

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ
ΥΠΟΛΟΓΙΣΤΩΝ
ΡΟΗ Δ - ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (COMPUTER
NETWORKS LAB)

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 03120827

ΑΝΑΦΟΡΑ 10ΗΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ

Ομάδα: 1

Λογισμικό: Linux Ubuntu 22.04

Όνομα PC: glaptop

ΑΣΚΗΣΗ 1:

- 1.1 Θα χρησιμοποιήσω τις εντολές:
hostname PC1
ifconfig em0 inet 192.168.1.2/24
(Ομοίως για το PC2)
- 1.2 Θα χρησιμοποιήσω την εντολή: kldload ipfw
- 1.3 Θα χρησιμοποιήσω την εντολή: kldstat
(Εμφανίζεται το αρχείο ipfw.ko)
- 1.4 Όχι, εμφανίζεται μήνυμα Permission denied
- 1.5 Θα χρησιμοποιήσω την εντολή: ipfw list
Υπάρχει μόνο ένας κανόνας με αριθμό 65535
deny ip from any to any
- 1.6 Θα χρησιμοποιήσω την εντολή:
ipfw add 100 allow all from any to any via lo0
- 1.7 Ναι, τώρα τα ping λειτουργούν κανονικά
- 1.8 Θα χρησιμοποιήσω την εντολή: ipfw show
- 1.9 Με την εντολή: ipfw zero
- 1.10 Όχι, το ping εμφανίζει Permission Denied
- 1.11 Θα χρησιμοποιήσω την εντολή:
ipfw add allow icmp from any to any
- 1.12 Ο κανόνας έλαβε τον αριθμό 200
(λογικό σύμφωνα με την ανάλυση στην αρχή της άσκησης)
- 1.13 Ναι, τώρα τα ping λειτουργούν κανονικά (και από τις 2 κατευθύνσεις)
- 1.14 Το traceroute δεν δουλεύει καθώς στέλνει μηνύματα UDP. Μπορώ να
χρησιμοποιήσω την μετατροπή -I ώστε να στέλνει ICMP μηνύματα
- 1.15 Θα χρησιμοποιήσω την εντολή:
ipfw add allow udp from any to any
- 1.16 Όχι, εμφανίζει Permission Denied
- 1.17 Θα χρησιμοποιήσω τις εντολές:
ipfw add allow tcp from any to any out

- ipfw add allow tcp from any to any in
- 1.18** Θα χρησιμοποιήσω τις εντολές:
ipfw zero
ssh lab@192.168.1.3
- 1.19** Οι κανόνες εφαρμόστηκαν:
47 φορές, για τα εξερχόμενα μηνύματα
44 φορές, για τα εισερχόμενα μηνύματα
Η διαφορά αυτή βγάζει νόημα, λόγω της τριμερούς χειραψίας
- 1.20** Ναι, μπορούμε να συνδεθούμε κανονικά με ssh απο το PC2 στο PC1. Αυτό συμβαίνει γιατί ορίσαμε κανόνες τόσο για την εισερχόμενη διέλευση όσο και για την εξερχόμενη και επίσης το PC2 δεν επηρεάζεται απο κάποιον κανόνα
- 1.21** Θα χρησιμοποιήσω την εντολή: service ftpd onestart
- 1.22** Ναι, μπορώ να συνδεθώ κανονικά με ftp απο το PC1 στο PC2 και να κατεβάσω αρχεία

ΑΣΚΗΣΗ 2:

- 2.1** Θα χρησιμοποιήσω την εντολή: kldload ipfw
- 2.2** Όχι, το ping δεν λειτουργεί
(Εμφανίζει Permission Denied)
- 2.3** Θα χρησιμοποιήσω την εντολή:
ipfw add 100 allow all from any to any via lo0
- 2.4** Θα χρησιμοποιήσω την εντολή:
ipfw add allow icmp from me to any icmptype 8
- 2.5** Τώρα το ping γίνεται αλλά δεν εμφανίζει απάντηση.
- 2.6** Παρατηρώ ότι το PC1 έχει διπλάσιες μετρήσεις απο το PC2. Επομένως περνάνε μόνο τα ICMP request πακέτα και τα Reply δεν περνάνε απο το PC2
- 2.7** Θα χρησιμοποιήσω τις εντολές:
ipfw delete 200
ipfw add allow icmp from me to any icmptype 8 keep-state
Ναι, τώρα το ping λειτουργεί. Χρη στο keep-state το PC2 αναγνωρίζει ότι ένα ICMP Reply οφείλεται σε ένα ICMP request που είχε στείλει το ίδιο πριν
- 2.8** Ναι και τα 2 ping λειτουργούν
- 2.9** Τώρα το ping απο το PC1 προς το PC2 δεν λειτουργεί. Αυτό συμβαίνει καθώς εφόσον δεν τρέχει ping απο το PC2 προς το PC1 ο δυναμικός κανόνας keep-state (που λειτουργεί για την αμφίδρομη κίνηση) δεν ισχύει
- 2.10** Θα χρησιμοποιήσω την εντολή:
ipfw add allow icmp from any to any icmptype 8 keep-state
- 2.11** Με τις εντολές αυτές παρατηρώ:
ipfw -d show: Πληροφορίες για όλους τους κανόνες (και δυναμικούς)
ipfw -D show: Πληροφορίες για τους δυναμικούς κανόνες μόνο
- 2.12** Πλέον δεν υπάρχει πληροφορία για τους δυναμικούς κανόνες. Επομένως

- η πληροφορία αυτή εμφανίζεται μόνο όταν αυτοι χρησιμοποιούνται
- 2.13** Θα χρησιμοποιήσω τις εντολές:
ipfw add allow udp from any to me
ipfw add allow icmp from me to any icmp type 3
- 2.14** Θα χρησιμοποιήσω τις εντολές:
ipfw add allow udp from me to any
ipfw add allow icmp from any to me icmp type 3
- 2.15** Καμία, καθώς στον κανόνα του PC1 έχουμε ορίσει from any to any
- 2.16** Θα χρησιμοποιήσω την εντολή:
ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state
(22 = tcp port for ssh)
- 2.17** Με την εντολή: ssh lab@192.168.1.3 συνδεόμαστε με επιτυχία
- 2.18** Θα χρησιμοποιήσω την εντολή:
ipfw add allow tcp from me to any 22 keep-state
- 2.19** Θα πρέπει να προσθέσουμε τον κανόνα:
ipfw add allow tcp from 192.168.1.3 to me 22
- 2.20** Ναι, μπορούμε κανονικά
- 2.21** Όχι, δεν μπορούμε να συνδεθούμε με ftp. Θα προσθέσουμε τον κανόνα:
ipfw add allow tcp from 192.168.1.3 to me 21 keep-state
- 2.22** Γιατί κατά την δεύτερη λειτουργία χρησιμοποιείται το port 20
(διαδικασία data transfer)
- 2.23** Θα προσθέσω τον κανόνα:
ipfw add allow tcp from any 21 to me keep-state
- 2.24** Ναι, μπορώ κανονικά
- 2.25** Θα πρέπει να προσθέσω τους κανόνες:
ipfw dd allow tcp from me 20 to any (PC2)
ipfw dd allow tcp from any 20 to me (PC1)
- 2.26** Όταν χρησιμοποιούμε πρωτόκολλα όπως το FTP κρίνεται απαραίτητο το τείχος προστασίας καθώς δεν υπάρχει κρυπτογράφηση (για ασφάλεια)
- 2.27** Θα χρησιμοποιήσω τις εντολές:
kldunload ipfw
kldstat

ΑΣΚΗΣΗ 3:

- 3.1** Θα χρησιμοποιήσω τις εντολές:
route add default 192.168.1.1
- 3.2** Θα χρησιμοποιήσω τις εντολές:
configure terminal
hostname R1
interface em0
ip address 192.0.2.2/30
exit
interface em1
ip address 192.0.2.6/30
- 3.3** Θα χρησιμοποιήσω τις εντολές:

```
hostname SRV1
ifconfig em0 inet 192.0.2.5/30
route add default 192.0.2.6
```

3.4 Θα χρησιμοποιήσω την εντολή: `service ftpd onestart`

3.5 Θα χρησιμοποιήσω την εντολή: `kldstart`

Παρατηρώ τα modules: `kernel / intpm / smbust / ipfw / ipfw_nat / libalias`

3.6 Ενεργοποιήθηκε το τείχος προστασίας `ipfw`

3.7 Χρησιμοποιώντας την εντολή: `sysrc firewall_type` βλέπω ότι:
`Firewall_type = UNKNOWN`

3.8 Παρατηρώ 11 κανόνες. Ο τελευταίος κανόνας είναι ο default:
`deny ip from any to any`

3.9 Θα χρησιμοποιήσω την εντολή: `ipfw nat show config`

Παρατηρώ ότι δεν έχουν ορισθεί πίνακες in-kernel NAT

3.10 Όχι, τα `ping` δεν εμφανίζουν απάντηση

3.11 Όχι, το `ping` δεν εμφανίζει απάντηση

3.12 Θα χρησιμοποιήσω την εντολή:

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

3.13 Θα χρησιμοποιήσω την εντολή: `ipfw add nat 123 ip from any to any`

3.14 Ναι, τώρα το `ping` πετυχαίνει

3.15 Χρησιμοποίησα την εντολή: `tcpdump -i em0 -v`

3.16 Θα χρησιμοποιήσω τις εντολές:

```
ipfw show
ipfw zero
```

3.17 Χρησιμοποίησα την εντολή: `ping -c 3 192.0.2.2`

Η διεύθυνση πηγής των IP πακέτων που βλέπω είναι 192.0.2.1 (δηλαδή αυτή του FW1)

3.18 Και πάλι η διεύθυνση προορισμού των ICMP echo reply είναι η 192.0.2.1

3.19 Για την επιτυχία του `ping` ευθύνεται ο κανόνας που προσθέσαμε στο ερώτημα 3.13

3.20 Ο κανόνας αυτός εφαρμόστηκε 12 φορές. Ένα `ping` χρειάζεται να σταλθεί από το PC1 στο FW1, από το FW1 στον R1, από τον R1 στο FW1 και τέλος πίσω στο PC1 (4 βήματα). Επίσης έχω 3 τέτοια `ping`. Αρα συνολικά χρειάστηκε 12 φορές να γίνει η μετάφραση των διευθύνσεων

3.21 Ναι, το `ping` πετυχαίνει κανονικά

3.22 Και πάλι, υπεύθυνος είναι ο κανόνας που προσθέσαμε στο ερώτημα 3.13

3.23 Όχι, η κίνηση αυτή ωθείται στο NAT, καθώς οι διευθύνσεις αυτές δεν είναι ιδιωτικές

3.24 Ναι μπορώ, χρησιμοποιώντας την εντολή: `ssh lab@192.0.2.5`

3.25 Είναι θέμα δρομολόγησης, καθώς δεν αυξάνονται οι φορές που χρησιμοποιείται ο κανόνας του 3.13 (όπου αν η κίνηση εφτανε μέχρι εκεί θα έπρεπε να χρησιμοποιηθεί) και επίσης δεν λειτουργούν ούτε τα `ping` και `traceroute`

3.26 Θα χρησιμοποιήσω την εντολή:

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

- 3.27** Θα χρησιμοποιήσω την εντολή: `ssh lab@192.0.2.1`
Τώρα παρατηρώ η προσπάθεια είναι επιτυχής και συνδέθηκα στο μηχάνημα PC2 (το παρατήρησα εκτελώντας την εντολή `who` ή `hostname`)
- 3.28** Θα χρησιμοποιήσω την 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** Τώρα συνδέθηκα στο PC1 (και παλι χρησιμοποιώντας την εντολή `hostname`)
- 3.30** Τώρα συνδέθηκα στο PC2 (το παρατηρώ χρησιμοποιώντας την εντολή `sockstat` στο PC2)
- 3.31** Ναι, οι εντολές `ls` και `get` δουλεύουν
- 3.32** Απαντάει το PC2
- 3.33** Θα συνδεθώ στο PC1 (λογικό και με βάση τον κανόνα 3.28)

ΑΣΚΗΣΗ 4:

- 4.1** Όχι, τώρα τα `ping` δεν πετυχαίνουν
- 4.2** Κάποια πακέτα γίνονται δεκτά. Ωστόσο το `ping` αποτυγχάνει γιατί έχει πλέον διαφοροποιηθεί η διαδικασία της αποδοχής απο την μετάφραση. Έτσι τα πακέτα μετά γίνονται `deny` απο τον `default`
- 4.3** Θα χρησιμοποιήσω τις εντολές:
`ipfw delete 1100`
`ipfw add 1100 allow all from any to any via em0`
- 4.4** Ναι, τώρα το `ping` προς όλες τις διεπαφές του FW1 είναι επιτυχές
- 4.5** Στο μηχάνημα FW1
- 4.6** Υπεύθυνος για αυτό είναι ο κανόνας που προσθέσαμε στο 4.3
- 4.7** Θα χρησιμοποιήσω την εντολή:
`ipfw add 3000 nat 123 all from any to any xmit em1`
- 4.8** Θα χρησιμοποιήσω την εντολή:
`ipfw add 3001 allow all from any to any`
- 4.9** Θα χρησιμοποιήσω την εντολή:
`ipfw add 2000 nat 123 all from any to any recv em1`
- 4.10** Θα χρησιμοποιήσω την εντολή:
`ipfw add 2001 check-state`
- 4.11** Απαντάει το μηχάνημα FW1
- 4.12** Απαντάει το PC2 (λόγω `redirect`) αλλά φαίνεται να απαντά το FW1
- 4.13** Συνδεόμαστε στο FW1
- 4.14** Συνδεόμαστε στο PC1 (`redirect` οταν έχουμε `tcp` στο `port 22`)
- 4.15** Συνδεόμαστε στο PC2 (`redirect` οταν έχουμε `tcp` σε `port` εκτός του 22)
- 4.16** Ναι, μπορώ να κάνω `ping`
- 4.17** Ναι, μπορώ
- 4.18** Ναι, μπορώ
- 4.19** Θα χρησιμοποιήσω την εντολή:
`ipfw add 2999 deny all from any to any via em1`

- 4.20** Επιτυγχάνουν μόνο οι κινήσεις εντός του LAN1 όπου απαντάει ο FW1
- 4.21** Θα χρησιμοποιήσω την εντολή:
ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
- 4.22** Ναι, τώρα το ping αυτο λειτουργεί κανονικά
- 4.23** Θα χρησιμοποιήσω την εντολή:
ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state
- 4.24** Ναι, τώρα μπορώ να συνδεθώ
- 4.25** Θα χρησιμοποιήσω την εντολή:
ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state
- 4.26** Απαντά το PC2
- 4.27** Θα χρησιμοποιήσω την εντολή:
ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state
- 4.28** Συνδεόμαστε στο PC1
- 4.29** Οχι δεν μπορω (το ftp δεν εμφανίζει απάντηση)
- 4.30** Θα πρέπει να προσθέσω τους κανόνες:
ipfw add 2300 skipto 3000 tcp from any to any 21 in via em1 keep-state
ipfw add 2400 skipto 3000 tcp from any to any 21 out via em1 keep-state

ΑΣΚΗΣΗ 5:

- 5.1** Για την em0 του FW1 η διεύθυνση είναι: 192.168.1.1
- 5.2** Για την em0 του FW1 η διεύθυνση είναι: 10.0.0.1
- 5.3** Το ποσοστό ελεύθερης μνήμης είναι 66% (Memory Usage = 34%)
- 5.4** Παρατηρώ 4 διεπαφές δικτύου. Χρειάζεται να αλλάξω το όνομα μόνο της 4ης (σε DMZ)
- 5.5** Για την DMZ του FW1 η διεύθυνση είναι: 172.22.1.1
- 5.6** Hostname = fw / Δεν ανήκει σε κάποια περιοχή DNS
- 5.7** Απο το General Setup αλλάζω το Hostname
- 5.8** Οχι, δεν υπάρχουν κανόνες για το WAN
- 5.9** Κάνω τις απαραίτητες αλλαγές απο το Interfaces / WAN
- 5.10** Ναι, τώρα υπάρχουν κανόνες για το WAN
- 5.11** Οχι, δεν παρατηρώ καποια ενεργοποιημένη υπηρεσία
- 5.12** Κάνω τις απαραίτητες αλλαγές απο το Services / DNS forwarder
- 5.13** Κάνω τις απαραίτητες αλλαγές απο το Services / DHCP server
enable 192.168.1.2 to 192.168.1.3
- 5.14** Χρησιμοποιώ την εντολή: dhclient em0
Αποδίδεται η εξής πληροφορία:
IP: 192.168.1.2
Default Gateway: 192.168.1.1
DNS Server : 192.168.1.1 (cat /etc/resolv.conf)
- 5.15** Χρειάστηκε καθώς τώρα το FW1 λειτουργεί και ως DNS server
(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)
- 5.16** Μπορω απο τις καρτέλες:

Diagnostics / ARP table

Diagnostics / DHCP leases

5.17 Παρατηρώ 6 εγγραφές στον ARP table

5.18 Όχι, το ping δεν πετυχαίνει

5.19 Στην καρτέλα αυτή παρατηρώ τις 50 τελευταίες καταγραφές Firewall

5.20 Παρατηρώ 2 states:

Diagnostics: Firewall states

Statistics snapshot control							
Start new		Last statistics snapshot: Never					
Source	Port	Destination	Port	Protocol	Packets	Bytes	TTL
192.168.56.1	35244	192.168.56.2	80	tcp	3	739	2:30:00
192.168.56.1	35260	192.168.56.2	80	tcp	2	112	2:30:00

5.21 Για το LAN δεν παρατηρώ κανέναν κανόνα

5.22 Η διαδικασία είναι:

Firewall / Rules / LAN / Add new rule

Pass / from any / to any

5.23 Ναι, τώρα τα ping πετυχαίνουν

5.24 Όχι, το ping δεν πετυχαίνει

5.25 Χρησιμοποιώ την εντολή: arp -a

Ναι παρατηρώ εγγραφή για την em1 (WAN1) του FW1

5.26 Η διαδικασία είναι η εξής:

Firewall / Rules / WAN / add new rule / ICMP / Wan address / Save /
Apply changes

5.27 Ναι, τώρα το ping πετυχαίνει

5.28 Όχι, γιατί το ping εμφανίζει no route to host.

5.29 Ναι, το ping από το PC1 στο R1 πετυχαίνει. Συμπεραίνω ότι λόγω του NAT η ιδιωτική διεύθυνση του PC1 μεταφράζεται, επιτρέποντας την επικοινωνία μεταξύ FW1 και R1 (όπου από πριν γνωρίζουμε ότι πετυχαίνει)

5.30 Χρησιμοποίησα την εντολή: ifconfig em0 inet 172.22.1.2

Το ping δεν πετυχαίνει καθώς το SRV1 δεν ξέρει πού να στείλει την απάντηση

5.31 Χρησιμοποίησα την εντολή: route add default 172.22.1.1

5.32 Ναι, τώρα το ping πετυχαίνει.

5.33 Όχι, το ping αυτό δεν λειτουργεί, καθώς δεν έχει ορισθεί κανόνας για το DMZ που να επιτρέπει αυτή την κίνηση

5.34 Όχι, το ping αυτό δεν λειτουργεί, καθώς δεν έχει ορισθεί κανόνας για το DMZ που να επιτρέπει αυτή την κίνηση

5.35 Η διαδικασία είναι η εξής:

Firewall / Rules / DMZ / Add new rule /

Interface: DMZ / Protocol: Any / Source: DMZ subnet /

Destination: not LAN subnet

5.36 Ναι, τώρα το ping πετυχαίνει

5.37 Ναι, τώρα το ping πετυχαίνει

5.38 Όχι, γιατί το ping εμφανίζει no route to host.

5.39 Ναι το ping αυτό πετυχαίνει, καθώς:

- Έχουμε ορίσει default στον SRV1 τον FW1
- Ο FW1 επιτρέπει αυτή την κίνηση
- Για την απάντηση, ο R1 ξέρουμε από προηγούμενο ερώτημα ότι επικοινωνεί με τον FW1

5.40 Χρησιμοποιώ την εντολή: dhclient em0

Αποδίδεται η εξής πληροφορία:

IP: 192.168.1.3

Default Gateway: 192.168.1.1

DNS Server : 192.168.1.1 (cat /etc/resolv.conf)

5.41 Η διαδικασία είναι η εξής:

Firewall / Rules / LAN / Add new rule / Action: Block

Interface: LAN / Protocol: Any / Source: Single Host or Alias:

192.168.1.3 / Destination: Single Host or Alias: 172.22.1.2

5.42 Ο κανόνας πρέπει να τοποθετηθεί πριν από αυτόν που ήδη υπάρχει, καθώς ο παλιός επιτρέπει όλη την κίνηση και αν ένας κανόνας επαληθεύεται αγνοεί τους επόμενους (first-match basis)

5.43 Όχι, το ping δεν εμφανίζει απάντηση

5.44 Ναι, καθώς δεν έχουμε αποκλίσει όλη την κίνηση προς το DMZ, παρα μόνο για το SRV1.

ΑΣΚΗΣΗ 6:

6.1 Θα χρησιμοποιήσω την εντολή: ip route 203.0.118.0/24 192.0.2.1

6.2 Η διαδικασία είναι: Firewall / Nat / Outbound / Enable / Save

6.3 Η διαδικασία είναι: Firewall / Nat / Outbound / Add new / Interface: WAN / Source: 192.168.1.2/32 / Destination: Any / Target: 203.0.118.14 / Save/ Apply

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

6.4 Η διαδικασία είναι: Firewall / Nat / Outbound / Add new / Interface: WAN / Source: 192.168.1.3/32 / Destination: Any / Target: 203.0.118.15 / Save/ Apply

	Interface	Source	Destination	Target	Description
<input type="checkbox"/>	WAN	192.168.1.0/24	*	203.0.118.15	
<input type="checkbox"/>	WAN	192.168.1.2/32	*	203.0.118.14	

6.5 Θα χρησιμοποιήσω την εντολή: tcpdump -i em0

6.6 Τα ping φτάνουν με διευθύνσεις 203.0.118.14 και 203.0.118.15


6.7 Η διαδικασία είναι η εξής:

Firewall / NAT / Server NAT / add new / 203.0.118.18 / save / apply

6.8 Η διαδικασία είναι η εξής:

Firewall / NAT / Inbound / External address: 203.0.118.18() / External port: SSH / NAT IP: 172.22.1.2 / Local Port: SSH / auto-add / Save / Apply

6.9 Έχει προστεθεί ο εξής κανόνας:

<input type="checkbox"/>		TCP	*	*	172.22.1.2	22 (SSH)	NAT
--------------------------	---	-----	---	---	------------	----------	-----

Ο κανόνας αυτός επιτρέπει την TCP κίνηση προς την διεύθυνση 172.22.1.2:22 και προστέθηκε λόγω του “auto-adda firewall rule to permit traffic through this NAT rule”

6.10 Χρησιμοποιώντας την εντολή `ssh lab@203.0.118.18` συνδέομαι στο SRV1

6.11 Όχι, το `ping` δεν λειτουργεί καθώς δεν υπάρχει κανόνας που να επιτρέπει την κίνηση ICMP πακέτων προς το 203.0.118.18 (παρα μόνο για συνδέσεις SSH)

6.12 Ναι μπορώ να συνδεθώ. Χρησιμοποιώντας `tcpdump` παρατηρώ ότι η διαδρομή που ακολουθούν τα πακέτα περιλαμβάνει και το R1.

6.13 Όχι, πλέον δεν μπορώ να συνδεθώ καθώς πλέον δεν υπάρχει μετάφραση στην διεύθυνση του PC1 (απο `private` σε 203.0.118.X) και άρα η κίνηση έχει ως πηγή την 192.168.1.2, η οποία όμως κόβεται απο το FW1 καθώς υπάρχει κανόνας που κόβει τις κινήσεις απο το WAN σε `private` διευθύνσεις

6.14 Ναι τα `ping` είναι επιτυχή
(Τα ICMP Requests φτάνουν με διεύθυνση 192.0.2.1)

6.15 Η σύνδεση SSH απο το R1 στο SRV1 είναι επιτυχής καθώς υπάρχει εγγραφή στον πίνακα δρομολόγησης για την 203.0.118.18. Η σύνδεση SSH ωστόσο δεν πετυχαίνει απο τα PC1 και PC2

6.16 Η σύνδεση TCP αποτυγχάνει καθώς εφόσον δεν υπάρχει εσωτερική μετάφραση διευθύνσεων, το FW1 δεν προωθεί τα

6.17 Ο λόγος βρίσκεται στην σημείωση στην καρτέλα Inbound. Δεν γίνεται να κάνουμε access σε NATed υπηρεσίες χρησιμοποιώντας WAN IP address μέσα απο το LAN, όπως ακριβώς πήγαμε να κάνουμε

ΑΣΚΗΣΗ 7:

7.1 Ξεμαρκάρω το πλαίσιο Cable Connected

7.2 Η διαδικασία είναι: Interfaces / MNG / IP address 192.168.56.3 / Save

7.3 Μαρκάρω το πλαίσιο Cable Connected

7.4 Ναι, καθώς χρησιμοποιώ διαφορετικές διευθύνσεις:

FW1: 192.168.56.2 / FW2: 192.168.56.3

7.5 Η διαδικασία είναι: System/ General Setup / Hostname: fw2 / Save

7.6 Η διαδικασία είναι: Interfaces / WAN / IP address: 192.0.2.5/30 /

Gateway: 192.0.2.6 / Block Private Networks / Save

7.7 Η διαδικασία είναι: Interfaces / LAN / IP address 192.168.2.1/24 / Save

7.8 Απο το τερματικό θα επιλέξω το `reboot system`

7.9 Η διαδικασία είναι: Firewall / Rules / LAN / Add new / Action: Pass /

Interface: LAN / Protocol: Any / Source: Any / Destination: Any / Save / Apply

7.10 Η διαδικασία είναι: Firewall / Rules / WAN/ Add new / Action: Pass / Interface: WAN / Protocol: ICMP / Source: Any / Destination: WAN address / Save / Apply

7.11 Μεταφέρω το PC2 στο LAN2 απο το Visual Box. Επίσης χρησιμοποιώ τις εντολές:

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

7.12 Ναι το ping πετυχαίνει κανονικά

7.13 Ναι το ping πετυχαίνει κανονικά

7.14 Όχι τα ping αυτά δεν πετυχαίνουν (εμφανίζει Host Unreachable). Αυτό συμβαίνει καθώς ο R1 δεν έχει εγγραφές στον πίνακα δρομολόγησής του για το LAN2

7.15 Οι διαδικασίες είναι:

- VPN / IPsec / Enable IPsec.
- VPN / IPsec / Add new / Local Subnet: LAN subnet / Remote subnet: 192.168.2.0/24 / Remote Gateway: 192.0.2.5 / Pre-shared Key: George / Save / Apply

7.16 Παρατηρώ έναν κανόνα που επιτρέπει όλες τις κινήσεις απο οποιαδήποτε πηγή προς οποιοδήποτε προορισμό

7.17 Όχι, δεν παρατηρώ σχέσεις μεταξύ 2 υποδικτύων

7.18 Ναι παρατηρώ τις εξής πολιτικές προώθησης:

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 Οι διαδικασίες είναι:

- VPN / IPsec / Enable IPsec.
- VPN / IPsec / Add new / Local Subnet: LAN subnet / Remote subnet: 192.168.1.0/24 / Remote Gateway: 192.0.2.1 / Pre-shared Key: George / Save / Apply

7.20 Όχι, δεν παρατηρώ σχέσεις μεταξύ 2 υποδικτύων

7.21 Ναι, παρατηρώ τις εξής πολιτικές προώθησης:

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 Ναι, το ping είναι επιτυχές

7.23 Ναι, το ping είναι επιτυχές

7.24 Ναι, προστέθηκαν 2 εγγραφές στον πίνακα SAD του FW1

7.25 Ναι, προστέθηκαν 2 εγγραφές στον πίνακα SAD του FW2

7.26 Θα χρησιμοποιήσω την εντολή: tcpdump -i em0 -v

- 7.27** Όχι, δεν παρατηρώ πακέτα ICMP
- 7.28** Εμφανίζονται πακέτα ESP. Αυτά έχουν:
Πηγή: 192.0.2.1
Προορισμό: 192.0.2.5
(Κατα το ring απο PC1 προς PC2)
- 7.29** Όχι, αυτή η πληροφορία κρύβεται
- 7.30** Ναι, μπορώ να συνδεθώ απο το PC2 με SSH στο SRV1 χρησιμοποιώντας την διεύθυνση 203.0.118.18, καθώς σε αυτή την άσκηση το PC2 χρησιμοποιεί την μεταφρασμένη διεύθυνση απο το FW2
- 7.31** Κατα την καταγραφή παρατηρώ πακέτα TCP. Για τα πακέτα με πηγή το PC2 ισχύει οτι:
IP πηγής: 192.0.2.5
Port πηγής: 45411
IP προορισμού: 203.0.118.18
Port προορισμού: 22 (SSH)
- 7.32** Είναι κρυπτογραφημένα αλλά όχι με το IPsec