

Όνοματεπώνυμο: Ιωάννης Γιαννούκος	Όνομα PC: John John
Ομάδα: 1	Ημερομηνία: 3/6/2023

Εργαστηριακή Άσκηση 10

Τείχη προστασίας (Firewalls) και NAT

Προετοιμασία στο σπίτι

Με την παρακάτω ακολουθία εντολών επεξεργάστηκα το αρχείο /etc/rc.conf και πρόσθεσα τους ορισμένες μεταβλητές:

```
sysrc -f /etc/rc.conf ifconfig_em0="192.168.1.1/24"
sysrc -f /etc/rc.conf ifconfig_em1="192.0.2.1/30"
sysrc -f /etc/rc.conf defaultrouter="192.0.2.2"
sysrc -f /etc/rc.conf gateway_enable="YES"
sysrc -f /etc/rc.conf firewall_enable="YES"
sysrc -f /etc/rc.conf firewall_nat_enable="YES"
sysrc -f /etc/rc.conf firewall_logif="YES"
```

Έπειτα, κλείνω το μηχάνημα, το ονομάζω FW1 και μέσω της διαδρομής *File* → *Export Appliance* στο Virtual Box αποθηκεύω την εικόνα του τείχους προστασίας ως FW1.ova, την οποία θα χρησιμοποιήσω στη συνέχεια της άσκησης.

Άσκηση 1

Προτού ξεκινήσω την άσκηση δίνω στα PCs διευθύνσεις IP στις διεπαφές τους με τις εντολές “ifconfig em0 inet 192.168.1.{2,3}/24” για τα PC{1,2}, αντίστοιχα.

1.1) Στο PC1 φορτώνω στον πυρήνα το τείχος προστασίας ipfw με την εντολή “kldload ipfw”.

1.2) Στο PC1 μπορώ να επιβεβαιώσω ότι είναι ενεργό το τείχος προστασίας με την εντολή “kldstat”. Στην λίστα ενεργών υπηρεσιών εμφανίζεται το όνομα του τείχους προστασίας ipfw.ko.

1.3) Κάνοντας ping στη διεύθυνση IP του βρόχου επιστροφής lo0 και της διεπαφής em0 (“ping 127.0.0.1” ή “ping localhost”, και “ping 192.168.1.2” αντιστοίχως) βλέπω ότι τα αυτά αποτυγχάνουν με το μήνυμα ‘Permission denied’.

1.4) Εμφανίζω τους κανόνες που υπάρχουν στο τείχος προστασίας του PC1 με την εντολή “ipfw list”.

```
root@PC:~ # ipfw list
65535 deny ip from any to any
root@PC:~ #
```

1.5) Εμφανίζω στοιχεία για τη χρήση των προηγούμενων κανόνων με την εντολή “`ipfw show`”.

```
root@PC:~ # ipfw show
65535 6 504 deny ip from any to any
root@PC:~ #
```

1.6) Μηδενίζω τους σχετικούς με τη χρήση των κανόνων μετρητές με την εντολή “`ipfw zero`” (εμφανίζεται το μήνυμα ‘*Accounting cleared*’).

1.7) Προσθέτω κανόνα στο τείχος προστασίας του PC1 με αύξοντα αριθμό 100 που να επιτρέπει μέσω της διεπαφής lo0 όλη την κίνηση με την εντολή “`ipfw add 100 allow all from any to any via lo0`”.

1.8) Ναι, τα pings του 1.3 είναι πλέον επιτυχή.

1.9) Όχι, δεν μπορώ να κάνω επιτυχές ping από το PC1 στο PC2. Εμφανίζεται μήνυμα λάθους ‘*Permission denied*’.

1.10) Προσθέτω κανόνα στο τείχος προστασίας του PC1 ώστε να επιτρέπεται η κίνηση ICMP από και προς οποιαδήποτε διεύθυνση IP με την εντολή “`ipfw add 200 allow icmp from any to any`”.

1.11) Ο κανόνας έλαβε αύξων αριθμό (α/α) 200, καθώς τέθηκε ρητά από εμένα. Εάν δεν συνέβαινε αυτό, τότε ο πυρήνας θα όριζε αυτόματα αριθμό μεγαλύτερο κατά 100 του αύξοντα αριθμού του τελευταίου πριν τον προκαθορισμένο κανόνα (που σε αυτήν την περίπτωση θα ήταν πάλι 200).

1.12) Ναι, πλέον μπορώ να κάνω ping από το PC1 στο PC2. Επίσης, το ping από το PC2 στο PC1 είναι επίσης επιτυχές.

1.13) Το traceroute δεν είναι δυνατό από το PC1 στο PC2, διότι η εντολή αυτή στο FreeBSD δεν χρησιμοποιεί πακέτα ICMP αλλά δεδομενογράμματα UDP. Επομένως, είναι λογικό αυτά να απορρίπτονται από το τείχος προστασίας του. Για να προσπεράσουμε το πρόβλημα αυτό μπορούμε να προσθέσουμε την επιλογή για να επιλέξουμε το πρωτόκολλο που θα χρησιμοποιηθεί και η εντολή θα έχει τελική μορφή “`traceroute -P icmp 192.168.1.3`”. Εναλλακτικά, θα μπορούσα να χρησιμοποιήσω την απλουστευμένη εντολή “`traceroute -I 192.168.1.3`”.

1.14) Προσθέτω κανόνα στο τείχος προστασίας του PC1, ώστε το traceroute από το PC1 προς οποιοδήποτε προορισμό να λειτουργεί, με την εντολή “`ipfw add 300 allow udp from any to any`”.

1.15) Προσπαθώντας να συνδεθώ με ssh από το PC1 στο PC2 με την εντολή “ssh 192.168.1.3” βλέπω ότι η προσπάθεια είναι ανεπιτυχής με το μήνυμα λάθους ‘*Permission denied*’.

1.16) Προσθέτω τους εξής δύο στατικούς κανόνες που να επιτρέπουν τη σύνδεση του PC1 σε απομακρυσμένους εξυπηρετητές με tcp: “ipfw add 400 allow tcp from any to any out” και “ipfw add 410 allow tcp from any to any in”.

1.17) Στο PC1 μηδενίζω τους μετρητές χρήσης των κανόνων με “ipfw zero” και συνδέομαι με ssh στο PC2 με την εντολή “ssh lab@192.168.1.3” (και ύστερα εισχωρώ κωδικό ‘ntua’), εκτελώ την εντολή “ls” και αποσυνδέομαι με “exit”.

1.18) Με την εντολή “ipfw show” εμφανίζω τη λίστα των κανόνων σε συνδυασμό με τους αντίστοιχους μετρητές χρήσης τους. Παρατηρώ, λοιπόν, ότι οι δύο τελευταίοι κανόνες που εισήγαγα εφαρμόστηκαν 42 και 35 φορές αντιστοίχως. Αυτό συνέβη επειδή στο πρωτόκολλο ssh κάθε φορά που πληκτρολογείται ένας χαρακτήρας από τον πελάτη, αυτός στέλνεται με ένα πακέτο στον εξυπηρετητή και αυτός στέλνει πίσω τον χαρακτήρα που έλαβε.

1.19) Μπορώ από το PC2 να συνδεθώ με ssh στο PC1. Αυτό είναι λογικό, επειδή προσέθεσα 2 κανόνες για το πρωτόκολλο tcp, μία για την εισερχόμενη ροή και μία για την εξερχόμενη.

1.20) Στο PC2 εκκινώ τον δαίμονα ftpd ώστε αυτό να λειτουργεί ως εξυπηρετητής FTP με την εντολή “service ftpd onestart” (εμφανίζεται το μήνυμα ‘*Starting ftpd*’).

1.21) Ναι, μπορώ να συνδεθώ με ftp στο PC2 ως χρήστης lab και να κατεβάσω ένα αρχείο από το /usr/bin του PC2 στο PC1.

Άσκηση 2

2.1) Στο PC2 φορτώνω στον πυρήνα το τείχος προστασίας ipfw με την εντολή “kldload ipfw”.

2.2) Όχι, δεν μπορώ να κάνω ping από το PC2 στο PC1, και αυτό είναι λογικό αφού δεν έχω προσθέσει κάποιον κανόνα στο ipfw (και ο τελευταίος απορρίπτει όλες τις κινήσεις δικτύου).

2.3) Προσθέτω στο τείχος προστασίας του PC2 κανόνα που επιτρέπει μέσω της διεπαφής lo0 όλη την κίνηση με `“ipfw add 100 allow all from any to any via lo0”`.

2.4) Προσθέτω κανόνα στο τείχος προστασίας του PC2 που επιτρέπει κίνηση ICMP τύπου echo request από το PC2 προς οποιαδήποτε διεύθυνση IP με `“ipfw add 110 allow icmp from me to any icmp types 8”`.

2.5) Όχι, δεν μπορώ να κάνω ping από το PC2 στο PC1.

2.6) Τα εξερχόμενα πακέτα ICMP echo request μπορούν να περάσουν το τείχος προστασίας του PC2, ωστόσο τα εισερχόμενα από το PC1 ICMP echo reply δεν μπορούν, και γι’ αυτό το ping αποτυγχάνει. Αυτό είναι αναμενόμενο, καθώς με τον κανόνα που προσέθεσα στο 2.4 επιτρέπω την κίνηση μόνο των εξερχόμενων ICMP πακέτων, δηλαδή με διεύθυνση προορισμού αυτήν του PC2.

2.7) Διαγράφω τον κανόνα που προσέθεσα στο 2.4 με `“ipfw delete 110”` και τον επανεισάγω προσθέτοντας στο τέλος το `“keep-state”`, δηλαδή εκτελώ `“ipfw add 110 allow icmp from me to any icmp types 8 keep-state”`. Πλέον, το ping από το PC2 στο PC1 είναι επιτυχές, επειδή με την επιλογή που προσέθεσα επισημαίνω στο τείχος προστασίας ότι τα πακέτα ICMP που αφορούν αντίστοιχα πακέτα-αιτήματα που στέλνει το PC2 θα πρέπει να γίνονται αποδεκτά.

2.8) Ξεκινώ πάλι το ping από το PC2 στο PC1 και το αφήνω να τρέχει. Παρατηρώ ότι μπορώ να κάνω ping από το PC1 στο PC2. Αφήνω το ping PC1 → PC2 να τρέχει.

2.9) Σταματώ τα ping από το PC2 και περιμένω λίγο. Ναι, το ping PC1 → PC2 συνεχίζει να επιτυγχάνει. Ωστόσο, εάν το σταματήσω και ξαναξεκινήσω το ping, τότε αυτό δεν θα επιτυγχάνει. Αυτό είναι λογικό, αφού οποιαδήποτε κίνηση ICMP πακέτων δεν είναι μέρος ενός ICMP echo request από το PC2 ή του αντιστοίχου ICMP echo reply από το PC1, απορρίπτεται σύμφωνα με τον κανόνα στο τείχος προστασίας του PC2.

2.10) Προσθέτω (stateful) κανόνα ώστε το PC2 να απαντά σε ICMP echo request ανεξάρτητα από πού προέρχονται με την εντολή `“ipfw add allow icmp from any to me icmp types 8 keep-state”`.

2.11) Ξεκινώ ένα ping από το PC1 στο PC2 και το αφήνω να τρέχει. Εκτελώ στο PC2 την εντολή `“ipfw -d show”`. Η επιλογή αυτή (`-d`) εκτός από τους κανόνες με τους μετρητές εφαρμογής τους εμφανίζει ξεχωριστά τους κανόνες που είναι δυναμικοί. Στην περίπτωση αυτή, εμφανίζεται ο τελευταίος προστιθέμενος κανόνας.

```

root@PC2:~ # ipfw -d show
00100 0 0 allow ip from any to any via lo0
00110 40 3360 allow icmp from me to any icmp types 8 keep-state :default
00210 100 8400 allow icmp from any to me icmp types 8 keep-state :default
65535 115 9660 deny ip from any to any
## Dynamic rules (1 136):
00210 100 8400 (4s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 :default
root@PC2:~ #

```

2.12) Σταματώ το ping PC1 → PC2, περιμένω λίγα δευτερόλεπτα και ξαναεκτελώ στο PC2 την εντολή “ipfw -d show”. Στην περίπτωση αυτή, η σημαία ‘-d’ δεν φαίνεται να επηρεάζει την λειτουργία της εντολής.

```

root@PC2:~ # ipfw -d show
00100 0 0 allow ip from any to any via lo0
00110 40 3360 allow icmp from me to any icmp types 8 keep-state :default
00210 502 42168 allow icmp from any to me icmp types 8 keep-state :default
65535 115 9660 deny ip from any to any
root@PC2:~ # ipfw show
00100 0 0 allow ip from any to any via lo0
00110 40 3360 allow icmp from me to any icmp types 8 keep-state :default
00210 502 42168 allow icmp from any to me icmp types 8 keep-state :default
65535 115 9660 deny ip from any to any
root@PC2:~ #

```

2.13) Προσθέτω τους εξής δύο κανόνες στο τείχος προστασίας του PC2 ώστε το traceroute προς το PC2 να λειτουργεί: “ipfw add allow udp from any to me” και “ipfw add allow icmp from me to any icmp types 3, 11”.

2.14) Προσθέτω τους εξής δύο κανόνες στο τείχος προστασίας του PC2 ώστε να λειτουργεί το traceroute από το PC2 προς οποιαδήποτε διεύθυνση IP: “ipfw add allow udp from me to any” και “ipfw add allow icmp from any to me icmp types 3,11”.

2.15) Για να απαντά το PC1 σε traceroute από οποιαδήποτε διεύθυνση IP πρέπει να προσθέσω κανόνα με την εντολή “ipfw add allow icmp from me to any icmp types 3,11”.

2.16) Προσθέτω έναν (stateful) κανόνα στο τείχος προστασίας του PC2 ώστε να μπορώ να συνδεθώ σε αυτό με ssh από οποιονδήποτε υπολογιστή του υποδικτύου 192.168.1.0/24 με την εντολή “ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state”.

2.17) Για να επιβεβαιώσω την ορθότητα του προηγούμενου κανόνα εκτελώ από το PC1 “ssh lab@192.168.1.3”. Σημειώνω ότι η σύνδεση ssh πέτυχε.

2.18) Προσθέτω έναν (stateful) κανόνα στο τείχος προστασίας του PC2 ώστε να μπορώ να συνδεθώ με ssh σε οποιοδήποτε άλλο μηχάνημα με την εντολή “ipfw add allow tcp from me to any 22 keep-state”.

2.19) Για να δέχεται το PC1 συνδέσεις ssh μόνο από το PC2 πρέπει να προσθέσω επιπλέον κανόνα στο τείχος προστασίας του PC1 με την εντολή `“ipfw add allow tcp from 192.168.1.3 to me 22 keep-state”`.

2.20) Ναι, μπορώ από το PC1 να συνδεθώ με sftp στο PC2 ως χρήστης lab και να κατεβάσω το αρχείο `/etc/rc.conf`.

2.21) Όχι, δεν μπορώ από το PC1 να συνδεθώ με απλό ftp στο PC2, επειδή το ftp «μιλά» στην πόρτα 21 και όχι στην 22. Για να επιτρέψω το ftp προσθέτω κανόνα στο PC2 με την εντολή `“ipfw add allow tcp from any to me 21 keep-state”`.

2.22) Συνδέομαι με ftp ως χρήστης lab από το PC1 στο PC2 με `“ftp lab@192.168.1.3”` και εκτελώ τις εντολές `“cd /usr”` και `“ls”`. Η πρώτη εκτελείται επιτυχώς, ενώ η δεύτερη αποτυγχάνει. Αυτό συμβαίνει επειδή η δεύτερη εντολή χρησιμοποιεί την θύρα 20, και όχι την 21 που ορίσαμε προηγουμένως.

2.23) Για να λειτουργεί το ftp σε passive mode πρέπει να προσθέσω στο τείχος προστασίας του PC2 κανόνα με την εντολή `“ipfw add allow tcp from any 21 to me keep-state”`.

2.24) Όχι, το κατέβασμα αρχείου από το PC2 στο PC1 με ftp εξακολουθεί να είναι αδύνατο.

2.25) Για να λειτουργεί και το active mode του ftp πρέπει να προσθέσω στο τείχος προστασίας του PC2 κανόνα με την εντολή `“ipfw add allow tcp from me 20 to any”` και σε αυτό του PC1 κανόνα με την εντολή `“ipfw add allow tcp from any 20 to me”`.

2.26) Όπως είναι γνωστό, το πρωτόκολλο ftp, σε αντίθεση με το ssh, δεν παρέχει μεθόδους απόκρυψης της πληροφορίας που μεταφέρει στο δίκτυο, όπως η κρυπτογράφηση. Για αυτόν το λόγο το πρωτόκολλο αυτό θεωρείται πολύ ανασφαλές σε σχέση με άλλα πρωτόκολλα μεταφοράς αρχείων, π.χ. ssh. Τα τείχη προστασίας από την άλλη αποτελούν μία μέθοδο προστασίας των υπολογιστών στο διαδίκτυο και αποτρέπουν ορισμένα πακέτα να φτάσουν είναι σταλούν προς ή από έναν υπολογιστή. Έτσι, αν το καλοσκεφτούμε, αυτά είναι απαραίτητα για την επικοινωνία ενός υπολογιστή με άλλους, καθώς ήδη γνωρίζουμε ορισμένες τεχνικές επιθέσεων με κακόβουλες προθέσεις.

2.27) Απενεργοποιώ το ipfw στα PC{1,2} με την εντολή `“kldunload ipfw”` και επιβεβαιώνω ότι απενεργοποιήθηκε με την εντολή `“kldstat”`.

Άσκηση 3

3.1) Ορίζω το όνομα, τη διεύθυνση IP και προεπιλεγμένη πύλη στα PC{1,2} με τις παρακάτω ακολουθίες εντολών:

PC1:

```
hostname PC1
ifconfig em0 inet 192.168.1.2/24
route add default 192.168.1.1
```

PC2:

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

3.2) Ορίζω μέσω cli του R1 το όνομα, τη διεύθυνση IP για τη διεπαφή στο WAN1 και τη διεπαφή στο LAN2 με την παρακάτω ακολουθία εντολών:

```
cli
configure terminal
hostname R1
interface em0
ip address 192.0.2.6/30
interface em1
ip address 192.0.2.2/30
```

3.3) Ορίζω το όνομα, τη διεύθυνση IP και προεπιλεγμένη πύλη στο SRV1 με την παρακάτω ακολουθία εντολών:

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

3.4) Στα PC2 και SRV1 ξεκινώ τον δαίμονα ftpd ώστε αυτά να λειτουργούν ως εξυπηρετητές FTP με την εντολή “service ftpd onestart”.

3.5) Εμφανίζω τα modules που έχουν φορτωθεί στον πυρήνα του FreeBSD στο FW1 με την εντολή “kldstat”.

```
root@PC:~ # kldstat
Id Refs Address      Size Name
1    11  0x8000000 196d6e4 kernel
2     1  0xf800000   6000 intpm.ko
3     1  0xf806000   4000 smbus.ko
4     2  0xf80a000  2d000 ipfw.ko
5     1  0xf837000   6000 ipfw_nat.ko
6     1  0xf83d000   f000 libalias.ko
root@PC:~ #
```

3.6) Το τείχος προστασίας ενεργοποιήθηκε με την εντολή firewall_enable=“YES” που έθεσα στο /etc/rc.conf είναι το ipfw.

3.7) Εμφανίζω το είδος λειτουργίας του τείχους προστασίας που έχει εγκατασταθεί με “sysrc firewall_type” και βλέπω ότι είναι ‘UNKNOWN’.

3.8) Στο FW1 με την εντολή “ipfw list” εμφανίζονται 11 κανόνες. Ο τελευταίος απορρίπτει οποιαδήποτε πακέτα δεν γίνουν αποδεκτά από τους υπόλοιπους 10 κανόνες.

```
root@PC:~ # sysrc firewall_type
firewall_type: UNKNOWN
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
65535 deny ip from any to any
root@PC:~ #
```

3.9) Εμφανίζω τους πίνακες in-kernel NAT στο FW1 με “ipfw nat show config”. Παρατηρώ ότι η εντολή δεν εμφανίζει κανένα αποτέλεσμα, δηλαδή δεν έχουν ορισθεί πίνακες.

3.10) Όχι, δεν μπορώ από το PC1 να κάνω ping τη διεπαφή του FW1 στο {L,W}AN1.

3.11) Όχι, δεν μπορώ από το SRV1 να κάνω ping τη διεπαφή του FW1 στο WAN1.

3.12) Δημιουργώ τείχος προστασίας του FW1 πίνακα in-kernel NAT με αριθμό παρουσίας 123 ώστε τα πακέτα με ιδιωτικές διευθύνσεις που ωθούνται σε αυτόν να υφίστανται μετάφραση στη διεύθυνση της διεπαφής του στο WAN1 και επιπλέον να αρχικοποιείται (reset) σε περίπτωση αλλαγής της διεύθυνσης IP της διεπαφής με την εντολή “ipfw nat 123 config ip 192.0.2.1 reset”.

3.13) Προσθέτω κανόνα στο τείχος προστασίας του FW1 ώστε όλη η κίνηση IPv4 να ωθείται προς μετάφραση στον πίνακα NAT με αριθμό παρουσίας 123 με την εντολή “ipfw add 50 nat 123 ip from any to any”.

3.14) Ναι, πλέον μπορώ να κάνω ping από το PC1 στο FW1, και στις δύο διεπαφές του.

3.15) Ξεκινώ μια καταγραφή πακέτων με το tcpdump στη διεπαφή του R1 στο WAN1 με “tcpdump -i em1”.

3.16) Βλέπω τους μετρητές πακέτων στο τείχος προστασίας του FW1 με `“ipfw show”` και τους μηδενίζω με `“ipfw zero”`.

3.17) Κάνω ping PC1 → R1 και στέλνω 3 ICMP echo request μηνύματα με την εντολή `“ping -c 3 192.0.2.2”`. Η IP διεύθυνση πηγής των πακέτων ICMP echo request που φαίνονται στην καταγραφή είναι 192.0.2.1.

3.18) Η IP διεύθυνση προορισμού των ICMP echo reply της καταγραφής στον R1 είναι (επίσης) 192.0.2.1.

3.19) Ο κανόνας του τείχους προστασίας που είναι υπεύθυνος για την επιτυχία του ping είναι ο πρώτος, *‘nat 123 ip from any to any’*.

3.20) Ο κανόνας αυτός εφαρμόστηκε 12 φορές, όπως φαίνεται με την εντολή `“ipfw show”`. Αυτό είναι λογικό, επειδή έγιναν 3 pings. Το κάθε ping αποτελείτο από 2 μηνύματα ICMP, στα οποία ο κανόνας εφαρμόστηκε 2 φορές στο καθένα· μία φορά για την κωδικοποίηση και μία ακόμη για την αποκωδικοποίηση των IP διευθύνσεών τους. Επομένως, $3 * 2 * 2 = 12$.

3.21) Ναι, μπορώ από το SRV1 να κάνω ping τη διεπαφή του FW1 στο WAN1.

3.22) Για την αποδοχή της προηγούμενης κίνησης είναι υπεύθυνος ο κανόνας που προσέθεσα στο 3.13.

3.23) Η προηγούμενη κίνηση προωθείται στο NAT προς μετάφραση διευθύνσεων, επειδή αυτή προέρχεται από ιδιωτική διεύθυνση.

3.24) Ναι, μπορώ να συνδεθώ με ssh από το PC2 ως χρήστης lab στο SRV1.

3.25) Δοκιμάζοντας να συνδεθώ με ssh SRV1 → PC2 βλέπω ότι δεν είναι δυνατή η σύνδεση. Κάνοντας tcpdump στον R1 στην διεπαφή του στο LAN2 βλέπω ότι στέλνει στον SRV1 μήνυμα ICMP host unreachable. Επομένως, η αποτυχία οφείλεται σε αδυναμία δρομολόγησης και όχι σε NAT.

3.26) Δημιουργώ πίνακα NAT με αριθμό παρουσίας 123 επαναλαμβάνοντας τις εντολές διάρθρωσης της ερώτησης 3.12 με την εντολή `“ipfw nat 123 config ip 192.0.2.1 reset”` και προσθέτοντας νέα εντολή ώστε η κίνηση προς τη διεύθυνση IPv4 του FW1 στο WAN1 να ανακατευθύνεται στο PC2 με την εντολή `“ipfw nat 123 config ip 192.0.2.1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1”`.

3.27) Από το SRV1 εκτελώ “ssh [lab@192.0.2.1](#)” και συνδέομαι σε κάποιον υπολογιστή. Αφού εκτελέσω την εντολή “hostname” και βλέπω ότι συνδέθηκα στο PC2.

3.28) Δημιουργώ πίνακα NAT με αριθμό παρουσίας 123 επαναλαμβάνοντας τις εντολές διάρθρωσης της ερώτησης 3.26 κάνοντας “ipfw nat 123 config ip 192.0.2.1 reset” και προσθέτοντας νέα εντολή ώστε η κίνηση tcp για τη θύρα 22 να ανακατευθύνεται στο PC1 στην αντίστοιχη θύρα με την εντολή “ipfw nat 123 config ip 192.0.2.1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1 redirect_port tcp 192.168.1.2:22 22”.

3.29) Συνδέομαι και πάλι από το SRV1 με ssh ως χρήστης lab στη διεύθυνση 192.0.2.1 (“ssh [lab@192.0.2.1](#)”). Εκτελώντας την εντολή “hostname” βλέπω ότι συνδέθηκα στο PC1.

3.30) Συνδέομαι από το SRV1 με ftp ως χρήστης lab στη διεύθυνση 192.0.2.1. Από σχετικό μήνυμα που εμφανίζεται στην οθόνη βλέπω ότι συνδέομαι στο PC2 (επίσης δεν έχουμε ενεργοποιήσει τον ftpd σε άλλο μηχάνημα).

3.31) Ναι, μπορώ να δω τα περιεχόμενα του φακέλου /etc και να κατεβάσω το αρχείο rc.conf.

3.32) Αν από το PC1 κάνω ftp στη διεύθυνση 192.0.2.1, τότε θα απαντήσει πάλι το PC2, καθώς η μετάφραση θα γίνει.

3.33) Εάν από το PC2 κάνω ssh στη διεύθυνση 192.0.2.1 τότε θα συνδεθώ στο PC1, πάλι λόγω της μετάφρασης από το NAT.

Άσκηση 4

4.1) Απενεργοποιώ τη λειτουργία one-pass (στο FW1) με την εντολή “ipfw disable one_pass”, διατηρώ όμως τον ορισμό του πίνακα NAT της ερώτησης 3.28. Δεν μπορώ να κάνω ping PC1 → FW1 (LAN1) ή ping SRV1 → FW1 (WAN1).

4.2) Ναι τα πακέτα γίνονται δεκτά από τον κανόνα ώθησης στο NAT του 3.13, ωστόσο το ping αποτυγχάνει επειδή με τη λειτουργία one-pass που ενεργοποίησα πρέπει τα πακέτα να γίνουν αποδεκτά από όλους τους υπόλοιπους κανόνες, σε κάποιον από τους οποίους απορρίπτονται.

4.3) Κατ’ αρχάς πρέπει να επιτρέψω την εντός του εταιρικού δικτύου κίνηση. Διαγράψω τον προηγούμενο κανόνα με “ipfw delete 50” και

προσθέτω νέο αύξοντα αριθμό 1100 που επιτρέπει όλη την κίνηση μέσω (via) της διεπαφής του FW1 στο LAN1 με την εντολή `"ipfw add 1100 allow all from any to any via em0"`.

4.4) Ναι, πλέον το ping PC1 → FW1(any) είναι επιτυχές.

4.5) Κάνοντας ssh από το PC2 στην διεπαφή του FW1 στο WAN1 βλέπω ότι συνδέομαι στο FW1, το οποίο αντιλαμβάνομαι κάνοντας `"hostname"`.

4.6) Για ό,τι παρατηρήθηκε προηγουμένως είναι υπεύθυνος ο κανόνας που προσέθεσα στο 4.3.

4.7) Για να επικοινωνούν τα μηχανήματα του LAN1 (εταιρικό δίκτυο) με το εξωτερικό δίκτυο (διαδίκτυο), πρέπει τα εξερχόμενα στο WAN1 πακέτα να υφίστανται μετάφραση από το NAT. Προς τούτο προσθέτω κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 3000 ώστε να ωθείται προς μετάφραση στον πίνακα NAT με αριθμό παρουσίας 123, η μεταδιδόμενη (xmit) κίνηση από τη διεπαφή του στο WAN1, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού με την εντολή `"ipfw add 3000 nat 123 ip from any to any xmit em1"`.

4.8) Επειδή έχει ακυρωθεί η λειτουργία one-pass, τα πακέτα που ταιριάζουν στον προηγούμενο κανόνα, θα απορριφθούν στη συνέχεια από τον τελικό κανόνα 65535 του ipfw. Προσθέτω αμέσως επόμενο κανόνα με αύξοντα αριθμό 3001 που να αποδέχεται οποιαδήποτε κίνηση μετά τη μετάφραση με την εντολή `"ipfw add 3001 allow all from any to any"`.

4.9) Τα πακέτα που φτάνουν σε απάντηση αυτών που εξήλθαν από το τείχος προστασίας, πρέπει και αυτά να υποστούν μετάφραση από το NAT. Προς τούτο προσθέτω κανόνα στο FW1 με αύξοντα αριθμό 2000 ώστε να ωθείται προς μετάφραση στον πίνακα NAT με αριθμό παρουσίας 123 η οποιαδήποτε εισερχόμενη κίνηση λαμβάνεται (recv) στη διεπαφή του στο WAN1, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού με την εντολή `"ipfw add 2000 nat 123 ip from any to any recv em1"`.

4.10) Στη συνέχεια θα εγκαταστήσω (stateful) κανόνες. Προσθέτω κανόνα με αύξοντα αριθμό 2001 που να ελέγχει εάν η κίνηση έχει γίνει αποδεκτή από δυναμικό κανόνα με την εντολή `"ipfw add 2001 check-state"`.

4.11) Εάν κάνω ping PC1 → 192.0.2.1 θα απαντήσει το FW1.

4.12) Εάν κάνω ping SRV1 → 192.0.2.1 θα απαντήσει το PC2.

4.13) Εάν κάνω ssh PC1 → 192.0.2.1 θα συνδεθώ στο FW1.

4.14) Εάν κάνω ssh SRV1 → 192.0.2.1 θα συνδεθώ στο PC1.

4.15) Εάν κάνω ftp PC1 → 192.0.2.1 θα συνδεθώ στο PC2.

4.16) Ναι, μπορώ να κάνω ping PC1 → SRV1.

4.17) Ναι, μπορώ να συνδεθώ με ssh PC1 → SRV1.

4.18) Ναι, μπορώ από το PC1 να συνδεθώ με ftp ως lab στο SRV1, να δω τα περιεχόμενα ενός φακέλου και να κατεβάσω ένα αρχείο.

4.19) Οι προηγούμενοι κανόνες ώθησης στο NAT επιτυγχάνουν τη μετάφραση διευθύνσεων αλλά επιτρέπουν οποιαδήποτε κίνηση ανεξάρτητα από το κατά πόσον αυτή είναι επιθυμητή. Προσθέτω στο τείχος προστασίας FW1 κανόνα με αύξοντα αριθμό 2999 που να απαγορεύει οποιαδήποτε κίνηση μέσω (via) της διεπαφής του στο WAN1, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού με την εντολή `ipfw add 2999 deny all from any to any via em1`".

4.20) Επιτυγχάνει το ping PC1 → FW1 και η σύνδεση ssh PC1 → FW1.

4.21) Προσθέτω (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2500 ώστε η μεταδιδόμενη (xmit) από τη διεπαφή του στο WAN1 κίνηση ICMP, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού, να στέλνεται (skipto) στη μετάφραση NAT του κανόνα 3000 με την εντολή `ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state`".

4.22) Ναι, μπορώ να κάνω το ping PC1 → SRV1.

4.23) Προσθέτω (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2600 ώστε η εξερχόμενη μέσω (out via) της διεπαφής του στο WAN1 κίνηση tcp για σύνδεση με προορισμό τη θύρα 22, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού, να στέλνεται στη μετάφραση NAT του κανόνα 3000 με την εντολή `ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state`".

4.24) Ναι, μπορώ να συνδεθώ με ssh PC1 → SRV1.

4.25) Τα εισερχόμενα από το WAN1 πακέτα στο FW1, εάν πρόκειται να γίνουν δεκτά, όσο και εάν φαίνεται λάθος, θα πρέπει να στέλνονται στον κανόνα 3000. Η μετάφραση όμως δεν θα εφαρμοσθεί στα εισερχόμενα, αλλά στα πακέτα που θα παραχθούν ως απάντηση σε αυτά. Προσθέτω (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2100 ώστε η εισερχόμενη μέσω (in via) της διεπαφής του στο WAN1 κίνηση ICMP, ανεξάρτητα διεύθυνσης πηγής και προορισμού, να

στέλνεται (skipto) στη μετάφραση NAT του κανόνα 3000 με την εντολή “ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state”.

4.26) Εάν κάνω ping από το SRV1 στη διεύθυνση 192.0.2.1 απαντά το PC2.

4.27) Προσθέτω (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2200 ώστε η λαμβανόμενη (recv) στη διεπαφή του στο WAN1 κίνηση tcp για σύνδεση με προορισμό τη θύρα 22, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού, να στέλνεται (skipto) στη μετάφραση NAT του κανόνα 3000 με την εντολή “ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state”.

4.28) Εάν από το SRV1 κάνω ssh ως χρήστης lab στη διεύθυνση 192.0.2.1, συνδέομαι στο PC1.

4.29) Όχι, το ftp από το SRV1 στη διεύθυνση 192.0.2.1 ακόμα αποτυγχάνει.

4.30) Για να λειτουργεί το προηγούμενο ftp σε active mode πρέπει να προσθέσω τους εξής δύο κανόνες: “ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state” και “ipfw add 2400 skipto 3000 tcp from any 20 to any setup out via em1 keep-state”.

Άσκηση 5

5.1) Η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο LAN1 είναι 192.168.1.1.

5.2) Η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο WAN1 είναι 10.0.0.1.

```
FW1 - firewall.ova (m0n0wall) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Copyright (C) 2002-2012 by Manuel Kasper. All rights reserved.
Visit http://m0n0.ch/wall for updates.

LAN IP address: 192.168.1.1
WAN IP address: 10.0.0.1


Port configuration:

LAN    -> em0
WAN    -> em1
OPT1   -> em2 (MNG)
OPT2   -> em3 (DMZ)

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: █
```

5.3) Το ποσοστό της ελεύθερης μνήμης που βλέπω στο FW1 μέσω του φυλλομετρητή μου είναι 67% (συγκεκριμένα βλέπω 33% δεσμευμένη μνήμη).

**webGUI Configuration**fw.lab.ntua.gr

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN
- MNG
- DMZ

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN
- Scheduler


VPN

- IPsec
- PPTP

Status

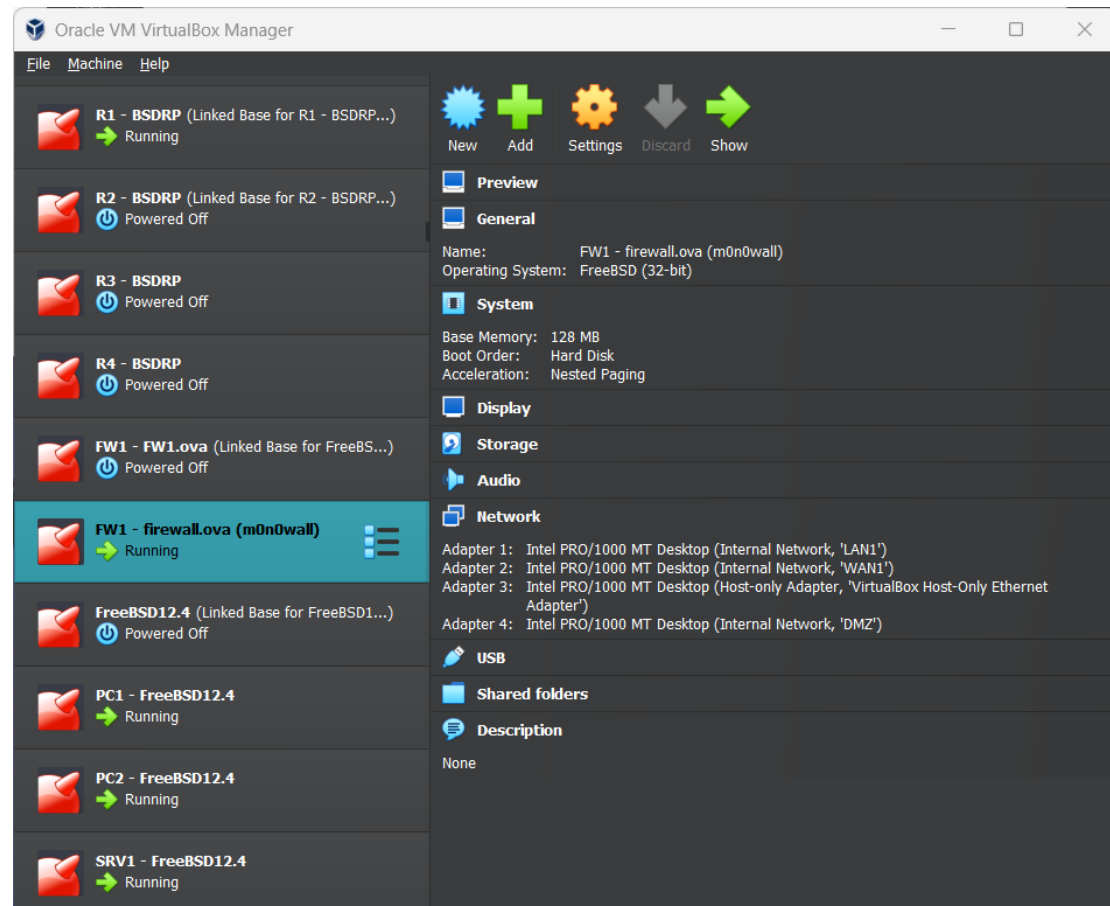
- System
- Interfaces
- Traffic graph
- Wireless

▶ Diagnostics

**m0n0wall®**

System information	
Name	fw.lab.ntua.gr
Version	1.8.1b540 built on Fri Apr 12 05:10:08 CEST 2013
Platform	Generic PC
Hardware crypto	Intel AES-NI
System Date	Thu Jun 1 16:12:48 UTC 2023
Uptime	00:00
Last config change	Sun May 26 21:44:37 UTC 2013
CPU usage	<div><div></div>9%</div>
Memory usage	<div><div></div>33%</div>
Notes	

5.4) Στο FW1 βλέπω συνολικά 4 διεπαφές δικτύου (όπως φαίνεται και στην εικόνα του 5.2 παραπάνω). Επιβεβαιώνω ότι στο Virtual Box οι κάρτες αυτές είναι συνδεδεμένες στα σωστά υποδίκτυα και με τον σωστό τρόπο.



5.5) Η διεύθυνση που έχει ρυθμιστεί στη διεπαφή DMZ του FW1 μπορεί να βρεθεί από το webGUI Configuration, από *Interfaces* → *DMZ* → *IP configuration* → *IP address*. Είναι 172.22.1.1.

5.6) Το όνομα (hostname) του FW1 είναι 'fw'. Αυτό μπορεί να βρεθεί από το webGUI Configuration, από *System: General setup* → *Hostname*.

5.7) Αλλάζω το hostname του FW1 σε 'fw1' από το πεδίο που αναφέρθηκε στο 5.6.










5.8) Στο μενού *Firewall* → *Rules* του FW1 δεν υπάρχουν κανόνες για το WAN.

5.9) Ορίζω τη σωστή διεύθυνση και προεπιλεγμένη πύλη του FW1 στο WAN1 και επιλέγω το 'Block private networks' από *Interfaces* → WAN (στο τέλος πατώ 'Save').

Static IP configuration	
IP address	192.0.2.1 / 30 ▼
Gateway	192.0.2.2

5.10) Στο μενού *Firewall* → *Rules* του FW1 πλέον υπάρχει ένας κανόνας για το WAN.


Firewall: Rules

LAN	WAN	MNG	DMZ												
<table><thead><tr><th>Proto</th><th>Source</th><th>Port</th><th>Destination</th><th>Port</th><th>Description</th></tr></thead><tbody><tr><td>* ✗</td><td>RFC 1918 networks</td><td>*</td><td>*</td><td>*</td><td>Block private networks</td></tr></tbody></table> <p>No rules are currently defined for this interface. All incoming connections on this interface will be blocked until you add pass rules. Click the  button to add a new rule.</p> <div><div> pass</div><div> block</div><div> reject</div><div> log</div><div> pass (disabled)</div><div> block (disabled)</div><div> reject (disabled)</div><div> log (disabled)</div></div>				Proto	Source	Port	Destination	Port	Description	* ✗	RFC 1918 networks	*	*	*	Block private networks
Proto	Source	Port	Destination	Port	Description										
* ✗	RFC 1918 networks	*	*	*	Block private networks										

5.11) Όχι, όλες οι υπηρεσίες των κατηγοριών 'Services' και 'VPN' είναι απενεργοποιημένες.

5.12) Ενεργοποιώ την υπηρεσία DNS forwarder χωρίς κάποια άλλη ρύθμιση.

Services: DNS forwarder

 The changes have been applied successfully.

☒ Enable DNS forwarder

5.13) Ενεργοποιώ την υπηρεσία DHCP server στο LAN1 ορίζοντας ως περιοχή διευθύνσεων την 192.168.1.2 έως 192.168.1.3.

Services: DHCP server



The changes have been applied successfully.

LAN

MNG

DMZ

Enable IPv4 DHCP server on LAN interface

☒ Enable

Deny unknown clients

☐ Only respond to reserved clients listed below.

Subnet

192.168.1.0

Subnet mask

255.255.255.0

Available range

192.168.1.1 - 192.168.1.254

Range

192.168.1.2

to

192.168.1.3

WINS servers

5.14) Στο PC1 ξεκινώ τον πελάτη DHCP με την εντολή “`dhclient em0`”. Αποδόθηκαν οι εξής διευθύνσεις:
Διεύθυνση IP: 192.168.1.2,
Προεπιλεγμένη πύλη: 192.168.1.1,
Διεύθυνση εξυπηρετητή DNS: 192.168.1.1.

5.15) Στην σελίδα ενεργοποίησης της υπηρεσίας DNS forwarder αναφέρεται αναλυτικά ο λόγος για τον οποίο χρειάστηκε η ενεργοποίησή της, γράφοντας το εξής:

“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. The DNS forwarder will use the DNS servers entered in [System: General setup](#) or those obtained via DHCP or PPP on WAN if the “Allow DNS server list to be overridden by DHCP/PPP on WAN” is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the [System: General setup](#) page.”

5.16) Μπορώ να δω ότι έχει αποδοθεί η συγκεκριμένη διεύθυνση στο PC1 στο μενού *Diagnostics* → *DHCP leases*.

5.17) Στο μενού *Diagnostics* → *ARP Table* βλέπω 7 εγγραφές ARP.

5.18) Όχι, δεν μπορώ να κάνω ping τη διεπαφή του FW1 στο LAN1 από το PC1.

5.19) Στο μενού *Diagnostics* → *Logs* καρτέλα *Firewall* βλέπω τα πακέτα που έχουν απορριφθεί από το τείχος προστασίας. Για παράδειγμα, βλέπω τα «αποτυχημένα» πακέτα από το ping από το PC1.

5.20) Από το αντίστοιχο μενού στο *Diagnostics* βλέπω 1 firewall state.

5.21) Από το μενού *Firewall* → *Rules* βλέπω ότι δεν υπάρχει κάποιος κανόνας για το LAN.

5.22) Προσθέτω στο FW1 κανόνα ώστε να επιτρέπω όλη την κίνηση από το LAN1 δίνοντας στα εξής πεδία τις παρακάτω τιμές:

Action: Pass


Interface: LAN

Protocol: any

Source: Type → any

Save

Firewall: Rules

 The changes have been applied successfully.

LAN

WAN

MNG

DMZ

	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/>	*	*	*	*	*	5.22	<div><div>←</div><div>⊕</div><div>⊕</div><div>←</div><div>⊗</div><div>⊕</div></div>

5.23) Ναι, μπορώ να κάνω ping από το PC1 σε όλες τις διεπαφές του FW1.

5.24) Όχι, δεν μπορώ να κάνω ping από τον R1 στη διεπαφή του FW1 στο WAN.

5.25) Εμφανίζω τον πίνακα ARP στον R1 με την εντολή “**arp -a**”. Δεν βλέπω κάποια εγγραφή για τη διεύθυνση MAC της διεπαφής του FW1 στο WAN1.

```
[root@router]~# arp -a
? (192.0.2.2) at 08:00:27:9d:2c:66 on em1 permanent [ethernet]
? (192.0.2.1) at (incomplete) on em1 expired [ethernet]
? (192.0.2.6) at 08:00:27:dd:aa:89 on em0 permanent [ethernet]
[root@router]~#
```

5.26) Προσθέτω στο FW1 κανόνα ώστε να επιτρέπω όλη την εισερχόμενη ICMP κίνηση με προορισμό την ‘WAN Address’ δίνοντας στα εξής πεδία τις παρακάτω τιμές:

Action: Pass

Interface: WAN


Protocol: ICMP

Source: Type → any

Destination: Type → WAN address

Save

Firewall: Rules







 The changes have been applied successfully.


LAN


WAN


MNG


DMZ


	Proto	Source	Port	Destination	Port	Description	
	*	RFC 1918 networks	*	*	*	Block private networks	 
<input type="checkbox"/> 	ICMP	*	*	WAN address	*	5.26	 


 pass


 block


 reject







 log

 pass (disabled)

 block (disabled)

 reject (disabled)

 log (disabled)

5.27) Μπορώ να κάνω ping από τον R1 στην διεπαφή του FW1 στο WAN1.

5.28) Όχι, δεν μπορώ να κάνω ping από τον R1 στο PC1. Εμφανίζεται το μήνυμα *'No route to host'*.

5.29) Ναι, μπορώ να κάνω ping από το PC1 στον R1. Αυτό φανερώνει την 'ικανότητα' του NAT να 'προστατεύει' τους υπολογιστές του ιδιωτικού δικτύου. Ο πραγματικός λόγος που το ping αυτό επιτυγχάνει και το αντίστροφο όχι είναι επειδή ο FW1 μεταφράζει την εσωτερική διεύθυνση του ιδιωτικού δικτύου σε δημόσια διεύθυνση, η οποία είναι WAN, την οποία αποδέχεται ο κανόνας που θέσαμε στο 5.26.

5.30) Αφού επιβεβαιώσω ότι έχω τοποθετήσει το SRV1 στο DMZ, ορίζω τη διεύθυνση IPv4 του με την εντολή `"ifconfig em0 inet 172.22.1.2/24"`, κάνω το ping PC1 → SRV1, και βλέπω ότι αυτό αποτυγχάνει. Αυτό είναι αναμενόμενο, αφού δεν έχω ορίσει προεπιλεγμένη πύλη στο SRV1, και έτσι δεν μπορεί να απαντήσει στο PC1 (κάνοντας tcpdump στο SRV1, βλέπω ότι αυτό λαμβάνει τα ICMP echo request).

5.31) Ορίζω τη σωστή προεπιλεγμένη πύλη στο SRV1 με την εντολή `"route add default 172.22.1.1"`.

5.32) Ναι, πλέον μπορώ να κάνω το ping PC1 → SRV1.

5.33) Όχι, δεν μπορώ να κάνω ping από το SRV1 στη διεπαφή του FW1 στο DMZ. Αυτό συμβαίνει επειδή δεν έχω ορίσει ακόμα κάποιον κανόνα στο τείχος προστασίας που να επιτρέπει τέτοιου είδους κίνηση.

5.34) Όχι, δεν μπορώ να κάνω τα pings SRV1 → {PC1,R1}. Αυτό συμβαίνει επειδή, και σε αυτήν την περίπτωση, δεν έχω ορίσει ακόμα κάποιον κανόνα στο τείχος προστασίας που να επιτρέπει τέτοιου είδους κίνηση.

5.35) Προσθέτω στο FW1 κανόνα ώστε να επιτρέπεται εξερχόμενη κίνηση από το DMZ προς οποιονδήποτε προορισμό πλην του LAN1 δίνοντας στα εξής πεδία τις παρακάτω τιμές:

Action: Pass

Interface: DMZ

Protocol: any

Source: Type → DMZ subnet

Destination: 'not' Type → LAN subnet

Save

5.36) Ναι, πλέον μπορώ να κάνω ping από το SRV1 στη διεπαφή του FW1 στο DMZ.

5.37) Ναι, μπορώ να κάνω ping από το SRV1 στη διεπαφή του FW1 στο WAN1.

5.38) Όχι, δεν μπορώ να κάνω το ping R1 → SRV1. Εμφανίζεται μήνυμα 'No route to host'. Αυτό είναι λογικό, αφού ο κανόνας που έχω προσθέσει στο τείχος προστασίας είναι μόνο για πακέτα ICMP προς WAN διευθύνσεις, και όχι προς DMZ.

5.39) Ναι, μπορώ να κάνω το ping SRV1 → R1. Αυτό είναι αναμενόμενο, καθώς έχω προσθέσει κανόνα (5.35) που επιτρέπει την κίνηση από το DMZ σε οποιοδήποτε εκτός LAN δικτύου.

5.40) Στο PC2 ξεκινώ τον πελάτη DHCP με την εντολή "dhclient em0". Αποδίδονται τα εξής:

Διεύθυνση IP: 192.168.1.3/24

Προεπιλεγμένη πύλη: 192.168.1.1

Διεύθυνση εξυπηρετητή DNS: 192.168.1.1

5.41) Προσθέτω στο FW1 κανόνα 'Block', ώστε να απαγορεύεται στο LAN1 όλη η κίνηση από το PC2 προς το SRV1 δίνοντας στα εξής πεδία τις παρακάτω τιμές:

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

Save

Firewall: Rules







 The changes have been applied successfully.


LAN


WAN


MNG


DMZ


	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> 	*	*	*	*	*	5.22	 
<input type="checkbox"/> 	*	192.168.1.3	*	172.22.1.2	*	5.41	 


 pass


 block


 reject

 log

 pass (disabled)


 block (disabled)

 reject (disabled)

 log (disabled)

5.42) Ο κανόνας αυτός πρέπει να τοποθετηθεί πριν τον προηγούμενο κανόνα, καθώς ο προηγούμενος κανόνας επιτρέπει όλες τις κινήσεις.

Firewall: Rules







 The changes have been applied successfully.


LAN


WAN


MNG


DMZ


	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> 	*	192.168.1.3	*	172.22.1.2	*	5.41	 
<input type="checkbox"/> 	*	*	*	*	*	5.22	 


 pass


 block


 reject

 log

 pass (disabled)

 block (disabled)

 reject (disabled)

 log (disabled)

5.43) Όχι, δεν μπορώ να κάνω το ping PC2 → SRV1.

5.44) Ναι, μπορώ να κάνω ping από το PC2 στη διεπαφή του FW1 στο DMZ. Αυτό είναι αναμενόμενο, καθώς δεν υπάρχει κάποιος κανόνας που να απαγορεύει την κίνηση αυτή. Σημειώνεται ότι με τον προηγούμενο κανόνα απαγόρευσα την κίνηση μόνο προς τον SRV1 συγκεκριμένα, και όχι γενικά για το DMZ.

Άσκηση 6

6.1) Προσθέτω στον R1 στατική εγγραφή για το 203.0.118.0/24 προς το FW1 ώστε η κίνηση προς το υποδίκτυό μου να διέρχεται μέσω του τείχους προστασίας με την εντολή “`route add 203.0.118.0/24 192.0.2.1`”.

6.2) Στο μενού *Firewall* → *NAT* του FW1 σελίδα *Outbound* ενεργοποιώ το ‘advanced outbound NAT’. Με αυτόν τον τρόπο απενεργοποιώ την αυτόματη δημιουργία κανόνων για απερχόμενη κίνηση (outbound NAT).

6.3) Προσθέτω αντιστοίχιση outbound NAT ώστε το PC1 να εμφανίζεται στον έξω κόσμο με τη διεύθυνση 203.0.118.14 και την ενεργοποιώ δίνοντας στα εξής πεδία τις παρακάτω τιμές:

Interface: WAN




Source: 192.168.1.2/32

Destination: any

Target: 203.0.118.14

Save

You may enter your own mappings below.

	Interface	Source	Destination	Target	Description	
<input type="checkbox"/>	WAN	192.168.1.2/32	*	203.0.118.14	6.3	  

6.4) Προσθέτω αντιστοίχιση outbound NAT ώστε το PC2 να εμφανίζεται στον έξω κόσμο με τη διεύθυνση 203.0.118.15 και την ενεργοποιώ δίνοντας στα εξής πεδία τις παρακάτω τιμές:

Interface: WAN





Source: 192.168.1.3/32

Destination: any

Target: 203.0.118.15

Save

You may enter your own mappings below.

	Interface	Source	Destination	Target	Description	
<input type="checkbox"/>	WAN	192.168.1.2/32	*	203.0.118.14	6.3	   
<input type="checkbox"/>	WAN	192.168.1.3/32	*	203.0.118.15	6.4	

6.5) Ξεκινώ καταγραφή πακέτων με το tcpdump στη διεπαφή του R1 με “`tcpdump -i em0`” και την αφήνω να τρέχει.


6.6) Ναι, μπορώ να κάνω τα pings PC{1,2} → R1. Τα πακέτα που φτάνουν στον R1 έχουν διευθύνσεις πηγής 203.0.118.{14,15}, αντίστοιχα.

6.7) Από νέο παράθυρο εντολών (Alt + Fi) στον R1 κάνω ping στο PC1 χρησιμοποιώντας τη διεύθυνση 203.0.118.14. Αυτό, φυσικά, αποτυγχάνει, καθώς έχω ορίσει outbound μετάφραση NAT, κατά την οποία δεν μεταφράζονται οι διευθύνσεις στην εισερχόμενη κίνηση. Σημειώνω, ότι ο FW1 δεν στέλνει πίσω στον R1 κάποιο μήνυμα, π.χ. 'No route to host', επειδή έχω επιλέξει να γίνεται 'Block', στο οποίο τα πακέτα που 'μπλοκάρονται' απορρίπτονται 'silently'.

6.8) Από το μενού *Firewall* → *NAT* του FW1 σελίδα 'Server NAT' προσθέτω αντιστοίχιση για την IP διεύθυνση 203.0.118.18 και την ενεργοποιώ.

6.9) Από το μενού *Firewall* → *NAT* του FW1 σελίδα 'Inbound' προσθέτω αντιστοίχιση ορίζοντας ως εξωτερική διεύθυνση IP τη 203.0.118.18, ως NAT IP τη διεύθυνση του SRV1, ως πρωτόκολλο το TCP, ως εξωτερική θύρα την SSH ή τον αριθμό 22 και ως τοπική θύρα την ίδια με την εξωτερική. Αφού επιλέξω το 'Auto-add a firewall rule to permit traffic though this NAT rule', την ενεργοποιώ.

Firewall: NAT: Inbound

 The changes have been applied successfully.




Inbound

Server NAT

1:1

Outbound

	If	Proto	Ext. port range	NAT IP	Int. port range	Description
<input type="checkbox"/>	WAN	TCP	22 (SSH)	172.22.1.2 (ext.: 203.0.118.18)	22 (SSH)	6.8



Note:
It is not possible to access NATed services using the WAN IP address from within LAN (or an optional network).

6.10) Ο παρακάτω (επιλεγμένος) κανόνας τοποθετείται αυτόματα στο Firewall για τη διεπαφή WAN. Η προσθήκη του κανόνα αυτού συνέβη επειδή ενεργοποίησα την επιλογή 'Auto-add a firewall rule to permit traffic though this NAT rule'.

Firewall: Rules

LAN

WAN

MNG

DMZ

	Proto	Source	Port	Destination	Port	Description
<input checked="" type="checkbox"/>	*	RFC 1918 networks	*	*	*	Block private networks
<input type="checkbox"/>	ICMP	*	*	WAN address	*	5.26
<input checked="" type="checkbox"/>	TCP	*	*	172.22.1.2	22 (SSH)	NAT 6.8

☒ pass

☒ pass (disabled)

☒ block

☒ block (disabled)

☒ reject

☒ reject (disabled)

☒ log

☒ log (disabled)

6.11) Ναι, μπορώ να συνδεθώ από τον R1 με ssh στο 203.0.118.18 (“[ssh lab@203.0.118.18](#)”). Εκτελώντας “hostname” μέσα από τη σύνδεση ssh βλέπω ότι έχω συνδεθεί στον SRV1.

6.12) Όχι, δεν μπορώ να κάνω το ping R1 → 203.0.118.18. Ο λόγος της αποτυχίας αυτής είναι το γεγονός ότι ο κανόνας που προσέθεσα παραπάνω επιτρέπει την κίνηση μόνο για SSH πακέτα.

6.13) Ναι, μπορώ να συνδεθώ με ssh από το PC2 στο SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.18. Τα πακέτα για τη σύνδεση αυτή στέλνονται στο SRV1 μέσω του R1, πράγμα που μπορώ να επιβεβαιώσω από την καταγραφή που τρέχει ακόμα στον R1.

6.14) Καταργώ την outbound NAT αντιστοίχιση για το PC1 από το μενού *Firewall* → *NAT* → *Outbound*, έπειτα επιλέγοντας την αντιστοίχιση για το PC1 και ‘*delete selected mappings*’.

Όχι, δεν μπορώ να κάνω το ping PC1 → R1. Αν μεταβώ στην οθόνη μέσω των παραπάνω βημάτων, θα δω μία σημείωση που επεξηγεί ακριβώς τον λόγο που το ping αποτυγχάνει:

«If advanced outbound NAT is enabled, no outbound NAT rules will be automatically generated anymore. Instead, only the mappings you specify below will be used. 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. If you use target addresses other than the WAN interface's IP address, then depending on the way your WAN connection is setup, you may also need [proxy ARP](#).»

6.15) Καταργώ το advanced outbound NAT (από την σελίδα που βρίσκουμε στο 6.14). Ναι, πλέον το ping PC1 → R1 επιτυγχάνει.

6.16) Ναι, εξακολουθώ να μπορώ να συνδεομαι με ssh από τον R1 στο SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.18. Επίσης, μπορώ να συνδεθώ με ssh από το PC1 στο SRV1, αλλά δεν μπορώ από το PC2 στο SRV1.

6.17) Ξεκινώ μια καταγραφή πακέτων στο SRV1 και άλλη μία στο R1 εμφανίζοντας επικεφαλίδες Ethernet με την εντολή “tcpdump -e”. Επιχειρώ να συνδεθώ πάλι με SSH από το PC2 στο SRV1. Από τις καταγραφές μπορώ να αντιληφθώ την κατάσταση αναλυτικά. Αρχικά, το PC2 στέλνει τα πακέτα στο FW1, αυτό μεταφράζει την διεύθυνσή του στην 203.0.118.15, λόγω της αντιστοίχισης outbound NAT που έχω ορίσει. Το FW1 με τη σειρά του μεταφράζει την διεύθυνση του PC2 στην δική του και στέλνει στον R1 το πακέτο tcp. Έπειτα, ο R1 στέλνει το πακέτο στο SRV1, αυτό απαντά στην διεύθυνση του FW1 (DMZ) και το FW1 απορρίπτει τη σύνδεση με τη σημαία ‘R’. Αυτό συμβαίνει, επειδή δεν έχω ορίσει εσωτερική αντιστοίχιση διευθύνσεων.

6.18) Για τη συμπεριφορά αυτή είναι υπεύθυνος ο κανόνας για το DMZ στην ερώτηση 5.35, ο οποίος απαγορεύει την εξερχόμενη κίνηση από το DMZ προς το LAN1.

Άσκηση 7

7.1) Αποσυνδέω το καλώδιο της κάρτας δικτύου #3 του FW1.

7.2) Συνδεομαι από τον φυλλομετρητή στο FW2 και αλλάζω τη διεύθυνση IP στη διεπαφή MNG από 192.168.56.2 σε 192.168.56.3.

7.3) Ξανασυνδέω από το Virtual Box το καλώδιο της κάρτας δικτύου #3 του FW1.

7.4) Ναι, μπορώ να συνδεθώ ταυτόχρονα από τον φυλλομετρητή του φιλοξενούντος μηχανήματος στα δύο τείχη προστασίας.

7.5) Αλλάζω το hostname του FW2 σε ‘fw2’ από την διαδρομή *System: General Setup* → *Hostname*. Δεν ξεχνώ να πατήσω *Save*.

7.6) Ορίζω τη σωστή διεύθυνση και προεπιλεγμένη πύλη του FW2 στο WAN2, επιλέγοντας το ‘Block private networks’.

Static IP configuration	
IP address	192.0.2.5 / 30 ▾
Gateway	192.0.2.6

7.7) Ορίζω τη σωστή διεύθυνση του FW2 στο LAN2 με αντίστοιχο τρόπο, όπως παραπάνω.

Interfaces: LAN

Primary configuration	Secondary IPs
IP address	192.168.2.1 / 24 ▾
<input type="button" value="Save"/>	
<p>Warning: after you click "Save", you must reboot your firewall for changes to take effect. You may also have to do one or more of the following steps before you can access your firewall again:</p> <ul style="list-style-type: none"> • change the IP address of your computer • renew its DHCP lease • access the webGUI with the new IP address 	

7.8) Επανεκκινώ το FW2, όπως προτείνεται και στο παραπάνω μήνυμα.

7.9) Προσθέτω στο FW2 κανόνα ώστε να επιτρέπεται όλη η κίνηση από το LAN2, ακολουθώντας *Firewall: Rules* → *WAN* → *add new rule*, δίνοντας στα εξής πεδία τις παρακάτω τιμές:

Action: Pass

















Interface: LAN

Protocol: any

Source: Type → any

Save *Apply changes*

Firewall: Rules

LAN	WAN	MNG	DMZ												
<input type="checkbox"/> 	<table border="1"> <thead> <tr> <th>Proto</th> <th>Source</th> <th>Port</th> <th>Destination</th> <th>Port</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>*</td> <td>*</td> <td>*</td> <td>*</td> <td>*</td> <td>7.9</td> </tr> </tbody> </table>	Proto	Source	Port	Destination	Port	Description	*	*	*	*	*	7.9	<div style="text-align: right;">        </div>	
Proto	Source	Port	Destination	Port	Description										
*	*	*	*	*	7.9										
<div style="display: flex; justify-content: space-between;"> <div>  pass  pass (disabled) </div> <div>  block  block (disabled) </div> <div>  reject  reject (disabled) </div> <div>  log  log (disabled) </div> </div>															

7.10) Προσθέτω στο FW2 κανόνα ώστε να επιτρέπεται όλη η εισερχόμενη ICMP κίνηση με προορισμό την 'WAN address' ακολουθώντας αντίστοιχη διαδρομή με την παραπάνω και δίνοντας στα εξής πεδία τις παρακάτω τιμές:

Action: Pass

Interface: WAN


Protocol: ICMP

Source: Type → any

Destination: Type → WAN address

Save *Apply changes*

Firewall: Rules



 The changes have been applied successfully.


LAN


WAN


MNG


DMZ


	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/> 	*	*	*	*	*	7.9
<input type="checkbox"/> 	ICMP	*	*	WAN address	*	7.10


 pass


 pass (disabled)


 block


 block (disabled)


 reject


 reject (disabled)


 log


 log (disabled)





























7.11) Επιβεβαιώνω ότι έχω μετακινήσεις το PC2 στο LAN2. Ορίζω τη σωστή διεύθυνση και προεπιλεγμένη πύλη με τις εντολές: “ifconfig em0 inet 192.168.2.2/24” και “route add default 192.168.2.1”.

7.12) Ναι, μπορώ να κάνω το ping PC1 → FW2(WAN2) (πριν εκτελέσω το ping αυτό επιβεβαιώνω ότι στις διεπαφές του R1 έχουν οριστεί οι σωστές διευθύνσεις και

7.13) Ναι, μπορώ να κάνω το ping PC2 → FW1(WAN1).

7.14) Όχι, δεν μπορώ να κάνω τα pings PC{1,2} → PC{2,1}. Αυτό είναι λογικό, αφού κατ’ αρχάς δεν υπάρχουν εγγραφές δρομολόγησης στον R1 για τις διαδρομές των PCs.

7.15) Στο μενού VPN του FW1 ενεργοποιώ το IPSec.

VPN: IPsec: Tunnels



The changes have been applied successfully.

Tunnels

Mobile clients

Pre-shared keys

CAs/CRLs

☒ Enable IPsec

Save

Local net	Interface	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description
Remote net	Remote gw				



Μετά δημιουργώ ένα IPsec tunnel ορίζοντας τα ακόλουθα: ως Local Subnet το τοπικό LAN, ως Remote Subnet τη διεύθυνση του LAN2, ως Remote Gateway τη διεύθυνση του FW2 στο WAN2, ως Pre-Shared Key το όνομά μου ('ioannisg') και το ενεργοποιώ.

VPN: IPsec: Tunnels

Tunnels

Mobile clients

Pre-shared keys

CAs/CRLs

☒ Enable IPsec

Save

Local net	Interface	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description
Remote net	Remote gw				
LAN 192.168.2.0/24	WAN 192.0.2.5	main	3DES	SHA-1	7.15



7.16) Στο *FW1* → *Firewall* → *Rules* → *IPsec VPN* βλέπω τον εξής κανόνα:

Firewall: Rules

LAN

WAN

IPsec VPN

MNG

DMZ

	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/> ↑	*	*	*	*	*	Default IPsec VPN



pass



block



reject



log



pass (disabled)



block (disabled)



reject (disabled)



log (disabled)

7.17) Στο *FW1* → *Diagnostics* → *IPSec* → *Security Association Database (SAD)* βλέπω ότι δεν έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων.

Diagnostics: IPSec

SAD **SPD**

No IPSec security associations.

7.18) Στο *FW1* → *Diagnostics* → *IPSec* → *Security Policy Database (SPD)* βλέπω ότι έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων.

Diagnostics: IPSec


SAD **SPD**

	Source	Destination	Direction	Protocol	Tunnel endpoints
<input type="checkbox"/>	192.168.2.0/24	192.168.1.0/24	➔	ESP	192.0.2.5 - 192.0.2.1
<input type="checkbox"/>	192.168.1.0/24	192.168.2.0/24	➔	ESP	192.0.2.1 - 192.0.2.5

➔ incoming (as seen by firewall)
➔ outgoing (as seen by firewall)

7.19) Στο μενού VPN του FW2 ενεργοποιώ το IPSec.

VPN: IPSec: Tunnels

 The changes have been applied successfully.

Tunnels **Mobile clients** **Pre-shared keys** **CAs/CRLs**

☒ Enable IPSec


Save

Local net	Interface	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description
Remote net	Remote gw				

Μετά δημιουργώ ένα IPSec tunnel ορίζοντας τα ακόλουθα: ως Local Subnet το τοπικό LAN, ως Remote Subnet τη διεύθυνση του LAN1, ως Remote Gateway τη διεύθυνση IP του FW1 στο WAN1, ως Pre-Shared

Key το όνομά μου (τη λέξη που δήλωσα προηγουμένως στην ερώτηση 7.15) και το ενεργοποιώ.

VPN: IPsec: Tunnels





 The changes have been applied successfully.

Tunnels Mobile clients Pre-shared keys CAs/CRLs

☒ Enable IPsec

Save

Local net Remote net	Interface Remote gw	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description
LAN 192.168.1.0/24	WAN 192.0.2.1	main	3DES	SHA-1	7.19




7.20) Στο *FW2* → *Diagnostics* → *IPSec* → *Security Association Database (SAD)* βλέπω ότι δεν έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων.



7.21) Στο *FW2* → *Diagnostics* → *IPSec* → *Security Policy Database (SPD)* βλέπω ότι έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων.

Diagnostics: IPsec

SAD **SPD**

	Source	Destination	Direction	Protocol	Tunnel endpoints
<input type="checkbox"/>	192.168.1.0/24	192.168.2.0/24	➔	ESP	192.0.2.1 - 192.0.2.5
<input type="checkbox"/>	192.168.2.0/24	192.168.1.0/24	➔	ESP	192.0.2.5 - 192.0.2.1



 incoming (as seen by firewall)
 outgoing (as seen by firewall)

7.22) Όχι, δεν μπορώ να κάνω το ping PC1 → PC2.

7.23) Όχι, δεν μπορώ να κάνω το ping PC2 → PC1.

7.24) Στο *FW1* → *Diagnostics* → *IPSec SAD* βλέπω ότι προστέθηκαν 2 εγγραφές.

Diagnostics: IPsec

SADSPD

☐

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.1	192.0.2.5	ESP	0ab80399	3des-cbc	hmac-sha1
192.0.2.5	192.0.2.1	ESP	0329d054	3des-cbc	hmac-sha1

☐

7.25) Στο FW2 → Diagnostics → IPsec SAD βλέπω ότι προστέθηκαν 2 εγγραφές.

Diagnostics: IPsec

SADSPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.5	192.0.2.1	ESP	0329d054	3des-cbc	hmac-sha1
192.0.2.1	192.0.2.5	ESP	0ab80399	3des-cbc	hmac-sha1

7.26) Ξεκινώ μια καταγραφή στον R1 στο WAN1 εμφανίζοντας λεπτομέρειες και το περιεχόμενο των πακέτων με “tcpdump -i em0 -nnnn” και αφήνω να τρέχει.

7.27) Όταν κάνω ping από το ένα PC στο άλλο δεν παρατηρώ πακέτα ICMP.

7.28) Εμφανίζονται μόνο πακέτα ESP(50), με πηγή και προορισμό 192.0.2.5 και 192.0.2.1, αντίστοιχα για την κάθε περίπτωση.

7.29) Όχι, δεν υπάρχει κάπου η πληροφορία για τις διευθύνσεις IP των PC{1,2}.

7.30) Ναι, μπορώ από το PC2 να συνδεθώ με SSH στο SRV1 στη διεύθυνση 203.0.118.18. Αυτό που άλλαξε σε σχέση με την προηγούμενη άσκηση είναι ότι πλέον το PC2 δεν ανήκει στο LAN1, για το οποίο υπάρχει πλέον ξεχωριστός κανόνας στο τείχος προστασίας.

7.31) Στην καταγραφή παρατηρώ πακέτα TCP, με διευθύνσεις πηγής και προορισμού 192.0.2.5 και 203.0.118.18, αντίστοιχα στην κάθε περίπτωση.

7.32) Ναι, τα πακέτα αυτά είναι κρυπτογραφημένα, και συγκεκριμένα με τον αλγόριθμο 3DES.