1
S>* 203.0.118.0/24 [1/0] via 192.0.2.1, em0
```

### 7.15 VPN -> IPsec -> Enable IPsec


| Local net<br>Remote net | Interface<br>Remote<br>gw | P1<br>mode | P1 Enc.<br>Algo | P1 Hash<br>Algo | Description |
|-------------------------|---------------------------|------------|-----------------|-----------------|-------------|
| LAN<br>192.168.2.0/24   | WAN<br>192.0.2.5          | main       | 3DES            | SHA-1           |             |









### 7.16









## Firewall: Rules

**LAN** **WAN** **IPsec VPN** **MNG** **DMZ**

|  | Proto | Source | Port | Destination | Port | Description       |
|--|-------|--------|------|-------------|------|-------------------|
| <input type="checkbox"/>  | *     | *      | *    | *           | *    | Default IPsec VPN |

 pass  block  reject  log  
 pass (disabled)  block (disabled)  reject (disabled)  log (disabled)



     



7.17 Όχι


7.18 Ναι

## Diagnostics: IPsec

**SAD** **SPD**

|                          | Source         | Destination    | Direction   | Protocol | Tunnel endpoints      |
|--------------------------|----------------|----------------|---|----------|-----------------------|
| <input type="checkbox"/> | 192.168.2.0/24 | 192.168.1.0/24 |  | ESP      | 192.0.2.5 - 192.0.2.1 |
| <input type="checkbox"/> | 192.168.1.0/24 | 192.168.2.0/24 |  | ESP      | 192.0.2.1 - 192.0.2.5 |

 incoming (as seen by firewall)  
 outgoing (as seen by firewall)





7.19 Κάνουμε τα ζητούμενα



7.20 Όχι


7.21 Ναι

## Diagnostics: IPsec

**SAD** **SPD**

|                          | Source         | Destination    | Direction   | Protocol | Tunnel endpoints      |
|--------------------------|----------------|----------------|---|----------|-----------------------|
| <input type="checkbox"/> | 192.168.1.0/24 | 192.168.2.0/24 |  | ESP      | 192.0.2.1 - 192.0.2.5 |
| <input type="checkbox"/> | 192.168.2.0/24 | 192.168.1.0/24 |  | ESP      | 192.0.2.5 - 192.0.2.1 |

 incoming (as seen by firewall)  
 outgoing (as seen by firewall)



7.22 Ναι

7.23 Ναι

7.24 Ναι

**SAD** **SPD**

|                          | Source    | Destination | Protocol | SPI      | Enc. alg. | Auth. alg. |
|--------------------------|-----------|-------------|----------|----------|-----------|------------|
| <input type="checkbox"/> | 192.0.2.1 | 192.0.2.5   | ESP      | 09b46935 | 3des-cbc  | hmac-sha1  |
| <input type="checkbox"/> | 192.0.2.5 | 192.0.2.1   | ESP      | 03f204eb | 3des-cbc  | hmac-sha1  |

7.25 Ναι

### Diagnostics: IPsec

**SAD** **SPD**

|                          | Source    | Destination | Protocol | SPI      | Enc. alg. | Auth. alg. |
|--------------------------|-----------|-------------|----------|----------|-----------|------------|
| <input type="checkbox"/> | 192.0.2.5 | 192.0.2.1   | ESP      | 03f204eb | 3des-cbc  | hmac-sha1  |
| <input type="checkbox"/> | 192.0.2.1 | 192.0.2.5   | ESP      | 09b46935 | 3des-cbc  | hmac-sha1  |

7.26 Εκτελούμε “tcpdump -vni em0” στον R1

7.27 Όχι

7.28 Εμφανίζονται πακέτα ESP. Το παραπάνω στιγμιότυπο είναι από το Ping του PC1 προς το PC2 και βλέπουμε πως εμφανίζεται ως διεύθυνση αποστολέα η 192.0.2.1 (διεπαφή WAN1 του FW1) και ως παραλήπτη η 192.0.2.5 (διεπαφή WAN2 του FW2).

7.29 Δε βλέπουμε κάποια σχετική πληροφορία.

7.30 Ναι μπορούμε.

7.31 Παρατηρούμε πακέτα τύπου TCP με πηγή την 192.0.2.5:56067 και προορισμό την 203.0.118.18:22 και αντιστρόφως.

```
21:21:28.133691 IP (tos 0x10, ttl 62, id 0, offset 0, flags [DF], proto TCP (6),  
  length 52)  
    192.0.2.5.56067 > 203.0.118.18.ssh: Flags [.], cksum 0xd88f (correct), seq 2  
371, ack 3743, win 1023, options [nop,nop,TS val 945363177 ecr 338549452], lengt  
h 0  
21:21:28.137178 IP (tos 0x10, ttl 63, id 0, offset 0, flags [DF], proto TCP (6),  
  length 104)  
    203.0.118.18.ssh > 192.0.2.5.56067: Flags [P.], cksum 0xc798 (correct), seq  
3743:3795, ack 2371, win 1026, options [nop,nop,TS val 338549452 ecr 945363177],  
  length 52
```

**7.32** Είναι μεν κρυπτογραφημένα, αλλά όχι με το IPsec, αλλά με το SSH.