



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΓΚΟΥΜΕ ΛΑΟΥΡΕΝΤΙΑΝ

ΑΜ: 031 18 014

ΕΞΑΜΗΝΟ: 8^ο

ΟΜΑΔΑ: 3

ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ



ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 10: ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ (FIRE-WALLS) ΚΑΙ NAT

Προετοιμασία στο σπίτι

Παραμετροποιούμε κατάλληλα:

```
root@PC:~ # sysrc -a
/etc/rc.conf: to: not found
defaultrouter: 192.0.2.2
firewaall_logif: YES
firewall_enable: YES
firewall_nat_enable: YES
gateway_enable: YES
hostname: FW1
ifconfig_em0: 192.168.1.1/24
ifconfig_em1: 192.0.2.1/30
syslogd_flags: -scc
```

Άσκηση 1: Ένα απλό τείχος προστασίας

1.1) Εκτελούμε στο PC1 “kldload ipfw”.

1.2)

```
root@PC:~ # service ipfw onestatus
/etc/rc.conf: to: not found
/etc/rc.conf: to: not found
ipfw is enabled
```

1.3) Όχι δε μπορούμε.

```
root@PC:~ # 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
ping: sendto: Permission denied
^C
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
root@PC:~ # 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
```

1.4)

```
root@PC:~ # 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

1.6) Με “ipfw zero”.

1.7)

```
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
```

1.8) Ναι.

1.9) 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
^C
--- 192.168.1.3 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

1.10)

```
root@PC:~ # 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.

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

1.15)

```
root@PC:~ # 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) Απαιτήθηκε πρώτα η ενεργοποίηση των υπηρεσιών ssh με “service sshd onestart”. Στη συνέχεια “ipfw zero” → “ssh lab@192.168.1.3” → “ls” → “exit”.

```
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 0 0 allow tcp from any to any established
00500 0 0 allow tcp from me to any setup
65535 49 3384 deny ip from any to any
```

1.18)

```
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).

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

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

Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

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, 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 icmp types 8 keep-state”.

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 στατικού 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.

```

root@PC:~ # sftp 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
/etc/rc.conf                                100% 160   51.3KB/s   00:00
sftp> █

```

2.21) Δε μπορούμε, οπότε εισάγουμε τον παρακάτω κανόνα:

```

root@PC2:~ # ipfw add allow tcp from any to me 21 setup keep-state
000000 allow tcp from any to me 21 setup keep-state :default

```

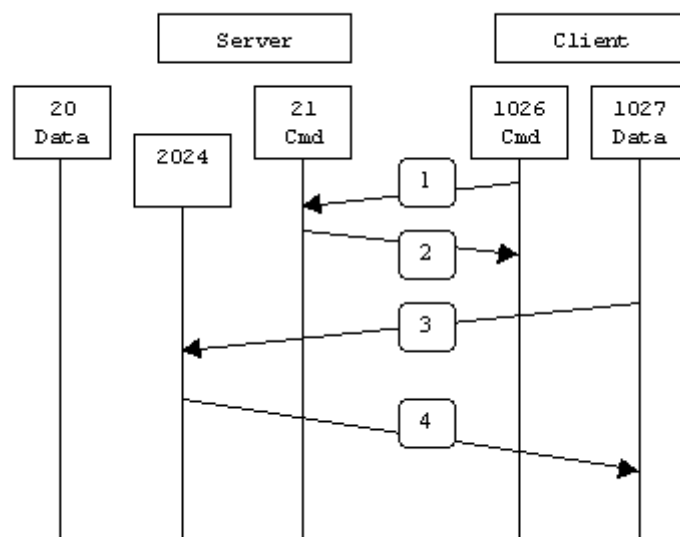
2.22) Έχουμε ενεργοποιήσει μόνο την θύρα 21, η οποία αφορά συνδέσεις Control FTP και όχι την 20 που αφορά FTP data transfer (το οποίο συμβαίνει με την εντολή ls).

```

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
00000 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: Απλό Network Address Translation

3.1)

PC1 [Running] - Oracle VM VirtualBox	PC2 [Running] - Oracle VM VirtualBox
<pre>File Machine View Input Devices Help 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</pre>	<pre>File Machine View Input Devices Help 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</pre>

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 ftp onestart”.

3.5)

```
root@FW1:~ # kldstat
Id Refs Address      Size      Name
1      7 0xc0400000 18664bc  kernel
2      2 0xc454b000 28000    ipfw.ko
3      1 0xc4586000 5000     ipfw_nat.ko
4      1 0xc4363000 c000     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 και στις 2.

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_{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_{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 μπορούμε.

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 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.

```
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 και το βλέπουμε από το prompt.

```
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.

```

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 μπορούμε.

3.32) Το PC2.

3.33) Στο PC1.

Άσκηση 4: Τείχος προστασίας και NAT

4.1) Όχι, και τα 2 ring 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) Επιτυχάνουν 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-state
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-state
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, length 64
07:30:12.297232 IP 192.168.1.3 > 192.0.2.5: ICMP echo reply, id 60166, seq 40, 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
Password for lab@PC1:█
```

4.29) Όχι, καθώς απορρίπτεται από τον κανόνα 2999.

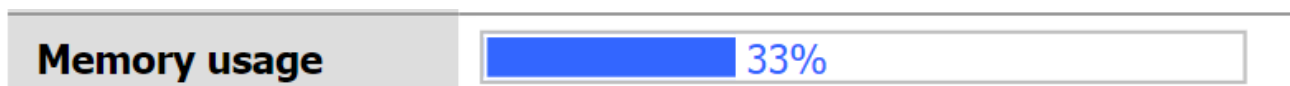
4.30) Εισάγουμε τους κανόνες “ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state” και “ipfw add 2700 skipto 3000 tcp from any 20 to any setup xmit em1 keep-state”.

Άσκηση 5: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

5.1) 192.168.1.1/24.

5.2) 10.0.0.1/30.

5.3) 67%.



5.4) Τις αναμενόμενες 4.

5.5) 172.22.1.1/24.

5.6)


Hostname	<input type="text" value="fw"/>
name of the firewall host, without domain part 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.

Firewall: Rules

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

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

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

5.9)

Static IP configuration

IP address	<input type="text" value="192.0.2.1"/> / <input type="text" value="30"/> ▼
Gateway	<input type="text" value="192.0.2.2"/>

5.10) Ναι, υπάρχει ο παρακάτω κανόνας:

Proto	Source	Port	Destination	Port	Description
*	RFC 1918 networks	*	*	*	Block private networks

No rules are currently defined for this interface.
All incoming connections on this interface will be blocked until you add pass rules.
Click the  button to add a new rule.

5.11) Όχι, καμία.

5.12) Την ενεργοποιούμε.

5.13)

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

```
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 2022/5/24 22:59:22;
    rebind 2 2022/5/24 23:44:22;
    expire 2 2022/5/24 23:59:22;
}
```

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	08:00:27:61:be:f7	PC1	2022/05/24 22:19:23	2022/05/25 00:19:23



Show active and expired 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:

Diagnostics: Firewall states

Statistics snapshot control							
Start new		Last statistics snapshot: Never					
Source	Port	Destination	Port	Protocol	Packets	Bytes	TTL
192.168.56.1	58724	192.168.56.2	80	tcp	3	749	2:30:00
192.168.56.1	57621	192.168.56.255	57621	udp	2	144	1:43
192.168.56.1	57621	192.168.56.255	57621	udp	2	144	1:07
192.168.56.1	57621	192.168.56.255	57621	udp	2	144	0:07
192.168.56.1	58725	192.168.56.2	80	tcp	2	92	2:30:00

Firewall connection states displayed: 5

5.21) Κανέναν.

5.22) Ορίζουμε τις παρακάτω επιλογές.

Firewall: Rules: Edit

Action	<div>Pass</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>LAN</div> <div>Choose on which interface packets must come in to match this rule.</div>
Protocol	<div>any</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</div>

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 08:00:27:65: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

Action	<div>Pass</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>WAN</div> <div>Choose on which interface packets must come in to match this rule.</div>
Protocol	<div>ICMP</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</div>
ICMP type	<div>any</div> <div>If you selected ICMP for the protocol above, you may specify an ICMP type here.</div>

5.27) Ναι.

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

```
[root@router]~# ping -c 1 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
ping: sendto: No route to host
```

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.

```
root@PC1:~ # ping -c 1 172.22.1.2
PING 172.22.1.2 (172.22.1.2): 56 data bytes
--- 172.22.1.2 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
root@PC1:~ #
```

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. All incoming connections on this interface will be blocked until you add pass rules. Click the  button to add a new rule.					

5.34) Όχι, για τον ίδιο λόγο με το 5.33.

5.35) Κάνουμε τις αλλαγές, τις οποίες παρουσιάζουμε στην αρχή της επόμενης σελίδας.

5.36) Ναι.

5.37) Ναι.

Action	<div>Pass ▼</div> <p>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.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>DMZ ▼</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. 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	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▼</div> Address: <div></div> / <div>▼</div>
Source port range	from: <div>(other) ▼</div> <div></div> to: <div>(other) ▼</div> <div></div> 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	<input checked="" type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>LAN subnet ▼</div> Address: <div></div> / <div>▼</div>

5.38) Όχι, καθώς δε μπορεί να κάνει δρομολόγηση.

Routing tables						
Internet:						
Destination	Gateway	Flags	Refs	Use	Netif	Expire
127.0.0.1	link#3	UH	0	113	lo0	
192.0.2.0/30	link#1	U	0	4	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:~ # 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 3 2022/5/25 00:01:43;
    rebind 3 2022/5/25 00:46:43;
    expire 3 2022/5/25 01:01:43;
}

```


5.41)

Firewall: Rules: Edit

Action	<div>Block ▼</div> <p>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.</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. 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"). 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>

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.

Firewall: Rules







 The changes have been applied successfully.


LAN


WAN


MNG


DMZ


		Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/>	✗	*	192.168.1.3	*	172.22.1.2	*		  
<input type="checkbox"/>	↑	*	*	*	*	*		  


 pass


 block


 reject

 log

 pass (disabled)

 block (disabled)

 reject (disabled)

 log (disabled)

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 που φαίνονται στην αρχή της παρακάτω σελίδας.

6.4) Εκτελούμε τις αλλαγές.

You may enter your own mappings below.

	Interface	Source	Destination	Target	Description	
<input type="checkbox"/>	WAN	192.168.1.2/32	*	203.0.118.14		
<input type="checkbox"/>	WAN	192.168.1.3/32	*	203.0.118.15		  

Firewall: NAT: Edit outbound mapping

Interface	<div>WAN ▾</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
Source	<div>192.168.1.3 / 32 ▾</div> <div>Enter the source network for the outbound NAT mapping.</div>
Destination	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: any ▾</div> <div>Address: / 24 ▾</div> <div>Enter the destination network for the outbound NAT mapping.</div>
Target	<div>203.0.118.15</div> <div>Packets matching this rule will be mapped to the IP address given here. Leave blank to use the selected interface's IP address.</div>
Portmap	<div><input type="checkbox"/> Avoid port mapping</div> <div>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).</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

Save

6.5) Εκτελούμε “tcpdump -i em0”.

6.6) Μπορούμε και τα πακέτα φτάνουν με τη διεύθυνση 203.0.118.14.

6.7) Μπορούμε και τα πακέτα φτάνουν με τη διεύθυνση 203.0.118.15.

6.8) 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.

6.9)

Firewall: NAT: Edit Server NAT

External IP address	<div>203.0.118.18</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

Save

6.10)

Firewall: NAT: Edit

Interface	<div>WAN ▾</div> <div>Choose which interface this rule applies to. 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 Server NAT page first).</div>
Protocol	<div>TCP ▾</div> <div>Choose which IP protocol this rule should match. 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. 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</div> <div>Enter the internal IP address of the server on which you want to map the ports. 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). 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

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

Firewall: Rules

LAN

WAN

MNG

DMZ

	Proto	Source	Port	Destination	Port	Description	
<div>✗</div>	*	RFC 1918 networks	*	*	*	Block private networks	<div>← e +</div>
<div><input type="checkbox"/> ↑</div>	ICMP	*	*	*	*		<div>← e +</div>
<div><input type="checkbox"/> ↑</div>	TCP	*	*	172.22.1.2	22 (SSH)	NAT	<div>← e +</div>

↑ pass

✗ block

✗ reject

📄 log

↑ pass (disabled)

✗ block (disabled)

✗ reject (disabled)

📄 log (disabled)

6.12) To SRV1.

```
[root@router1]~# 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 0c:dc:88:e4:1e:8a:02:36:3f:3a:22:11:f3:0d:e9:b5.
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:
```

6.13) 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
```

6.14) 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
<input type="checkbox"/>	172.22.1.2	08:00:27:a3:f1:04		DMZ
<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"/>	192.0.2.2	08:00:27:65:a2:78		WAN
<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"/>	192.168.1.3	08:00:27:9a:04:ce		LAN



6.15) Διαγράφουμε την αντιστοίχιση και δε μπορούμε πλέον να λάβουμε απάντηση στο ring. 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.

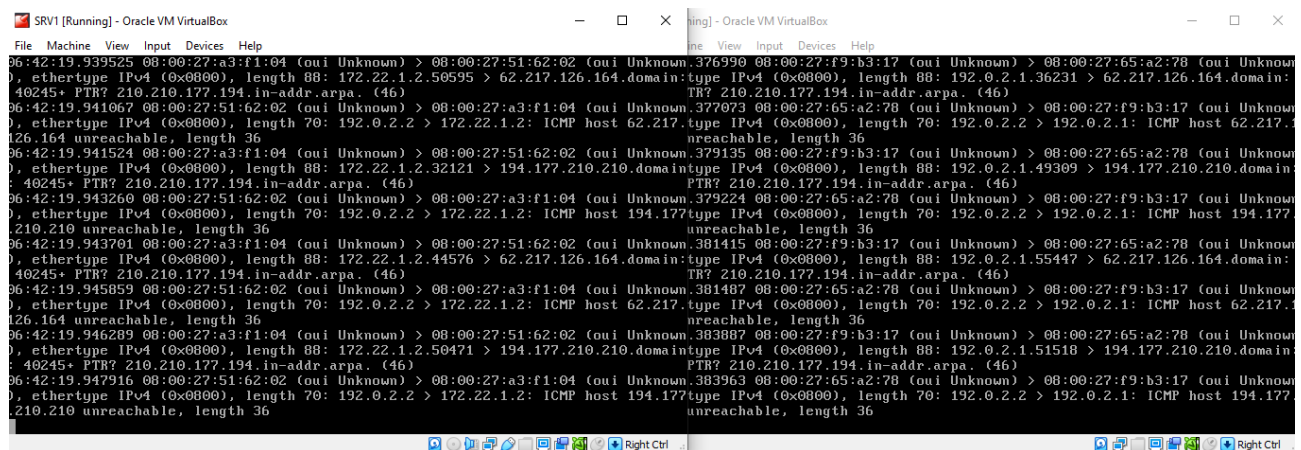
Routing tables

Internet:						
Destination	Gateway	Flags	Refs	Use	Netif	Expire
localhost	link#3	UH	0	327	lo0	
192.0.2.0/30	link#1	U	0	5	em0	
192.0.2.2	link#1	UHS	0	7	lo0	
203.0.118.0	192.0.2.1	UG1	0	1122	em0	

6.16) Ναι, πλέον επιτυγχάνει.

6.17) Μπορούμε να συνδεθούμε με ssh από τον R1 στον SRV1, αλλά όχι από τον PC2.

6.18) Καταγράφουμε τα παρακάτω.



6.19) 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://192.168.56.2”.

Interfaces: Optional 1 (MNG)

Primary configuration		Secondary IPs	
<input checked="" type="checkbox"/> Enable Optional 1 interface			
Description	<input type="text" value="MNG"/> <small>Enter a description (name) for the interface here.</small>		
IP configuration			
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"/>			
Note: 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) Κάνουμε την αλλαγή.

System: General setup

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

7.6) Κάνουμε τις αλλαγές.

7.7) Κάνουμε την αλλαγή.

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. 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. 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
<input type="checkbox"/> 	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)

Local subnet	Type: LAN subnet ▼ Address: <input type="text"/> / <input type="text"/>
Remote subnet	<input type="text"/> 192.168.2.0 / 24 ▼
Remote gateway	<input type="text"/> 192.0.2.5 <small>Enter the public IP address or host name of the remote gateway. For ipv6, use an ipv6 IP address.</small>

Pre-Shared Key	<input type="text"/> laurentjan
Certificate	<input type="text"/>

7.16) Βλέπουμε τον παρακάτω κανόνα:

Firewall: Rules

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

↑ pass
↑ pass (disabled)

✗ block
✗ block (disabled)

✗ reject
✗ reject (disabled)

📄 log
📄 log (disabled)

7.17) Όχι.

Diagnostics: IPsec

SAD SPD

No IPsec security associations.

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 -vvni em0” στον R1.

7.27) Όχι.

```
[root@router1~]# tcpdump -vvni em0
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 65535 bytes
21:18:09.176097 IP (tos 0x0, ttl 64, id 1990, offset 0, flags [none], proto ESP (50), length 136)
    192.0.2.1 > 192.0.2.5: ESP(spi=0x09b46935,seq=0x16), length 116
21:18:09.178620 IP (tos 0x0, ttl 63, id 649, offset 0, flags [none], proto ESP (50), length 136)
    192.0.2.5 > 192.0.2.1: ESP(spi=0x03f204eb,seq=0x16), length 116
```

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.