ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 10: ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ (FIREWALLS) ΚΑΙ NAT

24 ΜΑΙΟΥ, 2023

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

Ονοματεπώνυμο: Θοδωρής Αράπης	**Ομάδα:** 3
Όνομα PC/ΛΣ: DESKTOP-JGHL94V/ WINDOWS 10	**Ημερομηνία:** 24/5/2023

Προετοιμασία στο σπίτι

Παραμετροποιούμε κατάλληλα:

```
root@PC:~ # sysrc -a
defaultrouter: 192.0.2.2
firewall_enable: YES
firewall_logif: YES
firewall_nat_enable: YES
gateway_enable: YES
hostname: FW1
ifconfig_em0: 192.168.1.1/24
ifconfig_em1: 192.0.2.1/30
sshd_enable: YES
syslogd_flags: -scc
```

Άσκηση 1: Ένα απλό τείχος προστασίας

1.1

Εκτελούμε στο PC1 "**kldload ipfw**".

1.2

```
root@PC1:~ # kldstat
Id Refs Address                Size Name
 1    7 0x800000  196d6e4 kernel
 2    1 0xf400000     6000 intpm.ko
 3    1 0xf406000     4000 smbus.ko
 4    1 0xf40a000    2d000 ipfw.ko
```

ή

```
root@PC1:~ # service ipfw onestatus
ipfw is enabled
```

1.3

Όχι δε μπορούμε.

```
root@PC1:~ # ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
^C
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
root@PC1:~ # ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

Βλέπουμε ως μήνυμα λάθους “Permission denied”.

1.4

```
root@PC1:~ # ipfw list
65535 deny ip from any to any
```

1.5

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

```
root@PC1:~ # ipfw show
65535 12 1008 deny ip from any to any
```

1.6

Με “**ipfw zero**”.

1.7

```
root@PC1:~ # ipfw add 00100 allow all from any to any via lo0
00100 allow ip from any to any via lo0
root@PC1:~ # ipfw show
00100  0    0 allow ip from any to any via lo0
65535 12 1008 deny ip from any to any
```

1.8

Ναι.

1.9

Όχι, παίρνουμε το ίδιο μήνυμα λάθους με πριν.

```
root@PC1:~ # 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
^C
--- 192.168.1.3 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

1.10

```
root@PC1:~ # ipfw add allow icmp from any to any
00200 allow icmp from any to any
```

1.11

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

1.12

Πετυχαίνουν αμφότερα.

1.13

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.

```
root@PC1:~ # traceroute 192.168.1.3
traceroute to 192.168.1.3 (192.168.1.3), 64 hops max, 40 byte packets
traceroute: sendto: Permission denied
 1 traceroute: wrote 192.168.1.3 40 chars, ret=-1
^C
root@PC1:~ # traceroute -I 192.168.1.3
traceroute to 192.168.1.3 (192.168.1.3), 64 hops max, 48 byte packets
 1  192.168.1.3 (192.168.1.3)  0.327 ms  0.167 ms  0.141 ms
```

1.14

Εκτελούμε "**ipfw add allow udp from me to any 33434-33534**".

1.15

```
root@PC1:~ # ssh 192.168.1.3
ssh: connect to host 192.168.1.3 port 22: Permission denied
```

1.16

Εκτελούμε "**ipfw add allow tcp from any to any established**" και "**ipfw add allow tcp from me to any setup**".

1.17

Εκτελούμε "**ipfw zero**" → "**ssh lab@192.168.1.3**" → "**ls**" → "**exit**".

```
root@PC1:~ # 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  0    0 allow tcp from any to any established
00500  0    0 allow tcp from me to any setup
65535 17 1360 deny ip from any to any
```

1.18

```
root@PC1:~ # 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 75 13700 allow tcp from any to any established
00500  1    60 allow tcp from me to any setup
65535 17  1360 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 75 φορές ο κανόνας 00400 (κατά τη μεταφορά δεδομένων στη σύνδεση ssh).

1.19

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

```
root@PC2:~ # ssh lab@192.168.1.2
ssh: connect to host 192.168.1.2 port 22: Operation timed out
```

1.20

Εκτελούμε "**service ftpd onestart**".

1.21

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> get whatis
local: whatis remote: whatis
229 Entering Extended Passive Mode (|||57849|)
150 Opening BINARY mode data connection for 'whatis' (382048 bytes).
100% |**********************************|   373 KiB   51.79 MiB/s    00:00 ETA
226 Transfer complete.
382048 bytes received in 00:00 (50.37 MiB/s)
ftp> exit
221 Goodbye.
root@PC1:~ # ls
.cshrc          .lesshst        .profile        whatis
.k5login        .login          .ssh
```

Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

2.1

Στο PC2 "**kldload ipfw**".

2.2

Όχι. (Permission denied)

```
root@PC2:~ # ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

2.3

```
root@PC2:~ # ipfw add allow all from any to any via lo0
00100 allow ip from any to any via lo0
```

2.4

Από το man page του ipfw βρίσκουμε:

```
icmptypes types
        Matches ICMP packets whose ICMP type is in the list types.  The
        list may be specified as any combination of individual types
        (numeric) separated by commas.  Ranges are not allowed.  The
        supported ICMP types are:

        echo reply (0), destination unreachable (3), source quench (4),
        redirect (5), echo request (8), router advertisement (9), router
        solicitation (10), time-to-live exceeded (11), IP header bad
        (12), timestamp request (13), timestamp reply (14), information
        request (15), information reply (16), address mask request (17)
        and address mask reply (18).
```

Οπότε τρέχουμε την ακόλουθη εντολή:

```
root@PC2:~ # ipfw add allow icmp from me to any icmptypes 8
00200 allow icmp from me to any icmptypes 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.

```
Accounting cleared.
root@PC2:~ # ipfw show
00100  0    0 allow ip from any to any via lo0
00200  0    0 allow icmp from me to any icmptypes 8
65535 12 1008 deny ip from any to any
root@PC2:~ # 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@PC2:~ # ipfw show
00100  0    0 allow ip from any to any via lo0
00200  1   84 allow icmp from me to any icmptypes 8
65535 13 1092 deny ip from any to any
```

2.7

Ναι, πλέον μπορούμε

```
root@PC2:~ # ipfw delete 00200
root@PC2:~ # ipfw add allow icmp from me to any icmptypes 8 keep-state
00000 allow icmp from me to any icmptypes 8 keep-state :default
root@PC2:~ # ping -c 1 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.517 ms

--- 192.168.1.2 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.517/0.517/0.517/0.000 ms
```

2.8

Ναι, μπορούμε.

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

Εκτελούμε "**ipfw add icmp allow from any to me icmptypes 8 keep-state**".

2.11

Βλέπουμε τη χρήση ενός δυναμικού κανόνα κατά την επικοινωνία.

```
root@PC2:~ # ipfw -d show
00100    0     0 allow ip from any to any via lo0
00200 1154 96936 allow icmp from me to any icmptypes 8 keep-state :default
00300   26  2184 allow icmp from any to me icmptypes 8 keep-state :default
65535   18  1512 deny ip from any to any
## Dynamic rules (1 136):
00300   26  2184 (5s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 :default
```

2.12

Πλέον βλέπουμε μόνο τους στατικούς κανόνες:

```
root@PC2:~ # ipfw -d show
00100    0     0 allow ip from any to any via lo0
00200 1154 96936 allow icmp from me to any icmptypes 8 keep-state :default
00300   84  7056 allow icmp from any to me icmptypes 8 keep-state :default
65535   18  1512 deny ip from any to any
```

2.13

```
root@PC2:~ # ipfw add allow udp from any to me 33434-33534
00400 allow udp from any to me 33434-33534
root@PC2:~ # ipfw add allow icmp from me to any icmptypes 3
00500 allow icmp from me to any icmptypes 3
```

2.14

```
root@PC2:~ # ipfw add allow udp from me to any 33434-33534
00600 allow udp from me to any 33434-33534
root@PC2:~ # ipfw add allow icmp from any to me icmptypes 3
00700 allow icmp from any to me icmptypes 3
```

2.15

```
root@PC1:~ # 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@PC1:~ # ssh lab@192.168.1.3
(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@PC1:~ # 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.

```
root@PC1:~ # sftp lab@192.168.1.3
(lab@192.168.1.3) Password for lab@PC2:
Connected to 192.168.1.3.
sftp> get /etc/rc.conf
Fetching /etc/rc.conf to rc.conf
rc.conf                                       100%  153   176.8KB/s   00:00
sftp> exit
```

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
```

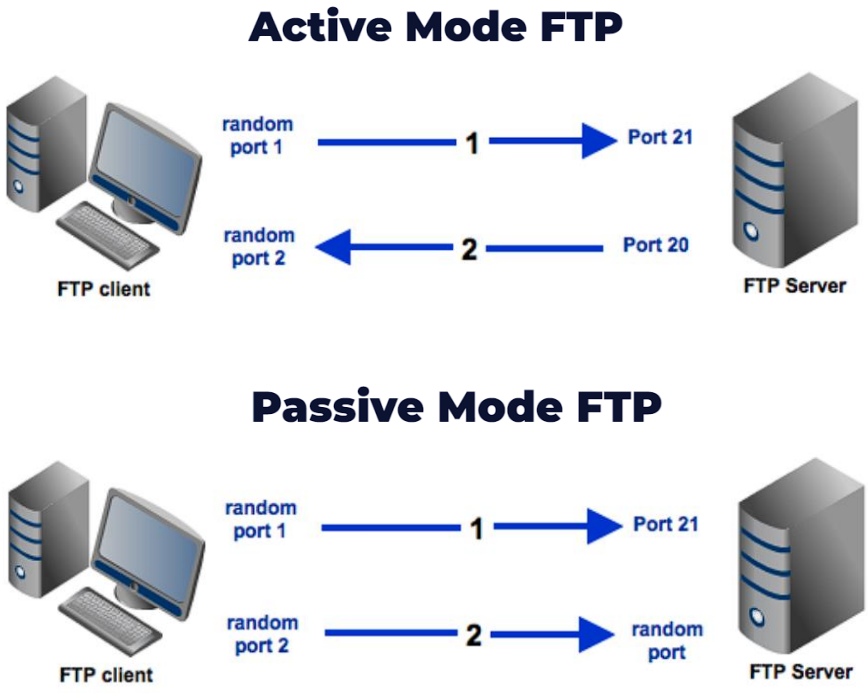
2.22

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@PC1:~ # ftp lab@192.168.1.3
Connected to 192.168.1.3.
220 PC2 FTP server (Version 6.00LS) ready.
331 Password required for lab.
Password:
230- No directory! Logging in with home=/.
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 (|||56071|)
ftp: Can't connect to `192.168.1.3:56071': 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.

```
root@PC1:~ # ftp lab@192.168.1.3
Connected to 192.168.1.3.
220 PC2 FTP server (Version 6.00LS) ready.
331 Password required for lab.
Password:
230- No directory! Logging in with home=/.
230 User lab logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get /usr/bin/whereis
local: /usr/bin/whereis remote: /usr/bin/whereis
229 Entering Extended Passive Mode (|||65376|)
150 Opening BINARY mode data connection for '/usr/bin/whereis' (13652 bytes).
100% |***********************************| 13652      147.94 MiB/s    00:00 ETA
226 Transfer complete.
13652 bytes received in 00:00 (46.00 MiB/s)
```

2.25

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

```
root@PC1:~ # ipfw add allow tcp from any 20 to me 1024-65535 setup
00800 allow tcp from any 20 to me 1024-65535 setup
```

```
root@PC2:~ # ipfw add allow tcp from me 20 to any 1024-65535 setup keep-state
00000 allow tcp from me 20 to any 1024-65535 setup keep-state :default
```

```
root@PC1:~ # ftp lab@192.168.1.3
Connected to 192.168.1.3.
220 PC2 FTP server (Version 6.00LS) ready.
331 Password required for lab.
Password:
230- No directory! Logging in with home=/.
230 User lab logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
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 85
-rw-r--r--   2 root  wheel     1089 Nov 30 07:34 .cshrc
-rw-r--r--   2 root  wheel      470 Nov 30 07:34 .profile
drwxrwxr-x   2 root  operator   512 Nov 30 07:28 .snap
-r--r--r--   1 root  wheel     6177 Nov 30 07:34 COPYRIGHT
drwxr-xr-x   2 root  wheel     1024 Nov 30 07:29 bin
drwxr-xr-x  10 root  wheel     1536 Mar 12 18:40 boot
dr-xr-xr-x  15 root  wheel      512 May 22 16:31 dev
-rw-------   1 root  wheel     4096 May 22 16:31 entropy
drwxr-xr-x  26 root  wheel     2560 May 22 16:31 etc
lrwxr-xr-x   1 root  wheel        8 Mar 12 18:13 home -> usr/home
drwxr-xr-x   5 root  wheel     1536 Nov 30 07:30 lib
drwxr-xr-x   3 root  wheel      512 Nov 30 07:29 libexec
drwxr-xr-x   2 root  wheel      512 Nov 30 07:28 media
drwxr-xr-x   2 root  wheel      512 Nov 30 07:28 mnt
drwxr-xr-x   2 root  wheel      512 Nov 30 07:28 net
```

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**".

```
root@PC1:~ # service ipfw onestop
root@PC1:~ # service ipfw onestatus
ipfw is not enabled
```

```
root@PC2:~ # service ipfw onestop
root@PC2:~ # service ipfw onestatus
ipfw is not enabled
```

Άσκηση 3: Απλό Network Address Translation

3.1

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

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

3.2

```
[root@router]~# 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
R1(config-if)# exit
```

3.3

```
root@SRV1:~ # hostname SRV1
root@SRV1:~ # ifconfig em0 192.0.2.5/30
root@SRV1:~ # 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 0x800000   196d6e4 kernel
 2    1 0xf400000     6000 intpm.ko
 3    1 0xf406000     4000 smbus.ko
 4    2 0xf40a000     2d000 ipfw.ko
 5    1 0xf437000     6000 ipfw_nat.ko
 6    1 0xf43d000     f000 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 show
00100 96 8128 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
65535  0    0 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 και στις 2.

3.15

Εκτελούμε στο R1 "**tcpdump -i em0**"

3.16

```
root@FW1:~ # ipfw show
00100 96 8128 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  6  504 nat 123 ip from any to any
65535  6  504 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 $em1_{FW1}$.

```
[root@router]~# 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
02:54:01.498378 IP 192.0.2.1 > 192.0.2.2: ICMP echo request, id 63406, seq 0, le
ngth 64
02:54:01.498488 IP 192.0.2.2 > 192.0.2.1: ICMP echo reply, id 63406, seq 0, leng
th 64
02:54:02.570752 IP 192.0.2.1 > 192.0.2.2: ICMP echo request, id 63406, seq 1, le
ngth 64
02:54:02.570774 IP 192.0.2.2 > 192.0.2.1: ICMP echo reply, id 63406, seq 1, leng
th 64
02:54:03.642359 IP 192.0.2.1 > 192.0.2.2: ICMP echo request, id 63406, seq 2, le
ngth 64
02:54:03.642380 IP 192.0.2.2 > 192.0.2.1: ICMP echo reply, id 63406, seq 2, leng
th 64
```

3.18

Διεύθυνση προορισμού των ICMP Echo reply είναι η 192.0.2.1 ($em1_{FW1}$).

3.19

Υπεύθυνος είναι ο κανόνας "**nat 123 ip from any to any**".

```
root@FW1:~ # ipfw show
00100  0     0 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 12  1008 nat 123 ip from any to any
65535  6   504 deny 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.

3.21

Ναι μπορούμε.

3.22

Είναι ο ίδιος κανόνας με παραπάνω, ο οποίος χρησιμοποιήθηκε 2 φορές αυτή τη φορά, για 2 echo request.

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

3.23

Ωθείται μεν 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.

```
[root@router]~# tcpdump -i em1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em1, link-type EN10MB (Ethernet), capture size 65535 bytes
03:38:08.279770 IP 192.0.2.5.28127 > 192.68.1.3.ssh: Flags [S], seq 2334387584,
win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 3681314264 ecr 0], lengt
h 0
03:38:08.279972 IP 192.0.2.6 > 192.0.2.5: ICMP host 192.68.1.3 unreachable, leng
th 68
03:38:09.291882 IP 192.0.2.5.28127 > 192.68.1.3.ssh: Flags [S], seq 2334387584,
win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 3681315280 ecr 0], lengt
h 0
```

```
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
```

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 για το password πως έχουμε συνδεθεί στο PC2.

```
root@SRV1:~ # ssh lab@192.0.2.1
(lab@192.0.2.1) Password for 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 και το βλέπουμε από το prompt.

```
root@SRV1:~ # ssh lab@192.0.2.1
(lab@192.0.2.1) Password for lab@PC1:
```

3.30

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

3.31

Ναι μπορούμε.

3.32

```
root@PC2:~ # netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 192.168.1.3.ftp       192.0.2.5.53795        ESTABLISHED
tcp4       0      0 *.ftp                 *.*                    LISTEN
tcp6       0      0 *.ftp                 *.*                    LISTEN
tcp4       0      0 localhost.smtp        *.*                    LISTEN
tcp4       0      0 *.ssh                 *.*                    LISTEN
tcp6       0      0 *.ssh                 *.*                    LISTEN
udp4       0      0 *.syslog              *.*
```

Το PC2.

3.33

Στο PC1.

Άσκηση 4: Τείχος προστασίας και NAT

4.1

Όχι, 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 προ-καθορισμένος που απέρριψε τα πακέτα.

4.3

```
root@FW1:~ # ipfw add 01100 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@PC2:~ # tcpdump -vi em0
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 262144 byte
s
16:26:28.550014 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.3
 tell 192.168.1.1, length 46
16:26:28.550035 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.3 is-at 08:
00:27:f4:91:03 (oui Unknown), length 28
16:26:28.550203 IP (tos 0x0, ttl 62, id 18446, offset 0, flags [none], proto ICM
P (1), length 84)
    192.0.2.5 > 192.168.1.3: ICMP echo request, id 28675, seq 0, length 64
16:26:28.550218 IP (tos 0x0, ttl 64, id 52407, offset 0, flags [none], proto ICM
P (1), length 84)
    192.168.1.3 > 192.0.2.5: ICMP echo reply, id 28675, seq 0, length 64
```

Όπως βλέπουμε παρακάτω, ο κανόνας 01100 εφαρμόστηκε 6 φορές για τα 3 ICMP Echo request που στείλαμε από το PC1 στο 192.0.2.1, 2 φορές εφαρμόστηκε ο ίδιος κανόνας για το ping από το SRV1 στο PC2 και από μία φορά οι κανόνες 02000 και 03000 για το ίδιο ping.

```
root@FW1:~ # May 23 16:28:51 FW1 login[914]: ROOT LOGIN (root) ON ttyv1
ipfw show
00100 0   0 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 8 672 allow ip from any to any via em0
02000 1  84 nat 123 ip from any to any recv em1
02001 0   0 check-state :default
03000 1  84 nat 123 ip from any to any xmit em1
03001 2 168 allow ip from any to any

65535 9 756 deny ip from any to any
```

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 02999 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
```

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 -vi em0**" στο FW1.

```
root@PC2:~ # tcpdump -vi em0
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 262144 byte
s
17:25:12.230046 IP (tos 0x0, ttl 62, id 18501, offset 0, flags [none], proto ICM
P (1), length 84)
    192.0.2.5 > 192.168.1.3: ICMP echo request, id 57603, seq 0, length 64
17:25:12.230066 IP (tos 0x0, ttl 64, id 52430, offset 0, flags [none], proto ICM
P (1), length 84)
    192.168.1.3 > 192.0.2.5: ICMP echo reply, id 57603, seq 0, length 64
```

4.27

Εκτελούμε "**ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state**".

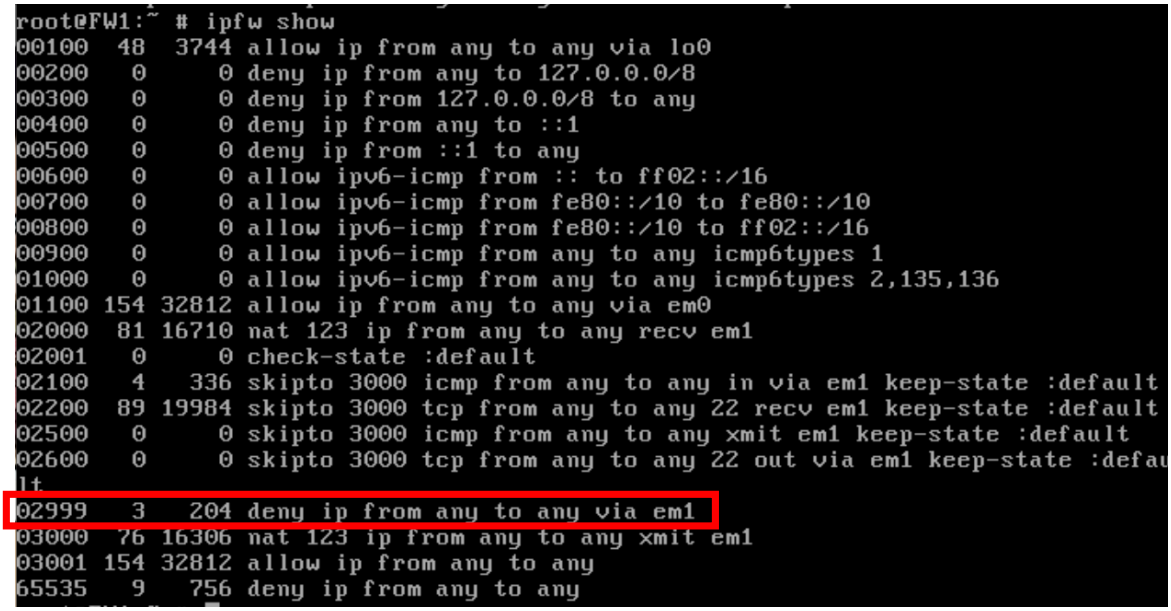
4.28

Στο PC1.

```
root@SRV1:~ # ssh lab@192.0.2.1
(lab@192.0.2.1) Password for lab@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: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

5.1

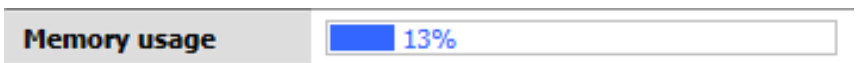
192.168.1.1/24

5.2

10.0.0.1/30.

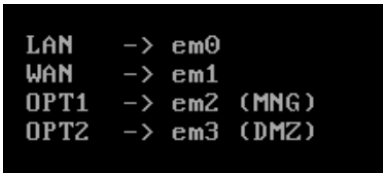
5.3

87%



5.4

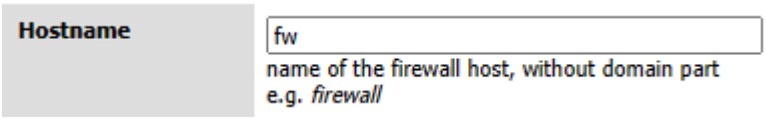
Τις αναμενόμενες 4.



5.5

172.22.1.1/24.

5.6

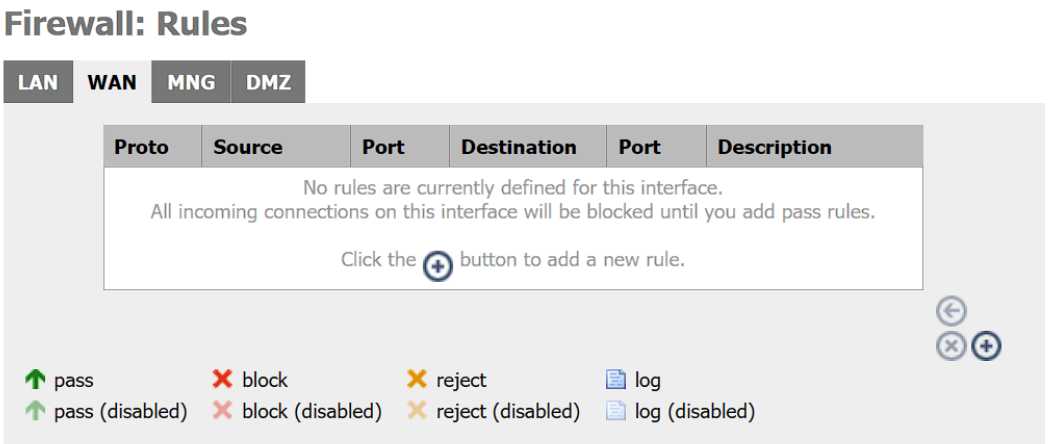


5.7

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.

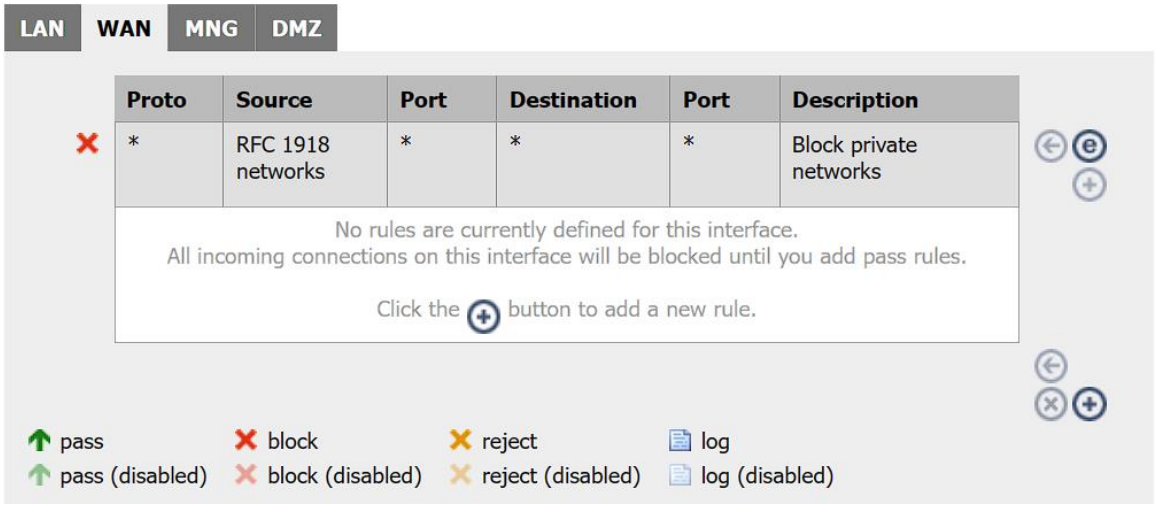


5.9

Static IP configuration	
IP address	192.0.2.1 / 30
Gateway	192.0.2.2

5.10

Ναι, υπάρχει ο παρακάτω κανόνας:



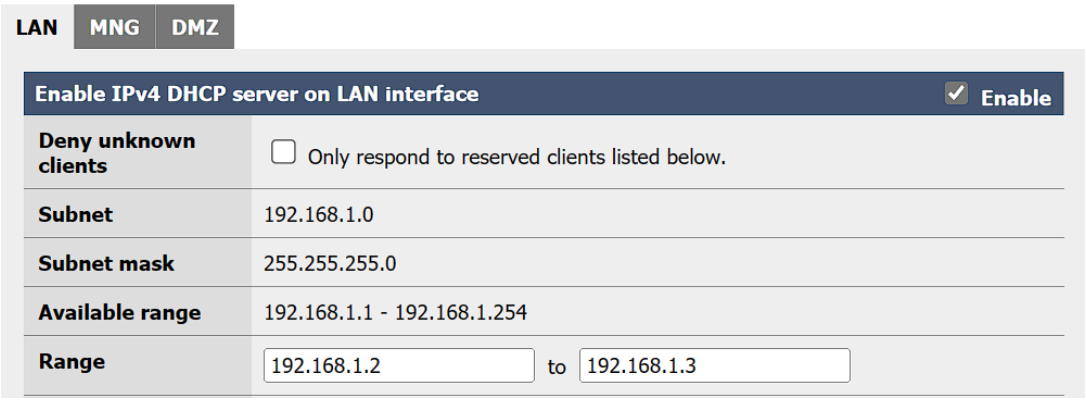
5.11

Όχι, καμία.

5.12

Την ενεργοποιούμε.

5.13



5.14

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

```
root@PC1:~ # dhclient em0
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 3
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 7
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 13
DHCPOFFER from 192.168.1.1
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 192.168.1.1
bound to 192.168.1.2 -- renewal in 3600 seconds.
root@PC1:~ # cat /var/db/dhclient.leases.em0
lease {
  interface "em0";
  fixed-address 192.168.1.2;
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.1;
  option domain-name "lab.ntua.gr";
  option dhcp-lease-time 7200;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.1.1;
  renew 2 2023/5/23 20:15:55;
  rebind 2 2023/5/23 21:00:55;
  expire 2 2023/5/23 21:15:55;
}
```

5.15

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

5.16

Στο “dhcp leases”.

Diagnostics: DHCP leases

IP address	MAC address	Hostname	Start	End
192.168.1.2	08:00:27:5d:38:30	PC1	2023/05/23 19:15:54	2023/05/23 21:15:54

5.17

Τις παρακάτω 6:

Diagnostics: ARP table

	IP address	MAC address	Hostname	Interface
☐	172.22.1.1	08:00:27:ea:0c:ff		DMZ
☐	192.168.56.1	0a:00:27:00:00:0a		MNG
☐	192.168.56.2	08:00:27:d0:a0:45		MNG
☐	192.0.2.1	08:00:27:d3:48:63		WAN
☐	192.168.1.1	08:00:27:66:af:d5		LAN
☐	192.168.1.2	08:00:27:5d:38:30	PC1	LAN

5.18

Όχι.

5.19

Βλέπουμε το αποτυχημένο ping.

Last 50 firewall log entries					
Act	**Time**	**If**	**Source**	**Destination**	**Proto**
✖	19:24:48.939133	LAN	192.168.1.2	192.168.1.1, type echo/0	ICMP

5.20

Τα εξής 4:

Diagnostics: Firewall states

Statistics snapshot control	
Start new	Last statistics snapshot: Never

Source	Port	Destination	Port	Protocol	Packets	Bytes	TTL
192.168.56.1	62911	192.168.56.2	80	tcp	14	1160	0:04
192.168.56.1	62912	192.168.56.2	80	tcp	11	1040	0:27
192.168.56.1	62913	192.168.56.2	80	tcp	3	746	2:30:00
192.168.56.1	62914	192.168.56.2	80	tcp	2	92	2:30:00

Firewall connection states displayed: 4

5.21

Κανέναν.

5.22

Ορίζουμε τις παρακάτω επιλογές

Firewall: Rules: Edit

Action	Pass Choose what to do with packets that match the criteria specified below. 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.
Disabled	**Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	LAN Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.

5.23

Ναι.

5.24

Όχι.

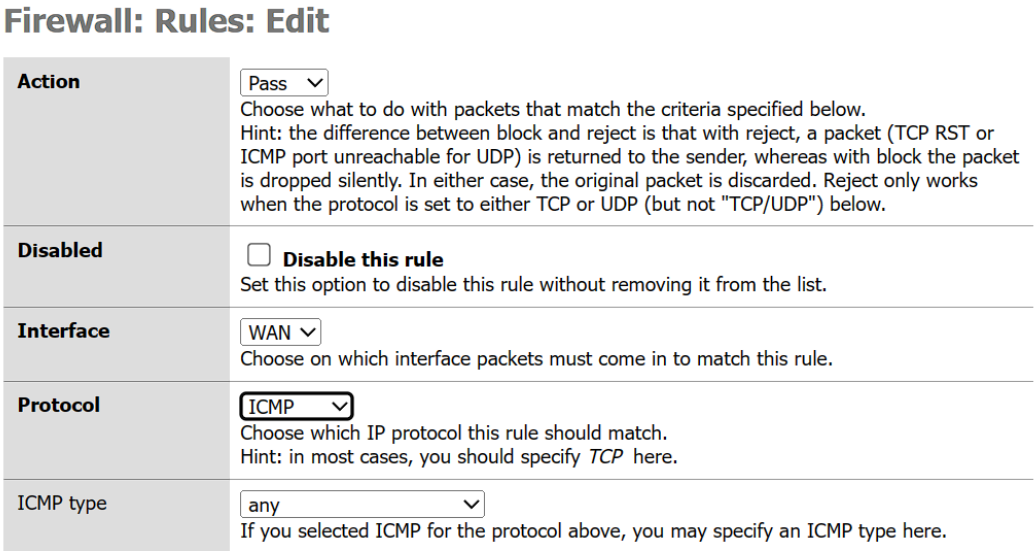
```
[root@router]~# ping -c 1 192.0.2.1
PING 192.0.2.1 (192.0.2.1): 56 data bytes
ping: sendto: No route to host

--- 192.0.2.1 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
```

5.25

Ναι.

```
[root@router]~# arp -a
? (192.0.2.2) at 08:00:27:37:89:a8 on em0 permanent [ethernet]
? (192.0.2.1) at 08:00:27:d3:48:63 on em0 expires in 1157 seconds [ethernet]
```

5.26

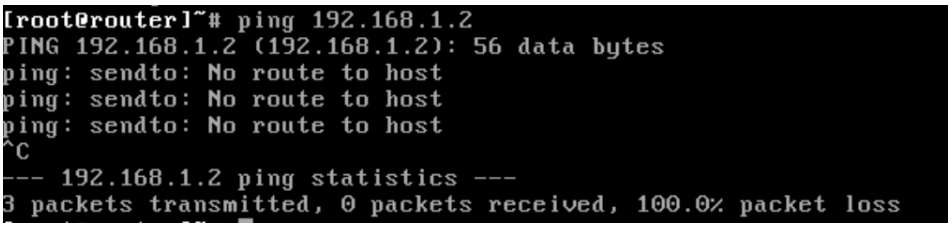


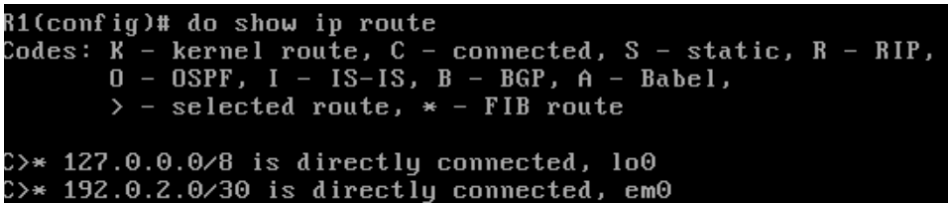
5.27

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

5.34

Όχι, για τον ίδιο λόγο με το 5.33.

5.35

Κάνουμε τις αλλαγές.

Firewall: Rules: Edit

Action	Pass Choose what to do with packets that match the criteria specified below. 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.
Disabled	☐ **Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	DMZ Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
ICMP type	any If you selected ICMP for the protocol above, you may specify an ICMP type here.
Source	☐ **not** Use this option to invert the sense of the match. Type: any Address: /
Source port range	from: (other) to: (other) 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"). Hint: you can leave the *'to'* field empty if you only want to filter a single port
Destination	☑ **not** Use this option to invert the sense of the match. Type: LAN subnet Address: /

5.36

Ναι.

5.37

Ναι.

5.38

Όχι, καθώς δε μπορεί να κάνει δρομολόγηση.

```
[root@router]~# netstat -r
Routing tables

Internet:
Destination        Gateway            Flags     Refs      Use  Netif Expire
localhost          link#3             UH           0      103    lo0
192.0.2.0/30       link#1             U            0       10    em0
192.0.2.2          link#1             UHS          0        0    lo0
```

5.39

Ναι μπορούμε. Ο SRV1 στέλνει το πακέτο στο default gateway του (FW1), το οποίο και λόγω του firewall rule που βάλαμε γίνεται δεκτό. Στη συνέχεια, ο FW1 εξετάζει τον ARP πίνακά του και δεδομένου ότι το R1 δεν ανήκει στο LAN1 το προωθεί κανονικά, ενώ ο R1 απαντάει στην διεπαφή του FW1 στο WAN1.

5.40

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

```
root@PC2:~ # dhclient em0
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 5
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 10
DHCPOFFER from 192.168.1.1
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 192.168.1.1
bound to 192.168.1.3 -- renewal in 3600 seconds.
root@PC2:~ # cat /var/db/dhclient.leases.em0
lease {
  interface "em0";
  fixed-address 192.168.1.3;
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.1;
  option domain-name "lab.ntua.gr";
  option dhcp-lease-time 7200;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.1.1;
  renew 2 2023/5/23 20:57:40;
  rebind 2 2023/5/23 21:42:40;
  expire 2 2023/5/23 21:57:40;
}
```

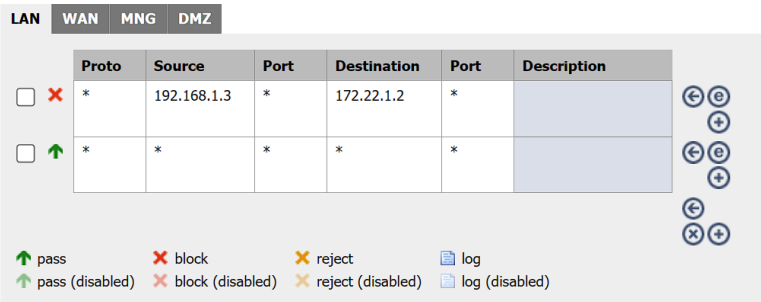
5.41

Firewall: Rules: Edit

Action	Block Choose what to do with packets that match the criteria specified below. 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.
Disabled	**Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	LAN Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
ICMP type	any If you selected ICMP for the protocol above, you may specify an ICMP type here.
Source	**not** Use this option to invert the sense of the match. Type: Single host or alias Address: 192.168.1.3 /
Source port range	from: (other) to: (other) 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"). Hint: you can leave the *'to'* field empty if you only want to filter a single port
Destination	**not** Use this option to invert the sense of the match. Type: Single host or alias Address: 172.22.1.2 /

5.42

Πρέπει να τοποθετηθεί πριν, καθώς διαφορετικά γίνεται match πρώτα ο προηγούμενος κανόνας, ο οποίος και επιτρέπει όλη την κίνηση από το LAN1 προς οπουδήποτε.



5.43

Όχι.

5.44

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

Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT

6.1

```
R1(config)# ip route 203.0.118.0/24 192.0.2.1
```

6.2

Εκτελούμε την αλλαγή.

6.3

Εκτελούμε τις αλλαγές.

Interface	WAN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Source	192.168.1.2 / 32 Enter the source network for the outbound NAT mapping.
Destination	not Use this option to invert the sense of the match. Type: any Address: / 24 Enter the destination network for the outbound NAT mapping.
Target	203.0.118.14 Packets matching this rule will be mapped to the IP address given here. Leave blank to use the selected interface's IP address.
Portmap	Avoid port mapping This option avoids remapping of the source port number for outbound packets whenever possible (i.e. when there is no other mapping for the same port). This may help with software that insists on the source ports being left unchanged when applying NAT (such as some IPsec VPN gateways, games and VoIP applications).
Description	You may enter a description here for your reference (not parsed).
	Save

6.4

Εκτελούμε τις αλλαγές.

Interface	Source	Destination	Target	Description
WAN	192.168.1.2/32	*	203.0.118.14	
WAN	192.168.1.3/32	*	203.0.118.15	

6.5

Εκτελούμε “**tcpdump -i em0**”

6.6

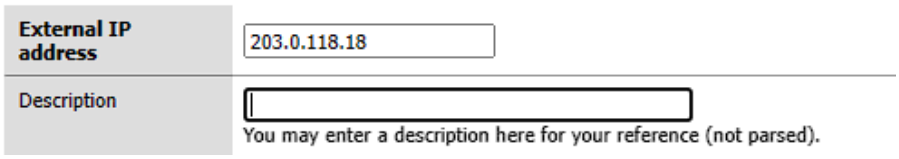
Μπορούμε και τα πακέτα φτάνουν με τις διευθύνσεις 203.0.118.14 και 203.0.118.15 αντίστοιχα.

```
[root@router]~# 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
21:27:08.419473 IP 203.0.118.14 > 192.0.2.2: ICMP echo request, id 43012, seq
 length 64
21:27:08.419494 IP 192.0.2.2 > 203.0.118.14: ICMP echo reply, id 43012, seq 0,
ength 64
21:27:29.044954 IP 203.0.118.15 > 192.0.2.2: ICMP echo request, id 18692, seq
 length 64
21:27:29.044976 IP 192.0.2.2 > 203.0.118.15: ICMP echo reply, id 18692, seq 0,
ength 64
```

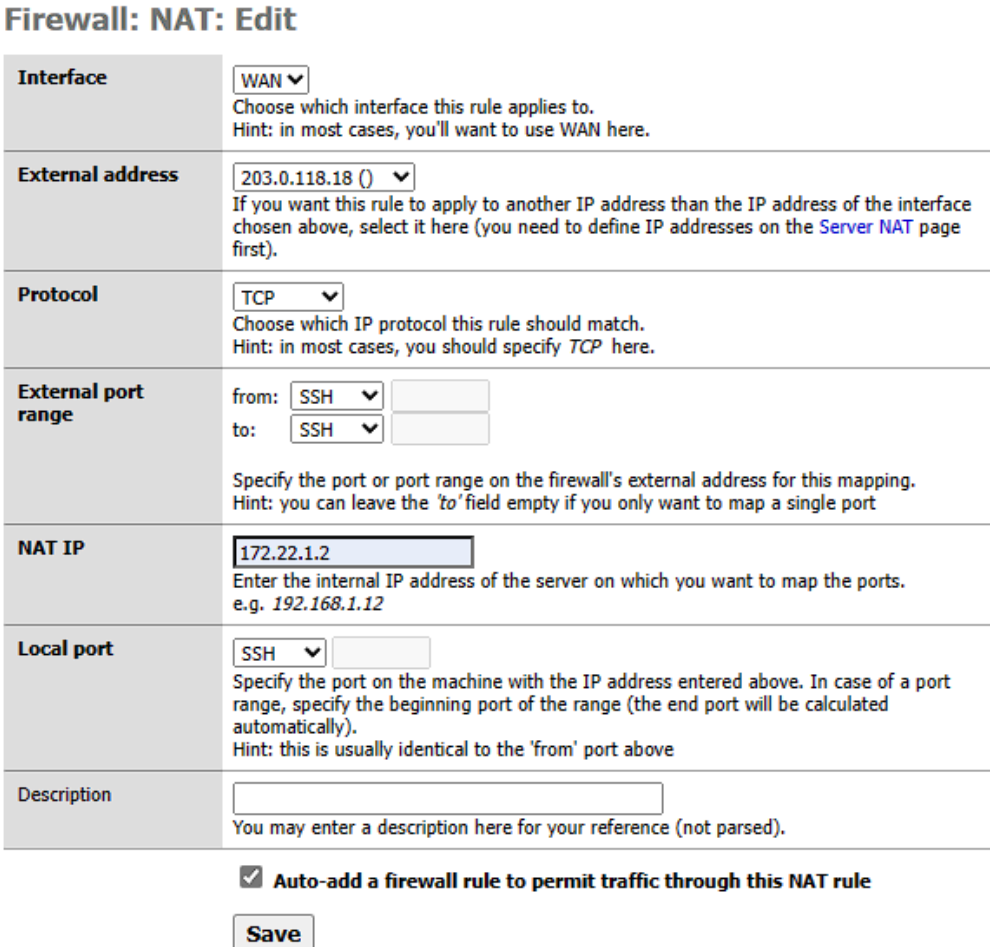
6.7

Αποτυγχάνει (TTL exceeded) επειδή δεν έχουμε ρύθμιση στον FW1 για inbound NAT, οπότε γίνεται αποστολή πακέτων μεταξύ των FW1 και R1 στις προεπιλεγμένες τους πύλες μεταξύ τους.

6.8

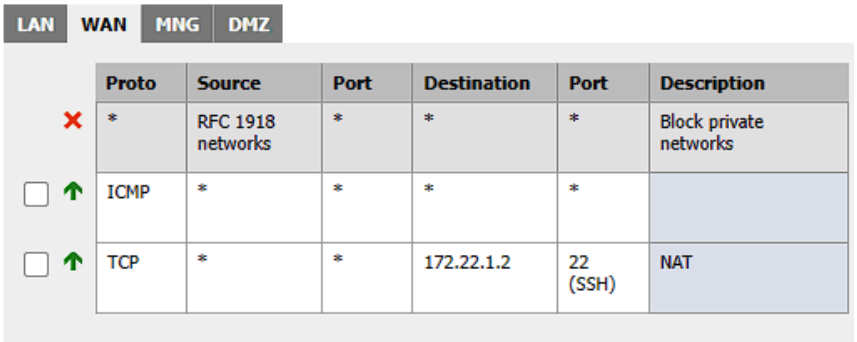


6.9



6.10

Βλέπουμε πως προστίθεται ο παρακάτω τρίτος κανόνας, ο οποίος επιτρέπει εισερχόμενη TCP σύνδεση προς την θύρα 22 του SRV1.



6.11

Το SRV1.

```
[root@router]~# 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 fa:fe:83:9b:f6:6a:cc:c7:13:b3:e3:0e:0d:da:43:b9.
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:
```

6.12

Δε μπορούμε και λαμβάνουμε ως απάντηση TTL exceeded. Βάσει του πίνακα δρομολόγησης του R1, τα πακέτα για την 203.0.118.18 δρομολογούνται στο FW1. Ωστόσο, δεν υπάρχει κατάλληλη μετάφραση όπως πριν για να φτάσουν τα πακέτα στον SRV1, καθώς επιτρέψαμε μόνο συνδέσεις στη θύρα 22 (ssh). Το FW1 τα δρομολογεί, επομένως ξανά στη δική του προκαθορισμένη πύλη, δηλαδή το R1, οπότε εμπλέκονται σε αυτό το loop μέχρι να λήξει το TTL.

```
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
S>* 203.0.118.0/24 [1/0] via 192.0.2.1, em0
```

6.13

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  * * *
```

Diagnostics: ARP table

	IP address	MAC address	Hostname	Interface
☐	172.22.1.2	08:00:27:1e:44:45		DMZ
☐	172.22.1.1	08:00:27:ea:0c:ff		DMZ
☐	192.168.56.1	0a:00:27:00:00:0a		MNG
☐	192.168.56.2	08:00:27:d0:a0:45		MNG
☐	192.0.2.2	08:00:27:37:89:a8		WAN
☐	192.0.2.1	08:00:27:d3:48:63		WAN
☐	192.168.1.1	08:00:27:66:af:d5		LAN
☐	192.168.1.3	08:00:27:f4:91:03	PC2	LAN

6.14

Διαγράφουμε την αντιστοίχιση και δε μπορούμε πλέον να λάβουμε απάντηση στο ping. Κάνοντας "**tcpdump**" στον R1 βλέπουμε πως λαμβάνει τα Requests από τη διεύθυνση 192.168.1.2. Ωστόσο, βλέποντας τον πίνακα δρομολόγησής του, βλέπουμε πως δε μπορεί να το δρομολογήσει πίσω στον PC1.

```
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
S>* 203.0.118.0/24 [1/0] via 192.0.2.1, em0
```

6.15

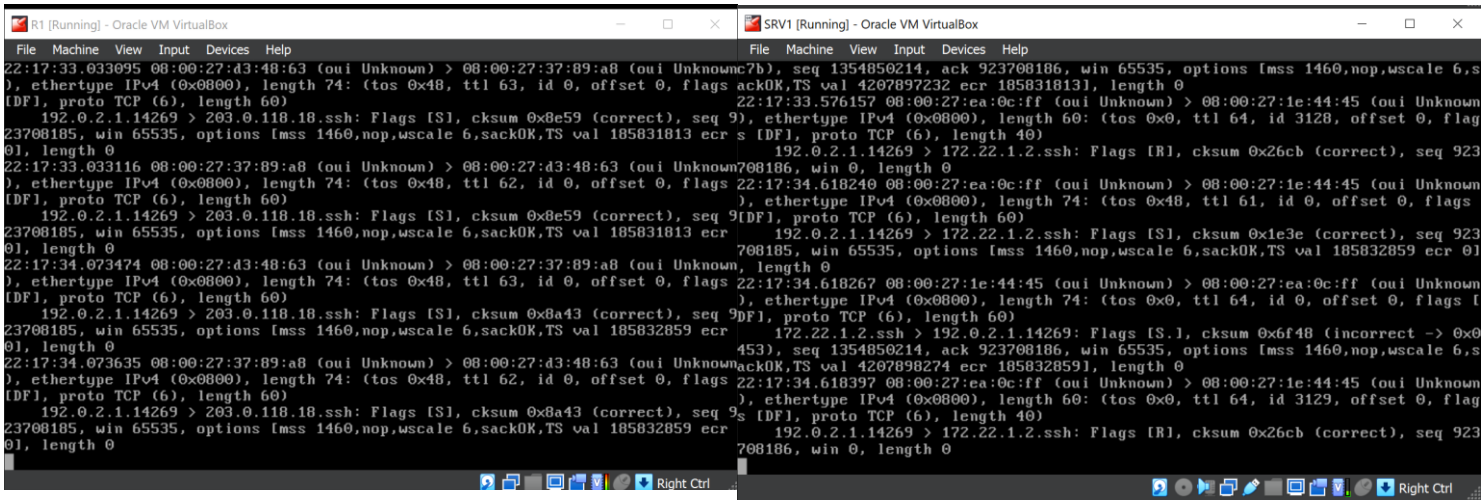
Ναι, πλέον επιτυγχάνει.

6.16

Μπορούμε να συνδεθούμε με ssh από τον R1 στον SRV1, αλλά όχι από τα PC1 και PC2.

6.17

Καταγράφουμε τα παρακάτω.



6.18

Ο παρακάτω κανόνας είναι υπεύθυνος για την παραπάνω συμπεριφορά.

Note:
It is not possible to access NATed services using the WAN IP address from within LAN (or an optional network).

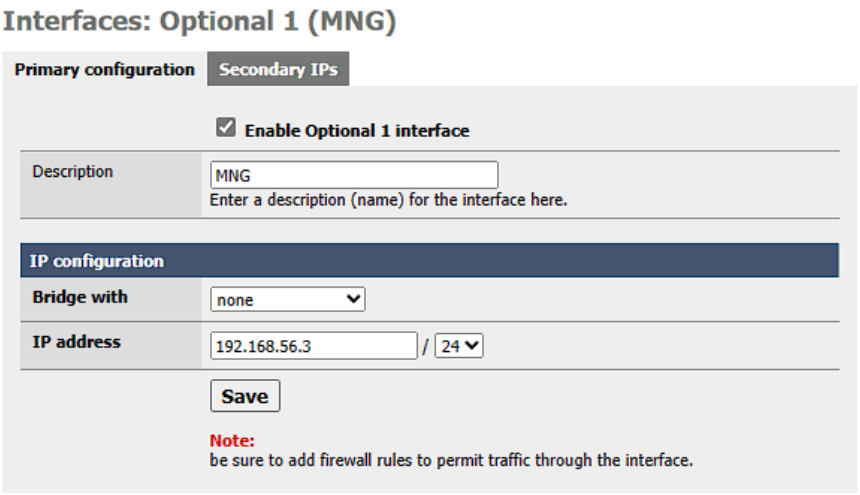
Άσκηση 7: IPSec site-to-site Vpn

7.1

Αποσυνδέουμε το καλώδιο.

7.2

Κάνουμε την αλλαγή και μετά πρέπει να συνδεθούμε στο “http://192.168.56.3”.



7.3

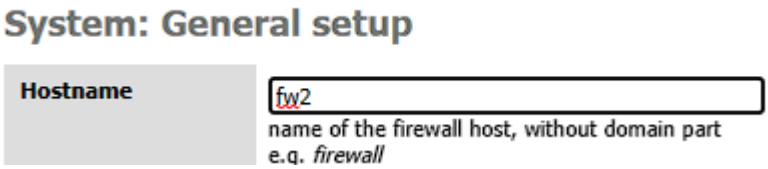
Επανασυνδέουμε την κάρτα.

7.4

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

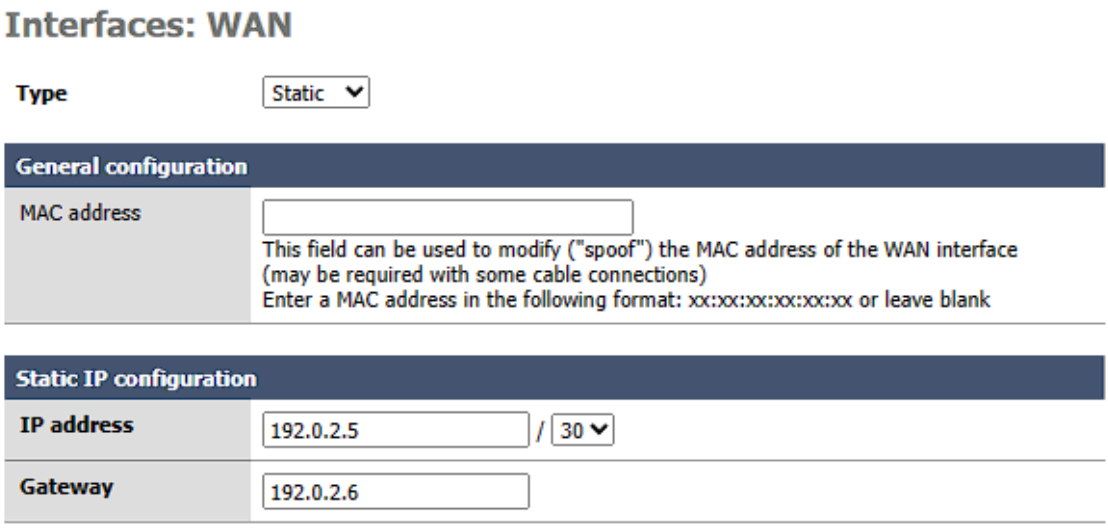
7.5

Κάνουμε την αλλαγή.



7.6

Κάνουμε τις αλλαγές.

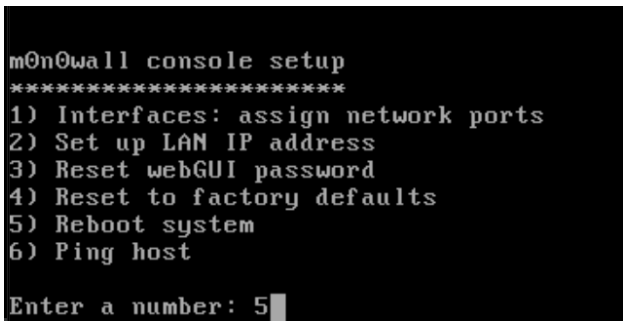


7.7

Κάνουμε την αλλαγή.

7.8

Κάνουμε reboot το FW2. (Εκτελούμε “**5**”)



7.9

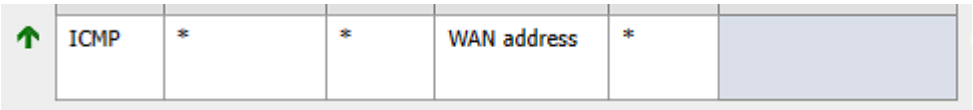
Προσθέτουμε τον κανόνα.

Firewall: Rules: Edit

Action	Pass Choose what to do with packets that match the criteria specified below. 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.
Disabled	**Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	LAN Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
ICMP type	any If you selected ICMP for the protocol above, you may specify an ICMP type here.
Source	**not** Use this option to invert the sense of the match. Type: any Address: /
Source port range	from: (other) to: (other) 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"). Hint: you can leave the *'to'* field empty if you only want to filter a single port
Destination	**not** Use this option to invert the sense of the match. Type: any Address: /

7.10

Όμοια με πριν:



↑	ICMP	*	*	WAN address	*	

7.11

```
root@PC2:~ # ifconfig em0 192.168.2.2/24
root@PC2:~ # route add default 192.168.2.1
add net default: gateway 192.168.2.1
```

7.12

Ναι.

7.13

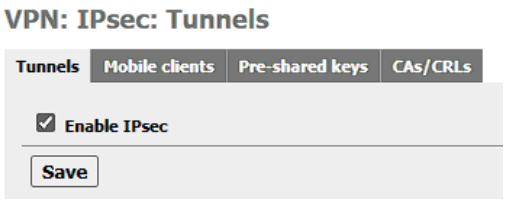
Ναι.

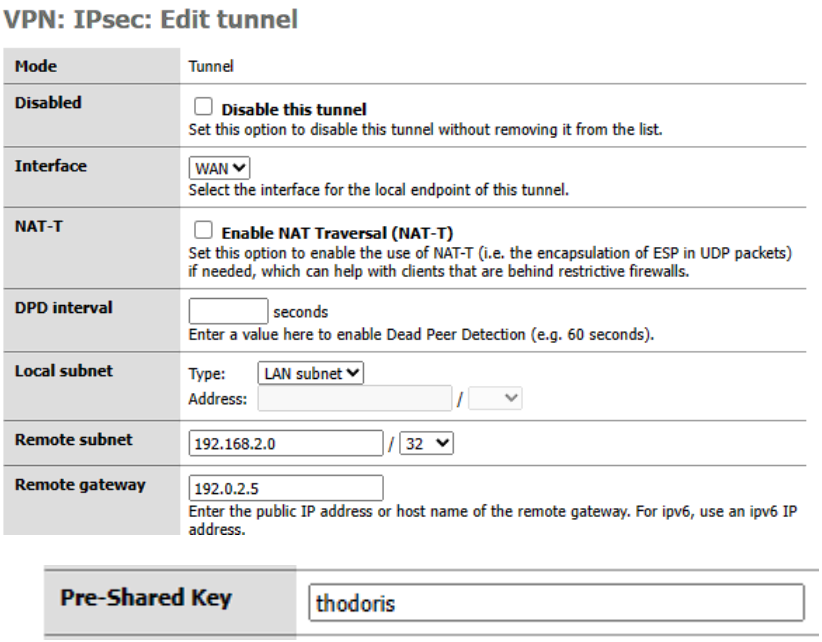
7.14

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

```
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
```

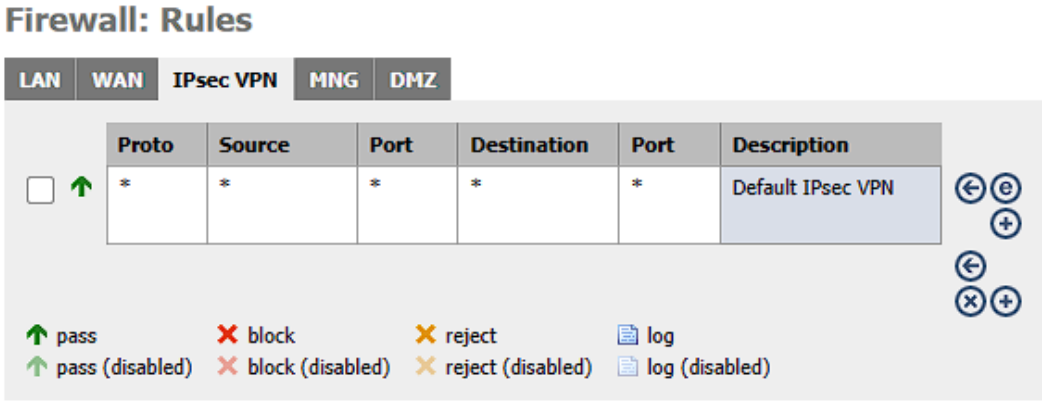
7.15





7.16

Βλέπουμε τον παρακάτω κανόνα.

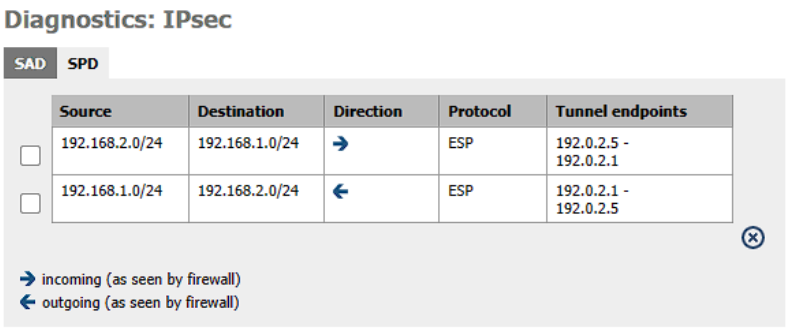


7.17

Όχι.

7.18

Ναι.



7.19

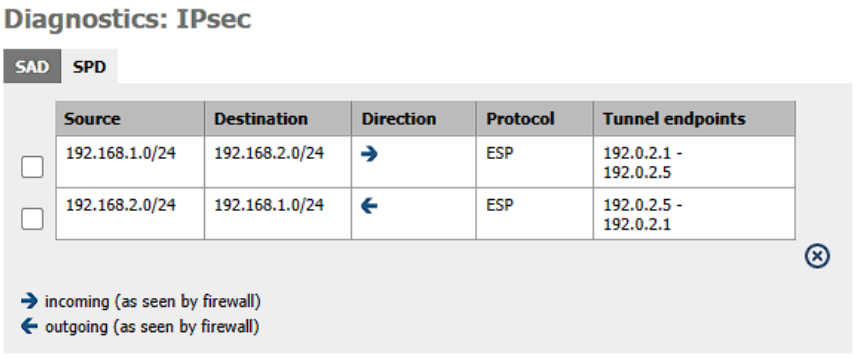
Κάνουμε τα ζητούμενα.

7.20

Όχι.

7.21

Ναι.



7.22

Ναι.

```
root@PC1:~ # ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=1 ttl=62 time=2.358 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=62 time=1.077 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=62 time=1.055 ms
^C
--- 192.168.2.2 ping statistics ---
4 packets transmitted, 3 packets received, 25.0% packet loss
round-trip min/avg/max/stddev = 1.055/1.497/2.358/0.609 ms
```

7.23

Ναι.

7.24

Ναι.

Diagnostics: IPsec

SAD SPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.1	192.0.2.5	ESP	0394a7bc	3des-cbc	hmac-sha1
192.0.2.5	192.0.2.1	ESP	0dad5e54	3des-cbc	hmac-sha1

7.25

Ναι.

Diagnostics: IPsec

SAD SPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.5	192.0.2.1	ESP	0dad5e54	3des-cbc	hmac-sha1
192.0.2.1	192.0.2.5	ESP	0394a7bc	3des-cbc	hmac-sha1

7.26

Εκτελούμε “**tcpdump -vvvi em0**” στον R1.

7.27

Όχι.

```
[root@router]~# tcpdump -vvvi em0
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 65535 bytes
00:23:02.307264 IP (tos 0x0, ttl 64, id 3908, offset 0, flags [none], proto ESP
(50), length 136)
    192.0.2.1 > 192.0.2.5: ESP(spi=0x0394a7bc,seq=0x7), length 116
00:23:02.307808 IP (tos 0x0, ttl 63, id 371, offset 0, flags [none], proto ESP (
50), length 136)
    192.0.2.5 > 192.0.2.1: ESP(spi=0x0dad5e54,seq=0x7), length 116
00:23:03.374474 IP (tos 0x0, ttl 64, id 3909, offset 0, flags [none], proto ESP
(50), length 136)
```

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, ενώ πριν δεν μπορούσαμε.

7.31

Παρατηρούμε πακέτα τύπου TCP με πηγή την 192.0.2.5:47756 και προορισμό την 203.0.118.18:22 (SSH) και αντιστρόφως.

```
00:31:58.215023 IP (tos 0x48, ttl 62, id 0, offset 0, flags [DF], proto TCP (6),
 length 52)
    192.0.2.5.47756 > 203.0.118.18.ssh: Flags [.], cksum 0x6630 (correct), seq 3
707, ack 4879, win 1010, options [nop,nop,TS val 3067820156 ecr 1002140804], len
gth 0
00:31:58.218533 IP (tos 0x48, ttl 63, id 0, offset 0, flags [DF], proto TCP (6),
 length 88)
    203.0.118.18.ssh > 192.0.2.5.47756: Flags [P.], cksum 0x2bfb (correct), seq
4879:4915, ack 3707, win 1027, options [nop,nop,TS val 1002140814 ecr 3067820156
], length 36
```

7.32

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