

ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

10^η ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ

ΠΑΝΑΓΙΩΤΗΣ ΠΑΠΑΔΕΑΣ

A.M el18039

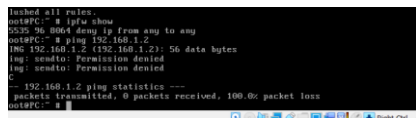
ΑΣΚΗΣΗ 1

1.1 sysrc firewall_enable="YES"

1.2 service -e | grep "ipfw"

1.3 sendto:Permission denied

1.4 ipfw list (αφού κάνουμε flush)



```
flushed all rules.
out@PC:~$ ipfw show
000: 50 0000 deny ip from any to any
out@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
^C
-- 192.168.1.2 ping statistics ---
  packets transmitted, 0 packets received, 100.0% packet loss
out@PC:~$
```

1.5 deny ip from any to any

1.6 ipfw zero

1.7 ipfw add 100 allow all from any to any via lo0

1.8 Επιτυχάνουν

1.9 sendto: Permission denied

1.10 ipfw add allow icmp from any to any

1.11 200

1.12 Μπορώ και από τα δύο PC το ένα στο άλλο

1.13 Γιατί επιτρέπονται μόνο πακέτα icmp και όχι πακέτα udp που στέλνονται by default με το traceroute. Για να πετύχει γράφω traceroute -I 192.168.1.3 ώστε να χρησιμοποιηθεί το πρωτόκολλο icmp.

1.14 ipfw add allow udp from me to any 33434-33523 out

1.15 Δεν μπορώ να συνδεθώ με ssh

1.16 ipfw add allow tcp from any to any established

ipfw add allow tcp from me to any setup

1.17 ipfw zero

ssh lab@192.168.1.3

exit

1.18

```
-- Brn @queneis@istar.ca)
lab@PC:~$ ls
lab@PC:~$ exit
logout
Connection to 192.168.1.3 closed.
root@PC:~# ifconfig show
000000 0 0 allow ip from any to any via lo0
000000 0 0 allow icmp from any to any
000000 0 0 allow udp from me to any 34-3523 out
000000 70 10952 allow tcp from any to any established
000000 1 60 allow tcp from me to any setup
000000 104 9700 deny ip from any to any
root@PC:~#
```

Μία φορά για την εγκατάσταση σύνδεσης και τα υπόλοιπα για την ανταλλαγή πακέτων κατά τη σύνδεση

1.19 Όχι γιατί το setup (εγκατάσταση σύνδεσης) επιτρέπεται μόνο από το PC1 προς το PC2 (στο PC1 είχα ορίσει στον κανόνα για το setup from me to any)

```
*1.20 /usr/libexec/ftpd -D -l -l, service ftpd start
```

1.21 Μπορώ να συνδεθώ με ftp και να κατεβάσω ένα αρχείο (έστω το ztest)

ΑΣΚΗΣΗ 2

2.1 sysrc firewall_enable="YES"

2.2 Δεν μπορώ να κάνω ring

2.3 ipfw add allow all from any to any via lo0

2.4 ipfw add allow icmp from me to any icmptypes 8

2.5 Δεν μπορώ να κάνω ring

2.6 Περνάνε αλλά δεν επιστρέφει η απάντηση

2.7 Τώρα μπορώ (με το keep-state)

2.8 Μπορώ να κάνω ring από το PC1 στο PC2 ενώ τρέχει το άλλο ring

2.9 Δεν μπορώ να κάνω πλέον ring. Πριν μπορούσα εξαιτίας του κανόνα keep-state που επέτρεπε την ανταλλαγή πακέτων όσο ίσχυε αυτός ο κανόνας

2.10 ipfw add allow icmp from any to me icmptypes 8 keep-state

2.11 ipfw -d show

```
root@PC:~# ipfw -d show
0100 0 0 allow ip from any to any via lo0
0200 72 6040 allow icmp from me to any icmpTypes 0 keep-state: default
0300 24 2016 allow icmp from any to me icmpTypes 0 keep-state: default
0535 0 692 deny ip from any to any
0 dynamic rules (1136):
0300 24 2016 (4) STATE icmp 192.168.1.2 0 (-) 192.168.1.3 0 : default
root@PC:~#
```

Βλέπω τους κανόνες που έχω ορίσει μαζί με έναν δυναμικό που δηλώνει την επικοινωνία μεταξύ PC1 και PC2 λόγω του keep-state.

2.12 Δεν φαίνεται πλέον ο δυναμικός κανόνας

2.13 ipfw add allow udp from any to me 33434-33523

```
ipfw add allow icmp from me to any icmptypes 3
```

2.14 ipfw add allow udp from me to any 33434-33523

ipfw add allow icmp from any to me icmp types 3

2.15 ipfw add allow udp from any to me 33434-33523

2.16 ipfw add allow tcp from 192.168.1.0/24 to me 22 setup keep-state

2.17 ssh lab@192.168.1.3

2.18 ipfw add allow tcp from me to any 22 setup keep-state

2.19 ipfw add allow tcp from 192.168.1.2 to me 22 setup

2.20 sftp lab@192.168.1.3

get /etc/rc.conf

2.21 Δεν μπορώ να συνδεθώ αρχικά. Εισάγω τον κανόνα ipfw add allow icmp from any to any 20-21 setup keep-state

2.22 ftp lab

Η πρώτη εντολή εκτελείται επιτυχώς καθώς είμαστε σε active mode ενώ για τη δεύτερη εισερχόμαστε σε passive mode το οποίο δεν έχουμε επιτρέψει μέσω του firewall ακόμα

2.23 ipfw add allow tcp from any to any 49152-65535 setup keep-state

2.24 Τώρα μπορώ να το κατεβάσω

2.25 Για να δουλεύουν και τα δύο παράλληλα πρέπει να επεκτείνω ακόμα περισσότερο τις θύρες που χρησιμοποιούμε καθώς επιλέγεται τυχαία στο active mode από τον client και ανήκει μεταξύ 1024-65535

Προσθέτω και στα δύο την εντολή:

ipfw add allow tcp from any to any 1024-65535 setup keep-state

2.26 Το ftp βλέπουμε ότι δεν είναι ασφαλές καθώς ακόμα και με την χρήση firewall αφήνουμε εκτεθειμένα πολλά ports

2.27 ipfw firewall_enable="NO"

reboot

ΑΣΚΗΣΗ 3

3.1 hostname RX

ifconfig em0 192.168.1.X/24

route add -net 0.0.0.0/0 192.168.1.1

3.2 hostname R1

ifconfig emX

ip address X.X.X.X/X

3.23 Όχι γιατί έχουμε ορίσει μόνο τις ιδιωτικές διευθύνσεις να μεταφράζονται δηλαδή τις απεχόμενες

3.24 ssh [lab@192.0.2.5](#)

Μπορώ να συνδεθώ

3.25 Είναι θέμα δρομολόγησης (μετά από λίγο λαμβάνουμε μήνυμα “No route to host”)

3.26 ipfw nat 123 config ip 192.0.2.1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1

3.27 Επιτυγχάνει και συνδέομαι στο PC2

3.28 ipfw nat 123 config ip 192.0.2.1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1
redirect_port tcp 192.168.1.2:22 22

3.29 Τώρα συνδέομαι στο PC1 (το βλέπω εύκολα με την εντολή hostname)

3.30 Συνδέομαι στο PC2 (εξάλλου μόνο σε αυτό έχω ενεργοποιήσει τον δαίμονα ftpd)

3.31 cd /etc

mget rc.conf

Μπορώ

3.32 Απαντάει πάλι το PC2 λόγω της μετάφρασης

3.33 Στο PC1 λόγω της μετάφρασης

ΑΣΚΗΣΗ 4

4.1 ipfw disable one_pass

Δεν μπορώ να κάνω ping

4.2 Γίνονται δεκτά αλλά αφού απενεργοποιήσαμε τη λειτουργία one-pass η μετάφραση είναι διαφορετική από την αποδοχή και προχωράει στον έλεγχο των υπόλοιπων κανόνων όπου και γίνεται deny

4.3 ipfw add allow 1100 from any to any via em0

4.4 Επιτυγχάνει

4.5 Στο FW1

4.6 allow ip from any to any

4.7 ipfw add 3000 nat 123 all from any to any xmit em1

4.8 ipfw add 3001 allow all from any to any

4.9 ipfw add 3000 nat 123 all from any to any recv em1

4.10 ipfw add 2001 check-state

4.11 To FW1

- 4.12 To PC2
- 4.13 Στο FW1
- 4.14 Στο PC1
- 4.15 Στο PC2
- 4.16 Ναι
- 4.17 Ναι
- 4.18 Μπορώ
- 4.19 ipfw add 2999 deny all from any to any via em1
- 4.20 Επιτυγχάνει μόνο το ping από το PC1 προς το 192.0.2.1 που είναι πρακτικά ο FW1
- 4.21 ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
- 4.22 Μπορώ
- 4.23 ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state
- 4.24 Μπορώ
- 4.25 ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state
- 4.26 To PC2
- 4.27 ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state
- 4.28 To PC1
- 4.29 Όχι
- 4.30 ipfw add 2700 skipto 3000 tcp from any to any 21 recv em1 keep-state
ipfw add 2700 skipto 3000 tcp from any 20 to any out via em1 keep-state

ΑΣΚΗΣΗ 5

- 5.1 LAN1: 192.168.1.1
- 5.2 WAN1: 10.0.0.1
- 5.3 Χρησιμοποιείται 34% άρα 66% ελεύθερο
- 5.4 4 κάρτες δικτύου (άλλαξα το LAN της 4^{ης} σε DMZ)
- 5.5 172.22.1.1
- 5.6 fw
- 5.7 fw1
- 5.8 Δεν έχουν ορισθεί
- 5.9 192.0.2.1/30

192.0.2.2

5.10 Υπάρχει το block private networks σαν κανόνας πλέον

5.11 Δεν είναι ενεργοποιημένες

5.12 enable DNS forwarder

5.13 enable DHCP server

5.14 dhclient em0

Αποδόθηκε διεύθυνση IP: 192.168.1.2

Default gateway: 192.168.1.1

DNS server: 192.168.1.1

5.15 Για το dhcp client

If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in [System: General setup](#) or those obtained via DHCP or PPP on WAN if the "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the [System: General setup](#) page.

5.16 DHCP Leases

5.17 7 εγγραφές

5.18 Δεν μπορώ να κάνω ping

5.19 Τα πακέτα της απόπειρας ping από το PC1

5.20 1 firewall state

5.21 Κανένα κανόνα

5.22 Pass, Source: LAN subnet

5.23 Μπορώ να κάνω ping από το PC1 σε όλες τις διεπαφές του FW1

5.24 Δεν μπορώ

5.26 Βλέπω εγγραφή για το FW1 στον arp table

5.26 proto: icmp, destination WAN address

5.27 Μπορώ να κάνω ping

5.28 Όχι γιατί δεν υπάρχει αντίστοιχη καταγραφή (no route to host)

5.29 Μπορώ να κάνω ping. Για τη λειτουργία NAT συμπεραίνω ότι προστατεύει τους υπολογιστές που ανήκουν στο εσωτερικό δίκτυο

5.30 ifconfig em0 172.22.1.2

Δεν μπορώ να κάνω ping από το PC1 γιατί δεν έχω ορίσει προεπιλεγμένη πύλη στο SRV1 για να μπορεί να απαντήσει

5.31 route add -net 0.0.0.0/0 172.22.1.1

5.32 Μπορώ τώρα να κάνω ping

5.33 Δεν μπορώ να κάνω ping γιατί δεν έχω ορίσει κάποιο κανόνα να το επιτρέπει

5.34 Δεν μπορώ να κάνω ping γιατί δεν έχω ορίσει κάποιο κανόνα να το επιτρέπει

5.35 destination ! LAN net

5.36 Μπορώ να κάνω ping

5.37 Μπορώ να κάνω ping

5.38 Όχι γιατί από τον R1 επιτρέπω μόνο προς την WAN1 διεπαφή του FW1 και δεν έχει καταχώρηση για υπόλοιπες διευθύνσεις

5.39 Μπορώ εφόσον επιτρέπω μέσω firewall κίνηση προς όλα τα δίκτυα πλην του lan1

5.40 dhclient em0

Αποδώθηκε:

IP address: 192.168.1.3

default gateway: 192.168.1.1

DNS server: 192.168.1.1

5.41 block, source: 192.168.1.3, dest: 172.22.1.2

5.42 Πριν αλλιώς η κίνηση θα περάσει

5.43 Δεν μπορώ να κάνω ping

5.44 Μπορώ καθώς απαγόρευσα μόνο την κίνηση προς τον SRV1

ΑΣΚΗΣΗ 6

6.1 ip route 203.0.118.0/24 192.0.2.1

6.2 enable advanced outbound NAT

6.3 Interface: WAN, Source: 192.168.1.2/32, Target: 203.0.118.14

6.4 Interface: WAN, Source: 192.168.1.3/32, Target: 203.0.118.15

6.5 tcpdump -vvvv

6.6 Φτάνουν με διεύθυνση 203.0.118.14

6.7 Φτάνουν με διεύθυνση 203.0.118.15

6.8 Γιατί δεν επιτρέπω την εισερχόμενη κίνηση παρά μόνο στην διεπαφή του FW1 στο WAN1 για ICMP

6.9 external ip address: 203.0.118.18

6.10 interface: wan, proto: tcp, ext port: 22, nat ip 172.22.1.2 (ext: 203.0.118.18) int port range: 22

6.11 Προστέθηκε κανόνας NAT proto: tcp, dest: 172.22.1.2, port: 22

6.12 ssh lab@203.0.118.18

Συνδέομαι επιτυχώς στον SRV1

6.13 Όχι γιατί επιτρέπουμε μόνο tcp

6.14 ssh lab@203.0.118.18

Πηγαίνουν μέσω WAN1 και ξανά πίσω (μπορώ να το επιβεβαιώσω με tcpdump στον R1)

6.15 Δεν μπορώ καθώς έχουμε ενεργοποιήσει το advanced outbound NAT Που επιτρέπει μόνο τα mappings που έχουμε ορίσει εμείς

6.16 Τώρα το ping επιτυγχάνει

6.17 Μπορώ να συνδεθώ με ssh από τον R1 στον SRV1. Δεν μπορώ από το PC2 όμως.

6.18 Βλέπουμε ότι στο τρίτο πακέτο της τριπλής χειραψίας στέλνεται πακέτο με σημαία R δηλαδή τερματισμό της προσπάθειας σύνδεσης

6.19 It is not possible to access NATed services using the WAN IP address from within LAN

ΑΣΚΗΣΗ 7

7.1 Adapter 3 Not connected

7.2 Interfaces -> MNG

7.3 Adapter 3 Connected

7.4 Μπορώ στα 192.168.56.2 και 192.168.56.3

7.5 General setup -> Hostname: fw2

7.6 192.0.2.5/30, 192.0.2.6

7.7 192.168.2.1/24

7.8 Από το virtual box FW2 -> reset

7.9 Firewall rules -> LAN -> allow all lan2

7.10 proto: icmp, dest: wan address

7.11 ifconfig em0 192.168.2.2/24

route add -net 0.0.0.0/0 192.168.2.1

7.12 Μπορώ να κάνω ping

7.13 Μπορώ να κάνω ping

7.14 Όχι γιατί δεν υπάρχει αντίστοιχη εγγραφή στον R1 και εξάλλου δεν θα επιτρεπόταν μέσω firewall

7.15 local subnet: lan subnet

remote subnet: 192.168.2.2/32

remote gateway: 192.0.2.5

Pre-Shared Key: PANAGIOTIS

7.16 Default IPsec VPN

7.17 Στο SAD δεν έχουν ορισθεί

7.18 Στο SPD έχουν ορισθεί

7.19 local subnet: lan subnet

remote subnet: 192.168.1.2/32

remote gateway: 192.0.2.1

Pre-Shared Key: PANAGIOTIS

7.20 Στο SAD όχι

7.21 Στο SPD ναι

7.22 Δεν μπορώ

7.23 Δεν μπορώ

7.24 Προστέθηκε μια εγγραφή

7.25 Προστέθηκε μια εγγραφή

7.26 tcpdump -vvvv

7.27 Όχι

7.28 Εμφανίζονται πακέτα udp κρυπτογραφημένα

src: 192.0.2.1, dest: 192.0.2.5 και αντίστροφα

7.29 Όχι

7.30 Μπορώ να συνδεθώ

7.31 Παρατηρώ πακέτα TCP

src: 192.0.2.5, dest: 203.0.118.18

7.32 Δεν είναι κρυπτογραφημένα

