Εργαστήριο Δικτύων Υπολογιστών
Εργαστηριακή Άσκηση 10

Δημήτριος Κόγιος
03119220
Όνομα PC: lekog-HP-Laptop-15s-fq1xxx

Άσκηση 1:

1.1)kldload ipfw

1.2) kldstat

1.3) Όχι δεν μπορώ.
ping: sendto: Permission denied

1.4) ipfw list
65535 deny ip from any to any

1.5) ipfw show
65535 7 588 deny ip from any to any
Άρα 7 και 588.

1.6) ipfw zero

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

1.8) Και τα δύο ping επιτυγχάνουν.

1.9) Όχι δεν μπορώ.

ping: sendto: Permission denied

1.10) ipfw add allow icmp from any to any

1.11) Πήρε 200 γιατί ο προηγούμενος ήταν ο 100 και ο πυρήνας ορίζει αυτόματα αριθμό μεγαλύτερο κατά 100 του αύξοντα αριθμού του τελευταίου πριν τον προκαθορισμένο κανόνα.

1.12) Ναι και ναι.

1.13) Δεν μπορούμε να κάνουμε traceroute στο PC2 γιατί στα UNIX μηχανήματα το traceroute στέλνει UDP datagrams και όχι icmp. Για να λειτουργήσει το traceroute πρέπει να γράψουμε:
traceroute -I 192.168.1.3 (ώστε να στέλνουμε ICMP αντί για UDP)

1.14) Σύμφωνα με το man page του traceroute:

```
Protocol specific. For UDP, UDP-Lite, TCP and SCTP, sets the base
port number used in probes (default is 33434).  Traceroute hopes
that nothing is listening on UDP ports (or UDP-Lite ports if used
by traceroute and supported by the peer) port + 1 to port +
(max_ttl - first_ttl + 1) * nprobes at the destination host (so
an ICMP PORT_UNREACHABLE message will be returned to terminate
the route tracing).  If something is listening on a port in the
default range, this option can be used to pick an unused port
range.
```

Δηλαδή χρησιμοποιεί τις θύρες 33435 (=33434 + 1) μέχρι και 33434 + (64 - 1 + 1) * 3= 33434 + 192 = 33626 (για τις default τιμές των max_ttl , first_ttl , nprobes.
Άρα:
ipfw add allow udp from me to any 33435-33626

1.15) Με ssh lab@192.168.1.3 παίρνουμε μήνυμα σφάλματος permission denied.

1.16) ipfw add allow tcp from me to any setup
ipfw add allow tcp from any to any established

1.17) ipfw zero
ssh lab@192.168.1.3
ls
exit

1.18) ipfw show
1 ο πρώτος λόγω του πρώτου πακέτου χειραψίας SYN , ACK
86 ο δεύτερος λόγω όλων των υπολοίπων TCP τεμαχίων.

1.19) Όχι γιατί δεν επιτρέπουμε το setup tcp συνδέσεων από ξένους στο PC1.

1.20) service ftpd onestart

1.21) ftp lab@192.168.1.3
Ενώ μπορούμε να συνδεθούμε , δεν μπορούμε να καταβάσουμε αρχεία με get γιατί πέρα από το control connection του FTP , ο server (ο PC2) πρέπει να ανοίξει data connection με τον πελάτη (PC1) . Όμως όπως είπαμε στο 1.19 δεν επιτρέπουμε το setup tcp συνδέσεων από ξένους στο PC1.

Άσκηση 2:

2.1) kldload ipfw

2.2) Όχι, permission denied.

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) Ναι, χωρίς απάντηση.

2.6) Μηδενίζουμε τους μετρητές με ipfw zero. Ύστερα εκτελούμε ping -c 1 192.168.1.2 για να στείλουμε μόνο ένα πακέτο. Με ipfw show βλέπουμε ότι ο κανόνας του 2.4 έχει χρησιμοποιηθεί μία φορά. Δηλαδή, το ICMP reply του PC1 προς το PC2 δεν πέρασε από το firewall του PC2 για αυτό και το ping κολλάει.

2.7) ipfw delete 200
ipfw add allow icmp from me to any icmptypes 8 keep-state

Ναι πλέον βλέπουμε απαντήσεις στα echo requests μας.

2.8) Ναι μπορούμε.

2.9) Όχι πλέον το PC1 δεν λαμβάνει απάντηση γιατί όπως λέει η θεωρία :Όταν υπάρξει ταίριασμα σε κανόνα που λήγει με το keep-state, τότε το τείχος προστασίας λειτουργεί βάσει της κατάστασης (stateful behavior). Δημιουργείται δηλαδή ένας δυναμικός κανόνας που ταιριάζει για το συγκεκριμένο πρωτόκολλο την αμφίδρομη κίνηση μεταξύ των διευθύνσεων πηγής και προορισμού

και των αντίστοιχων θυρών πηγής και προορισμού. **Οι δυναμικοί κανόνες έχουν περιορισμένο χρόνο ζωής που ανανεώνεται όσο υπάρχει κίνηση που ταιριάζει.**

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

2.11) Βλέπω ότι υπάρχει ενεργός δυναμικός κανόνας με βάση τον κανόνα με αύξοντα αριθμό 300 που είναι ο κανόνας του 2.10.

2.12) Ο δυναμικός κανόνας σβήστηκε.

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

2.14) ipfw add allow udp from me to any 33435-33626
ipfw add allow icmp from any to me icmptypes 0,3,11
0: echo reply , 3 : destination unreachable , 11 :: ttl exceeded

2.15) ipfw add allow udp from any to me 33435-33626

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

2.17) ssh lab@192.168.1.3 => μας ζητάει το password

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

2.19) ipfw add allow tcp from 192.168.1.3 to me 22

2.20) Ναι με sftp lab@192.168.1.3 και get .

2.21) Όχι δεν μπορούμε.

Άρα στο PC2 προσθέτουμε: ipfw add allow tcp from any to me 21 keep-state

2.22) Γιατί η δεύτερη εκτελείται σε passive mode και δεν έχουμε κάνει allow την κίνηση σε αυτές τις θύρες.

2.23) ipfw add allow tcp from any to me 1024-65535 keep-state

the server. When opening an FTP connection, the client opens two random unprivileged ports locally (N > 1023 and N+1). The first port contacts the server on

2.24) Ναι.

2.25) PC2 : ipfw add allow tcp from me 20 to any keep-state
PC1 : ipfw add allow tcp from any 20 to me keep-state

2.26) Το ftp μπορεί να χρησιμοποιεί πολλές θύρες όπως είδαμε στο ερώτημα 2.23 . Επίσης, ανάλογα με το version του ftp μπορεί ο client να ανοίγει την tcp σύνδεση ή ο server να την ανοίγει. Αυτό προσθέτει δυσκολία στη δημιουργία κανόνων του firewall αφού άμα βάλουμε πολλούς κανόνες ώστε να καλύψουμε όλες τις μορφές του ftp μπορεί να μειώσουμε την προστασία του χρήστη έναντι σε κακόβουλους. Από την άλλη, άμα παραλείψουμε κανόνες κάνοντας υποθέσεις για το πως ακριβώς θα λειτουργήσει το ftp κινδυνεύουμε να μην λειτουγεί καθόλου.

2.27) kldunload ipfw
kldstat ===> δεν υπάρχει το ipfw

Άσκηση 3:

3.1) hostname PCx
route add default 192.168.1.1

3.2) cli

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) hostname SRV1

ifconfig em0 192.0.2.5/30
route add default 192.0.2.6

3.4) service ftpd onestart

3.5) intpm.ko

smbus.ko
ipfw.ko
ipfw_nat.ko
libalias.ko

3.6) Το ipfw.

3.7) UNKNOWN

3.8) Βλέπουμε 11 κανόνες με τελευταίο να είναι ο προκαθορισμένος κανόνα (deny ip from any to any).

3.9) ipfw nat show config -> όχι δεν έχει οριστεί.

3.10) Όχι δεν λαμβάνουμε απάντηση.

3.11) Όχι, δεν λαμβάνουμε απάντηση.

3.12) ipfw nat 123 config unreg_only if em1 reset

3.13) ipfw add nat 123 ip4 from any to any

3.14) Ναι πλέον μπορούμε.

3.15) tcpdump -i em0

3.16) ipfw show
ipfw zero

3.17) ping -c 3 192.0.2.2
Στην καταγραφή βλέπουμε ότι η διεύθυνση πηγής των ICMP echo request είναι 192.0.2.1 (δηλαδή η διεύθυνση της διεπαφής του FW1 στο WAN1).

3.18) Είναι επίσης 192.0.2.1 .

3.19) Αυτός που πρσθέσαμε στο ερώτημα 3.13 που στέλνει όλα το IPv4 πακέτα για μετάφραση στον πίνακα NAT 123.

3.20) Εφαρμόστηκε 12 φορές αφού 3 ICMP πακέτα στέλνει ο PC1 στο FW1 , 3 στέλνει το FW1 στο R1 , 3 στέλνει το R1 στο FW1 και 3 στέλνει το FW1 στο PC1.

3.21) Ναι .

3.22) Είναι πάλι αυτός του ερωτήματος 3.13 .

3.23) Δεν γίνεται μετάφραση γιατί η διεύθυνση 192.0.2.5 δεν είναι ιδιωτική.

3.24) Ναι με ssh lab@192.0.2.5 .

3.25) Δεν μπορούμε. Είναι θέμα δρομολόγησης αφού ούτε ping στο PC2 μπορούμε να κάνουμε αλλά ούτε και traceroute.

3.26) ipfw nat 123 config unreg_only if em1 reset redirect_addr 192.168.1.3 192.0.2.1

3.27) Είμαστε συνδεδεμένοι στο PC2 . Το καταλαβαίνουμε από το prompt lab@PC2 , hostname -> PC2 αλλά και από το PC2 με netstat βλέπουμε σύνδεση ssh.

3.28) 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) Είμαστε συνδεδεμένοι στο PC1 . Το καταλαβαίνουμε από το prompt lab@PC1 , hostname -> PC1 αλλά και από το PC1 με netstat βλέπουμε σύνδεση ssh.

3.30) Τώρα είμαστε συνδεδεμένοι στο PC1. Το καταλαβαίνουμε κάνοντας netstat από το PC1 και βλέπουμε ανοιχτή ftp σύνδεση.

3.31) Ναι με ls και ναι με get.

3.32) Είναι το PC2 αφού αυτό ορίσαμε στο ερώτημα 3.26 .

3.33) Στο PC1 αφού το ssh χρησιμοποιεί την θύρα 22 και στο ερώτημα 3.28 ορίσαμε ότι tcp κίνηση στη διεπαφή του FW1 στο WAN1 με θύρα προορισμού την 22 ανακατευθύνεται στο PC1.

Άσκηση 4:

4.1) Όχι δεν μπορούμε πλέον να κάνουμε ping.

4.2) Γιατί αφού απενεργοποιήσαμε το one-pass ξεχωρίσαμε τη διαδικασία της μετάφρασης και της αποδοχής. Δηλαδή ενώ γίνεται μετάφραση σύμφωνα με τον κανόνα του 3.13 , δεν αποδέχεται το πακέτο το οποίο μετά γίνεται deny λόγω του προκαθορισμένου κανόνα.

4.3) ipfw delete 100
ipfw add 1100 allow all from any to any via em0

4.4) Ναι είναι επιτυχές.

4.5) Συνδεόμαστε στο FW1.

4.6) Είναι υπεύθυνοι οι κανόνες 100 και 1100 δηλαδή ο allow ip from any to any via lo0 (=100) και ο allow ip from any to any via em0 (=100) .

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 2000 nat 123 all from any to any recv em1

4.10) ipfw add 2001 check-state

4.11) Απαντάει το FW1.

4.12) Το PC2 λόγω του redirect_addr που έχουμε ορίσει στο NAT 123.

4.13) Στο FW1.

4.14) Στο PC1 λόγω το redirect_port που έχουμε ορίσει στο NAT 123.

4.15) Στο PC2 λόγω του redirect_addr που έχουμε ορίσει στο NAT 123.

4.16) Ναι μπορούμε.

4.17) Ναι μπορούμε.

4.18) Ναι μπορούμε με ls και get.

4.19) ipfw add 2999 deny all from any to any via em1

4.20) Το 4.11 επιτυγχάνει.
Το 4.12 αποτυγχάνει.
Το 4.13 επιτυγχάνει.
Το 4.14 αποτυγχάνει.
Το 4.15 αποτυγχάνει.
Το 4.16 αποτυγχάνει.
Το 4.17 αποτυγχάνει.
Το 4.18 αποτυγχάνει.

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

4.22) Ναι το ping είναι επιτυχές.

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

(Σημείωση : “out via = out xmit + out recv , δηλαδή εξερχόμενη κίνηση που μεταδίδεται από τη διεπαφή (xmit) ή εξερχόμενη κίνηση που έγινε receive από τη διεπαφή (recv) .
+
Using "via ifo" is like using three rules: "in recv ifo",
"out xmit ifo", and "out recv ifo".)

4.24) Ναι μπορούμε να συνδεθούμε.

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

(Σημείωση : Using "in via ifo" is like using "in recv ifo".)

4.26) Το PC2 λόγω του redirect_addr στο NAT 123.
Βάζοντας -c 1 στο ping και κάνοντας ipfw show βλέπουμε ότι χρησιμοποιούνται οι παρακάτω κανόνες:
1100 2 allow ip from any to any via em0
2000 1 nat 123 ip from any to any recv em1
2100 2 skipto 3000 icmp from any to any in via em1 keep-state
3000 1 nat 123 ip from any to any xmit em1
3001 2 allow ip from any to any via em1

Όταν το ICMP echo request του SRV1 φτάνει στο FW1 , γίνεται match με τον κανόνα 2000 και πηγαίνει στο NAT 123 όπου αλλάζει η διεύθυνση προορισμού λόγω του redirect_addr. Το matching συνεχίζεται γίνεται match με το 2100 και κάνουμε skipto 3000 όπου δεν matchάρει με το 3000 άρα συνεχίζει και

κάνει match με το 3001. Το πακέτο φεύγει από το FW1 για να προωθηθεί στο PC2. Εκεί γίνεται match ο 1100.
Μετά φτάνει στο FW1 το ICMP echo reply του PC2 και γίνεται match με το 1100. Για να φύγει από το FW1 και να φτάσει στο SRV1 γίνεται match με τον δυναμικό κανόνα 2100 και μετά γίνεται match με το 3000 και μεταφράζεται. Τέλος γίνεται match με το 3001 και προωθείται.

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

4.28) Συνδεόμαστε στο PC1 λόγω του redirect_port στο NAT 123. Συμβαίνουν αντίστοιχα βήματα με το ερώτημα 4.26 .

4.29) Όχι.

4.30) ipfw add 2300 skipto 3000 tcp from any to any 21 recv em1 keep-state
ipfw add 2301 skipto 3000 tcp from any 20 to any out via em1 keep-state

```
root@PC:~ # ipfw list
00100 allow ip from any to any via lo0
00200 deny ip from any to 127.0.0.0/8
00300 deny ip from 127.0.0.0/8 to any
00400 deny ip from any to ::1
00500 deny ip from ::1 to any
00600 allow ipv6-icmp from :: to ff02::/16
00700 allow ipv6-icmp from fe80::/10 to fe80::/10
00800 allow ipv6-icmp from fe80::/10 to ff02::/16
00900 allow ipv6-icmp from any to any icmp6types 1
01000 allow ipv6-icmp from any to any icmp6types 2,135,136
01100 allow ip from any to any via em0
02000 nat 123 ip from any to any recv em1
02001 check-state :default
02100 skipto 3000 icmp from any to any in via em1 keep-state :default
02200 skipto 3000 tcp from any to any 22 in recv em1 keep-state :default
02500 skipto 3000 icmp from any to any xmit em1 keep-state :default
02600 skipto 3000 tcp from any to any 22 out via em1 keep-state :default
02999 deny ip from any to any via em1
03000 nat 123 ip from any to any xmit em1
03001 allow ip from any to any via em1
65535 deny ip from any to any
```

Άσκηση 5:

5.1) 192.168.1.1/24

5.2) 10.0.0.1/30

5.3) Memory usage : 34%

5.4) Έχει 4 διεπαφές : em0 LAN , em1 WAN , em2 MNG, em3 DMZ.

5.5) 172.22.1.1/24

5.6) fw

5.7) fw1 + Save

5.8) Όχι δεν υπάρχουν.

5.9) IP address : 192.0.2.1 / 30
Gateway : 192.0.2.2

5.10) Ναι υπάρχει ο κανόνας Block private networks.

5.11) Είναι όλες απενεργοποιημένες.

5.12) Enable DNS forwarder + Save

5.13) Enable + ορισμός περιοχής + Save

5.14) dhclient em0
Αποδόθηκε η 192.168.1.2 /24 στο PC1

Με cat /etc/resolv.conf :
nameserver 192.168.1.1

Με netstat -rn :
default 192.168.1.1

5.15) Γιατί όταν είναι ενεργοποιημένος ο DNS forwarder , το FW1 λειτουργεί και ως DHCP.

5.16) Στα DHCP leases.

5.17) Βλέπουμε 7 εγγραφές.

5.18) Όχι .

5.19) Βλέπουμε ότι έγιναν deny τα πακέτα του ping μεταξύ άλλων logs.

5.20) Βλέπουμε 7 states.

Source	Port	Destination	Port	Protocol	Packets	Bytes	TTL
192.168.56.1	38968	192.168.56.2	80	tcp	17	1383	2:39
192.168.56.1	47066	192.168.56.2	80	tcp	13	1190	3:28
192.168.56.1	38144	192.168.56.2	80	tcp	13	1182	0:17
192.168.56.1	35964	192.168.56.2	80	tcp	13	1174	0:28
192.168.56.1	35952	192.168.56.2	80	tcp	6	1027	0:28
192.168.56.1	47064	192.168.56.2	80	tcp	6	1013	3:28
192.168.56.1	44558	192.168.56.2	80	tcp	3	666	2:30:00

Firewall connection states displayed: 7

5.21) Δεν υπάρχουν κανόνες.

5.22) Action : Pass

Interface : LAN
Protocol : any
Source : any
Destination : any

5.23) Ναι και τα τρία pings είναι επιτυχημένα.

5.24) Όχι δεν μπορούμε.

5.25) arp -a
Ναι υπάρχει εγγραφή για τη διεπαφή του FW1 στο WAN1.

5.26) Action : Pass
Interface : WAN
Protocol : ICMP
Source : any
Destination : WAN address

5.27) Ναι.

5.28) Όχι γιατί το R1 δεν έχει route to host.

5.29) Ναι μπορούμε δηλαδή το R1 στέλνει πίσω ICMP echo reply άρα γίνεται μετάφραση NAT της ιδιωτικής διεύθυνσης του PC1 στη WAN address.

5.30) Όχι δεν παίρνουμε απάντηση αφού το SRV1 δεν έχει route to host.

5.31) route add default 172.22.1.1

5.32) Ναι πλέον μπορούμε.

5.33) Όχι γιατί δεν έχουμε ορίσει κάποιον κανόνα για το DMZ.
Everything that isn't explicitly passed is blocked by default.

5.34) Όχι γιατί δεν έχουμε ορίσει κάποιον κανόνα για το DMZ.
Everything that isn't explicitly passed is blocked by default.

5.35) Action : Pass
Interface : DMZ
Protocol : any
Destination : not LAN subnet

5.36) Ναι.

5.37) Ναι.

5.38) Όχι , no route to host .

5.39) Ναι μπορούμε. Το NAT λειτουργεί και για την κίνηση μεταξύ DMZ - WAN1.

5.40) dhclient em0
Πήρε το PC2 την 192.168.1.3 με nameserver 192.168.1.1 και default gateway το 192.168.1.1 (με τον ίδιο τρόπο που εξηγήσαμε στο ερώτημα 5.14) .

5.41) Action : Block
Interface : LAN
Protocol : any
Source : type : single host or alias , address : 192.168.1.3
Dest : type : single host or alias , address : 172.22.1.2

5.42) Πρέπει να τοποθετηθεί πριν αφού όπως μας λέει το Hint:Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order.

5.43) Όχι.

5.44) Ναι μπορούμε γιατί επιτρέπουμε την κίνηση στο LAN1 και προφανώς επιτρέπεται η κίνηση μέσω του loopback itnerface του FW1 όπως φάνηκε και στο 5.23 .

Άσκηση 6:

6.1) ip route 203.0.118.0/24 192.0.2.1

6.2) Firewall -> NAT -> Outbound -> Enable advanced outbound NAT

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

+ Save + Apply Changes

6.4) Interface : WAN
Source : 192.168.1.3/32
Destination : any
Target : 203.0.118.15

+ Save + Apply Changes

6.5) tcpdump -i em0

6.6) Του PC1 φτάνουν με την IP : 203.0.118.14
Του PC2 φτάνουν με την IP : 203.0.118.15

6.7) Το ping αποτυγχάνει γιατί δεν υπάρχει κανόνας στο Firewall που να επιτρέπει την ICMP από WAN address προς το LAN.

6.8) Firewall -> NAT -> Server NAT -> External IP address 203.0.118.18

+ Save + Apply changes

6.9) Interface : WAN
External address : 203.0.118.18
Protocol : TCP
External port range : from : 22
to : 22
NAT IP : 172.22.1.2
Local port : 22

+ auto-add a firewall rule to permit traffic through this NAT rule + Save + Apply changes

6.10) Τοποθετήθηκε κανόνας που επιτρέπει την TCP κίνηση προς τη θύρα 22 της διεύθυνσης 172.22.1.2 γιατί επιλέξαμε το auto-add a firewall rule to permit traffic through this NAT rule.

6.11) Με lab@203.0.118.18 συνδεθήκαμε στο SRV1 .

6.12) Με ping 203.0.118.18 το ping αποτυγχάνει αφού δεν έχουμε ορίσει κάποιον κανόνα στο WAN που να επιτρέπει την ICMP κίνηση από το R1 προς την 203.0.118.18 .

6.13) Ναι συνδεόμαστε στο SRV1. Τα πακέτα IP από το PC2 προς το SRV1 πηγαίνουν μέσω του R1 από tcpdump.

6.14) Όχι γιατί πλέον τα icmp echo requests φτάνουν στον R1 με διεύθυνση πηγής 192.168.1.2 και ο R1 δεν έχει εγγραφή στον πίνακα δρομολόγησής του για αυτήν τη διεύθυνση.

6.15) Ναι πλέον είναι επιτυχές γιατί τα icmp echo requests φτάνουν στον R1 με διεύθυνση πηγής 192.0.2.1 που είναι η δημόσια διεύθυνση IPv4 του FW1.
With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN) and any mappings specified below will be ignored.

6.16) Από τον R1 μπορούμε.
Δεν μπορούμε όμως από τα PC1 και PC2.

6.17) Βλέπουμε ότι ενώ ανταλλάσονται τα δύο πρώτα τεμάχια της χειραψίας , μετά γίνεται reset της σύνδεσης.

6.18) Η σημείωση στη σελίδα του inbound μας λέει ότι δεν γίνεται να έχουμε πρόσβαση σε NATed services χρησιμοποιώντας την WAN IP address από μέσα από το LAN. Αυτό ακριβώς προσπαθούμε να κάνουμε τώρα αφού τα πακέτα του PC2 έχουν πλεόν μεταφρασμένη διεύθυνση 192.0.2.1 που είναι η WAN address.

Άσκηση 7:

7.1) Done.

7.2) Interfaces -> MNG -> IP address 192.168.56.3 / 24

+ Save

7.3) Done.

7.4) Ναι, στο FW1 μέσω της 192.158.56.2 και στο FW2 μέσω της 192.158.56.3 .

7.5) System -> General setup -> Hostname fw2

+ Save

7.6) Interfaces -> WAN -> IP address 192.0.2.5/30
Gateway 192.0.2.6

+ Block private networks + Save

7.7) Interfaces -> LAN -> IP address 192.168.2.1/24

+ Save

7.8) Diagnostics -> Reboot system -> Yes

7.9) Action : Pass
Interface : LAN
Protocol : any
Source : any
Destination : any

+ Save + Apply changes

7.10) Action : Pass
Interface : WAN
Protocol : ICMP
Source : any
Destination : WAN address

+ Save + Apply changes

7.11) ifconfig em0 192.168.2.2/24
route add default 192.168.2.1

7.12) Ναι το ping είναι επιτυχές.

7.13) Ναι το ping είναι επιτυχές.

7.14) Όχι δεν μπορούμε αφού ο R1 δεν έχει εγγραφές στον πίνακα δρομολόγησής του για τα PC1 και PC2.

7.15) VPN -> IPsec -> Enable IPsec

Local Subnet : LAN subnet
Remote subnet : 192.168.2.0/24
Remote gateway : 192.0.2.5
Pre-shared Key : lekog

+Save + Apply changes

7.16) Βλέπουμε τον κανόνα :

7.17) Όχι.

7.18) Ναι :

7.19)
Local subnet : LAN subnet
Remote subnet : 192.168.1.0/24
Remote gateway : 192.0.2.1
Pre-shared Key : lekog

+Save + Apply changes

7.20) Όχι.
7.21) Ναι :

7.22) Ναι.

7.23) Ναι.

7.24) Ναι πλέον έχουμε 2 SAD:

SAD SPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.1	192.0.2.5	ESP	00beaefc	3des-cbc	hmac-sha1
192.0.2.5	192.0.2.1	ESP	00203671	3des-cbc	hmac-sha1

7.25) Ναι έχουμε και εκεί 2 SAD:

SAD SPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.5	192.0.2.1	ESP	00203671	3des-cbc	hmac-sha1
192.0.2.1	192.0.2.5	ESP	00beaefc	3des-cbc	hmac-sha1

7.26) tcpdump -i em0 -vv

7.27) Όχι παρατηρούμε ESP πακέτα.

7.28) Εμφανίζονται ESP πακέτα. Τα πακέτα με πηγή το PC1 έχουν διεύθυνση πηγής 192.0.2.1 και διεύθυνση προορισμού 192.0.2.5. Αντίστοιχα, τα πακέτα με πηγή το PC2 έχουν διεύθυνση πηγής 192.0.2.5 και διεύθυνση προορισμού 192.0.2.1.

7.29) Όχι.

7.30) Ναι μπορώ. Πλέον το PC2 δεν έχει το firewall του LAN1 (FW1) αλλά το FW2 και συνεπώς μπορεί να χρησιμοποιήσει τις NATed υπηρεσίες του FW1 αφού χρησιμοποιείται η WAN διεύθυνση του FW2 για τη σύνδεση με το SRV1.

7.31) Παρατηρούμε πακέτα TCP. Για τα πακέτα με πηγή το PC2 βλέπουμε διεύθυνση πηγής 192.0.2.5 , θύρα πηγής 45411 και διεύθυνση προορισμού 203.0.118.18 και θύρα προοριμού ssh (=22).

7.32) Είναι κρυπτογραφημένα αλλά όχι με το IPsec.