Ονοματεπώνυμο: Μάρκος Δεληγιάννης	Όνομα PC: Lenovo-Laptop
Ομάδα: 1	Ημερομηνία: 16 / 5 / 2023

Εργαστηριακή Άσκηση 10
Τείχη προστασίας (Firewalls) και NAT

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Εντολή: **kldload ipfw**

1.2 Εντολή: **kldstat**. Στις εγγραφές υπάρχει το **ipfw.ko**, οπότε αυτό είναι **ενεργοποιημένο**.

1.3 **Όχι**, δεν μπορούμε. Εμφανίζεται μήνυμα λάθους **permission denied**.
Εντολές: 1) **ping 127.0.0.1** 2) **ping 192.168.1.2**

1.4 Εντολή: **ipfw list**. Εμφανίζεται **μόνο ο default κανόνας**:
65535 deny ip from any to any

1.5 Εντολή: **ipfw show**. Τώρα εμφανίζονται και οι μετρητές χρήσης του **default κανόνα**:
65535 2 168 deny ip from any to any

1.6 Εντολή: **ipfw zero [*α/α_κανόνα*]**

1.7 Εντολή: **ipfw add 100 allow all from any to any via lo0**

1.8 **Ναι**, και τα δύο ping είναι επιτυχή.

1.9 **Όχι**, δεν μπορούμε. Εμφανίζεται μήνυμα λάθους **permission denied**. Εντολή: **ping 192.168.1.3**

1.10 Εντολή: **ipfw add allow icmp from any to any**

1.11 Έλαβε αύξοντα αριθμό **200**.

1.12 **Ναι**, μπορούμε. Εντολές: PC1) **ping 192.168.1.3** PC2) **ping 192.168.1.2**

1.13 Επειδή η traceroute στέλνει **UDP datagrams**, όχι μηνύματα ICMP. Αυτό μπορεί να διορθωθεί εύκολα με χρήση της σημαίας -I. Εντολή: **traceroute -I 192.168.1.3**

1.14 Εντολή: **ipfw add allow udp from me to any 33435-33626** αρχική θύρα η 33434+1 (manpage) και ο αριθμός των θυρών είναι 64 (max_ttl) * 3 (attempts) = **192**.

1.15 **Όχι**, δεν μπορούμε. Εντολή: **ssh lab@192.168.1.3**

1.16 Εντολές: 1) **ipfw add 200 allow tcp from any to any established**
2) **ipfw add 210 allow tcp from me to any setup**

1.17 Εντολές: 1) **ipfw zero** 2) **ssh lab@192.168.1.3**
3) **ls** 4) **exit**

1.18 Ο μετρητής του κανόνα **210** είναι **1**, αφού η εγκατάσταση σύνδεσης TCP έγινε μία φορά. Ο μετρητής του κανόνα **200** είναι **73**, αφού ανταλλάχτηκαν τόσα τεμάχια TCP μεταξύ PC1 και PC2 μετά την εκτατάσταση της σύνδεσης. Εντολή: **ipfw show** και επισκόπηση του πρώτου μετρητή.

1.19 **Όχι**, δεν μπορούμε, αφού τα setup τεμάχια TCP (πρώτο **SYN**) επιτρέπονται μόνο από τον PC1 προς άλλους υπολογιστές. Έτσι, κατά την προσπάθεια σύνδεσης από το PC2 στο PC1 πυροδοτείται ο τελευταίος κανόνας και τα πακέτα απορρίπτονται σιωπηλά. Εντολή: **ssh lab@192.168.1.2**

1.20 Εντολή: **service ftpd onestart**

1.21 **Ναι**, μπορούμε, με τις εξής εντολές:
1) **ftp lab@192.168.1.3** 2) **bin** 3) **get /usr/bin/hd ./hd** 4) **bye**

2

2.1 Εντολή: **kldload ipfw**

2.2 **Όχι**, δεν μπορούμε. Εμφανίζεται μήνυμα λάθους **permission denied**. Εντολή: **ping 192.168.1.2**

2.3 Εντολή: **ipfw add allow all from any to any via lo0**

2.4 Εντολή: **ipfw add allow icmp from me to any icmptypes 8**

2.5 **Όχι**, δεν μπορούμε. Εντολή: **ping 192.168.1.2**

2.6 Τα **ICMP echo request περνούν**, αφού ο μετρητής του κανόνα που ορίσαμε έχει τιμή διάφορη του μηδενός. Τα **ICMP echo reply δεν περνούν**, αφού δεν ταιριάζουν με κανέναν κανόνα, εκτός του default. Εντολή: **ipfw show**

2.7 **Ναι**, μπορούμε. Εντολές: 1) **ipfw delete 200**
2) **ipfw add allow icmp from me to any icmptypes 8 keep-state** 3) **ping 192.168.1.2**

2.8 **Ναι**, μπορούμε. Εντολή: **ping 192.168.1.3**

2.9 Τώρα το ping **αποτυγχάνει**. Αυτό συμβαίνει καθώς ο κανόνας "keep-state" δημιουργεί μία δυναμική εγγραφή για την αμφίδρομη επικοινωνία PC1↔PC2 με περιορισμένο χρόνο ζωής, που ανανεώνεται με την εμφάνιση σχετικών πακέτων. Όσο λοιπόν τα PC1,2 επικοινωνούν, η εγγραφή ανανεώνεται και το ping πετυχαίνει. Αν διακόψουμε όλα τα ping και περιμένουμε λίγο η εγγραφή θα διαγραφεί, με αποτέλεσμα το ping PC1 → PC2 να αποτυγχάνει. Εντολή: **ping 192.168.1.3**

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

2.11 Η εντολή αυτή εμφανίζει **και τους δυναμικούς κανόνες**. Εν προκειμένω βλέπουμε τον δυναμικό κανόνα για τα PC1↔PC2 που δημιουργείται από την προηγούμενη εντολή και το **ping 192.168.1.3**.

2.12 Τώρα ο δυναμικός κανόνας του 2.11 **έχει διαγραφεί**.

2.13 Εντολές: 1) **ipfw add allow udp from any to me 33435-33626**
2) **ipfw add allow icmp from me to any icmptypes 3**

2.14 Εντολές: 1) **ipfw add allow udp from me to any 33435-33626**
2) **ipfw add allow icmp from any to me icmptypes 3**

2.15 Εντολή: **ipfw add allow udp from any to me 33435-33626**

2.16 Εντολή: **ipfw add allow tcp from 192.168.1.0/24 to me ssh setup keep-state**

2.17 Εντολή: **ssh lab@192.168.1.3**

2.18 Εντολή: **ipfw add allow tcp from me to any ssh setup keep-state**

2.19 Εντολή: **ipfw add allow tcp from 192.168.1.3 to me ssh setup**

2.20 **Ναι**, μπορούμε, με τις εντολές: 1) **sftp lab@192.168.1.3** 2) **get /etc/rc.conf ./rc.conf** 3) **bye**

2.21 **Όχι**, δεν μπορούμε. Για να το διορθώσουμε, εκτελούμε την ακόλουθη εντολή:
ipfw add allow tcp from any to me ftp setup keep-state

2.22 Για την πρώτη χρησιμοποιείται η ήδη υπάρχουσα σύνδεση TCP, οπότε πετυχαίνει. Για την δεύτερη ο PC2 στέλνει μία θύρα στον PC1 και αυτός επιχειρεί να συνδεθεί σε αυτήν (passive mode). Ο PC2 όμως δεν δέχεται τις συνδέσεις TCP σε αυτόν σε θύρες διαφορετικές των 21,22, οπότε η σύνδεση, και κατά συνέπεια η δεύτερη εντολή, αποτυγχάνει. Εντολή: **ftp lab@192.168.1.3**

2.23 Εντολή: **ipfw add allow tcp from any 1024-65535 to me 1024-65535 setup keep-state**

2.24 **Ναι**, μπορούμε με τις εντολές του 1.21.

2.25 PC1: **ipfw add allow tcp from any 20 to me 1024-65535 setup**
PC2: **ipfw add allow tcp from me 20 to any 1024-65535 setup keep-state**

2.26 Πρωτόκολλα όπως το FTP χρησιμοποιούν πολλές συνδέσεις TCP, με διαφορετικές θύρες πηγής και προορισμού. Αυτό τα καθιστά ιδιαιτέρως απρόβλεπτα και δυσκολεύει την δημιουργία κατάλληλων φίλτρων που θα επιτρέπουν τη λειτουργία τους.

2.27 Εντολές: **kldunload ipfw** και **kldstat**. Πλέον στις εγγραφές δεν υπάρχει το **ipfw.ko**.

3

3.1 PC1: 1) **hostname PC1** 2) **ifconfig em0 192.168.1.2/24** 3) **route add default 192.168.1.1**
PC2: 1) **hostname PC2** 2) **ifconfig em0 192.168.1.3/24** 3) **route add default 192.168.1.1**

3.2 Εντολές: 1) **cli** 2) **configure terminal** 3) **hostname R1**
4) **interface em0** 5) **ip address 192.0.2.2/30**
6) **interface em1** 7) **ip address 192.0.2.6/30**

3.3 Εντολές: 1) **hostname SRV1** 2) **ifconfig em0 192.0.2.5/30** 3) **route add default 192.0.2.6**

3.4 Εντολή: **service ftpd onestart**

3.5 Εντολή: **kldstat**. Τα modules είναι τα εξής (αγνοώντας τον ίδιο τον kernel):
1) **intpm.ko** 2) **smbus.ko** 3) **ipfw.ko** 4) **ipfw_nat.ko** 5) **libalias.ko**

3.6 Το **ipfw**. Εντολή: **service -e**

3.7 Έχουμε **UNKNOWN** λειτουργία firewall. Εντολή: **sysrc firewall_type**

3.8 Βλέπουμε **11 κανόνες στο FW1**. Ο τελευταίος είναι ο "**65535 deny ip from any to any**", δηλαδή ο προεπιλεγμένος κανόνας, ο οποίος απορρίπτει σιωπηλά όλα τα πακέτα.

3.9 **Όχι**, δεν έχουν ορισθεί. Εντολή: **ipfw nat show config**

3.10 **Όχι**, δεν μπορούμε. Εντολές: **ping 192.168.1.1** και **ping 192.0.2.1**

3.11 **Όχι**, δεν μπορούμε. Εντολή: **ping 192.0.2.1**

3.12 Εντολή: **ipfw nat 123 config if em1 unreg_only reset**

3.13 Εντολή: **ipfw add nat 123 ip4 from any to any**

3.14 **Ναι**, μπορούμε. Εντολές: **ping 192.168.1.1** και **ping 192.0.2.1**

3.15 Εντολή: **tcpdump -i em0**

3.16 Εντολές: 1) **ipfw show** 2) **ipfw zero**

3.17 Η διεύθυνση πηγής είναι η **192.0.2.1** (em1 του FW1). Εντολή: **ping -c 3 192.0.2.2**

3.18 Η διεύθυνση προορισμού είναι η **192.0.2.1** (em1 του FW1).

3.19 **Ο κανόνας του 3.13**, ο οποίος προωθεί όλη την κίνηση IPv4 στον πίνακα NAT 123.

3.20 Εφαρμόστηκε **12 φορές**. Αυτό συμβαίνει καθώς κάθε πακέτο ICMP echo request/reply περνά από τον πίνακα NAT **2 φορές**, κατά την **είσοδο** και **έξοδο** από τον δρομολογητή. Έχουμε 3 echo request και 3 echo reply, οπότε έχουμε 2*(3+3)=**12 εφαρμογές του κανόνα**.

3.21 **Ναι**, μπορούμε. Εντολή: **ping 192.0.2.1**

3.22 **Ο κανόνας του 3.13**, ο οποίος προωθεί όλη την κίνηση IPv4 στον πίνακα NAT 123.

3.23 **Ναι**, καθώς ο κανόνας που ωθεί ένα πακέτο στο NAT 123 πυροδοτείται από οποιοδήποτε πακέτο IPv4.

3.24 **Ναι**, μπορούμε. Εντολή: **ssh lab@192.0.2.5**

3.25 Είναι θέμα **δρομολόγησης**, καθώς ο R1 δεν έχει εγγραφή για τον 192.168.1.3 στο routing table του. Το διαπιστώνουμε από το μήνυμα "**ssh: connect to host 192.168.1.3 port 22: No route to host**"

3.26 Εντολή: **ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1**

3.27 Συνδεθήκαμε στο **PC2**, το οποίο φαίνεται από το prompt "**lab@PC2**". Εντολή: **ssh lab@192.0.2.1**

3.28 Εντολή: **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 22**

3.29 Συνδεόμαστε στο **PC1**, το οποίο φαίνεται από το prompt "**lab@PC1**". Εντολή: **ssh lab@192.0.2.1**

3.30 Συνδεόμαστε στο **PC2**, το οποίο φαίνεται από το ftp greeting "**220 PC2 FTP server**".
Εντολή: **ftp lab@192.0.2.1**

3.31 **Ναι**, μπορούμε με τις εντολές: 1) **ls /etc** 2) **get /etc/rc.conf rc.conf**

3.32 Συνδεόμαστε στο **PC2**, το οποίο φαίνεται από το ftp greeting "**220 PC2 FTP server**".
Εντολή: **ftp lab@192.0.2.1**

3.33 Συνδεόμαστε στο **PC1**, το οποίο φαίνεται από το prompt "**lab@PC1**". Εντολή: **ssh lab@192.0.2.1**

4

4.1 **Όχι**, δεν μπορούμε. Εντολές: PC1) **ping 192.168.1.1** SRV1) **ping 192.0.2.1**

4.2 **Ναι**, γίνονται, καθώς αυξάνεται ο μετρητής στην **ipfw show**. Το ping αποτυγχάνει γιατί πλέον η ώθηση στον πίνακα NAT είναι ανεξάρτητη από την αποδοχή της κίνησης, και δεν υπάρχει κάποιος τέτοιος κανόνας, με αποτέλεσμα τα πακέτα να απορρίπτονται.

4.3 Εντολές: 1) **ipfw delete 1100** 2) **ipfw add 1100 allow all from any to any via em0**

4.4 **Ναι**, είναι επιτυχές. Εντολές: 1) **ping 192.168.1.1** 2) **ping 192.0.2.1**

4.5 Συνδεόμαστε στο **FW1**, το οποίο φαίνεται από το prompt "**lab@FW1**". Εντολή: **ssh lab@192.0.2.1**

4.6 Υπεύθυνος είναι ο **κανόνας με α/α 1100** που προσθέσαμε στο **4.3**, αφού επιτρέπει όλη την κίνηση μέσω της διεπαφής του FW1 στο LAN1, καθώς επίσης και ο **κανόνας allow ip from any to any via lo0**.

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

4.8 Εντολή: **ipfw add 3001 allow all from any to any**

4.9 Εντολή: **ipfw add 2000 nat 123 all from any to any recv em1**

4.10 Εντολή: **ipfw add 2001 check-state**

4.11 Απαντά το **FW1**. Εντολή: **ping 192.0.2.1**

4.12 Απαντά το **PC2**. Εντολή: **ping 192.0.2.1**

4.13 Συνδεόμαστε στο **FW1**, το οποίο φαίνεται από το prompt "**lab@FW1**". Εντολή: **ssh lab@192.0.2.1**

4.14 Συνδεόμαστε στο **PC1**, το οποίο φαίνεται από το prompt "**lab@PC1**". Εντολή: **ssh lab@192.0.2.1**

4.15 Συνδεόμαστε στο **PC2**, το οποίο φαίνεται από ftp greeting "**220 PC2 FTP server**".
Εντολή: **ftp lab@192.0.2.1**

4.16 **Ναι**, μπορούμε. Εντολή: **ping 192.0.2.5**

4.17 **Ναι**, μπορούμε. Εντολή: **ssh lab@192.0.2.5**

4.18 **Ναι**, μπορούμε. Εντολές: 1) **ftp lab@192.0.2.5** 2) **ls** 3) **get .shrc ./temp_file**

4.19 Εντολή: **ipfw add 2999 deny all from any to any via em1**

4.20 Επιτυγχάνει μόνο το **ping PC1 → 192.0.2.1 και ssh PC1 → 192.0.2.1**, αφού όλα τα άλλα χρειάζονται πρόσβαση στη ζεύξη FW1 → WAN1, την οποία έχουμε αποκόψει με τον προηγούμενο κανόνα.

4.21 Εντολή: **ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state**

4.22 **Ναι**, μπορούμε. Εντολή: **ping 192.0.2.5**

4.23 Εντολή: **ipfw add 2600 skipto 3000 tcp from any to any 22 setup out via em1 keep-state**

4.24 **Ναι**, μπορούμε. Εντολή: **ssh lab@192.0.2.5**

4.25 Εντολή: **ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state**

4.26 Απαντά το **PC2**. Εντολή: **ping 192.0.2.1**

4.27 Εντολή: **ipfw add 2200 skipto 3000 tcp from any to any 22 setup recv em1 keep-state**

4.28 Συνδεόμαστε στο **PC1**, το οποίο φαίνεται από το prompt "**lab@PC1**". Εντολή: **ssh lab@192.0.2.1**

4.29 **Όχι**, δεν πετυχαίνει. Εντολή: **ftp lab@192.0.2.1**

4.30 Εντολές: 1) **ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state**
2) **ipfw add 2400 skipto 3000 tcp from any 20 to any 1024-65535 setup xmit em1 keep-state**

5

5.1 Είναι η **192.168.1.1/24**. (Interfaces → LAN)

5.2 Είναι η **10.0.0.1/30**. (Interfaces → WAN)

5.3 Χρησιμοποιείται το 35% της μνήμης, οπότε είναι ελεύθερο το **65%** (Κεντρικό μενού → Memory usage).

5.4 Βλέπουμε **4 διεπαφές δικτύου**. Επιλέγουμε τις σωστές ρυθμίσεις στο Virtualbox από το FW1 → Settings → Network.

5.5 Είναι η **172.22.1.1/24**. (Interfaces → DMZ)

5.6 Είναι το **fw**. (System → General setup → Hostname)

5.7 Αλλάζουμε το **fw → fw1** και πατάμε **Save**.

5.8 **Όχι**, δεν υπάρχουν ("No rules are currently defined for this interface").

5.9 IP address: **192.0.2.1/30** (Interfaces → WAN)
Gateway: **192.0.2.2** Τσεκάρουμε επίσης το "Block private networks" και κάνουμε **save**.

5.10 **Ναι**, υπάρχει **ένας κανόνας**, με περιγραφή "**Block private networks**".

5.11 **Όχι**, όλες αυτές οι υπηρεσίες είναι απενεργοποιημένες.

5.12 Services → DNS forwarder → **Enable DNS forwarder** & **save**

5.13 Services → DHCP server → LAN → **Enable** & **Range = 192.168.1.2 to 192.168.1.3** & **save**

5.14 Εντολή: **dhclient em0**: IP PC1: **192.168.1.2** DCHP server IP: **192.168.1.1**
Εντολή: **cat /etc/resolv.conf**: DNS server: **192.168.1.1**

5.15 Όταν η υπηρεσία DNS forwarder είναι ενεργοποιημένη ο DHCP server παρέχει και υπηρεσίες DNS στους DHCP clients, δίνοντας την δική του IP ως την IP του DNS server.

5.16 Diagnostics → DHCP Leases → **IP address = 192.168.1.2 / Hostname = PC1**.

5.17 Βλέπουμε **6 εγγραφές ARP**.

5.18 **Όχι**, δεν μπορούμε. Εντολή: **ping 192.168.1.1**

5.19 Βλέπουμε **entries για διάφορα πρωτόκολλα**, οι οποίες αντιστοιχούν σε **απόρριψη** των πακέτων. Έπειτα, πατάμε το "**Clear log**".

5.20 Βλέπουμε **2 firewall states**.

5.21 Δεν βλέπουμε **κανέναν κανόνα** για το LAN1 (“No rules are currently defined for this interface”).

5.22 Επιλέγουμε + → **protocol = any → allow fragmented packets → Save → Apply changes**.

5.23 **Ναι**, μπορούμε. Εντολές: 1) **ping 192.168.1.1** 2) **ping 192.0.2.1** 3) **ping 172.22.1.1**

5.24 **Όχι**, δεν μπορούμε. Εντολή: **ping 192.0.2.1**

5.25 **Ναι**, βλέπουμε για το FW1 – WAN1. Εντολή: **arp -a**

5.26 Επιλέγουμε + → **interface = WAN → protocol = ICMP → Destination = WAN address**

5.27 **Ναι**, μπορούμε. Εντολή: **ping 192.0.2.1**

5.28 **Όχι**, δεν μπορούμε. Ο λόγος είναι ότι **ο R1 δεν έχει εγγραφή για το PC1** στο routing table του, το οποίο επιβεβαιώνεται από το μήνυμα **no route to host** που λαμβάνουμε.
Εντολή: **ping 192.168.1.2**

5.29 **Ναι**, μπορούμε. Συμπεραίνουμε ότι η λειτουργία **NAT είναι ενεργή στο FW1**, αφού δείξαμε ότι ο R1 μπορεί να επικοινωνήσει μόνο με την 192.0.2.1 και όχι με την 192.168.1.2.
Εντολή: **ping 192.0.2.2**

5.30 **Όχι**, δεν μπορούμε. Ο λόγος είναι ότι ο SRV1 δεν έχει default gateway, ούτε εγγραφή για το ίδιο το PC1, οπότε δεν μπορεί να απαντήσει στο ping του. Εντολή: **ping 172.22.1.2**

5.31 Εντολή: **route add default 172.22.1.1**

5.32 **Ναι**, μπορούμε. Εντολή: **ping 172.22.1.2**

5.33 **Όχι**, δεν μπορούμε. Αυτό συμβαίνει καθώς οι εισερχόμενες συνδέσεις στο **FW1 – DMZ απορρίπτοναι** από προεπιλογή. Εξαίρεση είναι η ύπαρξη δυναμικού κανόνα, ο οποίος δημιουργείται σε περιπτώσεις όπως στο 5.32. Εντολή: **ping 172.22.1.1**

5.34 **Όχι**, δεν μπορούμε, για τον ίδιο λόγο με το 5.33. Εντολές: 1) **ping 192.168.1.2** 2) **ping 192.0.2.2**

5.35 Επιλέγουμε + → **Interfacae DMZ → protocol = any → Destination = not LAN subnet → allow fragmented packets → Save → Apply changes**.

5.36 **Ναι**, μπορούμε. Εντολή: **ping 172.22.1.1**

5.37 **Ναι**, μπορούμε. Εντολή: **ping 192.0.2.1**

5.38 **Όχι**, δεν μπορούμε. Αυτό συμβαίνει διότι ο R1 δεν έχει εγγραφή στο routing table για τον SRV1, ούτε για προεπιλεγμένη πύλη (“No route to host”). Εντολή: **ping 172.22.1.2**

5.39 **Ναι**, μπορούμε, αφού **έχουμε επιτρέψει την κίνηση DMZ → WAN1** και το **FW1 εκτελεί NAT**. Έτσι, ο R1 στέλνει το ICMP echo reply στο **FW1**, για το οποίο έχει φυσικά εγγραφή στο routing table. Εντολή: **ping 192.0.2.2**

5.40 Εντολή: **dhclient em0**: IP PC1: **192.168.1.3** DCHP server IP: **192.168.1.1**
Εντολή: **cat /etc/resolv.conf**: DNS server: **192.168.1.1**

5.41 Επιλέγουμε + → **Action = Block → Interfacae LAN → protocol = any**
→ **Source = Single host or alias / 192.168.1.3**
→ **Destination = Single host or alias / 172.22.1.2**
→ **allow fragmented packets → Save → Apply changes**.

5.42 Πρέπει να τοποθετηθεί **πριν** από αυτόν που υπάρχει, καθώς είναι **πιο ειδικός**. Αν τοποθετηθεί μετά, τότε ο κανόνας που επιτρέπει ολόκληρη την κίνηση μέσω του LAN1 θα πυροδοτείται πάντα και όλα τα πακέτα από το LAN1 θα γίνονται αποδεκτά.

5.43 **Όχι**, δεν μπορούμε. Εντολή: **ping 172.22.1.2**

5.44 **Ναι**, μπορούμε, αφού ο κανόνας του 5.41 δεν πυροδοτείται (ο προορισμός δεν είναι ο SRV1), και έτσι η κίνηση επιτρέπεται. Εντολή: **ping 172.22.1.2**

6

6.1 Εντολή: **route add 203.0.118.0/24 192.0.2.1**

6.2 Firewall → NAT → Outbound → **Enable advanced outbound NAT**

6.3 **+ → Source = 192.168.1.2/32 → Target = 203.0.118.14 → Save → Apply changes**.

6.4 **+ → Source = 192.168.1.3/32 → Target = 203.0.118.15 → Save → Apply changes.**

6.5 Εντολή: **tcpdump -i em0**

6.6 **Ναι**, μπορούμε. Τα πακέτα φτάνουν με τις IP διευθύνσεις **203.0.118.14** και **203.0.118.15** για τα PC1,2 αντίστοιχα. Εντολή: **ping 192.0.2.2** (από PC1,2)

6.7 Ο λόγος που το ping αποτυγχάνει είναι ότι ο κανόνας NAT είναι **outbound από το FW1 – WAN**, οπότε **δεν εφαρμόζεται για εισερχόμενα πακέτα** από το WAN1. Εντολή: **ping 203.0.118.14**

6.8 **+ → External IP address = 203.0.118.18 → Save → Apply changes**.

6.9 **+ → External IP address = 203.0.118.18 () → Protocol = TCP**
→ External port range = from SSH to SSH → NAT IP = 172.22.1.2 → Local port = SSH
→ Auto-add a firewall rule to permit traffic through this NAT rule → Save → Apply changes.

6.10 Προστέθηκε κανόνας που **επιτρέπει τεμάχια TCP με προορισμό το 172.22.1.2 στην θύρα 22 (SSH)**. Όπως δηλώνει και η περιγραφή, αυτός ο κανόνας προστέθηκε ώστε να επιτρέπονται τα πακέτα τα οποία ταιριάζουν με τον κανόνα NAT που δημιουργήσαμε στο **6.9**.

6.11 Συνδεόμαστε στο **SRV1**, το οποίο φαίνεται από το prompt "**lab@SRV1**".
Εντολή: **ssh lab@203.0.118.18**

6.12 **Όχι**, δεν μπορούμε. Ο λόγος είναι ότι **δεν υπάρχει κανένας κανόνας NAT** για την ICMP κίνηση προς το 203.0.118.18. Έτσι, δεν συμβαίνει μετάφραση NAT και το firewall **απορρίπτει τα πακέτα**, καθώς ούτε σε αυτό υπάρχει κάποιο ταίριασμα. Εντολή: **ping 203.0.118.18**

6.13 **Ναι**, μπορούμε. Η διαδρομή που ακολουθείται είναι:
PC2 → FW1 → R1 → FW1 → SRV1 → FW1 → R1 → FW1 → PC2. Αυτό φαίνεται στην καταγραφή του R1, στην οποία βλέπουμε τεμάχια TCP προς την 203.0.118.18 (SRV1) αλλά και προς την 203.0.118.15 (PC2). Εντολή: **ssh lab@203.0.118.18**

6.14 Firewall → NAT → outbound → επιλέγουμε την εγγραφή για την **192.168.1.2/32** → x.
Δεν μπορούμε να κάνουμε ping (εντολή: **ping 192.0.2.2**). Αυτό συμβαίνει διότι τα πακέτα IP που φέρουν το ICMP echo request **δεν υφίστανται NAT**, αφού έχουμε ενεργοποιήσει το advanced outbound NAT και δεν έχουμε εγγραφή για το PC1. Έτσι, ο R1 λαμβάνει πακέτα IP με διεύθυνση πηγής την 192.168.1.2, για την οποία φυσικά **δεν έχει διαδρομή**.

6.15 Firewall → NAT → outbound → uncheck "Enable advanced outbound NAT" → Save.
Το ping τώρα είναι επιτυχές.

6.16 **Μπορούμε να συνδεθούμε από τον R1 στον SRV1** χρησιμοποιώντας την 203.0.118.18.
Το ίδιο **δεν ισχύει για τα PC1,2**.

6.17 Το PC2 προωθεί το τεμάχιο TCP [S] στον FW1. Ο FW1 εκτελεί NAT, δημιουργεί μία δυναμική **εγγραφή για το PC2 και τη διεπαφή στο WAN** και προωθεί μέσω αυτής το τεμάχιο TCP στον R1. Ο R1 προωθεί το τεμάχιο πίσω στον FW1. Σε αυτόν πυροδοτείται ο inbound NAT κανόνας για τον SRV1, οπότε το πακέτο IP μεταφράζεται κατάλληλα και προωθείται στον SRV1. Αυτός απαντά με TCP[S.], το οποίο φτάνει στον FW1 μέσω της διεπαφής στο DMZ. Επειδή η διεπαφή είναι διαφορετική ο δυναμικός κανόνας NAT για τον PC2 **δεν ενεργοποιείται**, και έτσι ο FW1 νομίζει ότι το πακέτο προορίζεται για αυτόν. Συνεπώς, το απορρίπτει, αφού έχει σημαία ACK (φαινομενικά απρόκλητη), και στέλνει στον SRV1 τεμάχιο TCP[R], τερματίζοντας την σύνδεση.
Εντολή: **tcpdump -ei em0** από SRV1, R1

6.18 **Όχι**, δεν ευθύνονται αυτοί οι κανόνες. Ο λόγος είναι ότι δεν είναι δυνατό να αποκτήσουμε πρόσβαση σε "NATed" υπηρεσίες χρησιμοποιώντας την WAN IP από το εσωτερικό του LAN, όπως αναφέρεται στην σημείωση στην καρτέλα **Inbound**. Η αναλυτική εξήγηση για την συγκεκριμένη περίπτωση έχει παρατεθεί στο 6.17.

7

7.1 FW1 → Settings → Network → Adapter 3 → Advanced → **Uncheck "Cable Connected"**

7.2 Interfaces → MNG → **IP address = 192.168.56.3/24** → Save

7.3 FW1 → Settings → Network → Adapter 3 → Advanced → **Check "Cable Connected"**

7.4 **Ναι**, μπορούμε.

7.5 System → General Setup → **Hostname = fw2** → Save

7.6 IP address: **192.0.2.5/30** (Interfaces → WAN)
Gateway: **192.0.2.6** Τσεκάρουμε επίσης το "Block private networks" και κάνουμε **save**.

7.7 Interfaces → LAN → **IP address = 192.168.2.1/24** → Save

7.8 Πατάμε το hyperlink "**reboot**" που εμφανίζεται στο ενημερωτικό μήνυμα. Έπειτα πατάμε **yes**.

7.9 Επιλέγουμε **Firewall → Rules → LAN → + → protocol = any → allow fragmented packets → Save → Apply changes**.

7.10 Επιλέγουμε **Firewall → Rules → WAN → + → protocol = ICMP → Destination/Type = WAN address → allow fragmented packets → Save → Apply changes**.

7.11 PC2 → Settings → Network → Adapter 1 → **Name: LAN2**
Εντολές: 1) **ifconfig em0 192.168.2.2/24**
2) **route add default 192.168.2.1**

7.12 **Ναι**, μπορούμε. Εντολή: **ping 192.0.2.5**

7.13 **Ναι**, μπορούμε. Εντολή: **ping 192.0.2.1**

7.14 **Όχι**, δεν μπορούμε, καθώς ο R1 **δεν έχει default gateway ούτε εγγραφή για τα LAN1,2**.
Εντολές: PC1) **ping 192.168.2.2** PC2) **ping 192.168.1.2**

7.15 **VPN → IPsec → Tunnels → Check "Enable IPsec" → Save**.
Έπειτα πατάμε **+ → Local subnet/Type = LAN subnet → Remote subnet = 192.168.2.0/24 → Remote gateway = 192.0.2.5 → Pre-Shared Key = "MarkosDeligiannis" → Save → Apply changes**

7.16 Βλέπουμε έναν κανόνα ο οποίος επιτρέπει **οποιαδήποτε κίνηση από οποιαδήποτε πηγή σε οποιονδήποτε προορισμό**.

7.17 **Όχι**, βλέπουμε "**No IPsec security associations.**"

7.18 **Ναι**, έχουν ορισθεί **δύο πολιτικές** προώθησης κίνησης, μία για το **LAN1 → LAN2** και μία για το **LAN2 → LAN1**.

7.19 **VPN → IPsec → Tunnels → Check "Enable IPsec" → Save.**
Έπειτα πατάμε **+ → Local subnet/Type = LAN subnet → Remote subnet = 192.168.1.0/24 → Remote gateway = 192.0.2.1 → Pre-Shared Key = "MarkosDeligiannis" → Save → Apply changes**

7.20 **Όχι**, βλέπουμε "**No Ipsec security associations.**"

7.21 **Ναι**, έχουν ορισθεί **δύο πολιτικές** προώθησης κίνησης, μία για το **LAN1 → LAN2** και μία για το **LAN2 → LAN1**.

7.22 **Ναι**, μπορούμε. Εντολή: **ping 192.168.2.2**

7.23 **Ναι**, μπορούμε. Εντολή: **ping 192.168.1.2**

7.24 **Ναι**, προστέθηκαν εγγραφές με **source = 192.0.2.5 (FW2)**, **destination = 192.0.2.1 (FW1)** και **source = 192.0.2.1 (FW1)**, **destination = 192.0.2.5 (FW2)**.

7.25 **Ναι**, προστέθηκαν εγγραφές με **source = 192.0.2.5 (FW2)**, **destination = 192.0.2.1 (FW1)** και **source = 192.0.2.1 (FW1)**, **destination = 192.0.2.5 (FW2)**.

7.26 Εντολή: **tcpdump -vXi em0**

7.27 **Όχι**, δεν παρατηρούμε.

7.28 Εμφανίζονται **πακέτα ESP** μεταξύ των **192.0.2.1** και **192.0.2.5**.

7.29 **Όχι**, δεν υπάρχει.

7.30 **Ναι**, μπορούμε. Στην προηγούμενη άσκηση, όπως αναφέρθηκε στο **6.18**, προσπαθούσαμε να αποκτήσουμε πρόσβαση σε "NATed" υπηρεσία χρησιμοποιώντας τη WAN IP της από το εσωτερικό του LAN. Σε αυτή την περίπτωση δε βρισκόμαστε εντός του ίδιου LAN, οπότε το **SSH επιτυγχάνει**.
Εντολή: **ssh lab@203.0.118.18**

7.31 Παρατηρούμε **πακέτα IP** που ενθυλακώνουν **τεμάχια TCP**. Τα πακέτα αυτά στέλνονται μεταξύ των **203.0.118.18, θύρα ssh (22)** και **192.0.2.5, θύρα 18128**.

7.32 **Ναι**, είναι κρυπτογραφημένα, αλλά με το **ssh, όχι το IPsec** (δεν αναγράφεται ESP στην καταγραφή).