Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή Άσκηση 10
Τείχη προστασίας (Firewalls) και NAT

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Όνομα PC:** nick-ubuntu
Ομάδα: 1 (Τρίτη 10:45)	**Ημερομηνία Εξέτασης:** Τρίτη 17/05/2022

Άσκηση 1: Ένα απλό τείχος προστασίας

Προετοιμασία στο σπίτι

Στο νέο FreeBSD 11.4 εκτελούμε:

```
sysrc ifconfig_em0="192.168.1.1/24"
sysrc ifconfig_em1="192.0.2.1/30"
sysrc defaultrouter="192.0.2.2"
sysrc gateway_enable="YES"
sysrc firewall_enable="YES"
sysrc firewall_nat_enable="YES"
sysrc firewall_logif="YES"
```

1.1

Στο PC1 εκτελούμε `kldload ipfw`.

1.2

Με την εντολή `kldstat | grep ipfw` ή `kldstat -m ipfw`.

1.3

Στο PC1 εκτελούμε:

```
ping 127.0.0.1
ping 192.168.1.2
```

Και τα δύο ping αποτυγχάνουν, ενώ εμφανίζεται μήνυμα λάθους ”Permission denied”.

1.4

Στο PC1 εκτελούμε `ipfw list`. Έχουμε:

```
65535 deny ip from any to any
```

1.5

Στο PC1 εκτελούμε `ipfw show`. Έχουμε:

```
65535 2 168 deny ip from any to any
```

Οι μετρητές είναι: `2 168`.

1.6

Με την εντολή `ipfw zero`.

1.7

Στο PC1 εκτελούμε:

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

1.8

Στο PC1 εκτελούμε:

```
ping 127.0.0.1
ping 192.168.1.2
```

Τώρα τα ping είναι επιτυχή.

1.9

Στο PC1 εκτελούμε `ping 192.168.1.3`. Το ping αποτυγχάνει με μήνυμα "Permission denied".

1.10

Στο PC1 εκτελούμε `ipfw add allow icmp from any to any`.

1.11

Έλαβε αύξοντα αριθμό 200, όπως φαίνεται από την έξοδο της παραπάνω εντολής (εναλλακτικά θα μπορούσαμε να εκτελέσουμε και `ipfw list`).

1.12

Εκτελούμε:

```
### PC1 ###

ping 192.168.1.3

### PC2 ###

ping 192.168.1.2
```

Και τα δύο ping είναι επιτυχή.

1.13

Στο PC1 εκτελούμε `traceroute 192.168.1.3` και επιβεβαιώνουμε ότι δεν μπορούμε, αφού εμφανίζεται μήνυμα λάθους "Permission denied". Αυτό συμβαίνει διότι by default η εντολή traceroute στέλνει πακέτα UDP, και δεν υπάρχει κανόνας στο firewall που επιτρέπει να περάσουν. Αλλάζοντας την εντολή σε:

```
traceroute -I 192.168.1.3
```

πλέον στέλνουμε ICMP πακέτα, τα οποία επιτρέπει ο κανόνας υπ' αριθμόν 200 που προσθέσαμε προηγουμένως.

1.14

Το traceroute χρησιμοποιεί τις θύρες με αριθμούς από

```
port + 1
```

μέχρι και

```
port + (max_ttl - first_ttl + 1) * nprobes
```

Αν αντικαταστήσουμε τις default τιμές:

```
port = 33434
max_ttl = 64
first_ttl = 1
nprobes = 3
```

βρίσκουμε ότι η κλήση της traceroute χωρίς παραμέτρους χρησιμοποιεί τις θύρες 33435-33626. Επομένως εκτελούμε στο PC1:

```
ipfw add allow udp from me to any 33435-33626
```

1.15

Στο PC1 εκτελούμε `ssh lab@192.168.1.3`. Το ssh αποτυγχάνει με μήνυμα λάθους "Permission denied".

1.16

Στο PC1 εκτελούμε:

```
ipfw add allow tcp from me to any setup
ipfw add allow tcp from any to any established
```

1.17

Στο PC1 εκτελούμε:

```
ipfw zero
ssh lab@192.168.1.3
ls
exit
```

1.18

Έχουμε:

```
No.          Rule                                    Times applied
00100        allow ip from any to any via lo0        0
00200        allow icmp from any to any              0
00300        allow udp from me to any 33435-33626    0
00400        allow tcp from me to any setup          1
00500        allow tcp from any to any established   68
```

- Ο κανόνας 100 δεν χρησιμοποιήθηκε καμία φορά, αφού κατά τη σύνδεση με ssh δεν χρησιμοποιείται η `lo0` από το PC1.
- Ο κανόνας 200 δεν χρησιμοποιήθηκε καμία φορά, αφού κατά τη σύνδεση με ssh δεν στέλνονται πακέτα ICMP.
- Ο κανόνας 300 δεν χρησιμοποιήθηκε καμία φορά, αφού κατά τη σύνδεση με ssh δεν στέλνονται πακέτα UDP.
- Ο κανόνας 400 χρησιμοποιήθηκε 1 φορά, στο πρώτο τεμάχιο της TCP χειραψίας, που προέρχεται από το PC1 (με σημαία SYN, όχι σημαία ACK).
- Ο κανόνας 500 χρησιμοποιήθηκε 68 φορές για όλα τα υπόλοιπα τεμάχια TCP που ανήκουν στη σύνδεση που εγκαταστάθηκε (με σημαία ACK ή RST).

1.19

Στο PC2 εκτελούμε `ssh lab@192.168.1.2`. Η εντολή αρχικά φαίνεται να ”κολλάει” και ύστερα από κάποιο χρονικό διάστημα εμφανίζεται μήνυμα ”Operation timed out”. Αυτό είναι λογικό, αφού κανένας από τους κανόνες που έχουμε ορίσει στο firewall του PC1 δεν επιτρέπουν TCP τεμάχια με σημαίες SYN=1, ACK=0 από απομακρυσμένα μηχανήματα, παρά μόνο από το PC1.

1.20

Στο PC2 εκτελούμε `service ftpd onestart`.

1.21

Στο PC1 εκτελούμε:

```
ftp lab@192.168.1.3
get /usr/bin/grep
exit
```

Μπορούμε να κατεβάσουμε το αρχείο με επιτυχία.

Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

2.1

Στο PC2 εκτελούμε `kldload ipfw`.

2.2

Στο PC2 εκτελούμε `ping 192.168.1.2`. Δεν μπορούμε, καθώς εμφανίζεται μήνυμα λάθους "Permission denied".

2.3

Στο PC2 εκτελούμε:

```
ipfw add allow all from any to any via lo0
```

2.4

Στο PC2 εκτελούμε:

```
ipfw add allow icmp from me to any icmptypes 8
```

2.5

Στο PC2 εκτελούμε `ping 192.168.1.2`. Δεν λαμβάνεται κάποια απάντηση.

2.6

Στο PC2 εκτελούμε:

```
ipfw zero
ping -c 1 192.168.1.2
ipfw show
```

Ο σχετικός μετρητής στον παραπάνω κανόνα αυξήθηκε κατά 1, οπότε τα πακέτα ICMP περνούν το τείχος προστασίας του PC2.

2.7

Στο PC2 εκτελούμε:

```
ipfw delete 200
ipfw add allow icmp from me to any icmptypes 8 keep-state
ping 192.168.1.2
```

Πλέον το ping είναι επιτυχές.

2.8

Εκτελούμε:

```
### PC2 ###

ping 192.168.1.3

### PC1 ###

ping 192.168.1.2
```

Μπορούμε να κάνουμε ping από το PC1 στο PC2.

2.9

Σταματάμε τα ping και ύστερα από λίγο εκτελούμε `ping 192.168.1.3` στο PC1. Πλέον το ping από το PC1 στο PC2 αποτυγχάνει, γιατί διακόπηκε η κίνηση που ανανέωνε τη διάρκεια του δυναμικού κανόνα που δημιουργήθηκε λόγω του ping από το PC2 στο PC1, και ο οποίος επέτρεπε την αμφίδρομη επικοινωνία μεταξύ PC1 και PC2. Έτσι, τα πακέτα ICMP request του PC1 πλέον απορρίπτονται από το τείχος προστασίας του PC2.

2.10

Στο PC2 εκτελούμε:

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

2.11

Στο PC1 εκτελούμε `ping 192.168.1.3`. Στο PC2 εκτελούμε `ipfw -d show`. Βλέπουμε ότι, εκτός από τους στατικούς κανόνες, εμφανίζονται και οι δυναμικοί κανόνες του τείχους προστασίας:

```
## Dynamic rules (1 136):
00300   34   2856 (5s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 :default
```

2.12

Σταματάμε το ping από το PC1 και εκτελούμε ξανά `ipfw -d show` στο PC2. Βλέπουμε ότι ο δυναμικός κανόνας έχει διαγραφεί.

2.13

Στο PC2 εκτελούμε:

```
ipfw add allow udp from any to me 33435-33626
ipfw add allow icmp from me to any icmptypes 3
```

2.14

Στο PC2 εκτελούμε:

```
ipfw add allow udp from me to any 33435-33626
ipfw add allow icmp from any to me icmptypes 3
```

2.15

Πρέπει να προσθέσουμε τον κανόνα (στο PC1):

```
ipfw add allow udp from any to me 33435-33626
```

2.16

Στο PC2 εκτελούμε:

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

2.17

Με την εντολή `ssh lab@192.168.1.3`.

2.18

Στο PC2 εκτελούμε:

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

2.19

Πρέπει να προσθέσουμε στο PC1 τον κανόνα:

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

2.20

Στο PC1 εκτελούμε:

```
sftp lab@192.168.1.2
get /etc/rc.conf
```

Μπορούμε να κατεβάσουμε το `/etc/rc.conf`.

2.21

Στο PC1 εκτελούμε `ftp lab@192.168.1.2`. Λαμβάνουμε μήνυμα λάθους "Connection refused", οπότε εκτελούμε στο PC2:

```
ipfw add allow tcp from 192.168.1.0/24 to me 21 keep-state
```

2.22

Στο PC1 εκτελούμε:

```
ftp lab@192.168.1.3
cd /usr
ls
```

Η `cd /usr` εκτελείται επιτυχώς, αφού υπάρχει κανόνας στο firewall του PC2 για τη θύρα 21, ενώ η `ls` αποτυγχάνει, γιατί εκτελώντας την μπαίνουμε Extended Passive Mode, στο οποίο επιλέγεται δυναμικά μια θύρα για τη σύνδεση δεδομένων, για την οποία δεν υπάρχει αντίστοιχος κανόνας στο firewall του PC2.

2.23

Σύμφωνα με την ιστοσελίδα της υπόδειξης, για να μπορεί ο FTP server (PC2) να υποστηρίξει παθητικό FTP, πρέπει εκτελέσουμε στον PC2:

```
ipfw add allow tcp from 192.168.1.0/24 to me 1024-65535 keep-state
```

2.24

Στο PC1 εκτελούμε:

```
ftp lab@192.168.1.3
get /usr/bin/grep
exit
```

Μπορούμε να κατεβάσουμε το αρχείο με επιτυχία.

2.25

Πρέπει να προσθέσουμε τους κανόνες:

```
### PC1 ###

ipfw add allow tcp from 192.168.1.0/24 20 to me keep-state

### PC2 ###

ipfw add allow tcp from me 20 to 192.168.1.0/24 keep-state
```

2.26

Φαίνεται ότι σε πρωτόκολλα όπως το FTP χρειάζεται να ορίσουμε πολλούς κανόνες, επειδή χρησιμοποιούνται πολλές θύρες ανάλογα τον τρόπο λειτουργίας (σύνδεση δεδομένων, σύνδεση εντολών/ελέγχου, ενεργητικός/παθητικός τρόπος λειτουργίας), ενώ άλλες φορές η σύνδεση εκκινείται από τον πελάτη και άλλες από τον εξυπηρετητή. Όλα αυτά κάνουν τη διαχείριση των κανόνων κάπως δύστροπη και επιρρεπή σε λάθη.

2.27

Εκτελούμε:

```
### PC1 ###

kldunload ipfw
kldstat

### PC2 ###

kldunload ipfw
kldstat
```

Επιβεβαιώνουμε ότι το `ipfw` έχει απενεργοποιηθεί και στα δύο μηχανήματα.

Άσκηση 3: Απλό Network Address Translation

3.1

Εκτελούμε:

```
### PC1 ###

hostname PC1
ifconfig em0 192.168.1.2/24
route add default 192.168.1.1

### PC2 ###

hostname PC2
ifconfig em0 192.168.1.3/24
route add default 192.168.1.1
```

3.2

Στον R1 εκτελούμε:

```
cli
configure terminal
```

```
hostname R1

interface em0
ip address 192.0.2.2/30

interface em1
ip address 192.0.2.6/30
```

3.3

Στον SRV1 εκτελούμε:

```
hostname SRV1

ifconfig em0 192.0.2.5/30

route add default 192.0.2.6
```

3.4

Εκτελούμε:

```
### PC2 ###

service ftpd onestart

### SRV1 ###

service ftpd onestart
```

3.5

Στο FW1 εκτελούμε `kldstat`. Έχουν φορτωθεί τα modules:

```
kernel
ipfw
ipfw_nat
libalias
```

3.6

Ενεργοποιήθηκε το IPFW.

3.7

Στο FW1 εκτελούμε `sysrc firewall_type` και έχουμε:

```
firewall_type: UNKNOWN
```

3.8

Στο FW1 εκτελούμε `ipfw list`. Βλέπουμε 11 κανόνες. Ο τελευταίος είναι ο default κανόνας (αύξων αριθμός 65535):

```
65535 deny ip from any to any
```

3.9

Με την εντολή `ip nat show config`. Βλέπουμε ότι δεν έχει οριστεί κανένας πίνακας in-kernel NAT.

3.10

Στο PC1 εκτελούμε:

```
ping 192.168.1.1
ping 192.0.2.1
```

Σε κανένα από τα δύο ping δε λαμβάνουμε απάντηση.

3.11

Στον SRV1 εκτελούμε `ping 192.0.2.1`. Δε λαμβάνουμε απάντηση.

3.12

Στο FW1 εκτελούμε:

```
ipfw nat 123 config unreg_only if em1 reset
```

3.13

Στο FW1 εκτελούμε:

```
ipfw add nat 123 ip4 from any to any
```

3.14

Στο PC1 εκτελούμε:

```
ping 192.168.1.1
ping 192.0.2.1
```

Πλέον και τα δύο ping είναι επιτυχή.

3.15

Στον R1 εκτελούμε `tcpdump -i em0`.

3.16

Στο FW1 εκτελούμε `ipfw show && ipfw zero`.

3.17

Στο PC1 εκτελούμε `ping -c 3 192.0.2.2`. Η IP διεύθυνση πηγής των ICMP echo request είναι `192.0.2.1` (FW1@em1).

3.18

Είναι πάλι η `192.0.2.1` (FW1@em1).

3.19

Εκτελούμε `ipfw show` στο FW1. Υπεύθυνος για την επιτυχία του ping είναι ο κανόνας:

```
01100 nat 123 ip4 from any to any
```

3.20

Εφαρμόστηκε 124 φορές. Αυτό συμβαίνει διότι στάλθηκαν συνολικά 31 (δηλαδή $124 \div 4$) ICMP echo request από το PC1, και κάθε φορά που στέλνεται ένα ICMP echo request συμβαίνουν τα εξής:

- Εφαρμόζεται ο κανόνας για το ICMP echo request με κατεύθυνση PC1 $\rightarrow$ FW1
- Εφαρμόζεται ο κανόνας για το ICMP echo request με κατεύθυνση FW1 $\rightarrow$ R1
- Εφαρμόζεται ο κανόνας για το αντίστοιχο ICMP echo reply με κατεύθυνση R1 $\rightarrow$ FW1
- Εφαρμόζεται ο κανόνας για το αντίστοιχο ICMP echo reply με κατεύθυνση FW1 $\rightarrow$ PC1

3.21

Στον SRV1 εκτελούμε `ping 192.0.2.1`. Το ping είναι επιτυχές.

3.22

Εκτελούμε:

```
### FW1 ###

ipfw zero

### SRV1 ###

ping -c 1 192.0.2.1

### FW1 ###

ipfw show
```

Βλέπουμε ότι υπεύθυνος για την αποδοχή της κίνησης είναι ο ίδιος κανόνας:

```
01100  2  168 nat 123 ip4 from any to any
```

3.23

Η κίνηση δεν ωθείται προς μετάφραση διευθύνσεων διότι η διεύθυνση `192.0.2.5` του SRV1 δεν είναι ιδιωτική. Υπενθυμίζουμε ότι στην προηγούμενη εντολή ορισμού του πίνακα NAT έχουμε δώσει τη ρύθμιση `unreg_only`.

3.24

Στο PC2 εκτελούμε `ssh lab@192.0.2.5`. Μπορούμε να συνδεθούμε κανονικά.

3.25

Στον SRV1 εκτελούμε `ssh lab@192.168.1.3`. Η εντολή φαίνεται αρχικά να μπλοκάρει, και ύστερα από λίγο εμφανίζεται μήνυμα "No route to host". Ο λόγος που δεν μπορεί να επιτευχθεί η σύνδεση είναι διότι ο SRV1 προωθεί αρχικά τα πακέτα στον R1 μέσω της προκαθορισμένης διαδρομής, αλλά ο R1 δεν διαθέτει εγγραφή σχετική με την (ιδιωτική) διεύθυνση `192.168.1.3`. Μπορούμε να επιβεβαιώσουμε τα παραπάνω αν εκτελέσουμε `traceroute 192.168.1.3` στον SRV1. Η έξοδος της εντολής είναι:

```
1  192.0.2.6 (192.0.2.6) 0.336 ms  0.150 ms  0.115 ms
2  192.0.2.6 (192.0.2.6) 0.114 ms !H  0.192 ms !H  0.089 ms !H
```

όπου το `"!H"` υποδηλώνει ότι ο προορισμός δεν είναι προσβάσιμος από τον R1.

3.26

Στο FW1 εκτελούμε:

```
ipfw nat 123 config unreg_only if em1 reset redirect_addr 192.168.1.3 192.0.2.1
```

3.27

Στον SRV1 εκτελούμε `ssh lab@192.0.2.1`. Η προσπάθεια είναι επιτυχής. Έχουμε συνδεθεί στο PC2, όπως φαίνεται και από το prompt στη γραμμή εντολών:

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

Μπορούμε επίσης να εκτελέσουμε `ifconfig em0` και να δούμε ότι η διεύθυνση IP της `em0` είναι `192.168.1.3`.

3.28

Στο FW1 εκτελούμε (όλο μαζί μία εντολή):

```
ipfw nat 123 config unreg_only if em1 reset \
redirect_addr 192.168.1.3 192.0.2.1 \
redirect_port tcp 192.168.1.2:22 22
```

3.29

Στον SRV1 εκτελούμε πάλι `ssh lab@192.0.2.1`. Αυτή τη φορά συνδεθήκαμε στο PC1, όπως φαίνεται από το prompt:

```
lab@PC1:~ %
```

ή από την έξοδο της εντολής `ifconfig em0`.

3.30

Στον SRV1 εκτελούμε `ftp lab@192.0.2.1`. Στην προτροπή για κωδικό εμφανίζεται:

```
220 PC2 FTP server (Version 6.00LS) ready.
```

οπότε καταλαβαίνουμε ότι έχουμε συνδεθεί από το PC2. Εναλλακτικά, μπορούμε μέσω ftp στον SRV1 να εκτελέσουμε `rstatus`. Στην πρώτη γραμμή της εξόδου της `rstatus` εμφανίζεται:

```
211- PC2 FTP server status:
```

Επίσης μπορούμε να εκτελέσουμε:

```
### PC1 ###

netstat | grep ftp

### PC2 ###

netstat | grep ftp
```

Στο PC1 η έξοδος της εντολής είναι κενή, ενώ στο PC2 εμφανίζεται:

```
tcp4    0    0    192.0.2.5.52490    192.0.2.1.ftp ESTABLISHED
```

3.31

Στον SRV1 εκτελούμε:

```
ls /etc
get /etc/rc.conf
```

Και οι δύο εντολές εκτελούνται με επιτυχία.

3.32

Στο PC1 εκτελούμε `ftp lab@192.0.2.1`. Με τους ίδιους τρόπους (βλ. 3.30) μπορούμε να εξακριβώσουμε ότι απαντά το PC2.

3.33

Στο PC2 εκτελούμε `ssh lab@192.0.2.1`. Συνδεόμαστε στο PC1, όπως φαίνεται από το prompt:

```
lab@PC1:~ %
```

ή από την έξοδο της εντολής `ifconfig em0`.

Άσκηση 4: Τείχος προστασίας και NAT

4.1

Εκτελούμε:

```
### FW1 ###

ipfw disable one_pass

### PC1 ###

ping 192.168.1.1

### SRV1 ###

ping 192.0.2.1
```

Σε κανένα από τα δύο ping δεν λαμβάνουμε απάντηση.

4.2

Στο FW1 εκτελούμε επανειλημμένα `ipfw show` και βλέπουμε ότι όσο το ping εκτελείται, οι μετρητές χρήσης του κανόνα `01100 nat 123 ip4 from any to any` αυξάνονται. Ωστόσο, επειδή μόλις απενεργοποιήσαμε τη λειτουργία one-pass, ύστερα από τη μετάφραση διευθύνσεων, η επεξεργασία των πακέτων συνεχίζει με τον επόμενο κανόνα του τείχους προστασίας. Έτσι, τα πακέτα περνούν από τον default κανόνα (αριθμός 65535), ο οποίος απορρίπτει όλη την κίνηση.

4.3

Στο FW1 εκτελούμε:

```
ipfw delete 1100
ipfw add 1100 allow all from any to any via em0
```

4.4

Στο PC1 εκτελούμε:

```
ping 192.168.1.1
ping 192.0.2.1
```

Και τα δύο ping είναι επιτυχή.

4.5

Στο PC2 εκτελούμε `ssh lab@192.0.2.1`. Με τις εντολές `hostname` ή/και `ifconfig em0` μπορούμε να διαπιστώσουμε ότι έχουμε συνδεθεί στο FW1.

4.6

Στο FW1 εκτελούμε `ipfw show`. Οι μετρητές που είναι μη-μηδενικοί δείχνουν και τους κανόνες που χρησιμοποιήθηκαν, οι οποίοι είναι:

```
01100 allow ip from any to any via em0
65535 deny ip from any to any
```

4.7

Στο FW1 εκτελούμε:

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

4.8

Στο FW1 εκτελούμε:

```
ipfw add 3001 allow all from any to any
```

4.9

Στο FW1 εκτελούμε:

```
ipfw add 2000 nat 123 all from any to any recv em1
```

4.10

Στο FW1 εκτελούμε:

```
ipfw add 2001 check-state
```

4.11

Στο PC1 εκτελούμε `ping 192.0.2.1`. Απαντά το FW1.

4.12

Στον SRV1 εκτελούμε `ping 192.0.2.1`. Απαντά το PC2.

4.13

Στο PC1 εκτελούμε `ssh lab@192.0.2.1`. Συνδεόμαστε στο FW1.

4.14

Στον SRV1 εκτελούμε `ssh lab@192.0.2.1`. Συνδεόμαστε στο PC1.

4.15

Στον SRV1 εκτελούμε `ftp lab@192.0.2.1`. Συνδεόμαστε στο PC2.

4.16

Στο PC1 εκτελούμε `ping 192.0.2.5`. Το ping είναι επιτυχές.

4.17

Στο PC1 εκτελούμε `ssh lab@192.0.2.5`. Μπορούμε να συνδεθούμε κανονικά.

4.18

Στο PC1 εκτελούμε:

```
ftp lab@192.0.2.5
ls /etc
get /etc/rc.conf
```

Μπορούμε να εκτελέσουμε όλες αυτές τις ενέργειες.

4.19

Στο FW1 εκτελούμε:

```
ipfw add 2999 deny all from any to any via em1
```

4.20

Εκτελούμε:

```
### 4.11 ###

PC1: ping 192.0.2.1          # SUCCESSFUL

### 4.12 ###

SRV1: ping 192.0.2.1         # FAILED

### 4.13 ###

PC1: ssh lab@192.0.2.1       # SUCCESSFUL

### 4.14 ###
```

```
SRV1: ssh lab@192.0.2.1      # FAILED

### 4.15 ###

SRV1: ftp lab@192.0.2.1      # FAILED

### 4.16 ###

PC1: ping 192.0.2.5          # FAILED

### 4.17 ###

PC1: ssh lab@192.0.2.5       # FAILED

### 4.18 ###

PC1: ftp lab@192.0.2.5       # FAILED
```

Βλέπουμε ότι μόνο οι εντολές των ερωτημάτων 4.11 και 4.13 επιτυγχάνουν.

4.21

Στο FW1 εκτελούμε:

```
ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
```

4.22

Στο PC1 εκτελούμε `ping 192.0.2.5`. Το ping είναι επιτυχές.

4.23

Στο FW1 εκτελούμε:

```
ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state
```

4.24

Στο PC1 εκτελούμε `ssh lab@192.0.2.5`. Μπορούμε να συνδεθούμε κανονικά.

4.25

Στο FW1 εκτελούμε:

```
ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state
```

4.26

Στον SRV1 εκτελούμε `ping 192.0.2.1`. Απαντά το PC2.

4.27

Στο FW1 εκτελούμε:

```
ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state
```

4.28

Στον SRV1 εκτελούμε `ssh lab@192.0.2.1`. Συνδεόμαστε στο PC1.

4.29

Στον SRV1 εκτελούμε `ftp lab@192.0.2.1`. Το ftp αποτυγχάνει.

4.30

Πρέπει να προσθέσουμε τους κανόνες:

```
ipfw add 2700 skipto 3000 tcp from any to any 21 recv em1 keep-state
ipfw add 2701 skipto 3000 tcp from any 20 to any out via em1 keep-state
```

Άσκηση 5: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

5.1

Από το γραφικό περιβάλλον:

```
Interfaces - LAN - Primary configuration - IP address
```

Έχει ρυθμιστεί η διεύθυνση `192.168.1.1/24`.

5.2

Από το γραφικό περιβάλλον:

```
Interfaces - WAN - Static IP configuration - IP address
```

Έχει ρυθμιστεί η διεύθυνση `10.0.0.1/30`.

5.3

Από το γραφικό περιβάλλον:

```
Status - System - Memory Usage
```

Χρησιμοποιείται το 34% της μνήμης, επομένως το ποσοστό της ελεύθερης μνήμης είναι 66%.

5.4

Από το γραφικό περιβάλλον:

`Interfaces (assign)`

Έχουμε:

```
Interface Network Port
LAN       em0 (Intel(R)...
WAN       em1 (Intel(R)...
MNG       em2 (Intel(R)...
DMZ       em3 (Intel(R)...
```

οπότε συνολικά βλέπουμε 4 διεπαφές. Επιβεβαιώνουμε ότι στο VirtualBox οι κάρτες δικτύου είναι σωστά ρυθμισμένες.

5.5

Από το γραφικό περιβάλλον:

`Interfaces - DMZ - IP configuration - IP address`

Έχει ρυθμιστεί η διεύθυνση `172.22.1.1/24`.

5.6

Από το γραφικό περιβάλλον:

`System - General setup - Hostname`

Το όνομα είναι `fw`.

5.7

Από το γραφικό περιβάλλον:

`System - General setup - Hostname`

Αλλάζουμε την τιμή σε ”fw1” και πατάμε ”Save”.

5.8

Από το γραφικό περιβάλλον:

`Firewall - Rules - WAN`

Δεν υπάρχουν κανόνες για το WAN.

5.9

Από το γραφικό περιβάλλον:

```
Interfaces - WAN
```

Στο υπο-μενού ”Static IP configuration” αλλάζουμε τις τιμές των πεδίων ”IP address” και ”Gateway” σε `192.0.2.1/30` και `192.0.2.2` αντίστοιχα, και ύστερα στο κάτω μέρος ενεργοποιούμε την επιλογή ”Block private networks”. Τέλος, πατάμε ”Save” για την εφαρμογή των αλλαγών.

5.10

Από το γραφικό περιβάλλον:

```
Firewall - Rules - WAN
```

Πλέον εμφανίζεται ο κανόνας:

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

5.11

Από το γραφικό περιβάλλον:

```
Services - DNS forwarder
Services - Dynamic DNS
Services - DHCP server
Services - DHCP relay
Services - SNMP
Services - Proxy ARP
Services - Captive portal
Services - Wake on LAN
Services - Scheduler
VPN - IPsec
VPN - PPTP
```

Καμία υπηρεσία δεν είναι ενεργοποιημένη.

5.12

Από το γραφικό περιβάλλον:

```
Services - DNS forwarder
```

Ενεργοποιούμε την επιλογή ”Enable DNS forwarder” και πατάμε ”Save”.

5.13

Από το γραφικό περιβάλλον:

`Services - DHCP server - LAN`

Τσεκάρουμε το κουτί ”Enable” και αλλάζουμε το πεδίο ”Range”:

`Range: 192.168.1.2 to 192.168.1.3`

Τέλος, πατάμε ”Save”.

5.14

Στο PC1 εκτελούμε:

```
dhclient em0
ifconfig em0 | grep inet
netstat -rn | grep default
cat /etc/resolv.conf | grep nameserver
```

Έχουμε:

```
IP address: 192.168.1.2
Default gateway: 192.168.1.1
DNS server address: 192.168.1.1
```

5.15

Χρειάστηκε προκειμένου η υπηρεσία DHCP να λειτουργεί και ως εξυπηρετητής DNS για τους πελάτες DHCP στο LAN, αλλιώς θα έπρεπε να ορίσουμε εξυπηρετητή DNS χειροκίνητα.

5.16

Στο μενού:

`Diagnostics - DHCP Leases`

5.17

Από το γραφικό περιβάλλον:

`Diagnostics - ARP Table`

Βλέπουμε 9 εγγραφές:

IP address	MAC address	Interface
172.22.1.2	08:00:27:62:6b:12	DMZ
172.22.1.1	08:00:27:2b:a4:d8	DMZ
192.168.56.1	0a:00:27:00:00:00	MNG
192.168.56.2	08:00:27:78:b0:f7	MNG
192.0.2.2	08:00:27:b1:c8:2f	WAN
192.0.2.1	08:00:27:cc:e3:72	WAN
192.168.1.1	08:00:27:03:6b:29	LAN
192.168.1.3	08:00:27:5e:eb:81	LAN
192.168.1.2	08:00:27:75:42:4f	LAN

5.18

Στο PC1 εκτελούμε `ping 192.168.1.1`. Δεν λαμβάνουμε απάντηση.

5.19

Από το γραφικό περιβάλλον:

`Diagnostics - Logs - Firewall`

Βλέπουμε τις 50 πιο πρόσφατες καταγραφές πακέτων που έχουν περάσει από το firewall, και την αντίστοιχη ενέργεια που εκτελέστηκε για κάθε πακέτο. Βλέπουμε ότι οι πρώτες 3 γραμμές του πίνακα αφορούν το ping που εκτελέσαμε προηγουμένως:

```
Act      If       Source           Destination                 Proto
X        LAN      192.168.1.2      192.168.1.1, type echo/0    ICMP
X        LAN      192.168.1.2      192.168.1.1, type echo/0    ICMP
X        LAN      192.168.1.2      192.168.1.1, type echo/0    ICMP
```

Καθαρίζουμε το αρχείο καταγραφών από το γραφικό περιβάλλον:

`Diagnostics - Logs - Firewall - Clear log`

5.20

Από το γραφικό περιβάλλον:

`Diagnostics - Firewall states`

Βλέπουμε 2 firewall states.

5.21

Από το γραφικό περιβάλλον:

`Firewall - Rules - LAN`

Δεν βλέπουμε κανέναν κανόνα.

5.22

Από το γραφικό περιβάλλον:

`Firewall - Rules - LAN`

Πατάμε το κουμπί ”+” και τροποποιούμε τα πεδία ως εξής:

```
Action: Pass
Interface: LAN
Protocol: any
Source:
    Type: LAN subnet
Destination:
    Type: any
```

Τέλος πατάμε ”Save” και ύστερα ”Apply changes”.

5.23

Στο PC1 εκτελούμε:

```
ping 192.168.1.1    # LAN1, successful
ping 192.0.2.1      # WAN1, successful
ping 172.22.1.1     # DMZ, successful
```

Και τα τρία ping είναι επιτυχή.

5.24

Στον R1 εκτελούμε `do ping 192.0.2.1`. Δεν λαμβάνουμε απάντηση.

5.25

Στον R1 εκτελούμε `arp -a`. Έχουμε:

```
IP address       MAC address             Interface
192.0.2.2        08:00:27:b1:c8:2f       em0
192.0.2.1        08:00:27:cc:e3:72       em0
```

Ναι, η δεύτερη εγγραφή αφορά τη ζητούμενη διεύθυνση MAC.

5.26

Από το γραφικό περιβάλλον:

`Firewall - Rules - WAN`

Πατάμε το κουμπί ”+” και τροποποιούμε τα πεδία ως εξής:

```
Action: Pass
Interface: WAN
Protocol: ICMP
ICMP type: any
Source:
    Type: any
Destination:
    Type: WAN address
```

Πατάμε ”Save” και ”Apply changes”.

5.27

Στον R1 εκτελούμε `do ping 192.0.2.1`. Το ping είναι επιτυχές.

5.28

Στον R1 εκτελούμε `do ping 192.168.1.2`. Εμφανίζεται μήνυμα λάθους ”No route to host”, αφού δεν υπάρχει εγγραφή στον πίνακα δρομολόγησης σχετική με την (ιδιωτική) διεύθυνση `192.168.1.2`.

5.29

Στο PC1 εκτελούμε `ping 192.0.2.2`. Το ping είναι επιτυχές. Συμπεραίνουμε ότι στο FW1, κατά την κατεύθυνση PC1 → R1 αντικαθίσταται η εσωτερική τοπική διεύθυνση IP του PC1 με την διεύθυνση της διεπαφής του FW1 στο WAN1, γι' αυτό και ο R1 μπορεί να απαντήσει κανονικά με ICMP reply. Επομένως έχουμε παραδοσιακό/απερχόμενο NAT (Traditional/Outbound NAT), .

5.30

Έχουμε ήδη τοποθετήσει τον SRV1 στο DMZ και έχουμε ήδη ορίσει τη διεύθυνση IP του με την εντολή:

```
ifconfig em0 172.22.1.2/24
```

Στο PC1 εκτελούμε `ping 172.22.1.2`. Δε λαμβάνουμε απάντηση. Αυτό συμβαίνει επειδή δεν γίνεται μετάφραση διευθύνσεων προς το DMZ και δεν υπάρχει εγγραφή σχετική με την εσωτερική τοπική διεύθυνση `192.168.1.2` του PC1 στον πίνακα δρομολόγησης του SRV1, επομένως δεν μπορεί να απαντήσει στα ICMP request του PC1, τα οποία όμως λαμβάνει κανονικά.

5.31

Στον SRV1 εκτελούμε `route add default 172.22.1.1`.

5.32

Στο PC1 εκτελούμε `ping 172.22.1.2`. Πλέον το ping είναι επιτυχές.

5.33

Στον SRV1 εκτελούμε `ping 172.22.1.1`. Δε λαμβάνουμε απάντηση. Αυτό συμβαίνει επειδή δεν έχουμε ορίσει κανέναν κανόνα στο FW1 που να επιτρέπει την εξερχόμενη κίνηση από το DMZ, οπότε τα ICMP reply απορρίπτονται.

5.34

Στον SRV1 εκτελούμε:

```
ping 192.168.1.2
ping 192.0.2.2
```

Σε κανένα από τα δύο ping δε λαμβάνουμε απάντηση. Αυτό συμβαίνει πάλι επειδή δεν έχουμε ορίσει κανέναν κανόνα στο FW1 που να επιτρέπει την εξερχόμενη κίνηση από το DMZ, οπότε τα ICMP reply απορρίπτονται.

5.35

Από το γραφικό περιβάλλον:

```
Firewall - Rules - DMZ
```

Πατάμε το ”+” και τροποποιούμε τα πεδία ως εξής (το `[v]` παρακάτω σημαίνει ότι το κουτάκι είναι τσεκαρισμένο):

```
Action: Pass
Interface: DMZ
Protocol: any
Source:
    Type: DMZ subnet
Destination: [v] not
    Type: LAN subnet
```

Πατάμε ”Save” και ”Apply changes”.

5.36

Στον SRV1 εκτελούμε `ping 172.22.1.1`. Το ping είναι επιτυχές.

5.37

Στον SRV1 εκτελούμε `ping 192.0.2.1`. Το ping είναι επιτυχές.

5.38

Στον R1 εκτελούμε `do ping 172.22.1.2`. Το ping αποτυγχάνει με μήνυμα ”No route to host”. Αυτό είναι λογικό, καθώς δεν υπάρχει εγγραφή σχετική με τη διεύθυνση `172.22.1.2` στον πίνακα δρομολόγησης του R1.

5.39

Στον SRV1 εκτελούμε `ping 192.0.2.2`. Το ping είναι επιτυχές. Αυτό συμβαίνει διότι τα πακέτα περνούν από το FW1 και εκεί γίνεται μετάφραση διευθύνσεων, στην οποία η διεύθυνση πηγής των ICMP request αλλάζει από `172.22.1.2` σε `192.0.2.1`, και έτσι ο R1 μπορεί πλέον να απαντήσει με ICMP reply, αφού διαθέτει εγγραφή σχετική με το δίκτυο `192.0.2.0/30`.

5.40

Στο PC2 εκτελούμε:

```
dhclient em0
ifconfig em0 | grep inet
netstat -rn | grep default
cat /etc/resolv.conf | grep nameserver
```

Έχουμε:

```
IP address: 192.168.1.3
Default gateway: 192.168.1.1
DNS server address: 192.168.1.1
```

5.41

Από το γραφικό περιβάλλον:

`Firewall - Rules - LAN`

Πατάμε το ”+” και τροποποιούμε κατάλληλα τα πεδία:

```
Action: Block
Interface: LAN
Protocol: any
Source:
    Type: Single host or alias
    Address: 192.168.1.3
Destination:
    Type: Single host or alias
    Address: 172.22.1.2
```

Πατάμε ”Save” και ”Apply changes”.

5.42

Πρέπει να τοποθετηθεί πριν από τον ήδη υπάρχοντα, αλλιώς δεν θα χρησιμοποιηθεί ποτέ, αφού ο ήδη υπάρχοντας επιτρέπει όλη την κίνηση από το LAN.

5.43

Στο PC2 εκτελούμε `ping 172.22.1.2`. Δεν λαμβάνουμε απάντηση.

5.44

Στο PC2 εκτελούμε `ping 172.22.1.1`. Το ping είναι επιτυχές. Αυτό συμβαίνει γιατί ο τελευταίος κανόνας που ορίσαμε σταματά μόνο την κίνηση από το PC2 προς τον SRV1, και όχι από το PC2 προς το FW1, και έτσι ο έλεγχος περνά στον επόμενο κανόνα που επιτρέπει όλη την κίνηση από το LAN.

Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT

6.1

Στον R1 εκτελούμε `ip route 203.0.118.0/24 192.0.2.1`.

6.2

Από το γραφικό περιβάλλον του FW1:

`Firewall - NAT - Outbound`

Τσεκάρουμε το κουτί ”Enable advanced outbound NAT” και πατάμε ”Save”.

6.3

Από το γραφικό περιβάλλον του FW1:

`Firewall - NAT - Outbound`

Πατάμε το ”+” και τροποποιούμε τα πεδία:

```
Interface: WAN
Source: 192.168.1.2/32
Destination:
    Type: any
Target: 203.0.118.14
```

Πατάμε ”Save” και ”Apply changes”.

6.4

Από το γραφικό περιβάλλον του FW1:

`Firewall - NAT - Outbound`

Πατάμε το ”+” και τροποποιούμε τα πεδία:

```
Interface: WAN
Source: 192.168.1.3
Destination:
    Type: any
Target: 203.0.118.15
```

Πατάμε ”Save” και ”Apply changes”.

6.5

Στον R1 εκτελούμε `tcpdump -i em0`.

6.6

Στο PC1 εκτελούμε `ping -c 1 192.0.2.2`. Το ping επιτυγχάνει, και τα πακέτα φτάνουν με διεύθυνση IP την `203.0.118.14`.

6.7

Στο PC2 εκτελούμε `ping -c 1 192.0.2.2`. Το ping επιτυγχάνει, και τα πακέτα φτάνουν με διεύθυνση IP την `203.0.118.15`.

6.8

Από νέο παράθυρο εντολών στον R1 εκτελούμε `ping 203.0.118.14`. Το ping όντως αποτυγχάνει. Αυτό συμβαίνει διότι δεν υπάρχει κανόνας στο firewall που να επιτρέπει την ICMP κίνηση από το WAN σε άλλη διεύθυνση εκτός από την WAN Address, δηλαδή την `192.0.2.1`.

6.9

Από το γραφικό περιβάλλον του FW1:

`Firewall - NAT - Server NAT`

Πατάμε το "+" και τροποποιούμε το πεδίο:

`External IP address: 203.0.118.18`

Πατάμε "Save" και "Apply changes".

6.10

Από το γραφικό περιβάλλον του FW1:

`Firewall - NAT - Inbound`

Πατάμε το "+" και τροποποιούμε τα πεδία (το `[v]` παρακάτω σημαίνει ότι το αντίστοιχο κουτί είναι τσεκαρισμένο):

```
Interface: WAN
External address: 203.0.118.18
Protocol: TCP
External port range:
    from: SSH
    to: SSH
NAT IP: 172.22.1.2
Local port: SSH
[v] Auto-add a firewall rule to permit traffic through this NAT rule
```

Πατάμε "Save" και "Apply changes".

6.11

Από το γραφικό περιβάλλον του FW1:

`Firewall - Rules - WAN`

Προστίθεται ο κανόνας:

Action	Proto	Source	Port	Destination	Port	Description
Allow	TCP	*	*	172.22.1.2	22 (SSH)	NAT

Ο παραπάνω κανόνας προστέθηκε επειδή τσεκάραμε το κουτί "Auto-add a firewall rule to permit traffic through this NAT rule" καθώς ορίζαμε τον παραπάνω κανόνα NAT.

6.12

Στον R1 εκτελούμε `ssh lab@203.0.118.18`. Συνδεόμαστε στον SRV1, όπως μπορούμε να δούμε και από την έξοδο της εντολής `hostname`.

6.13

Στο R1 εκτελούμε `do ping 203.0.118.18`. Δεν λαμβάνουμε απάντηση. Αυτό συμβαίνει διότι από τη μία δεν υπάρχει κάποιος NAT κανόνας για την κίνηση ICMP που παράγεται από το ping, και από την άλλη δεν υπάρχει κάποιος κανόνας που να επιτρέπει την ICMP κίνηση προς τον προορισμό `203.0.118.18`, οπότε τα πακέτα απορρίπτονται από το firewall.

6.14

Στο PC2 εκτελούμε:

```
ssh lab@203.0.118.18
```

Μπορούμε να συνδεθούμε κανονικά. Εκτελώντας καταγραφές στις διεπαφές:

```
PC2@em0, R1@em0, SRV1@em0
```

παρακολουθούμε την πορεία ενός συγκεκριμένου TCP τεμαχίου (επιλέγουμε ένα που έχει συγκεκριμένη τιμή `seq` και το παρατηρούμε). Διαπιστώνουμε ότι ακολουθείται η πορεία:

- PC2 → SRV1:
  - PC2 → FW1 → R1 → FW1 → SRV1
- SRV1 → PC2:
  - SRV1 → FW1 → R1 → FW1 → PC2

Αναλύουμε τα βήματα της διαδρομής, καταγράφοντας κάθε φορά τις διευθύνσεις πηγής και προορισμού του πακέτου και σχολιάζοντας τι γίνεται σε κάθε βήμα:

- PC2 → SRV1:
  - PC2 → FW1: `192.168.1.3` → `203.0.118.18`
    Το πακέτο προωθήθηκε με βάση την προκαθορισμένη διαδρομή του PC2 μέσω του FW1.

    Στο FW1 γίνεται μετάφραση NAT στη διεύθυνση πηγής: `192.168.1.3` → `203.0.118.15`, γιατί το πακέτο πρόκειται να εξέλθει στο WAN.

    Δεν γίνεται μετάφραση NAT στη διεύθυνση προορισμού, γιατί το πακέτο δεν προέρχεται από το WAN.

  - FW1 → R1: `203.0.118.15` → `203.0.118.18`
    Το πακέτο προωθήθηκε με βάση την προκαθορισμένη διαδρομή του FW1 μέσω του R1.

  - R1 → FW1: `203.0.118.15` → `203.0.118.18`
    Το πακέτο προωθήθηκε με βάση την εγγραφή για το δίκτυο `203.0.118.0/24` στον πίνακα δρομολόγησης του R1 μέσω του FW1.

Στο FW1 γίνεται μετάφραση NAT στη διεύθυνση προορισμού: `203.0.118.18` → `172.22.1.2`, γιατί το πακέτο προέρχεται από το WAN.

Δεν γίνεται μετάφραση NAT στη διεύθυνση πηγής, γιατί το πακέτο δεν πρόκειται να εξέλθει στο WAN.

- FW1 → SRV1: `203.0.118.15` → `172.22.1.2`
  Το πακέτο προωθείται τελικά στον προορισμό με επιτυχία.

6.15

Από το γραφικό περιβάλλον του FW1:

`Firewall - NAT - Outbound`

Επιλέγουμε τον κανόνα για το PC1 (Source `192.168.1.2`) και πατάμε "Delete selected mappings". Ύστερα στο PC1 εκτελούμε `ping 192.0.2.2`. Δεν λαμβάνουμε απάντηση. Με tcpdump στον R1 βλέπουμε ότι τα ICMP request έχουν διεύθυνση πηγής την `192.168.1.2` (δεν έχουν υποστεί δηλαδή μετάφραση, επειδή διαγράψαμε τον σχετικό κανόνα Outbound NAT), για την οποία δεν υπάρχει σχετική εγγραφή στον πίνακα δρομολόγησης του R1, επομένως ο R1 δεν μπορεί να απαντήσει με ICMP reply.

6.16

Από το γραφικό περιβάλλον του FW1:

`Firewall - NAT - Outbound`

Αποεπιλέγουμε το κουτί "Enable advanced outbound NAT", πατάμε "Save" και εκτελούμε ξανά στο PC1 `ping 192.0.2.2`. Αυτή τη φορά το ping είναι επιτυχές.

6.17

Εκτελούμε:

```
### R1 ###

ssh lab@203.0.118.18

### PC2 ###

ssh lab@203.0.118.18
```

Μπορούμε να συνδεθούμε κανονικά από τον R1, αλλά όχι από το PC2.

6.18

Στον SRV1 εκτελούμε `tcpdump -i em0` και στο PC2 εκτελούμε `ssh lab@203.0.118.18`. Στην καταγραφή φαίνεται ότι γίνονται συνεχώς προσπάθειες για σύναψη τριμερούς TCP χειραψίας, οι οποίες αποτυγχάνουν. Συγκεκριμένα, ενώ αποστέλλονται τα δύο πρώτα τεμάχια (πρώτο τεμάχιο -σημαία SYN- από τη διεύθυνση `192.0.2.1`, δεύτερο τεμάχιο -σημαίες SYN, ACK- από τη διεύθυνση `172.22.1.2`), αμέσως μετά αποστέλλεται από τη διεύθυνση `192.0.2.1` πακέτο για τερματισμό της σύνδεσης -σημαία RST-. Αυτό επαναλαμβάνεται μέχρι να γίνει timeout από τη μεριά του PC2.

6.19

Για την παραπάνω συμπεριφορά δεν ευθύνονται οι δύο κανόνες που ορίσαμε παραπάνω, πρώτον επειδή ο PC2 προσπαθεί να επικοινωνήσει με τον SRV1 μέσω της διεύθυνσης `203.0.118.18` και όχι μέσω της `172.22.1.2`, και δεύτερον επειδή ο SRV1 χρησιμοποιεί τη διεύθυνση `192.0.2.1` και όχι το LAN net `192.168.1.0/24` για να αποστείλει τα τεμάχια TCP.

Λαμβάνοντας υπόψιν τη σημείωση στην καρτέλα για το Inbound NAT ("It is not possible to access NATed services using the WAN IP address from within LAN"), βλέπουμε πως το πρόβλημα έγκειται στο γεγονός ότι προσπαθούμε να χρησιμοποιήσουμε τη διεύθυνση `203.0.118.18` (NATed service) μέσα από το LAN, χρησιμοποιώντας την WAN IP διεύθυνση `192.0.2.1`. Αυτός είναι και ο λόγος που τερματίζεται συνεχώς η σύνδεση στο ερώτημα 6.18.

Άσκηση 7: IPSec site-to-site VPN

7.1

Από το VirtualBox (το `[ ]` σημαίνει ότι αποεπιλέγουμε το αντίστοιχο κουτί):

`FW1 - Network - Adapter 3 - Advanced - [ ] Cable connected`

7.2

Πηγαίνουμε στη διεύθυνση `http://192.168.56.2` και από το γραφικό περιβάλλον (του FW2):

`Interfaces - MNG - Primary configuration - IP configuration - IP address`

Αλλάζουμε το πεδίο σε `192.168.56.3/24` και πατάμε "Save".

7.3

Από το VirtualBox (το `[v]` σημαίνει ότι τσεκάρουμε το αντίστοιχο κουτί):

`FW1 - Network - Adapter 3 - Advanced - [v] Cable connected`

7.4

Πηγαίνουμε στις διευθύνσεις `http://192.168.56.2` και `http://192.168.56.3`. Και οι δύο σελίδες φορτώνουν κανονικά, και εμφανίζονται τα hostnames `fw1.lab.ntua.gr` και `fw.lab.ntua.gr`, οπότε έχουμε συνδεθεί ταυτόχρονα και στα δύο τείχη προστασίας.

7.5

Από το γραφικό περιβάλλον του FW2:

`System - General setup - Hostname`

Αλλάζουμε την τιμή του πεδίου σε `fw2` και πατάμε "Save".

7.6

Από το γραφικό περιβάλλον του FW2:

`Interface - WAN - Static IP configuration`

Αλλάζουμε τα πεδία ”IP address” και ”Gateway” σε `192.0.2.5/30` και `192.0.2.6` αντίστοιχα, επιλέγουμε το κουτί ”Block private networks” και πατάμε ”Save”.

7.7

Από το γραφικό περιβάλλον του FW2:

`Interfaces - LAN - Primary configuration`

Αλλάζουμε την τιμή του πεδίου ”IP address” σε `192.168.2.1/24` και πατάμε ”Save”.

7.8

Από το γραφικό περιβάλλον του FW2:

`Diagnostics - Reboot system - Yes`

7.9

Από το γραφικό περιβάλλον του FW2:

`Firewall - Rules - LAN`

Πατάμε το ”+” και τροποποιούμε κατάλληλα τα πεδία:

```
Action: Pass
Interface: LAN
Protocol: any
Source:
    Type: LAN subnet
Destination:
    Type: any
```

Πατάμε ”Save” και ”Apply changes”.

7.10

Από το γραφικό περιβάλλον του FW2:

`Firewall - Rules - WAN`

Πατάμε το ”+” και τροποποιούμε κατάλληλα τα πεδία:

```
Action: Pass
Interface: WAN
Protocol: ICMP
ICMP type: any
Source:
    Type: any
Destination:
    Type: WAN address
```

Πατάμε ”Save” και ”Apply changes”.

7.11

Έχουμε ήδη μετακινήσει το PC2 στο LAN2. Ορίζουμε διεύθυνση και προεπιλεγμένη πύλη στο PC2 με τις εντολές:

```
ifconfig em0 192.168.2.2/24
route add default 192.168.2.1
```

7.12

Στο PC1 εκτελούμε `ping 192.0.2.5`. Το ping είναι επιτυχές.

7.13

Στο PC2 εκτελούμε `ping 192.0.2.1`. Το ping είναι επιτυχές.

7.14

Εκτελούμε:

```
### PC1 ###

ping 192.168.2.2

### PC2 ###

ping 192.168.1.2
```

Και τα δύο ping αποτυγχάνουν με μήνυμα λάθους ”Destination Host Unreachable”, το οποίο έρχεται από τη διεύθυνση `192.0.2.2`, δηλαδή τον R1. Αυτό συμβαίνει διότι ο R1 δεν διαθέτει εγγραφή στον πίνακα δρομολόγησής του (`do show ip route`) σχετική με τις διευθύνσεις `192.168.1.2` και `192.168.2.2`, οπότε δεν μπορεί να προωθήσει τα πακέτα στον προορισμό.

7.15

Από το γραφικό περιβάλλον του FW1:

```
VPN - IPsec - Tunnels - [v] Enable IPsec - Save
```

Ύστερα πατάμε το ”+” και τροποποιούμε τα πεδία:

```
Local subnet:
    Type: LAN subnet
Remote subnet: 192.168.2.0/24
Remote gateway: 192.0.2.5
Pre-Shared Key: nick
```

Πατάμε ”Save” και ”Apply changes”.

7.16

Από το γραφικό περιβάλλον του FW1:

`Firewall - Rules - IPsec VPN`

Εμφανίζεται ο κανόνας:

Action	Proto	Source	Port	Destination	Port	Description
Allow	*	*	*	*	*	Default IPsec VPN

7.17

Από το γραφικό περιβάλλον του FW1:

`Diagnostics - IPsec - SAD`

Δεν έχουν ορισθεί σχέσεις.

7.18

Από το γραφικό περιβάλλον του FW1:

`Diagnostics - IPsec - SPD`

Έχουν ορισθεί 2 πολιτικές:

Source	Destination	Direction	Protocol	Tunnel endpoints
192.168.2.0/24	192.168.1.0/24	-->	ESP	192.0.2.5-192.0.2.1
192.168.1.0/24	192.168.2.0/24	<--	ESP	192.0.2.1-192.0.2.5

7.19

Από το γραφικό περιβάλλον του FW2:

`VPN - IPsec - Tunnels - [v] Enable IPsec - Save`

Ύστερα πατάμε το ”+” και τροποποιούμε τα πεδία:

```
  Local subnet:
      Type: LAN subnet
  Remote subnet: 192.168.1.0/24
  Remote gateway: 192.0.2.1
  Pre-Shared Key: nick
```

Πατάμε ”Save” και ”Apply changes”.

7.20

Από το γραφικό περιβάλλον του FW2:

`Diagnostics - IPsec - SAD`

Δεν έχουν ορισθεί σχέσεις.

7.21

Από το γραφικό περιβάλλον του FW2:

`Diagnostics - IPsec - SPD`

Έχουν ορισθεί 2 πολιτικές:

Source	Destination	Direction	Protocol	Tunnel endpoints
192.168.1.0/24	192.168.2.0/24	-->	ESP	192.0.2.1-192.0.2.5
192.168.2.0/24	192.168.1.0/24	<--	ESP	192.0.2.5-192.0.2.1

7.22

Στο PC1 εκτελούμε `ping 192.168.2.2`. Το ping είναι επιτυχές.

7.23

Στο PC2 εκτελούμε `ping 192.168.1.2`. Το ping είναι επιτυχές.

7.24

Από το γραφικό περιβάλλον του FW1:

`Diagnostics - IPsec - SAD`

Πλέον έχουν ορισθεί 2 σχέσεις:

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.1	192.0.2.5	ESP	08911c49	3des-cbc	hmac-sha1
192.0.2.5	192.0.2.1	ESP	0a631651	3des-cbc	hmac-sha1

7.25

Από το γραφικό περιβάλλον του FW2:

`Diagnostics - IPsec - SAD`

Πλέον έχουν ορισθεί 2 σχέσεις:

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.5	192.0.2.1	ESP	0a631651	3des-cbc	hmac-sha1
192.0.2.1	192.0.2.5	ESP	08911c49	3des-cbc	hmac-sha1

7.26

Στον R1 εκτελούμε `tcpdump -vi em0`.

7.27

Εκτελούμε:

```
### PC1 ###

ping 192.168.2.2

### PC2 ###

ping 192.168.1.2
```

Δεν παρατηρούμε πακέτα ICMP.

7.28

Εμφανίζονται πακέτα ESP, κάποια με πηγή `192.0.2.1` και προορισμό `192.0.2.5`, και τα υπόλοιπα με πηγή `192.0.2.5` και προορισμό `192.0.2.1`.

7.29

Όχι, δεν υπάρχει κάπου η πληροφορία για τις διευθύνσεις IP των PC1 και PC2.

7.30

Στο PC2 εκτελούμε `ssh lab@203.0.118.18`. Μπορούμε να συνδεθούμε κανονικά. Ο λόγος είναι ότι παρόλο που ακόμα προσπαθούμε να χρησιμοποιήσουμε NATed υπηρεσίες μέσα από ένα LAN, πλέον ως διεύθυνση πηγής δεν χρησιμοποιείται η WAN IP του FW1 (`192.0.2.1`), αλλά η WAN IP του FW2 `192.0.2.5`, οπότε μπορούν να χρησιμοποιηθούν οι NATed services.

7.31

Παρατηρούμε πακέτα TCP, κάποια με πηγή `192.0.2.5` και προορισμό `203.0.118.18`, και τα υπόλοιπα με πηγή `203.0.118.18` και προορισμό `192.0.2.5`.

7.32

Ναι, είναι κρυπτογραφημένα με το IPsec.