Ονοματεπώνυμο: Αλεξάνδρα Μωραϊτάκη	**Όνομα PC:**
Ομάδα: 1	**Ημερομηνία: 15/05/2025**

Εργαστηριακή Άσκηση 10
Τείχη προστασίας (Firewalls) και NAT

ΑΣΚΗΣΗ 1 Ένα απλό τείχος προστασίας

ΕΡΩΤΗΣΗ 1.1

Ορισμός ονόματος, IP address στο PC1:

```
hostname PC1
ifconfig em0 192.168.1.2/24
```

Ορισμός ονόματος, IP address, route στο PC2:

```
hostname PC2
ifconfig em0 192.168.1.3/24
```

ΕΡΩΤΗΣΗ 1.2

Φόρτωση τείχους προστασίας στο PC1:

```
kldload ipfw
```

ΕΡΩΤΗΣΗ 1.3

```
kldstat
```

ΕΡΩΤΗΣΗ 1.4

Ping PC1-> lo0/em0 αποτυγχάνει. Permission denied.

ΕΡΩΤΗΣΗ 1.5

```
ipfw list
```

Rules: 65535 deny ip from any to any

ΕΡΩΤΗΣΗ 1.6

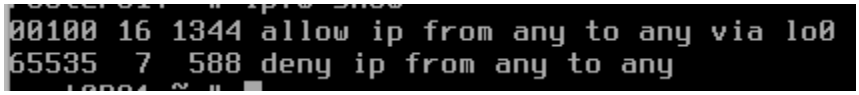
```
ipfw add 100 allow all from any to any via lo0
```

ΕΡΩΤΗΣΗ 1.7

Ping PC1-> lo0/em0 επιτυγχάνει.

ΕΡΩΤΗΣΗ 1.8

```
ipfw show
```



ΕΡΩΤΗΣΗ 1.9

```
ipfw zero 100
```

ΕΡΩΤΗΣΗ 1.10

Ping PC1-> PC2 Permission denied

ΕΡΩΤΗΣΗ 1.11

```
ipfw add allow icmp from any to any
```

ΕΡΩΤΗΣΗ 1.12

Αύξων αριθμός 200. Αφού δεν δώσαμε εμείς συγκεκριμένο αριθμό, αυξάνεται κατά 100 από τον μεγαλύτερο.

ΕΡΩΤΗΣΗ 1.13

Ping PC1-> PC2 επιτυγχάνει.

ΕΡΩΤΗΣΗ 1.14

traceroute 192.168.1.3 Permission denied

Ο λόγος που δεν επιτυγχάνει είναι επειδή by default η εντολή traceroute χρησιμοποιεί UDP. Ωστόσο εμείς επιτρέπουμε μόνο τα icmp. Άρα πρέπει να ορίσουμε -i (icmp)

ΕΡΩΤΗΣΗ 1.15

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

ΕΡΩΤΗΣΗ 1.16

PC1: `ssh lab@192.168.1.3`
Permission denied

ΕΡΩΤΗΣΗ 1.17

```
ipfw add 10 check-state
ipfw add allow tcp from me to any 22 out setup keep-state
```

ΕΡΩΤΗΣΗ 1.18

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

ΕΡΩΤΗΣΗ 1.19

Εφαρμοστηκε 387 φορές.

ΕΡΩΤΗΣΗ 1.20

Δεν μπορούμε γιατί δεν έχουμε τον κανόνα setup.

ΕΡΩΤΗΣΗ 1.21

```
service ftpd onestart
```

ΕΡΩΤΗΣΗ 1.22

ftp 192.168.1.3
Can't connect γιατί δεν έχουμε επιτρέψει κίνηση στην port 21(ftp).

ΑΣΚΗΣΗ 2 Λειτουργία του BGP

ΕΡΩΤΗΣΗ 2.1

Φόρτωση τείχους προστασίας στο PC2:

```
kldload ipfw
```

ΕΡΩΤΗΣΗ 2.2

Ping PC2->PC1: Permission denied

ΕΡΩΤΗΣΗ 2.3

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

ΕΡΩΤΗΣΗ 2.4

```
ipfw add allow all from me to any out icmptypes 8
```

ΕΡΩΤΗΣΗ 2.5

Ping PC2->PC1: αποτυγχάνει

ΕΡΩΤΗΣΗ 2.6

Περνάνε πακέτα γιατί οι μετρητές του κανόνα για icmp αυξάνονται.

ΕΡΩΤΗΣΗ 2.7

ipfw delete 200

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

Ping PC2->PC1: επιτυγχάνει.

ΕΡΩΤΗΣΗ 2.8

Επιτυγχάνουν και τα 2 ping.

ΕΡΩΤΗΣΗ 2.9

Ping PC1-> PC2 αποτυγχάνει. Αυτό συμβαίνει γιατί στον PC2 έχουμε μόνο έναν stateful κανόνα που επιτρέπει εξερχόμενα echo-request (και κρατάει state για τα echo-reply), όχι όμως ένα κανόνα που να επιτρέπει εισερχόμενα echo-request από το PC1.

ΕΡΩΤΗΣΗ 2.10

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

ΕΡΩΤΗΣΗ 2.11

Ping PC1->PC2

```
ipfw -d show
```

Με αυτήν την εντολή εμφανίζονται τόσο οι στατικοί όσο και οι δυναμικοί κανόνες.

```
ipfw -D show
```

Με αυτήν την εντολή εμφανίζονται μόνο οι δυναμικοί κανόνες. Εμφανίζεται κανόνας PC1->PC2.

ΕΡΩΤΗΣΗ 2.12

```
ipfw -D show
```

Τώρα που τελείωσε το ping, δεν έχουμε κανέναν δυναμικό κανόνα.

ΕΡΩΤΗΣΗ 2.13

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

ΕΡΩΤΗΣΗ 2.14

```
ipfw add allow udp from me to any 33435-33626 out
ipfw add allow icmp from any to me icmptypes 3,11
```

ΕΡΩΤΗΣΗ 2.15

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

ΕΡΩΤΗΣΗ 2.16

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

ΕΡΩΤΗΣΗ 2.17

```
ssh lab@192.168.1.3
```

ΕΡΩΤΗΣΗ 2.18

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

ΕΡΩΤΗΣΗ 2.19

```
ipfw add allow tcp from 192.168.1.3 to me 22 in setup keep-state
```

ΕΡΩΤΗΣΗ 2.20

```
sftp lab@192.168.1.3
```

Ναι.

ΕΡΩΤΗΣΗ 2.21

```
ftp lab@192.168.1.3
```

Permission denied

```
ipfw add allow tcp from any to me 21 in setup keep-state
ipfw add allow tcp from me to any 21 out setup keep-state
```

ΕΡΩΤΗΣΗ 2.22

- cd /usr πετυχαίνει γιατί το control-channel (TCP 21) επιτρέπεται.
- ls αποτυγχάνει γιατί το data-channel (port 20) δεν επιτρέπεται.

ΕΡΩΤΗΣΗ 2.23

```
ipfw add allow tcp from any to me 1024-65535 in setup keep-state
ipfw add allow tcp from me to any 1024-65535 out setup keep-state
```

ΕΡΩΤΗΣΗ 2.24

Όχι.

ΕΡΩΤΗΣΗ 2.25

PC1:

```
ipfw add allow tcp from me 20 to any 1024-65535 out setup keep-state
```

PC2:

```
ipfw add allow tcp from any 20 to me 1024-65535 in setup keep-state
```

ΕΡΩΤΗΣΗ 2.26

Το FTP χρησιμοποιεί control-channel (21) και data-channel (θύρα 20), οπότε χωρίς stateful rules ή ειδικούς FTP helpers πρέπει να ανοίγεις πολλές θύρες. Είναι μη ασφαλής υπηρεσία και για αυτό βάζουμε κανόνες firewall.

ΕΡΩΤΗΣΗ 2.27

```
kldunload ipfw
kldstat
```

ΑΣΚΗΣΗ 3 Απλό Network Address Translation

ΕΡΩΤΗΣΗ 3.1

PC1, PC2:

```
route add default 192.168.1.1
```

ΕΡΩΤΗΣΗ 3.2

R1:

```
cli
configure terminal
interface em0
ip address 192.0.2.2/30
interface em1
ip address 192.0.2.6/30
```

ΕΡΩΤΗΣΗ 3.3

SRV1:

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

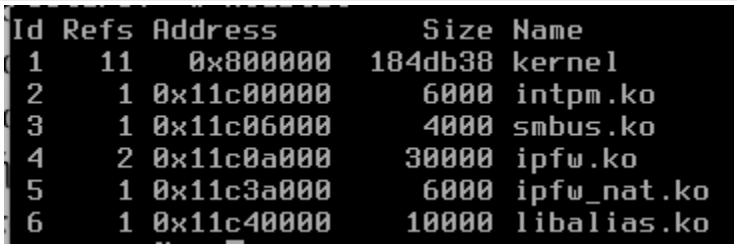
ΕΡΩΤΗΣΗ 3.4

PC2, SRV1:

```
service ftpd onestart
```

ΕΡΩΤΗΣΗ 3.5

```
kldstat
```



```
Id Refs Address            Size Name
 1   11 0x800000   184db38 kernel
 2    1 0x11c00000     6000 intpm.ko
 3    1 0x11c06000     4000 smbus.ko
 4    2 0x11c0a000    30000 ipfw.ko
 5    1 0x11c3a000     6000 ipfw_nat.ko
 6    1 0x11c40000    10000 libalias.ko
```

ΕΡΩΤΗΣΗ 3.6

ipfw

ΕΡΩΤΗΣΗ 3.7

```
sysrc firewall_type
```

UNKNOWN

ΕΡΩΤΗΣΗ 3.8

11 κανόνες με τελευταίο τον deny ip from any to any.

ΕΡΩΤΗΣΗ 3.9

```
ipfw nat show config
```

Δεν εμφανίζεται κανένα.

ΕΡΩΤΗΣΗ 3.10

Ping PC1->FW1: αποτυγχάνει

ΕΡΩΤΗΣΗ 3.11

Ping SRV1->FW1: αποτυγχάνει

ΕΡΩΤΗΣΗ 3.12

FW1:

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

ΕΡΩΤΗΣΗ 3.13

FW1:

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

ΕΡΩΤΗΣΗ 3.14

Ping PC1->FW1: επιτυγχάνει.

ΕΡΩΤΗΣΗ 3.15

R1: `tcpdump -i em0 -n -vv`

ΕΡΩΤΗΣΗ 3.16

FW1:

```
Ipfw show
Ipfw zero
```

ΕΡΩΤΗΣΗ 3.17

Ping PC1->R1.
IP source address ICMP Echo Request: 192.0.2.1

ΕΡΩΤΗΣΗ 3.18

IP dst address ICMP Echo Reply: 192.0.2.1

ΕΡΩΤΗΣΗ 3.19

```
nat 123 ip from any to any
```

ΕΡΩΤΗΣΗ 3.20

12 φορές.

ΕΡΩΤΗΣΗ 3.21

Ping SRV1->FW1(WAN1): επιτυγχάνει.

ΕΡΩΤΗΣΗ 3.22

```
nat 123 ip from any to any
```

ΕΡΩΤΗΣΗ 3.23

Ναι ωθείται.

ΕΡΩΤΗΣΗ 3.24

```
ftp lab@192.0.2.5
```

ΕΡΩΤΗΣΗ 3.25

```
ssh lab@192.0.2.5
```

ΕΡΩΤΗΣΗ 3.26

Στην περίπτωση της αντίστροφης σύνδεσης, τα πακέτα αποστέλλονται στη διεύθυνση 192.168.1.3, αλλά ο R1 δεν γνωρίζει πώς να δρομολογήσει το δίκτυο 192.168.1.0/24 και απαντά με ICMP Host Unreachable. Έτσι το πρόβλημα δεν είναι το NAT, αλλά έλλειψη route προς το υποδίκτυο. Το διαπιστώσαμε με tcpdump στον R1, όπου φαίνεται το ICMP Host Unreachable αμέσως μετά την αρχική προσπάθεια σύνδεσης.

ΕΡΩΤΗΣΗ 3.27

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

ΕΡΩΤΗΣΗ 3.28

```
ssh lab@192.0.2.1
```

Συνδέθηκα επιτυχώς στο PC2.

ΕΡΩΤΗΣΗ 3.29

```
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
```

```
ssh lab@192.0.2.1
```

Συνδέθηκα επιτυχώς στο PC2.

ΕΡΩΤΗΣΗ 3.30

Συνδέθηκα επιτυχώς στο PC1.

ΕΡΩΤΗΣΗ 3.31

Συνδέθηκα επιτυχώς στο PC2.

ΕΡΩΤΗΣΗ 3.32

rc.conf

ΕΡΩΤΗΣΗ 3.33

```
ftp lab@192.0.2.1
```

PC2.

ΕΡΩΤΗΣΗ 3.34

```
ssh lab@192.0.2.1
```

PC1.

ΑΣΚΗΣΗ 4 Τείχος προστασίας και NAT

ΕΡΩΤΗΣΗ 4.1

FW1: `ipfw disable one_pass`
Ping -> αποτυγχανουν.

ΕΡΩΤΗΣΗ 4.2

Περνάνε από αυτόν τον κανόνα αλλά μπλοκάρουν στον επόμενο.

ΕΡΩΤΗΣΗ 4.3

FW1:

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

ΕΡΩΤΗΣΗ 4.4

Ping -> επιτυγχανουν.

ΕΡΩΤΗΣΗ 4.5

```
ssh lab@192.0.2.1
```

FW1.

ΕΡΩΤΗΣΗ 4.6

`ipfw add 1100 allow ip from any to any via em0`

ΕΡΩΤΗΣΗ 4.7

FW1:

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

ΕΡΩΤΗΣΗ 4.8

FW1:

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

ΕΡΩΤΗΣΗ 4.9

FW1:

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

ΕΡΩΤΗΣΗ 4.10

FW1:

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

ΕΡΩΤΗΣΗ 4.11

FW1(WAN1)

ΕΡΩΤΗΣΗ 4.12

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.13

```
ssh lab@192.0.2.1
```

FW1

ΕΡΩΤΗΣΗ 4.14

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.15

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.16

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.17

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.18

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.19

FW1:

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

ΕΡΩΤΗΣΗ 4.20

Επιτυγχάνουν μόνο αυτά του LAN1.

ΕΡΩΤΗΣΗ 4.21

FW1:

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

ΕΡΩΤΗΣΗ 4.22

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.23

FW1:

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

ΕΡΩΤΗΣΗ 4.24

Ναι

ΕΡΩΤΗΣΗ 4.25

FW1:

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

ΕΡΩΤΗΣΗ 4.26

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.27

FW1:

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

ΕΡΩΤΗΣΗ 4.28

Ενώ με tcpdump σε όλα τα μηχανήματα φαίνονται τα ICMP Echo requests/replies, τα ping δεν επιτυγχάνουν. Το είχαμε δει στο εργαστήριο αλλά μάλλον ήταν θέμα του Virtual Box.

ΕΡΩΤΗΣΗ 4.29

Όχι.

ΕΡΩΤΗΣΗ 4.30

FW1:

```
ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state
ipfw add 2400 skipto 3000 tcp from any 20 to any setup out via em1
keep-state
```

ΑΣΚΗΣΗ 5 Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

ΕΡΩΤΗΣΗ 5.1

Console: LAN1 192.168.1.1

ΕΡΩΤΗΣΗ 5.2

Console: WAN1 10.0.0.1

ΕΡΩΤΗΣΗ 5.3

GUI: memory saved 33%
Free memory: 66%

ΕΡΩΤΗΣΗ 5.4

4 interfaces

ΕΡΩΤΗΣΗ 5.5

DMZ: 172.22.1.1

ΕΡΩΤΗΣΗ 5.6

Hostname: fw
Domain(DNS): lab.ntua.gr

ΕΡΩΤΗΣΗ 5.7

Hostname: fw1
DNS: ntua.lab

ΕΡΩΤΗΣΗ 5.8

0 κανόνες.

ΕΡΩΤΗΣΗ 5.9

WAN:
Ip address: 192.0.2.1/30
Gateway: 192.0.2.2
Block Private Networks

ΕΡΩΤΗΣΗ 5.10

Rules:

1. Block private networks

ΕΡΩΤΗΣΗ 5.11

Είναι όλα απενεργοποιημένα.

ΕΡΩΤΗΣΗ 5.12

Enable DNS forwarder.

ΕΡΩΤΗΣΗ 5.13

Enable DHCP server on LAN interface with range: 192.168.1.2-192.168.1.3

ΕΡΩΤΗΣΗ 5.14

PC1: `dhclient em0`
IP address: 192.168.1.2
Default gateway: 192.168.1.1
DNS server: 192.168.1.1 (grep nameserver | /etc/resolv.conf)

ΕΡΩΤΗΣΗ 5.15

Η ενεργοποίηση του DNS forwarder ήταν απαραίτητη ώστε ο DHCP server να μοιράζει την ίδια τη LAN IP του FW1 ως DNS server και αυτός να ακούει/απαντάει στα ερωτήματα των clients. Επιπλέον ο forwarder προωθεί τα ερωτήματα στα upstream DNS που ορίζουμε στο System -> General Setup.

ΕΡΩΤΗΣΗ 5.16

Diagnostics -> DHCP Leases

ΕΡΩΤΗΣΗ 5.17

Diagnostics -> ARP table -> 7 εγγραφές

ΕΡΩΤΗΣΗ 5.18

Ping PC1-> FW1(LAN1) αποτυγχάνει.

ΕΡΩΤΗΣΗ 5.19

Diagnostics->Logs->FIrewall
5 logs icmp πακέτων που απορρίφθηκαν.

ΕΡΩΤΗΣΗ 5.20

Diagnostics->FIrewall States
2 states

ΕΡΩΤΗΣΗ 5.21

Κανένας κανόνας για το LAN1.

ΕΡΩΤΗΣΗ 5.22

Rules->new->pass->LAN->any->save

ΕΡΩΤΗΣΗ 5.23

Ping PC1->FW1 επιτυγχάνει τώρα

ΕΡΩΤΗΣΗ 5.24

Ping R1->FW1(WAN1) αποτυγχάνει

ΕΡΩΤΗΣΗ 5.25

Ναι υπάρχει εγγραφή που αντιστοιχεί στην MAC της διεπαφής WAN1 του FW1.

ΕΡΩΤΗΣΗ 5.26

Rules->pass->WAN->icmp->type:WAN address->save

ΕΡΩΤΗΣΗ 5.27

Ping R1->FW1(WAN1) επιτυγχάνει τώρα

ΕΡΩΤΗΣΗ 5.28

Ping R1->PC1 αποτυγχάνει αφού ο R1 δεν διαθέτει route για το 192.168.1.0/2.

ΕΡΩΤΗΣΗ 5.29

Ping PC1->R1 επιτυγχάνει αφού το NAT μεταφράζει τη διεύθυνση πηγής και αναστρέφει τη μετάφραση στις επιστροφές, επιτρέποντας στο PC1 να βλέπει τον R1.

ΕΡΩΤΗΣΗ 5.30

SRV1: `ifconfig em0 172.22.1.2/24 up`
Ping PC1->SRV1 αποτυγχάνει αφού το FW1 δεν έχει κανόνα που να επιτρέπει προώθηση ICMP από το LAN (em0) στο DMZ (em2).

ΕΡΩΤΗΣΗ 5.31

SRV1: `route add default 172.22.1.1`

ΕΡΩΤΗΣΗ 5.32

Ping PC1->SRV1 επιτυγχάνει

ΕΡΩΤΗΣΗ 5.33

Ping SRV1->FW1(DMZ) αποτυγχάνει αφού τα icmp πακέτα με πηγή DMZ απορρίπτονται από το firewall.

ΕΡΩΤΗΣΗ 5.34

Ping SRV1->PC1/R1 αποτυγχάνει αφού τα icmp πακέτα με πηγή DMZ απορρίπτονται από το firewall.

ΕΡΩΤΗΣΗ 5.35

Rules->
Action:pass
Interface: DMZ
Protocol:any
Dst: not, LAN subnet

ΕΡΩΤΗΣΗ 5.36

Ping SRV1->FW1(DMZ) επιτυγχάνει

ΕΡΩΤΗΣΗ 5.37

Ping SRV1->FW1(WAN1) επιτυγχάνει

ΕΡΩΤΗΣΗ 5.38

Ping R1->SRV1 αποτυγχάνει αφού ο R1 δεν διαθέτει route για το 192.168.1.2.

ΕΡΩΤΗΣΗ 5.39

Ping SRV1->R1 επιτυγχάνει αφού επειδή ο κανόνας επιτρέπει ICMP από το DMZ προς το WAN και το NAT φροντίζει για τη σωστή μετάφραση του SRV1 σε 192.0.2.1 και την επιστροφή των πακέτων.

ΕΡΩΤΗΣΗ 5.40

PC2: `dhclient em0`
IP address: 192.168.1.3
Default gateway: 192.168.1.1
DNS server: 192.168.1.1 (grep nameserver | /etc/resolv.conf)

ΕΡΩΤΗΣΗ 5.41

rules->block->
Interface: LAN
Protocol: any
Source: type: single host or alias
Source: address 192.168.1.3
Destination: type: single host or alias
Destination: address 172.22.1.2

ΕΡΩΤΗΣΗ 5.42

Ο κανόνας πρέπει να τοποθετηθεί πριν τον υπάρχοντα για να μπλοκάρονται τα επιθυμητά πακέτα.

ΕΡΩΤΗΣΗ 5.43

Ping PC2->SRV1 αποτυγχάνει

ΕΡΩΤΗΣΗ 5.44

Ping PC2->FW1(DMZ) επιτυγχάνει

ΑΣΚΗΣΗ 6 Τείχος προστασίας και προχωρημένο NAT

ΕΡΩΤΗΣΗ 6.1

R1:

```
cli
configure terminal
ip route 203.0.118.0/24 192.0.2.1
```

ΕΡΩΤΗΣΗ 6.2

firewall->nat-> outbound-> enable advanced outbound NAT

ΕΡΩΤΗΣΗ 6.3

firewall->nat-> outbound->
Interface: WAN

Source: 192.168.1.2/32
Target: 203.0.118.14

ΕΡΩΤΗΣΗ 6.4

firewall->nat-> outbound->
Interface: WAN
Source: 192.168.1.3/32
Target: 203.0.118.15

ΕΡΩΤΗΣΗ 6.5

R1: `tcpdump -i em0`

ΕΡΩΤΗΣΗ 6.6

Ping PC1/PC2->R1: επιτυγχάνουν και φτάνουν με διεύθυνση 102.0.118.14/15

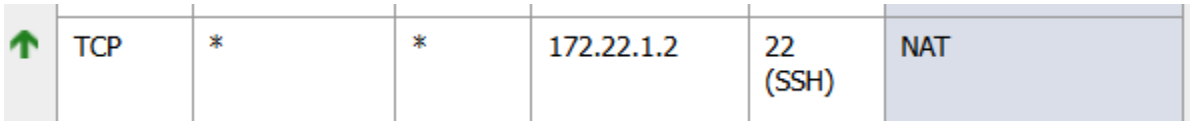
ΕΡΩΤΗΣΗ 6.7

firewall->NAT->Server NAT-> IP 203.0.118.18

ΕΡΩΤΗΣΗ 6.8

firewall->NAT->Inbound

ΕΡΩΤΗΣΗ 6.9



Το GUI φροντίζει να δημιουργήσει αυτόματα και τον αντίστοιχο pass-κανόνα, ώστε τα TCP/22 πακέτα να περνούν.

ΕΡΩΤΗΣΗ 6.10

R1: `ssh lab@203.0.118.18`
Ναι, η σύνδεση επιτυγχάνει και καταλήγει στον SRV1 (η δημόσια IP 203.0.118.18 έχει NAT 1:1 και port-forwarding στον SRV1).

ΕΡΩΤΗΣΗ 6.11

Ping R1->203.0.118.18 αποτυγχάνει αφού έχουμε τον κανόνα deny-all στο WAN.

ΕΡΩΤΗΣΗ 6.12

PC1/PC2: `ssh lab@172.22.1.2` επιτυγχάνει.
Παρατηρούμε με tcpdump τη διαδρομή.
PC1/PC2->FW1->R1->FW1->SRV1

Η σύνδεση SSH από τα PC1/PC2 προς τον SRV1 μέσω της δημόσιας διεύθυνσης 203.0.118.18 λειτουργεί κανονικά διότι στο FW1 έχουμε NAT και port-forwarding, οπότε τα TCP SYN πακέτα φτάνουν από το LAN στο FW1, εκεί μεταφράζονται σε προορισμό 172.22.1.5 (SRV1) και προωθούνται στον R1, ο οποίος τα επιστρέφει πάλι στο FW1 και τελικά στο SRV1.

ΕΡΩΤΗΣΗ 6.13

PC1: `ssh lab@203.0.118.0` αποτυγχάνει.

ΕΡΩΤΗΣΗ 6.14

firewall->nat-> outbound-> disable advanced outbound NAT

ΕΡΩΤΗΣΗ 6.15

R1: `ssh lab@203.0.118.18`
Ναι, η σύνδεση επιτυγχάνει και καταλήγει στον SRV1 αφού ο outbound κανόνας δεν επηρέαζε.
Ωστόσο με τα PC1/PC2 έχουμε αποτυχία σύνδεσης.

ΕΡΩΤΗΣΗ 6.16

SRV1: `tcpdump -i em0 -e`
R1: `tcpdump -i em0 -e`
PC1/PC2: `ssh lab@203.0.118.18`
Με απενεργοποιημένο το Advanced outbound NAT, το FW1 εφαρμόζει αυτόματο SNAT μόνο σε πακέτα που προωθούνται από το LAN στο WAN, αλλά **όχι** σε πακέτα που επιστρέφουν από το WAN στο DMZ/LAN. Έτσι, όταν το PC1 επιχειρεί SSH (TCP SYN) προς τη δημόσια διεύθυνση 203.0.118.14, το SYN φτάνει κανονικά στο SRV1· όμως ο SYN-ACK επιστρέφει πηγαίνοντας στο FW1 ως προορισμός WAN χωρίς να έχει γίνει reverse-NAT, οπότε το FW1 το θεωρεί προς το ίδιο και επειδή δεν υπάρχει σχετικό state στέλνει RST. Το SRV1 λαμβάνει αυτό το RST αντί της απάντησης, και το PC1/PC2 δεν ολοκληρώνουν ποτέ τη σύνδεση.

ΕΡΩΤΗΣΗ 6.17

Ο κανόνας που εισαγάγαμε στο ερώτημα 5.41 αφορά μόνο την επίτρεψη κίνηση από το PC2 προς τη διεύθυνση 172.22.1.2 και δεν φιλτράρει ούτε επηρεάζει το NAT. Στο ερώτημα 6.16, η αποτυχία προκύπτει αποκλειστικά από την απενεργοποίηση του Advanced Outbound NAT, οπότε το σφάλμα δεν έχει καμία σχέση με τον κανόνα 5.41.

ΑΣΚΗΣΗ 7 IPSec site-to-site VPN

ΕΡΩΤΗΣΗ 7.1

Αποσύνδεση network adapter 3(FW1).

ΕΡΩΤΗΣΗ 7.2

Interfaces->MNG->Ip address 192.168.56.3

ΕΡΩΤΗΣΗ 7.3

Επανασύνδεση network adapter 3(FW1).

ΕΡΩΤΗΣΗ 7.4

Ναι.

ΕΡΩΤΗΣΗ 7.5

Hostname_fw2
DNS: ntua.lab

ΕΡΩΤΗΣΗ 7.6

fw2->interfaces->WAN2->
Ip address 192.0.2.5/30
Getaway: 192.0.2.6
Block private networks

ΕΡΩΤΗΣΗ 7.7

fw2->interfaces->LAN2->
Ip address 192.168.2.1/24

ΕΡΩΤΗΣΗ 7.8

diagnostics->reboot

ΕΡΩΤΗΣΗ 7.9

fw2->rules->LAN->
Action:pass
interface:LAN
Protocol: any

ΕΡΩΤΗΣΗ 7.10

fw2->rules->WAN->
Action:pass
interface:WAN
Protocol: icmp
Dst: type WAN address

ΕΡΩΤΗΣΗ 7.11

PC2 configuration

ΕΡΩΤΗΣΗ 7.12

Ping PC1->FW2(WAN2) επιτυγχάνει

ΕΡΩΤΗΣΗ 7.13

Ping PC2->FW1(WAN1) επιτυγχάνει

ΕΡΩΤΗΣΗ 7.14

Ping PC1<->PC2 αποτυγχάνει αφού τα PC1 και PC2 βρίσκονται σε διαφορετικά υποδίκτυα πίσω από ξεχωριστά firewalls και ο R1 δεν διαθέτει διαδρομές για να δρομολογήσει την κυκλοφορία μεταξύ LAN1 και LAN2.

ΕΡΩΤΗΣΗ 7.15

fw1->VPN->Enable IPSec
Interface: WAN
Local subnet: type:LAN subnet
Remote subnet: 192.168.2.0/24
Remote gateway: 192.0.2.5
Pre shared key : alexandra

ΕΡΩΤΗΣΗ 7.16

fw1 ->Firewall->Rules->IPsec VPN
Default IPSec VPN

ΕΡΩΤΗΣΗ 7.17

fw1->Diagnostics ->IPSec -> SAD

No IPsec security associations.

ΕΡΩΤΗΣΗ 7.18

fw1->Diagnostics ->IPSec -> SPD

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

ΕΡΩΤΗΣΗ 7.19

fw2->VPN->Enable IPSec
Interface: WAN
Local subnet: type:LAN subnet
Remote subnet: 192.168.1.0/24
Remote gateway: 192.0.2.1
Pre shared key : alexandra

ΕΡΩΤΗΣΗ 7.20

fw2->Diagnostics ->IPSec -> SAD

No IPsec security associations.

ΕΡΩΤΗΣΗ 7.21

fw2->Diagnostics ->IPSec -> SPD

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

ΕΡΩΤΗΣΗ 7.22

Ping PC1->PC2 επιτυγχάνει

ΕΡΩΤΗΣΗ 7.23

Ping PC2->PC1 επιτυγχάνει

ΕΡΩΤΗΣΗ 7.24

fw1->Diagnostics ->IPSec -> SAD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.1	192.0.2.5	ESP	0e781089	3des-cbc	hmac-sha1
192.0.2.5	192.0.2.1	ESP	05379236	3des-cbc	hmac-sha1

ΕΡΩΤΗΣΗ 7.25

fw2->Diagnostics ->IPSec -> SAD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.5	192.0.2.1	ESP	05379236	3des-cbc	hmac-sha1
192.0.2.1	192.0.2.5	ESP	0e781089	3des-cbc	hmac-sha1

ΕΡΩΤΗΣΗ 7.26

R1: `tcpdump -i em0 -vv -n`

ΕΡΩΤΗΣΗ 7.27

Όχι.

ΕΡΩΤΗΣΗ 7.28

Βλέπουμε μόνο IP πακέτα ESP.
Ip src-dst addresses: 192.0.2.5, 192.0.2.1

ΕΡΩΤΗΣΗ 7.29

Όχι.

ΕΡΩΤΗΣΗ 7.30

PC2: `ssh lab@203.0.118.18`
Επιτυχής σύνδεση. Σε σχέση με την προηγούμενη άσκηση, το PC2 βρίσκεται πίσω από το FW2 (LAN2) και πριν το IPSec tunnel, δεν υπήρχε διαδρομή που να του επιτρέπει να φτάσει στο 203.0.118.18.

ΕΡΩΤΗΣΗ 7.31

Βλέπουμε πακέτα tcp με ip src-dst addresses: 192.0.2.5, 203.0.118.18. (port 22)

ΕΡΩΤΗΣΗ 7.32

Όχι δεν έχουμε κρυπτογράφηση αφού το 203.0.118.18 είναι δημόσια διεύθυνση άρα μετά το fw2 τα πακέτα βγαίνουν στο δημόσιο δίκτυο.