

Εργαστηριακή Άσκηση 10

Τείχη Προστασίας (Firewalls) και NAT

| | |
|------------------------------|---------------------------|
| Όνοματεπώνυμο: Άννα Κουτσώνη | Όνομα PC: DESKTOP-90FT571 |
| Ομάδα: 1 | Ημερομηνία: 28/04/2024 |

Άσκηση 1

- 1.1 PC1: ifconfig em0 192.168.1.2/24
vi /etc/rc.conf
hostname="PC1"
PC2: ifconfig em0 192.168.1.3/24
vi /etc/rc.conf
hostname="PC2"
- 1.2 kldload ipfw
- 1.3 kldstat
- 1.4 ping 127.0.0.1
ping 192.168.1.2
Όχι, δεν μπορούμε. Παίρνουμε μήνυμα λάθους Permission denied.
- 1.5 ipfw list
Υπάρχει ο κανόνας 65535 deny ip from any to any
- 1.6 ipfw add 100 allow all from any to any via 127.0.0.1
- 1.7 Ναι, είναι επιτυχής.
- 1.8 ipfw show
Προκύπτει: 00100 20 1680 allow ip from any to any via 127.0.0.1
65535 14 1048 deny ip from any to any
Άρα οι μετρητές είναι 20 1680 και 14 1048 αντίστοιχα για τον κάθε κανόνα.
- 1.9 ipfw zero
- 1.10 ping 192.168.1.3
Όχι, δεν μπορούμε. Παίρνουμε μήνυμα λάθους Permission denied.
- 1.11 ipfw add allow icmp from any to any
- 1.12 Πήρε τον αύξοντα αριθμό 200, ο οποίος δόθηκε αυτόματα από τον πυρήνα ως ο μεγαλύτερος κατά 100 του αύξοντα αριθμού του τελευταίου πριν τον προκαθορισμένο κανόνα.
- 1.13 Ναι, μπορούμε. Και τα δύο ping είναι επιτυχής.
- 1.14 traceroute 192.168.1.3
Λαμβάνουμε μήνυμα λάθους Permission denied. Αυτό συμβαίνει διότι η traceroute στέλνει by default δεδομενογράμματα UDP και δεν υπάρχει σχετικός κανόνας στο firewall που να επιτρέπει τα πακέτα UDP. Αλλάζουμε την εντολή σε traceroute -I 192.168.1.3 ώστε να στέλνει πακέτα ICMP, για τα οποία υπάρχει κανόνας που να τα επιτρέπει. Η traceroute πλέον λειτουργεί και λαμβάνουμε απάντηση.
- 1.15 ipfw add allow udp from me to any 33435-33626
Σύμφωνα με το man traceroute το traceroute χρησιμοποιεί τις θύρες από port+1 έως port+(max_ttl-first_ttl+1)*nprobes. Θέτουμε τις default τιμές port=33434 ,

nprobes=3, max_ttl=64 και first_ttl=1 και προκύπτει ότι το traceroute χρησιμοποιεί τις UDP θύρες 33435 έως 33626.

1.16 ssh lab@192.168.1.3

Όχι, δεν μπορούμε. Λαμβάνουμε μήνυμα λάθους Permission denied.

1.17 ipfw add allow tcp from any to any established
ipfw add allow tcp from me to any setup

1.18 ipfw zero
ssh lab@192.168.1.3
ls
exit

1.19 ipfw show

Ο κανόνας allow tcp from me to any setup εφαρμόστηκε μια φορά κατά την εγκατάσταση της σύνδεσης λόγω του πρώτου πακέτου της τριπλής χειραψίας. Ο κανόνας allow tcp from any to any established εφαρμόστηκε 75 φορές λόγω των υπόλοιπων TCP τεμαχίων που ανταλλάχθηκαν κατά τη σύνδεση.

1.20 ssh lab@192.168.1.2

Λαμβάνουμε μετά από λίγη ώρα μήνυμα λάθους Operation timed out. Αυτό συμβαίνει διότι έχουμε επιτρέψει με τον κανόνα ipfw add allow tcp from me to any setup την εγκατάσταση συνδέσεων από το PC1 προς απομακρυσμένους εξυπηρετητές και όχι την εγκατάσταση συνδέσεων από ξένους στο PC1. Επιτρέπονται δηλαδή μόνο οι απερχόμενες tcp συνδέσεις και όχι οι εισερχόμενες.

1.21 service ftpd onestart

1.22 Μπορούμε και να συνδεθούμε και να κατεβάσουμε ένα αρχείο.
ftp lab@192.168.1.2
ls /usr/bin (για να δούμε τα αρχεία του /usr/bin)
get /usr/bin/zstream

Άσκηση 2

2.1 kldload ipfw

2.2 ping 192.168.1.2

Όχι, δεν μπορούμε. Λαμβάνουμε μήνυμα Permission denied.

2.3 ipfw add allow all from any to any via lo0

2.4 ipfw add allow icmp from me to any icmp types 8

2.5 Δεν λαμβάνεται καμία απάντηση.

2.6 ipfw zero

ping -c 1 192.168.1.2

ipfw show

Ο μετρητής του κανόνα allow icmp from me to any icmp types 8 έχει γίνει 1.

Δηλαδή το icmp echo request περνάει το firewall αλλά το icmp echo reply όχι διότι δεν υπάρχει αντίστοιχος κανόνας και για αυτό και δεν λαμβάνεται απάντηση στο ping.

2.7 ipfw delete 200

ipfw add allow icmp from me to any icmp types 8 keep-state

ping 192.168.1.2

Το ping είναι επιτυχές.

2.8 ping 192.168.1.2

ping 192.168.1.3

Ναι, μπορούμε.

2.9 Όχι, δεν είναι επιτυχές ο κανόνας που επιτρέπει την αμφίδρομη επικοινωνία των PC1,PC2 λήγει με το keep-state, είναι δηλαδή δυναμικός και ανανεώνεται όσο υπάρχει κίνηση που ταιριάζει. Εφόσον η κίνηση αυτή διακόπηκε όταν σταμάτησε το ping από το PC2 προς το PC1, πλέον το τείχος προστασίας απορρίπτει τα icmp πακέτα και το ping από το PC1 προς το PC2 αποτυγχάνει.

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

2.11 Εμφανίζονται και οι δυναμικοί κανόνες.

00300 34 2856 (5s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 : default

2.12 Δεν εμφανίζεται τίποτα, ο δυναμικός κανόνας έχει διαγραφεί.

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 3

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

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 sftp [lab@192.168.1.3](#)

get /etc/rc.conf

Ναι, μπορούμε.

2.21 Όχι, δεν μπορούμε.

ipfw add allow tcp from any to me 21 keep-state

2.22 ftp [lab@192.168.1.3](#)

cd /usr

ls

Η cd /usr επιτυγχάνει διότι χρησιμοποιεί την θύρα 21 για την οποία έχουμε ορίσει κανόνα που να επιτρέπει την κίνηση στον PC2. Η ls αποτυγχάνει διότι η εκτέλεση της μας εισάγει σε extended passive mode γίνεται μεταφορά αρχείων δεδομένων και γίνεται δυναμική χρήση της θύρας 20 για την οποία δεν έχουμε ορίσει κανόνα στο firewall του PC2.

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

2.24 Συνδεόμαστε ξανά με ftp στον PC2 από τον PC1.

ftp [lab@192.168.1.2](#)

ls /usr/bin (για να δούμε τα αρχεία του /usr/bin)

get /usr/bin/zstream

Ναι, μπορούμε.

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 Η χρήση πολλών και διαφορετικών θυρών για τους διάφορους τρόπους λειτουργίας του ftp απαιτεί τη χρήση πολλών και διαφορετικών κανόνων ώστε να επιτρέπεται κάθε φορά η επιθυμητή λειτουργία. Παράλληλα η μη στοχευμένη δημιουργία εξειδικευμένων κανόνων μπορεί να επιτρέψει την επικοινωνία από θύρες που δεν επιθυμούμε και να μειώσει έτσι την προστασία του υπολογιστή εκθέτοντας τον σε κακόβουλους κινδύνους.

2.27 kldunload ipfw
 kldstat

Άσκηση 3

3.1 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
exit
```

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 kldstat

Έχουν φορτωθεί τα εξής modules:
kernel , intpm , smbus , ipfw , ipfw_nat , libalias

3.6 Ενεργοποιήθηκε το ipfw.

3.7 sysrc firewall_type

Είναι firewall_type: UNKNOWN

3.8 ipfw list

Βλέπουμε 11 κανόνες και ο τελευταίος είναι ο default:
65535 deny ip from any to any

3.9 ipfw nat show config

Όχι, δεν έχουν οριστεί.

3.10 ping 192.168.1.1

ping 192.0.2.1

Κανένα από τα δύο ping δεν είναι επιτυχές, δεν λαμβάνουμε απάντηση.

3.11 ping 192.0.2.1

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 ping 192.168.1.1

ping 192.0.2.1

Ναι, μπορούμε. Και τα δύο ping είναι επιτυχή.

3.15 tcpdump -i em0

3.16 ipfw show

ipfw zero

3.17 ping -c 3 192.0.2.2

Είναι η 192.0.2.1

3.18 Είναι η 192.0.2.1

3.19 Είναι ο ipfw add nat 123 ip4 from any to any.

- 3.20 Εφαρμόστηκε 12 φορές, μια κάθε πακέτο που στέλνεται. Στέλνουμε 3 ICMP echo request. Σε κάθε ένα στέλνονται τα εξής πακέτα: 1 πακέτο από τον PC1 προς το FW1, 1 πακέτο από το FW1 προς τον R1, 1 πακέτο από τον R1 προς το FW1, 1 πακέτο από το FW1 προς τον PC1. Ανταλλάσσονται δηλαδή συνολικά 4 πακέτα σε κάθε ICMP echo request που στέλνουμε, άρα σύνολο $3 \times 4 = 12$.
- 3.21 `ping 192.0.2.1`
Ναι, μπορούμε, το ping είναι επιτυχές.
- 3.22 Είναι και πάλι ο `ipfw add nat 123 ip4 from any to any`.
- 3.23 Όχι, γιατί η 192.0.2.5 του SRV1 δεν είναι ιδιωτική.
- 3.24 `ssh lab@192.0.2.5`
Ναι, μπορούμε.
- 3.25 `ssh lab@192.168.1.3`
Όχι, δεν μπορούμε. Εμφανίζεται μήνυμα λάθους No route to host. Είναι άρα θέμα δρομολόγησης διότι ο R1, στον οποίο προωθούνται τα πακέτα από τον SRV1 λόγω της default διαδρομής, δεν έχει εγγραφή για το 192.168.1.3.
- 3.26 `ipfw nat 123 config unreg_only if em1 reset redirect_addr 192.168.1.3 192.0.2.1`
- 3.27 `ssh lab@192.0.2.1`
Η προσπάθεια είναι επιτυχής. Συνδεόμαστε στο PC2 όπως φαίνεται από την προτροπή lab@PC2 στην γραμμή εντολών.
- 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 `ssh lab@192.0.2.1`
Συνδεόμαστε στο PC1 όπως φαίνεται από την προτροπή lab@PC1 στην γραμμή εντολών.
- 3.30 `ftp lab@192.0.2.1`
Συνδεόμαστε στο PC2. Το εξακριβώνουμε εκτελώντας netstat στον PC2 και βλέποντας ότι υπάρχει ανοιχτή σύνδεση ftp με foreign address την 192.0.2.5 που ανήκει στον SRV1.
- 3.31 Ναι, μπορούμε.
`ls /etc`
`get /etc/rc.conf`
- 3.32 `ftp lab@192.0.2.1`
Συνδεόμαστε στο PC2. Το εξακριβώνουμε εκτελώντας netstat στον PC2 και βλέποντας ότι υπάρχει ανοιχτή σύνδεση ftp με foreign address την 192.0.2.1 που ανήκει στον PC1.
- 3.33 `ssh lab@192.0.2.1`
Συνδεόμαστε στο PC1 όπως φαίνεται από την προτροπή lab@PC1 στην γραμμή εντολών.

Άσκηση 4

- 4.1 `ipfw disable one_pass`
PC1: `ping 192.168.1.1`
SRV1: `ping 192.0.2.1`
Όχι, δεν μπορούμε, κανένα από τα δύο ping δεν είναι επιτυχές.

- 4.2 Βλέπουμε ότι κατά την εκτέλεση του ping ο μετρητής του κανόνα του ερωτήματος 3.13 αυξάνεται, άρα τα πακέτα γίνονται δεκτά. Λόγω της απενεργοποίησης του one-pass τα πακέτα επεξεργάζονται στη συνέχεια από τους υπόλοιπους κανόνες και απορρίπτονται από τον default κανόνα deny ip from any to any.
- 4.3 ipfw delete 1100
ipfw add 1100 allow all from any to any via em0
- 4.4 Ναι, είναι επιτυχές.
- 4.5 ssh [lab@192.0.2.1](#)
Συνδεόμαστε στο FW1. Το εξακριβώνουμε εκτελώντας netstat στον FW1 και βλέποντας ότι υπάρχει ανοιχτή σύνδεση ssh με foreign address την 192.168.1.3 που ανήκει στον PC2.
- 4.6 Με ipfw βλέπουμε ότι μετά την ssh σύνδεση αυξάνονται οι μετρητές των ακόλουθων κανόνων και άρα αυτοί είναι υπεύθυνοι: 00100 allow ip from any to any via lo0 και 01100 allow ip from any to any via em0
- 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 Με tcpdump βλέπουμε ότι απαντάει το FW1.
- 4.12 Απαντάει το PC2.
- 4.13 ssh [lab@192.0.2.1](#)
Συνδεόμαστε στο FW1. Το εξακριβώνουμε εκτελώντας netstat στο FW1 και βλέποντας ότι υπάρχει ανοιχτή σύνδεση ssh με foreign address την 192.0.2.1 που ανήκει στον PC1.
- 4.14 ssh [lab@192.0.2.1](#)
Συνδεόμαστε στο PC1. Το εξακριβώνουμε εκτελώντας netstat στο PC1 και βλέποντας ότι υπάρχει ανοιχτή σύνδεση ssh με foreign address την 192.0.2.5 που ανήκει στον SRV1.
- 4.15 ftp [lab@192.0.2.1](#)
Συνδεόμαστε στο PC2. Το εξακριβώνουμε εκτελώντας netstat στο PC2 και βλέποντας ότι υπάρχει ανοιχτή σύνδεση ssh με foreign address την 192.0.2.5 που ανήκει στον SRV1.
- 4.16 Ναι, μπορούμε.
- 4.17 Ναι, μπορούμε.
- 4.18 Ναι, μπορούμε.
ls /etc
get /etc/rc.conf
- 4.19 ipfw add 2999 deny all from any to any via em1
- 4.20 Επιτυγχάνουν το ping από το PC1 προς την 192.0.2.1 και το ssh από το PC1 προς την 192.0.2.1, τα οποία δεν απαιτούν διέλευση πακέτων από το WAN1, την οποία απαγορέψαμε.
- 4.21 ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
- 4.22 Ναι, μπορούμε.
- 4.23 ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state
- 4.24 Ναι, μπορούμε.
- 4.25 ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state
- 4.26 Απαντάει το PC2.

- 4.27 ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state
- 4.28 ssh [lab@192.0.2.1](#)
 Συνδεόμαστε στο PC1. Το εξακριβώνουμε εκτελώντας netstat στο PC1 και βλέποντας ότι υπάρχει ανοιχτή σύνδεση ssh με foreign address την 192.0.2.5 που ανήκει στον SRV1.
- 4.29 ftp [lab@192.0.2.1](#)
 Όχι, δεν μπορούμε.
- 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

Άσκηση 5

- 5.1 Γραφικό Περιβάλλον → Interfaces → LAN → Primary configuration → IP address → 192.168.1.1/24
- 5.2 Γραφικό Περιβάλλον → Interfaces → WAN → Static IP configuration → IP address → 10.0.0.1/30
- 5.3 Γραφικό Περιβάλλον → Status → System → Memory Usage → 34%
 Άρα το ποσοστό ελεύθερης μνήμης είναι 66%.
- 5.4 Γραφικό Περιβάλλον → Interfaces
 Έχουμε 4 διεπαφές: LAN→em0
 WAN→em1
 MNG→em2
 DMZ→em3

Επιβεβαιώνουμε ότι και στο Virtualbox είναι σωστά:

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

- 5.5 Γραφικό Περιβάλλον → Interfaces → DMZ → IP configuration → IP address → 172.22.1.1/24
- 5.6 Γραφικό Περιβάλλον → System → General setup → Hostname → fw
 Γραφικό Περιβάλλον → System → General setup → Domain → lab.ntua.gr
- 5.7 Γραφικό Περιβάλλον → System → General setup → Hostname → fw1 → Save
- 5.8 Γραφικό Περιβάλλον → Firewall → Rules → WAN
 Δεν υπάρχουν κανόνες.
- 5.9 Γραφικό Περιβάλλον → Interfaces → WAN → Static IP configuration →
 → IP address → 192.0.2.1/30
 → Gateway → 192.0.2.2
 Επιλέγουμε και το Block private networks.
 → Save
- 5.10 Γραφικό Περιβάλλον → Firewall → Rules → WAN
 Ναι, υπάρχει ο κανόνας Block private networks
- 5.11 Όχι, καμία δεν είναι ενεργοποιημένη.
- 5.12 Γραφικό Περιβάλλον → Services → DNS forwarder → Enable DNS forwarder → Save
- 5.13 Γραφικό Περιβάλλον → Services → DHCP server → LAN → Enable → Range → 192.168.1.2 to 192.168.1.3 → Save

- 5.14 dhclient em0
 ifconfig em0
 Αποδόθηκε η 192.168.1.2
 netstat -r
 Default Gateway: 192.168.1.1
 cat /etc/resolv.conf
 nameserver 192.168.1.1
- 5.15 Για να αποφύγουμε τον ορισμό εξυπηρετητή DNS χειροκίνητα αλλά να επιτρέψουμε στο FW να λειτουργεί και ως DNS server μέσω της υπηρεσίας DHCP.
- 5.16 Γραφικό Περιβάλλον → Diagnostics → DHCP leases
- 5.17 Βλέπουμε 7 εγγραφές:

Diagnostics: ARP table

| | IP address | MAC address | Hostname | Interface |
|--------------------------|--------------|-------------------|----------|-----------|
| <input type="checkbox"/> | 172.22.1.1 | 08:00:27:e3:93:a6 | | DMZ |
| <input type="checkbox"/> | 192.168.56.1 | 0a:00:27:00:00:0a | | MNG |
| <input type="checkbox"/> | 192.168.56.2 | 08:00:27:ef:48:f2 | | MNG |
| <input type="checkbox"/> | 192.0.2.1 | 08:00:27:c3:e4:0c | | WAN |
| <input type="checkbox"/> | 192.168.1.1 | 08:00:27:fe:6c:95 | | LAN |
| <input type="checkbox"/> | 192.168.1.3 | 08:00:27:76:f4:6d | PC1 | LAN |
| <input type="checkbox"/> | 192.168.1.2 | 08:00:27:65:94:65 | PC1 | LAN |

- 5.18 ping 192.168.1.1
 Όχι, δεν λαμβάνουμε απάντηση.
- 5.19 Βλέπουμε μια λίστα με τις τελευταίες 50 καταγραφές και λεπτομέρειες για αυτές. Βλέπουμε τα πακέτα του ping τα οποία έγιναν deny.
 Γραφικό Περιβάλλον → Diagnostics → Logs → Firewall → Clear log
- 5.20 Γραφικό Περιβάλλον → Diagnostics → Firewall states
 Βλέπουμε 11 καταγραφές:

| Statistics snapshot control | | | | | | | |
|-----------------------------|-------|-----------------|-------|---------------------------------|---------|-------|---------|
| Start new | | | | Last statistics snapshot: Never | | | |
| Source | Port | Destination | Port | Protocol | Packets | Bytes | TTL |
| 192.168.56.1 | 17500 | 255.255.255.255 | 17500 | udp | 7 | 1218 | 1:37 |
| 192.168.56.1 | 17500 | 255.255.255.255 | 17500 | udp | 7 | 1218 | 0:07 |
| 192.168.56.1 | 49930 | 192.168.56.2 | 80 | tcp | 3 | 735 | 2:30:00 |
| 192.168.56.1 | 17500 | 192.168.56.255 | 17500 | udp | 3 | 522 | 0:37 |
| 192.168.56.1 | 17500 | 255.255.255.255 | 17500 | udp | 2 | 348 | 0:37 |
| 192.168.56.1 | 17500 | 255.255.255.255 | 17500 | udp | 2 | 348 | 0:07 |
| 192.168.56.1 | 17500 | 255.255.255.255 | 17500 | udp | 2 | 348 | 1:07 |
| 192.168.56.1 | 17500 | 255.255.255.255 | 17500 | udp | 2 | 348 | 1:37 |
| 192.168.56.1 | 17500 | 192.168.56.255 | 17500 | udp | 2 | 348 | 1:37 |
| 192.168.56.1 | 17500 | 255.255.255.255 | 17500 | udp | 2 | 348 | 0:37 |
| 192.168.56.1 | 49931 | 192.168.56.2 | 80 | tcp | 2 | 92 | 2:30:00 |

Firewall connection states displayed: 11

- 5.21 Γραφικό Περιβάλλον → Firewall → Rules → LAN
Δεν υπάρχει κανένας κανόνας
- 5.22 Γραφικό Περιβάλλον → Firewall → Rules → LAN → +
Προσθέτουμε νέο κανόνα δίνοντας τις εξής τιμές στα πεδία:
Action→Pass
Interface→LAN
Protocol→any
Source→any
Destination→any
→ Save
→ Apply changes
- 5.23 ping 192.168.1.1
 ping 192.0.2.1
 ping 172.22.1.1
Ναι, μπορούμε. Και τα τρία ping είναι επιτυχή.
- 5.24 ping 192.0.2.1
Δεν λαμβάνουμε καμία απάντηση.
- 5.25 arp -a
Ναι, υπάρχει εγγραφή.
192.0.2.1 at 08:00:27:c3:e4:0c
- 5.26 Γραφικό Περιβάλλον → Firewall → Rules → WAN → +
Προσθέτουμε νέο κανόνα δίνοντας τις εξής τιμές στα πεδία:
Action→Pass
Interface→WAN
Protocol→ICMP
ICMP type→any
Source→any
Destination→WAN address
→ Save
→ Apply changes
- 5.27 ping 192.0.2.1
Ναι, μπορούμε.
- 5.28 ping 192.168.1.2
Όχι, δεν μπορούμε. Λαμβάνουμε μήνυμα λάθους No route to host, διότι ο R1 δεν έχει ούτε default gateway ούτε εγγραφή για το PC1.
- 5.29 ping 192.0.2.2
Ναι, μπορούμε. Γίνεται μετάφραση NAT της ιδιωτικής διεύθυνσης του PC1 στη διεύθυνση του FW στο WAN1.
- 5.30 ifconfig em0 172.22.1.2/24
 ping 172.22.1.2
Όχι, δεν μπορούμε. Δεν λαμβάνουμε απάντηση. Αυτό συμβαίνει διότι ναί μεν τα echo requests του PC1 φτάνουν στον SRV1 αλλά αυτός στη συνέχεια δεν μπορεί να απαντήσει διότι ούτε διαθέτει εγγραφή στον πίνακα δρομολόγησης του σχετικά με τον PC1 αλλά ούτε και υπάρχει σχετικός κανόνας στο FW για το DMZ ώστε να γίνεται μετάφραση NAT.
- 5.31 route add default 172.22.1.1
- 5.32 ping 172.22.1.2
Ναι, μπορούμε.

- 5.33 ping 172.22.1.1
Όχι, δεν μπορούμε, διότι δεν έχει οριστεί κάποιος κανόνας στο FW για το DMZ που να επιτρέπει την εξερχόμενη κίνηση σε αυτό.
- 5.34 ping 192.168.1.2
 ping 192.0.2.2
Όχι, δεν μπορούμε, διότι όπως και πριν δεν έχει οριστεί κάποιος κανόνας στο FW για το DMZ που να επιτρέπει την εξερχόμενη κίνηση σε αυτό.
- 5.35 Γραφικό Περιβάλλον → Firewall → Rules → DMZ → +
Προσθέτουμε νέο κανόνα δίνοντας τις εξής τιμές στα πεδία:
Action→Pass
Interface→DMZ
Protocol→any
Source→DMZ subnet
Destination→ not
LAN subnet
→ Save
→ Apply changes
- 5.36 ping 172.22.1.1
Ναι, μπορούμε.
- 5.37 ping 192.0.2.1
Ναι, μπορούμε.
- 5.38 ping 172.22.1.2
Όχι, δεν μπορούμε. Λαμβάνουμε μήνυμα λάθους No route to host, διότι ο R1 δεν έχει ούτε default gateway ούτε εγγραφή για το SRV1.
- 5.39 ping 192.0.2.2
Ναι, μπορούμε, διότι πλέον έχει προστεθεί κανόνας που να επιτρέπει την κίνηση από το DMZ και γίνεται μετάφραση NAT των διευθύνσεων στο FW.
- 5.40 dhclient em0
 ifconfig em0
 Αποδόθηκε η 192.168.1.3
 netstat -r
 Default Gateway: 192.168.1.1
 cat /etc/resolv.conf
 nameserver 192.168.1.1
- 5.41 Γραφικό Περιβάλλον → Firewall → Rules → LAN → +
Προσθέτουμε νέο κανόνα δίνοντας τις εξής τιμές στα πεδία:
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
→ Apply changes

- 5.42 Πρέπει να τοποθετηθεί πριν γιατί οι κανόνες εφαρμόζονται με τη σειρά που εμφανίζονται και αν μπει μετά δεν θα εφαρμοστεί ποτέ αφού ο κανόνας που υπάρχει επιτρέπει όλη την κίνηση.
- 5.43 `ping 172.22.1.2`
Όχι, δεν μπορούμε.
- 5.44 `ping 172.22.1.1`
Ναι, μπορούμε. Δεν υπάρχει κάποιος κανόνας που να απαγορεύει αυτή την κίνηση. Ο τελευταίος κανόνας που ορίσαμε στο FW απαγορεύει μόνο την κίνηση από το PC2 προς το SRV1 και όχι προς το FW.

Άσκηση 6

- 6.1 cli
configure terminal
ip route 203.0.118.0/24 192.0.2.1
- 6.2 Γραφικό Περιβάλλον → Firewall → NAT → Outbound → Enable advance outbound NAT
- 6.3 Γραφικό Περιβάλλον → Firewall → NAT → Outbound → +
Interface→WAN
Source→192.168.1.2/24
Destination→ any
Target→203.0.118.14
→ Save
→ Apply changes
- 6.4 Γραφικό Περιβάλλον → Firewall → NAT → Outbound → +
Interface→WAN
Source→192.168.1.3/24
Destination→ any
Target→203.0.118.15
→ Save
→ Apply changes
- 6.5 `tcpdump -i em0`
- 6.6 Ναι, μπορούμε. Από τον PC1 φτάνουν με την 203.0.118.14 και από το PC2 με την 203.0.118.15.
- 6.7 Γραφικό Περιβάλλον → Firewall → NAT → Server NAT → +
External IP address→203.0.118.18
→ Save
→ Apply changes
- 6.8 Γραφικό Περιβάλλον → Firewall → NAT → Inbound → +
Interface→WAN
External 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

- 6.9 Τοποθετήθηκε ο κανόνας που επιτρέπει την TCP κίνηση προς την θύρα 22 της 172.22.1.2 λόγω του Auto-add a firewall rule to permit traffic through this NAT rule

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

- 6.10 ssh lab@203.0.118.18

Ναι, μπορούμε. Συνδεόμαστε στο SRV1 λόγω του προηγούμενου κανόνα.

- 6.11 ping 203.0.118.18

Το ping αποτυγχάνει διότι δεν υπάρχει κανόνας που να επιτρέπει την ICMP κίνηση προς την 203.0.118.18.

- 6.12 ssh lab@203.0.118.18

Ναι, μπορούμε. Με tcpdump διαπιστώνουμε ότι τα πακέτα φτάνουν στον SRV1 διερχόμενα από τον R1.

- 6.13 Όχι, δεν μπορούμε. Τα πακέτα που στέλνει ο PC1 φτάνουν στον R1 αλλά απορρίπτονται στη συνέχεια από το FW και δεν φτάνουν στον SRV1.

- 6.14 Ναι, είναι επιτυχή.

- 6.15 Μπορούμε από τον R1 αλλά όχι από τα PC1,PC2.

- 6.16 tcpdump -i em0 -e

Παρατηρούμε ότι τα δύο πρώτα πακέτα της χειραψίας στέλνονται κανονικά. Αλλά στη συνέχεια γίνεται reset της σύνδεσης.

- 6.17 Με βάση την σημείωση στην καρτέλα Inbound δεν μπορούμε να έχουμε πρόσβαση σε NATed services χρησιμοποιώντας την WAN IP address μέσα από το LAN. Αυτό επιχειρείται να γίνει προηγουμένως κατά την απόπειρα ssh σύνδεσης και για αυτό και αποτυγχάνει.

Άσκηση 7

- 7.1 FW1→Network→Adapter 3→Advanced→Cable connected

- 7.2 Γραφικό Περιβάλλον → Interfaces → MNG → IP configuration → IP address → 192.168.56.3

- 7.3 FW1→Network→Adapter 3→Advanced→Cable connected

- 7.4 Ναι, μπορούμε. Συνδεόμαστε στο FW1 μέσω της <http://192.168.56.2> και στο FW2 μέσω της <http://192.168.56.3>

- 7.5 Γραφικό Περιβάλλον → System → General setup → Hostname → fw2 → Save

- 7.6 Γραφικό Περιβάλλον → Interfaces → WAN → Static IP configuration →

→ IP address → 192.0.2.5/30

→ Gateway → 192.0.2.6

Επιλέγουμε και το Block private networks.

→ Save

- 7.7 Γραφικό Περιβάλλον → Interfaces → LAN → Primary configuration → IP address → 192.168.2.1/24

- 7.8 Γραφικό Περιβάλλον → Diagnostics → Reboot system → Yes

- 7.9 Γραφικό Περιβάλλον → Firewall → Rules → LAN → +

Προσθέτουμε νέο κανόνα δίνοντας τις εξής τιμές στα πεδία:

Action→Pass

Interface→LAN

Protocol→any

Source→any

Destination→any

→ Save

→ Apply changes

7.10 Γραφικό Περιβάλλον → Firewall → Rules → WAN → +

Προσθέτουμε νέο κανόνα δίνοντας τις εξής τιμές στα πεδία:

Action→Pass

Interface→WAN

Protocol→ICMP

ICMP type→any

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 ping 192.0.2.5

Ναι, μπορούμε, το ping είναι επιτυχές.

7.13 ping 192.0.2.1

Ναι, μπορούμε, το ping είναι επιτυχές.

7.14 Όχι, δεν μπορούμε και τα δύο ping είναι αποτυχημένα διότι παρόλο που τα FW επιτρέπουν την κίνηση, ο R1 δεν διαθέτει εγγραφές για τα PC1,PC2 και δεν μπορεί να προωθήσει τα πακέτα.

7.15 Γραφικό Περιβάλλον → IPsec → VPN → Tunnels → Enable IPsec → Save

Γραφικό Περιβάλλον → IPsec → VPN → Tunnels → +

Local subnet→LAN subnet

Remote subnet→192.168.2.0/24


Remote gateway→192.0.2.5

Pre-Shared Key→anna

→ Save

→ Apply changes

7.16 Βλέπουμε τον εξής κανόνα:

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

7.17 Όχι, δεν έχουν οριστεί.

7.18 Ναι, έχουν οριστεί δύο πολιτικές.

| | 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 |

- 7.19 Γραφικό Περιβάλλον → IPsec → VPN → Tunnels → Enable IPsec → Save
 Γραφικό Περιβάλλον → IPsec → VPN → Tunnels → +
 Local subnet→LAN subnet
 Remote subnet→192.168.1.0/24
 Remote gateway→192.0.2.1
 Pre-Shared Key→anna
 → Save
 → Apply changes
- 7.20 Όχι, δεν έχουν οριστεί.
- 7.21 Ναι, έχουν οριστεί δύο πολιτικές.

| | 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 |

- 7.22 Ναι, μπορούμε, το ping είναι επιτυχές.
- 7.23 Ναι, μπορούμε, το ping είναι επιτυχές.
- 7.24 Ναι, ορίστηκαν 2 σχέσεις.

| | Source | Destination | Protocol | SPI | Enc. alg. | Auth. alg. |
|--------------------------|-----------|-------------|----------|----------|-----------|------------|
| <input type="checkbox"/> | 192.0.2.1 | 192.0.2.5 | ESP | 07846617 | 3des-cbc | hmac-sha1 |
| <input type="checkbox"/> | 192.0.2.5 | 192.0.2.1 | ESP | 0ee723ea | 3des-cbc | hmac-sha1 |

- 7.25 Ναι, ορίστηκαν 2 σχέσεις.

| | Source | Destination | Protocol | SPI | Enc. alg. | Auth. alg. |
|--------------------------|-----------|-------------|----------|----------|-----------|------------|
| <input type="checkbox"/> | 192.0.2.5 | 192.0.2.1 | ESP | 0ee723ea | 3des-cbc | hmac-sha1 |
| <input type="checkbox"/> | 192.0.2.1 | 192.0.2.5 | ESP | 07846617 | 3des-cbc | hmac-sha1 |

- 7.26 tcpdump -i em0 -vvn
- 7.27 Όχι, δεν παρατηρούμε πακέτα ICMP.
- 7.28 Παρατηρούμε πακέτα ESP. Όσα πηγάζουν από τον PC1 έχουν ως διεύθυνση πηγής την 192.0.2.1 και διεύθυνση προορισμού την 192.0.2.5 ενώ Όσα πηγάζουν από τον PC2 έχουν ως διεύθυνση πηγής την 192.0.2.5 και διεύθυνση προορισμού την 192.0.2.1.
- 7.29 Όχι, δεν υπάρχει.
- 7.30 ssh lab@203.0.118.18
 Ναι, μπορούμε να συνδεθούμε κανονικά διότι πλέον το PC2 χρησιμοποιεί το WAN του FW2 ι όχι του FW1 του LAN1.
- 7.31 Παρατηρούμε πακέτα TCP. Όσα πηγάζουν από τον PC2 έχουν ως διεύθυνση πηγής την 192.0.2.5 και θύρα 21240 και διεύθυνση προορισμού την 203.0.118.18 και θύρα ssh (22).
- 7.32 Ναι, είναι κρυπτογραφημένα, με ssh.