ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Εργαστήριο Δικτύων Υπολογιστών

Αναφορά 10ης Εργαστηριακής Άσκησης

Ραπτόπουλος Πέτρος (el19145)

Ημερομηνία: 16/5/2023

Άσκηση 1: Ένα απλό τείχος προστασίας

1.1) Στο PC1 φορτώστε στον πυρήνα το τείχος προστασίας ipfw. **kldload ipfw**

1.2) Με ποια εντολή στο PC1 μπορείτε να επιβεβαιώσετε ότι είναι ενεργό το τείχος προστασίας ipfw;
kldstat, πρέπει να συμπεριλαμβάνεται το module ipfw.ko στον πυρήνα.

1.3) Μπορείτε να κάνετε ping στη διεύθυνση IP του βρόχου επιστροφής lo0 ή της διεπαφής em0; Ποιο λάθος βλέπετε;
ping 192.168.1.2 -> Permission Denied

1.4) Βρείτε τους κανόνες που υπάρχουν στο τείχος προστασίας του PC1. **ipfw list -> 65535 deny ip from any to any**

1.5) Βρείτε στοιχεία για τη χρήση των προηγούμενων κανόνων. **ipfw show**

1.6) Πώς μπορείτε να μηδενίσετε τους σχετικούς με τη χρήση των κανόνων μετρητές; **ipfw zero**

1.7) Προσθέστε στο τείχος προστασίας του PC1 κανόνα με αύξοντα αριθμό 100 που να επιτρέπει μέσω της διεπαφής lo0 όλη την κίνηση (οποιοδήποτε πρωτόκολλο, από και προς οποιαδήποτε διεύθυνση).
ipfw add 100 allow all from any to any via lo0

1.8) Είναι τώρα τα ping της 1.3 επιτυχή; **Ναι**

1.9) Μπορείτε να κάνετε ping από το PC1 στο PC2; Ποιο λάθος βλέπετε; **Όχι, Permission Denied**

1.10) Προσθέστε κανόνα στο τείχος προστασίας του PC1 ώστε να επιτρέπεται η κίνηση ICMP από προς οποιαδήποτε διεύθυνση IP. **ipfw add allow icmp from any to any**

1.11) Τι αύξοντα αριθμό έλαβε ο κανόνας; **200**

1.12) Μπορείτε τώρα να κάνετε ping από το PC1 στο PC2; **Ναι** Μπορείτε από το PC2 στο PC1; **Ναι**

1.13) Γιατί δεν μπορείτε από το PC1 να κάνετε traceroute στο PC2; **Γιατί η εντολή traceroute για το FREEBSD στέλνει δεδομενογράμματα UDP ώστε να ανακαλύψει την διαδρομή ενός πακέτου από μια πηγή σε έναν προορισμό. Έχουμε προσθέσει κανόνα στο τείχος προστασίας μόνο για icmp πακέτα**
Με ποια απλή αλλαγή στη σύνταξη της εντολής traceroute θα λάβετε απάντηση από το PC2; **Χρησιμοποιώντας -I**

1.14) Προσθέστε κανόνα στο τείχος προστασίας του PC1 ώστε το traceroute από το PC1 προς οποιοδήποτε προορισμό να λειτουργεί. **ipfw add allow udp from any to any**

1.15) Μπορείτε από το PC1 να συνδεθείτε με ssh στο PC2; **Permission Denied**

1.16) Προσθέστε δύο στατικούς κανόνες που επιτρέπουν τη σύνδεση του PC1 σε απομακρυσμένους εξυπηρετητές με tcp
ipfw add allow tcp from any to any out, ipfw add allow tcp from any to any in

1.17) Στο PC1 μηδενίστε τους μετρητές χρήσης των κανόνων και συνδεθείτε με ssh στο PC2, εκτελέστε την εντολή ls και αποσυνδεθείτε. **ipfw zero, ssh lab@192.168.1.3, ls, exit**

1.18) Πόσες φορές εφαρμόσθηκε ο κάθε κανόνας που προσθέσατε; **43 φορές για τα εξερχόμενα και 38 για τα εισερχόμενα** Γιατί; **Τα tcp segments περιέχουν την πληροφορία αυτή καθαυτή προς μετάδοση αλλά υπάρχουν και τεμάχια τα οποία συμβάλουν στην εγκατάσταση της σύνδεσης**

1.19) Μπορείτε από το PC2 να συνδεθείτε με ssh στο PC1; Γιατί;
Ναι μπορεί διότι έχουμε επιτρέψει την ροή τεμαχίων και προς τις δύο κατευθύνσεις (εισερχόμενα/εξερχόμενα)

1.20) Στο PC2 ξεκινήστε τον δαίμονα ftpd ώστε αυτό να λειτουργεί ως εξυπηρετητής FTP. **service ftpd onestart**

1.21) Μπορείτε από το PC1 να συνδεθείτε με ftp στο PC2 ως χρήστης lab και να κατεβάσετε ένα αρχείο από το /usr/bin του PC2 στο PC1; **ftp lab@192.168.1.3, ναι μπορούμε να συνδεθούμε και να κατεβάσουμε το αρχείο**

Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

2.1) Στο PC2 φορτώστε στον πυρήνα το τείχος προστασίας ipfw. **kldload ipfw**

2.2) Μπορείτε να κάνετε ping από το PC2 στο PC1; **Όχι, Permission Denied**

2.3) Προσθέστε στο τείχος προστασίας του PC2 κανόνα που να επιτρέπει μέσω της διεπαφής lo0 όλη την κίνηση. **ipfw add 100 allow all from any to any via lo0**

2.4) Προσθέστε κανόνα στο τείχος προστασίας του PC2 που να επιτρέπει κίνηση ICMP τύπου echo request από το PC2 προς οποιαδήποτε διεύθυνση IP. **ipfw add allow icmp from me to any**

2.5) Μπορείτε να κάνετε ping από το PC2 στο PC1; **Όχι**

2.6) Περνούν τα πακέτα ICMP το τείχος προστασίας του PC2; Τεκμηριώστε την απάντησή σας παρατηρώντας του σχετικούς με τον προηγούμενο κανόνα μετρητές πακέτων. **Περνούν τα ICMP Requests και απορρίπτονται τα Replies**

2.7) Διαγράψτε τον κανόνα για το ICMP και επανεισάγετέ τον προσθέτοντας στο τέλος το "keep- state". **ipfw delete 200, ipfw add allow icmp from me to any keep-state** Μπορείτε να κάνετε ping από το PC2 στο PC1; **Ναι**

2.8) Ξεκινήστε το ping από το PC2 στο PC1 και αφήστε το να τρέχει. Μπορείτε να κάνετε ping από το PC1 στο PC2; **Ναι μπορούμε**

2.9) Σταματήστε τα ping στο PC2 και περιμένετε λίγο. Επιτυγχάνει τώρα το ping από το PC1 στο PC2; Γιατί; **Όχι, Όταν υπάρξει ταίριασμα σε κανόνα που λήγει με το keep-state δημιουργείται ένας δυναμικός κανόνας που ταιριάζει για το συγκεκριμένο πρωτόκολλο την αμφίδρομη κίνηση μεταξύ των διευθύνσεων πηγής και προορισμού και των αντίστοιχων θυρών πηγής και προορισμού. Οι δυναμικοί κανόνες έχουν περιορισμένο χρόνο ζωής που ανανεώνεται όσο υπάρχει κίνηση που ταιριάζει. Σταματώντας το ping από το PC2 και περιμένοντας ο κανόνας λήγει και συνεπώς δεν μπορούμε πλέον να κάνουμε ping από το PC1 στο PC2.**

2.10) Προσθέστε (stateful) κανόνα ώστε το PC2 να απαντά σε ICMP echo request ανεξάρτητα από πού προέρχονται. **ipfw add allow icmp from any to me icmptypes 8 keep-state**

2.11) Ξεκινήστε ping από PC1 στο PC2 και αφήστε το. Εκτελέστε στο PC2 την εντολή "ipfw –d show". Τι βλέπετε;

```
## Dynamic rules (1 136):
00300  22  1848 (4s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 :default
```

2.12) Σταματήστε το ping από το PC1, περιμένετε και ξαναεκτελέστε στο PC2 την προηγούμενη εντολή. Τι βλέπετε; **Ο κανόνας διεγράφη**

2.13) Προσθέστε δύο κανόνες στο τείχος προστασίας του PC2 ώστε το traceroute προς το PC2 να λειτουργεί. Ο πρώτος να επιτρέπει τη λήψη από οποιαδήποτε διεύθυνση IP των πακέτων UPD που παράγει η traceroute. Ο δεύτερος να επιτρέπει την αποστολή μηνυμάτων ICMP destination unreachable προς οποιονδήποτε προορισμό.

ipfw add allow udp from any to me, ipfw add allow icmp from me to any icmptypes 3, 11

Το traceroute λειτουργεί

2.14) Προσθέστε 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, ipfw add allow icmp from any to me icmptypes 3,11**

2.15) Ποιον κανόνα πρέπει να προσθέσετε στο PC1 ώστε να απαντά σε traceroute από οποιαδήποτε διεύθυνση IP; **ipfw add allow icmp from me to any icmptypes 3, 11**

2.16) Προσθέστε ένα (stateful) κανόνα στο τείχος προστασίας του PC2 ώστε να μπορείτε να συνδεθείτε σε αυτό με ssh από οποιονδήποτε υπολογιστή του υποδικτύου 192.168.1.0/24.

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

2.17) Με ποια εντολή επιβεβαιώσατε στο PC1 την ορθότητα του προηγούμενου κανόνα; **ssh lab@192.168.1.3**

2.18) Προσθέστε ένα (stateful) κανόνα στο τείχος προστασίας του PC2 ώστε να μπορείτε να συνδεθείτε με ssh σε οποιοδήποτε άλλο μηχάνημα. **ipfw add allow tcp from me to any 22 keep-state**

2.19) Ποιον έναν επιπλέον κανόνα πρέπει να προσθέσετε στο PC1 ώστε να δέχεται συνδέσεις ssh μόνο από το PC2; **ipfw add allow tcp from 192.168.1.3 to me 22**

2.20) Μπορείτε από το PC1 να συνδεθείτε με sftp στο PC2 ως χρήστης lab και να κατεβάσετε το αρχείο /etc/rc.conf; **Ναι μπορούμε**

2.21) Μπορείτε από το PC1 να συνδεθείτε με ftp στο PC2; Εάν όχι, προσθέστε κανόνα στο τείχος προστασίας του PC2 ώστε να επιτρέπει τη σύνδεση ftp. **Όχι δεν μπορούμε διότι το ftp χρησιμοποιεί διαφορετική θύρα tcp από το ssh**
ipfw add allow tcp from any to me 21 keep-state
2.22) Συνδεθείτε με ftp ως χρήστης lab και εκτελέστε τις εντολές "cd /usr" και "ls". Γιατί η πρώτη εκτελείται επιτυχώς ενώ η δεύτερη αποτυγχάνει; **Διότι η δεύτερη εντολή χρησιμοποιεί διαφορετική θύρα**
2.23) Ποιον κανόνα πρέπει να προσθέσετε στο τείχος προστασίας του PC2 ώστε το ftp σε passive mode να λειτουργεί;
ipfw add allow tcp from any 21 to me keep-state
2.24) Μπορείτε τώρα να κατεβάσετε ένα αρχείο από το /usr/bin του PC2 στο PC1; **Όχι**
2.25) Εάν θέλετε να λειτουργεί και το active mode του ftp, ποιον κανόνα πρέπει να προσθέσετε στο τείχος προστασίας του PC2 και ποιον στο τείχος προστασίας του PC1;
PC2: ipfw add allow tcp from me 20 to any, PC1: ipfw add allow tcp from any 20 to me
2.26) Σχολιάστε το θέμα χρήσης πρωτοκόλλων όπως το FTP και τειχών προστασίας.
Το ftp χρειάζεται δύο κανόνες τείχους προστασίας καθώς έχει δύο διαφορετικά mode λειτουργίας.
2.27) Απενεργοποιήστε το ipfw στα PC1, PC2 και επιβεβαιώστε ότι απενεργοποιήθηκε. **kldunload ipfw, kldstat**

Άσκηση 3: Απλό Network Address Translation

3.1) Ορίστε το όνομα, τη διεύθυνση IP και προεπιλεγμένη πύλη στα PC1 και PC2.

```
root@PC1:~ # hostname PC1
root@PC1:~ # ifconfig em0 192.168.1.2/24
root@PC1:~ # route add default 192.168.1.1
add net default: gateway 192.168.1.1
```

```
root@PC2:~ # hostname PC2
root@PC2:~ # ifconfig em0 192.168.1.3/24
root@PC2:~ # route add default 192.168.1.1
add net default: gateway 192.168.1.1
```

3.2) Ορίστε μέσω cli του R1 το όνομα, τη διεύθυνση IP για τη διεπαφή στο WAN1 και τη διεπαφή στο LAN2.

```
[root@router]~# cli

Hello, this is Quagga (version 0.99.17.11).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

router.ntua.lab# configure terminal
router.ntua.lab(config)# hostname R1
R1(config)# interface em0
R1(config-if)# ip address 192.0.2.2/30
R1(config-if)# interface em1
R1(config-if)# ip address 192.0.2.6/30
```

3.3) Ορίστε το όνομα, τη διεύθυνση IP και προεπιλεγμένη πύλη στο SRV1.

```
root@PC:~ # hostname SRV1
root@PC:~ # ifconfig em0 192.0.2.5/30
root@PC:~ # route add default 192.0.2.6
add net default: gateway 192.0.2.6
```

3.4) Στα PC2-SRV1 ξεκινήστε τον δαίμονα ftpd ώστε αυτά να λειτουργούν ως εξυπηρετητές FTP. **service ftpd onestart**
3.5) Ποια modules έχουν φορτωθεί στον πυρήνα του FreeBSD στο FW1;

```
root@PC:~ # kldstat
Id Refs Address        Size Name
 1   11 0x800000   196d6e4 kernel
 2    1 0xf400000     6000 intpm.ko
 3    1 0xf406000     4000 smbus.ko
 4    2 0xf40a000    2d000 ipfw.ko
 5    1 0xf437000     6000 ipfw_nat.ko
 6    1 0xf43d000     f000 libalias.ko
```

3.6) Ποιο τείχος προστασίας ενεργοποιήθηκε με την εντολή firewall_enable="YES" που θέσατε στο /etc/rc.conf; **ipfw**
3.7) Τι είδους λειτουργία του τείχους προστασίας έχει εγκατασταθεί;

```
root@PC:~ # sysrc firewall_type
firewall_type: UNKNOWN
```

3.8) Πόσους κανόνες βλέπετε στο FW1; **ipfw list -> 11** Ποιος είναι ο τελευταίος; **deny ip from any to any**
3.9) Έχουν ορισθεί πίνακες in-kernel NAT στο FW1; **ipfw nat show config -> Όχι** Εάν ναι, ποιοι;
3.10) Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1 ή στο WAN1; **Όχι, permission denied**
3.11) Μπορείτε από το SRV1 να κάνετε ping τη διεπαφή του FW1 στο WAN1; **Όχι**
3.12) Δημιουργήστε στο 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.
ipfw nat 123 config ip 192.0.2.1 reset

3.13) Προσθέστε κανόνα στο τείχος προστασίας του FW1 ώστε όλη η κίνηση IPv4 (από οποιαδήποτε πηγή προς οποιοδήποτε προορισμό) να ωθείται προς μετάφραση στον πίνακα NAT με αριθμό παρουσίας 123.
ipfw add 50 nat 123 ip from any to any
3.14) Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1 (ή στο WAN1); **Ναι**
3.15) Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή του R1 στο WAN1. **tcpdump -i emo**
3.16) Δείτε και μηδενίστε τους μετρητές πακέτων στο τείχος προστασίας του FW1. **ipfw show, ipfw zero**
3.17) Κάντε ping από το PC1 στο R1 και στείλτε τρία ICMP Echo request. **ping -c 3 192.0.2.2** Ποια η IP διεύθυνση πηγής των πακέτων ICMP echo request που βλέπετε στην καταγραφή; **192.0.2.1 (ipv4 του FW1 στο WAN1)**
3.18) Ποια η IP διεύθυνση προορισμού των ICMP Echo reply της καταγραφής στον R1; **192.0.2.1 (η ίδια)**
3.19) Ποιος κανόνας του τείχους προστασίας είναι υπεύθυνος για την επιτυχία του ping;
nat 123 ip from any to any (για τη μετάφραση των διευθύνσεων)
3.20) Πόσες φορές εφαρμόσθηκε και γιατί; **Εφαρμόστηκε 12 φορές, έχουμε 6 πακέτα (3 Echo Requests - 3 Echo Replies) και κάθε πακέτο διέρχεται από 2 διεπαφές του FW1.**
3.21) Μπορείτε από το SRV1 να κάνετε ping τη διεπαφή του FW1 στο WAN1; **Ναι**
3.22) Ποιος κανόνας είναι υπεύθυνος για την αποδοχή της προηγούμενης κίνησης; **nat 123 ip from any to any**
3.23) Ωθείται αυτή στο NAT προς μετάφραση διευθύνσεων; Γιατί;
Ναι μπορούμε να το δούμε από τους μετρητές. Ωθείται διότι ακολουθείται ο εν λόγω κανόνας
3.24) Μπορείτε από το PC2 να συνδεθείτε με ssh ως χρήστης lab στο SRV1; **ssh lab@192.0.2.5, ναι μπορούμε**
3.25) Γιατί δεν μπορείτε να κάνετε το αντίστροφο; Είναι θέμα δρομολόγησης ή NAT; Πώς το διαπιστώσατε;
Είναι θέμα δρομολόγησης. Μόλις προσπαθούμε να συνδεθούμε εμφανίζεται μήνυμα No route to host. Ακόμη και το ping αποτυγχάνει. Τα πακέτα προωθούνται από το SRV1 στο R1 λόγω προεπιλεγμένης πύλης. Ο R1 όμως δεν έχει εγγραφή σχετική με τη διεύθυνση IP του PC2 ενώ δεν έχει καθοριστεί και προεπιλεγμένη πύλη και άρα το πακέτο απορρίπτεται.
3.26) Δημιουργήστε πίνακα NAT με αριθμό παρουσίας 123 (θα αντικαταστήσει τον υπάρχοντα) επαναλαμβάνοντας τις εντολές διάρθρωσης της ερώτησης 3.12 και προσθέτοντας νέα εντολή ώστε η κίνηση προς τη διεύθυνση IPv4 του FW1 στο WAN1 να ανακατευθύνεται στο PC2. **ipfw nat 123 config if em1 reset redirect_addr 192.168.1.3 192.0.2.1**
3.27) Από το SRV1 συνδεθείτε με ssh ως χρήστης lab στη διεύθυνση 192.0.2.1. Είναι η προσπάθεια επιτυχής; **Ναι**
Εάν ναι, σε ποιο μηχάνημα συνδεθήκατε; **Στο PC2**Πως το εξακριβώσατε; **Από το hostname**
3.28) Δημιουργήστε πίνακα NAT με αριθμό παρουσίας 123 επαναλαμβάνοντας τις εντολές διάρθρωσης της ερώτησης 3.26 και προσθέτοντας νέα εντολή ώστε η κίνηση tcp για τη θύρα 22 να ανακατευθύνεται στο PC1 στην αντίστοιχη θύρα.
ipfw nat 123 config if em1 reset redirect_addr 192.168.1.3 192.0.2.1 redirect_port tcp 192.168.1.2:22 22
3.29) Συνδεθείτε και πάλι από το SRV1 με ssh ως χρήστης lab στη διεύθυνση 192.0.2.1. **ssh lab@192.0.2.1**
Σε ποιο μηχάνημα συνδέεστε τώρα και πώς το εξακριβώνετε; **Στο PC1 λόγω hostname**
3.30) Συνδεθείτε από το SRV1 με ftp ως χρήστης lab στη διεύθυνση 192.0.2.1. **ftp lab@192.0.2.1**
Σε ποιο μηχάνημα συνδέεστε και πώς το εξακριβώνετε; **Στο PC2 από το hostname. Στο PC1 ανακατευθύνεται η κίνηση μόνο για τη θύρα 22 η οποία δεν χρησιμοποιείται στην περίπτωση του ftp.**
3.31) Μπορείτε να δείτε τα περιεχόμενα το φακέλου /etc και να κατεβάσετε το αρχείο rc.conf; **Ναι**
3.32) Ποιο μηχάνημα απαντά εάν από το PC1 κάνετε ftp στη διεύθυνση 192.0.2.1; **Το PC2**
3.33) Σε ποιο μηχάνημα θα συνδεθείτε εάν από το PC2 κάνετε ssh στη διεύθυνση 192.0.2.1; **Στο PC1**

Άσκηση 4: Τείχος προστασίας και NAT

4.1) Με την εντολή "ipfw disable one_pass" απενεργοποιήστε τη λειτουργία one-pass, διατηρήστε όμως τον ορισμό του πίνακα NAT της ερώτησης 3.28. Μπορείτε τώρα να κάνετε ping από το PC1 στη διεπαφή του FW1 στο LAN1 ή από το SRV1 στη διεπαφή του FW1 στο WAN1; **ipfw disable one_pass, όχι δεν είναι το ping επιτυχές**

4.2) Γίνονται δεκτά τα πακέτα από τον κανόνα ώθησης στο NAT της ερώτησης 3.13; Εάν ναι, γιατί αποτυγχάνει το ping; **Από τους μετρητές των κανόνων συμπεραίνουμε ότι τα πακέτα γίνονται δεκτά από τον κανόνα ώθησης στο NAT της ερώτησης 3.13. Το ping αποτυγχάνει διότι έχουμε ενεργοποιήσει την λειτουργία one_pass και δεν υπάρχει επόμενος κανόνας που να αποδέχεται τα πακέτα ip. Συνεπώς τα πακέτα ακολουθούν τον τελευταίο κανόνα 65535 deny ip from any to any ο οποίος τα απορρίπτει.**

4.3) Ως πρώτο βήμα πρέπει να επιτρέψετε την εντός του εταιρικού δικτύου κίνηση. Διαγράψτε τον προηγούμενο κανόνα και προσθέστε νέο με αύξοντα αριθμό 1100 που να επιτρέπει όλη την κίνηση μέσω διεπαφής του FW1 στο LAN1. **ipfw delete 50, ipfw add 1100 allow all from any to any via em0**

4.4) Είναι τώρα το ping από το PC1 προς οποιαδήποτε διεπαφή του FW1 επιτυχές; **Ναι**

4.5) Σε ποιο μηχάνημα θα συνδεθείτε εάν από το PC2 κάνετε ssh στη διεύθυνση 192.0.2.1;

Στο FW1 διότι διαγράψαμε τον κανόνα μετασχηματισμού για τον πίνακα NAT.

4.6) Ποιοι κανόνες είναι υπεύθυνοι για ό,τι παρατηρήσατε προηγουμένως;

allow ip from any to any via em0, allow ip from any to any via lo0

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 προσθέστε 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. **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. Προσθέστε αμέσως επόμενο κανόνα με αύξοντα αριθμό 3001 που να αποδέχεται οποιαδήποτε κίνηση μετά τη μετάφραση. **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 προσθέστε 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.

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

4.10) Στη συνέχεια θα εγκαταστήσετε (stateful) κανόνες. Προσθέστε κανόνα με αύξοντα αριθμό 2001 που να ελέγχει εάν η κίνηση έχει γίνει αποδεκτή από δυναμικό κανόνα. **ipfw add 2001 check-state**

4.11) Ποιο μηχάνημα απαντά εάν κάνετε ping από το PC1 στη διεύθυνση 192.0.2.1; **Το FW1 (λόγω του κανόνα 1100)**

4.12) Ποιο μηχάνημα απαντά εάν κάνετε ping από το SRV1 στη διεύθυνση 192.0.2.1; **Το PC2 (λόγω του κανόνα 2000)**

4.13) Σε ποιο μηχάνημα συνδέεστε εάν κάνετε ssh από το PC1 στη διεύθυνση 192.0.2.1; **FW1**

4.14) Σε ποιο μηχάνημα συνδέεστε εάν κάνετε ssh από το SRV1 στη διεύθυνση 192.0.2.1; **PC1**

4.15) Σε ποιο μηχάνημα συνδέεστε εάν κάνετε ftp από το SRV1 στη διεύθυνση 192.0.2.1; **PC2**

4.16) Μπορείτε να κάνετε ping από το PC1 στο SRV1; **Ναι**

4.17) Μπορείτε να συνδεθείτε με ssh από το PC1 στο SRV1; **Ναι**

4.18) Μπορείτε από το PC1 να συνδεθείτε με ftp ως χρήστης lab στο SRV1, να δείτε τα περιεχόμενα κάποιου φακέλου και να κατεβάσετε ένα αρχείο; **Ναι**

4.19) Οι προηγούμενοι κανόνες ώθησης στο NAT επιτυγχάνουν τη μετάφραση διευθύνσεων αλλά επιτρέπουν οποιαδήποτε κίνηση ανεξάρτητα από το κατά πόσον αυτή είναι επιθυμητή. Προσθέστε 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. **ipfw add 2999 deny all from any to any via em1**

4.20) Ποια από τα ping, ssh ftp των προηγούμενων ερωτήσεων επιτυγχάνουν;

Συνδέσεις με "αφετηρία" το LAN1 και στόχο διεπαφή του FW1.

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

4.22) Μπορείτε να κάνετε ping από το PC1 στο SRV1; **Ναι**

4.23) Προσθέστε (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.

ipfw add 2500 skipto 3000 tcp from any to any 22 out via em1 keep-state

4.24) Μπορείτε να συνδεθείτε με ssh από το PC1 στο SRV1; **Ναι**

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. Προσθέστε (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 IP πηγής και προορισμού, να στέλνεται (skipto) στη μετάφραση NAT του κανόνα 3000.

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

4.26) Ποιο μηχάνημα απαντά εάν κάνετε ping από το SRV1 στη διεύθυνση 192.0.2.1; **Το PC2**

4.27) Προσθέστε (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.

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

4.28) Σε ποιο μηχάνημα συνδέεστε εάν από το SRV1 κάνετε ssh ως χρήστης lab στη διεύθυνση 192.0.2.1; **Στο PC1**

4.29) Επιτυγχάνει τώρα το ftp από το SRV1 στη διεύθυνση 192.0.2.1; **Όχι**

4.30) Ποιους δύο νέους κανόνες πρέπει να προσθέσετε ώστε να λειτουργεί το προηγούμενο ftp σε active mode;

ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state

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

Άσκηση 5: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

5.1) Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο LAN1; **192.168.1.1**

5.2) Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο WAN1; **10.0.0.1**

5.3) Ποιο είναι το ποσοστό της ελεύθερης μνήμης που βλέπετε στο FW1; **Memory Usage 34%**

5.4) Πόσες διεπαφές δικτύου βλέπετε συνολικά στο FW1; **4 Από console 1η επιλογή**

Επιβεβαιώστε ότι στο VirtualBox οι κάρτες δικτύου έχουν το σωστό τρόπο δικτύωσης και βρίσκονται στα σωστά υποδίκτυα. Εάν όχι διορθώστε.

5.5) Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή DMZ του FW1; **Interfaces -> DMZ -> IP address: 172.22.1.1**

5.6) Ποιο είναι το όνομα (hostname) του FW1; **System -> General Setup -> Hostname: fw**

5.7) Αλλάξτε το hostname του FW1 σε "fw1". **Hostname: fw -> Save**

5.8) Στο μενού Firewall Rules του FW1 υπάρχουν κανόνες για το WAN; **Όχι**

5.9) Ορίστε τη σωστή διεύθυνση και προεπιλεγμένη πύλη του FW1 στο WAN1 και επιλέξτε "Block private networks".

Interfaces -> WAN -> IP address: 192.0.2.1/30, Gateway: 192.0.2.2, Block Private Networks, Save

5.10) Στο μενού Firewall Rules του FW1 υπάρχουν τώρα κανόνες για το WAN; **Ναι**

5.11) Βλέπετε να είναι ενεργοποιημένη κάποια υπηρεσία από αυτές των κατηγοριών "Services" και "VPN"; **Όχι**

5.12) Ενεργοποιήστε την υπηρεσία DNS forwarder. **Services -> DNS forwarder -> Enable DNS forwarder**

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

Services -> DHCP Server -> Enable -> Range 192.168.1.2 to 192.168.1.3

5.14) Στο PC1 ξεκινήστε τον πελάτη DHCP. **dhclient emo** Ποια είναι η διεύθυνση IP: **192.168.1.2**
η προεπιλεγμένη πύλη: **192.168.1.1** και η διεύθυνση εξυπηρετητή DNS που αποδόθηκε;: **192.168.1.1**

5.15) Γιατί χρειάστηκε η ενεργοποίηση της υπηρεσίας DNS forwarder;

Ώστε το firewall να λειτουργήσει και σαν DNS server

5.16) Σε πιο μέρος του μενού Diagnostics μπορείτε να δείτε ότι έχει αποδοθεί η συγκεκριμένη διεύθυνση στο PC1;

Diagnostics -> DHCP Leases

5.17) Πόσες εγγραφές ARP βλέπετε στο μενού Diagnostics -> ARP Table; **6**

5.18) Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1; **Όχι**

5.19) Στο μενού Diagnostics -> Logs καρτέλα Firewall τι βλέπετε; **Βλέπουμε έναν error log με 50 εγγραφές**
Καθαρίστε το αρχείο καταγραφών. **-> Clear log**

5.20) Πόσα firewall states βλέπετε από το αντίστοιχο μενού στο Diagnostics; **10 (2 διαφορετικά conncections)**

5.21) Πόσους κανόνες για το LAN βλέπετε από το μενού Firewall -> Rules; **Κανένα**

5.22) Προσθέστε στο FW1 κανόνα ώστε να επιτρέψετε όλη την κίνηση από το LAN1.

Firewall -> Rules -> LAN -> 'Add new rule' -> interface LAN from any to any

5.23) Μπορείτε τώρα από το PC1 να κάνετε ping τις διεπαφές του FW1 στα LAN1, WAN1, DMZ; **Ναι**

5.24) Από τον R1 μπορείτε να κάνετε ping τη διεπαφή του FW1 στο WAN1; **Όχι**

5.25) Εμφανίστε πίνακα ARP στον R1. **arp -a** Βλέπετε εγγραφή για τη διεύθυνση MAC της διεπαφής του FW1 στο WAN1; **Ναι βλέπουμε**

5.26) Προσθέστε στο FW1 κανόνα ώστε να επιτρέψετε όλη την εισερχόμενη ICMP κίνηση με προορισμό την "WAN Address".

☐	↑	ICMP	*	*	WAN address	*

5.27) Μπορείτε τώρα από τον R1 να κάνετε ping τη διεπαφή του FW1 στο WAN1; **Ναι**

5.28) Μπορείτε από τον R1 να κάνετε ping το PC1; Γιατί;

Δεν υπάρχει αντίστοιχη εγγραφή στον πίνακα δρομολόγησης του R1 (και δεν υπάρχει ούτε προεπιλεγμένη πύλη)

5.29) Μπορείτε από το PC1 να κάνετε ping τον R1; **Ναι** Τι συμπεραίνετε όσον αφορά τη λειτουργία NAT;

Γίνεται μετάφραση των διευθύνσεων του ιδιωτικού δικτύου με τη διεύθυνση της διεπαφής του Firewall στο WAN1.

5.30) Εάν δεν το έχετε ήδη κάνει, τοποθετήστε το SRV1 στο DMZ και ορίστε τη διεύθυνση IPv4 όπως στο σχήμα.
Μπορείτε από το PC1 να κάνετε ping τον SRV1; **Όχι**
Γιατί; **Δεν έχουμε ορίσει προεπιλεγμένη πύλη στο SRV1**

5.31) Ορίστε τη σωστή προεπιλεγμένη πύλη στον SRV1. **route add default 172.22.1.1**

5.32) Μπορείτε τώρα από το PC1 να κάνετε ping τον SRV1; **Ναι (Δεν χρειάζεται κανόνας για το DMZ?)**

5.33) Μπορείτε από τον SRV1 να κάνετε ping τη διεπαφή του FW1 στο DMZ; Γιατί;

Όχι διότι δεν έχουμε ορίσει σχετικό κανόνα για τη κίνηση δια μέσου της διεπαφής DMZ του FW1.

5.34) Μπορείτε από τον SRV1 να κάνετε ping το PC1 ή το R1; Γιατί;

Όχι διότι δεν υπάρχει κανόνας στο firewall για την διέλευση πακέτων δια μέσω του DMZ.

5.35) Προσθέστε στο FW1 κανόνα ώστε να επιτρέψετε εξερχόμενη κίνηση από το DMZ προς οποιονδήποτε προορισμό πλην του LAN1.

Proto	Source	Port	Destination	Port	Description
*	DMZ net	*	! LAN net	*	

5.36) Μπορείτε τώρα από τον SRV1 να κάνετε ping τη διεπαφή του FW1 στο DMZ; **Ναι**

5.37) Μπορείτε τώρα από τον SRV1 να κάνετε ping τη διεπαφή του FW1 στο WAN1; **Ναι**

5.38) Μπορείτε από τον R1 να κάνετε ping τον SRV1; **Όχι** Γιατί;

Δεν υπάρχει αντίστοιχη εγγραφή στον πίνακα δρομολόγησης του R1 αλλά και ούτε προεπιλεγμένη πύλη.

5.39) Μπορείτε από τον SRV1 να κάνετε ping τον R1; Αιτιολογήστε. **Ναι γιατί αφενός υπάρχει προεπιλεγμένη πύλη για το SRV1 και αφετέρου έχουν ορισθεί οι απαραίτητοι κανόνες για να επιτραπεί η κίνηση δια μέσου του FW1.**

5.40) Στο PC2 ξεκινήστε τον πελάτη DHCP. Ποια είναι η διεύθυνση IP: **192.168.1.3** η προεπιλεγμένη πύλη: **192.168.1.1** και η διεύθυνση εξυπηρετητή DNS που αποδόθηκε;: **192.168.1.1**

5.41) Προσθέστε στο FW1 κανόνα "Block", ώστε να απαγορεύσετε στο LAN1 όλη την κίνηση από το PC2 προς το SRV1.

*	192.168.1.3	*	172.22.1.2	*	

5.42) Πρέπει ο κανόνας να τοποθετηθεί πριν ή μετά από αυτόν που υπάρχει; Γιατί;

Πρέπει να τοποθετηθεί πριν από τον ήδη υπάρχοντα καθώς οι κανόνες ελέγχονται σειριακά και ο πρώτος κανόνας είναι πιο γενικός, συνεπώς θα περνάει όλη η κίνηση.

5.43) Μπορείτε από το PC2 να κάνετε ping τον SRV1; **Όχι**

5.44) Μπορείτε από το PC2 να κάνετε ping τη διεπαφή του FW1 στο DMZ; Γιατί; **Ναι μπορούμε διότι ο κανόνας που δημιουργήσαμε προηγουμένως μπλοκάρει μόνο τη κίνηση με προορισμό την 172.22.1.2**

Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT

6.1) Προσθέστε στον R1 στατική εγγραφή για το 203.0.118.0/24 προς το FW1 ώστε η κίνηση προς το υποδίκτυό σας να διέρχεται μέσω του τείχους προστασίας. **route add 203.0.118.0/24 192.0.2.1**

6.2) Στο μενού Firewall NAT του FW1 σελίδα Outbound ενεργοποιήστε το "advanced outbound NAT". Με αυτό τον τρόπο απενεργοποιείτε (δείτε και σχετική σημείωση) την αυτόματη δημιουργία κανόνων για απερχόμενη κίνηση (outbound NAT). **Firewall -> NAT -> Outbound -> Enable advanced outbound NAT -> Save**

6.3) Προσθέστε αντιστοίχιση outbound NAT ώστε το PC1 να εμφανίζεται στον έξω κόσμο με τη διεύθυνση 203.0.118.14 και ενεργοποιήστε την.

Interface	Source	Destination	Target	Description
WAN	192.168.1.2/32	*	203.0.118.14	

6.4) Προσθέστε αντιστοίχιση outbound NAT ώστε το PC2 να εμφανίζεται στον έξω κόσμο με τη διεύθυνση 203.0.118.15 και ενεργοποιήστε την.

WAN	192.168.1.3/32	*	203.0.118.15	

6.5) Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή του R1 και αφήστε τη να τρέχει. **tcpdump -i emo**

6.6) Μπορείτε να κάνετε ping από PC1, PC2 στον R1; Αν ναι, με ποια διεύθυνση IP φτάνουν τα πακέτα από τα PC1, PC2; **Μπορούμε να κάνουμε ping από PC1, PC2 στον R1 και τα πακέτα φτάνουν με την διεύθυνση αντιστοίχισης.**

6.7) Από νέο παράθυρο εντολών στον R1 κάντε ping στο PC1 χρησιμοποιώντας τη διεύθυνση 203.0.118.14; Για ποιο λόγο αποτυγχάνει; **Έχουμε ορίσει το NAT μόνο ως outbound και συνεπώς δεν γίνεται αντιστοίχιση των διευθύνσεων IPv4 για τα εισερχόμενα πακέτα.**

6.8) Από το μενού Firewall NAT του FW1 σελίδα "Server NAT" προσθέστε αντιστοίχιση για την IP διεύθυνση 203.0.118.18 και ενεργοποιήστε την. **Firewall -> NAT -> Server NAT -> External IP address: 203.0.118.18**

6.9) Από το μενού Firewall NAT του FW1 σελίδα "Inbound" προσθέστε 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 επιλέξετε το "Auto-add a firewall rule to permit traffic through this NAT rule", ενεργοποιήστε την.

If	Proto	Ext. port range	NAT IP	Int. port range	Description
WAN	TCP	22 (SSH)	172.22.1.2 (ext.: 203.0.118.18)	22 (SSH)	

6.10) Ποιος κανόνας τοποθετείται αυτόματα στο Firewall για τη διεπαφή WAN και γιατί;

TCP	*	*	172.22.1.2	22 (SSH)	NAT

6.11) Μπορείτε από τον R1 να συνδεθείτε με ssh στο 203.0.118.18; Σε ποιο σύστημα συνδέεστε;

Ναι μπορούμε, συνδεόμαστε στο SRV1 λόγω του κανόνα NAT που δημιουργήσαμε προηγουμένως

6.12) Μπορείτε από τον R1 να κάνετε ping το 203.0.118.18; **Όχι** Ποιος είναι ο λόγος της αποτυχίας;

Ο κανόνας που προσθέσαμε αφορά μόνο για ssh σύνδεση (διαφορετική tcp θύρα)

6.13) Μπορείτε να συνδεθείτε με ssh από το PC2 στο SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.118; **Ναι μπορούμε** Εάν ναι, ποια διαδρομή ακολουθούν τα πακέτα IP από το PC2 προς το SRV1 και αντιστρόφως; Πώς το επιβεβαιώνετε; **Ακολουθούν τη διαδρομή μέσω R1. Το επιβεβαιώνουμε από το tcpdump στο R1.**
6.14) Καταργήστε την outbound NAT αντιστοίχιση για το PC1. Μπορείτε να κάνετε ping στον R1 από το PC1; Γιατί; Firewall -> NAT -> Outbound -> 'delete selected mappings'. **'Οχι δεν μπορούμε να κάνουμε ping γιατί υπάρχει εγγραφή στο τείχος προστασίας που μπλοκάρει πακέτα από private addresses.**
6.15) Καταργήστε το advanced outbound NAT. Είναι το ping προς τον R1 επιτυχές; **Ναι, πλέον γίνεται η αντιστοίχιση με τη διεύθυνση της διεπαφής του FW1 στο WAN1 και τα πακέτα που φθάνουν στον R1 έχουν διεύθυνση 192.0.2.1.**
6.16) Εξακολουθείτε να μπορείτε να συνδέεστε από τον R1 στο SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.18; **Ναι.**Ισχύει το ίδιο για τα PC1, PC2; **Από το PC2 δεν μπορούμε γιατί υπάρχει κανόνας που μπλοκάρει τη σχετική κίνηση.**
6.17) Ξεκινήστε μια καταγραφή πακέτων στο SRV1 και άλλη στο R1 εμφανίζοντας επικεφαλίδες Ethernet. **tcpdump -i emo -e** Επιχειρήστε πάλι να συνδεθείτε με SSH από το PC2 στο SRV1. **ssh lab@172.22.1.2** Εξηγήστε γιατί αποτυγχάνει η σύνδεση tcp. **Connection refused από το τείχος προστασίας**
6.18) Για τη συμπεριφορά που παρατηρήσατε προηγουμένως είναι υπεύθυνος ο κανόνας Block που θέσατε στην ερώτηση 5.41 ή ο κανόνας για το DMZ στην ερώτηση 5.35; Εάν όχι, ποιος είναι ο λόγος;
Υπεύθυνος είναι ο κανόνας Block που θέσαμε στην ερώτηση 5.41 καθώς παρατηρούμε ότι δεν φθάνουν πακέτα στα μηχανήματα R1, SRV1. Συνεπώς μπλοκάρονται από το τείχος προστασίας.

Άσκηση 7: IPSec site-to-site VPN

7.1) Αποσυνδέστε από το Virtualbox το καλώδιο της κάρτας δικτύου #3 του FW1.
Στο παράθυρο του FW1 δεξί κλικ στο "Computers" Icon και κλικ στη 3η κάρτα δικτύου.
7.2) Συνδεθείτε από browser στο FW2 και αλλάξτε τη IP στη διεπαφή MNG από 192.168.56.2 σε 192.168.56.3.
Interfaces -> MNG -> IP address 192.168.56.3/24
7.3) Ξανασυνδέστε από το Virtualbox το καλώδιο της κάρτας δικτύου #3 του FW1.
Στο παράθυρο του FW1 δεξί κλικ στο "Computers" Icon και κλικ στη 3η κάρτα δικτύου.
7.4) Μπορείτε να συνδεθείτε ταυτόχρονα από τον browser του φιλοξενούντος μηχανήματος στα δύο τείχη προστασίας; Ναι για το FW1: http://192.168.56.2 ενώ για το FW2: http://192.168.56.3
7.5) Αλλάξτε το hostname του FW2 σε "fw2". **System -> General Setup -> hostname: fw2**
7.6) Ορίστε τη διεύθυνση και προεπιλεγμένη πύλη του FW2 στο WAN2, επιλέγοντας το "Block private networks".
Interfaces -> WAN -> ip address: 192.0.2.5/30, Gateway: 192.0.2.6
7.7) Ορίστε τη σωστή διεύθυνση του FW2 στο LAN2. **Interfaces -> LAN -> ip address: 192.168.2.1/24**
7.8) Επανεκκινήστε το FW2. **Δίνουμε την τιμή 5 (reboot system) στο command line**
7.9) Προσθέστε στο FW2 κανόνα ώστε να επιτρέψετε όλη την κίνηση από το LAN2. **Firewall -> Rules**

Proto	Source	Port	Destination	Port	Description
*	*	*	*	*	Allow all traffic from LAN2

7.10) Προσθέστε κανόνα ώστε να επιτρέψετε όλη την εισερχόμενη ICMP κίνηση με προορισμό την "WAN Address".

ICMP	*	*	WAN address	*	Allow incoming ICMP traffic with "WAN Address" destination

7.11) Μετακινήστε το PC2 στο LAN2. Ορίστε τη σωστή διεύθυνση και προεπιλεγμένη πύλη στο PC2.
ifconfig emo 192.168.2.2/24, route add default 192.168.2.1
7.12) Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW2 στο WAN2; **Ναι**
7.13) Μπορείτε από το PC2 να κάνετε ping τη διεπαφή του FW1 στον WAN1; **Ναι**
7.14) Μπορείτε από το PC1 να κάνετε ping το PC2 ή το αντίστροφο. **'Οχι** Τεκμηριώστε την απάντησή σας.

Δεν υπάρχουν εγγραφές για τα LAN στον R1 και ούτε υπάρχει προεπιλεγμένη πύλη. Συνεπώς τα πακέτα απορρίπτονται

7.15) Στο μενού VPN του FW1 ενεργοποιήστε το IPSec. **VPN -> IPsec -> Enable IPSec**

Μετά δημιουργήστε 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 κάποια λέξη (π.χ. το όνομά σας) και ενεργοποιήστε το.

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

7.16) Ποιο κανόνα βλέπετε στο FW1 -> Firewall -> Rules -> IPsec VPN;

Proto	Source	Port	Destination	Port	Description
*	*	*	*	*	Default IPsec VPN

7.17) Στο FW1 -> Diagnostics -> IPSec -> Security Association Database (SAD) βλέπετε να έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων; **Όχι**

7.18) Στο FW1 -> Diagnostics -> IPSec -> Security Policy Database (SPD) βλέπετε να έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων;

Source	Destination	Direction	Protocol	Tunnel endpoints
192.168.2.0/24	192.168.1.0/24	→	ESP	192.0.2.5 - 192.168.1.1
192.168.1.0/24	192.168.2.0/24	←	ESP	192.168.1.1 - 192.0.2.5

7.19) Στο μενού VPN του FW2 ενεργοποιήστε το IPSec. Μετά δημιουργήστε 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 τη λέξη που δηλώσατε προηγουμένως στην ερώτηση 7.15 και ενεργοποιήστε το.

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	

7.20) Στο FW2 -> Diagnostics -> IPSec -> Security Association Database (SAD) βλέπετε να έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων; **Όχι**

7.21) Στο FW2 -> Diagnostics -> IPSec -> Security Policy Database (SPD) βλέπετε να έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων;

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

7.22) Μπορείτε από το PC1 να κάνετε ping το PC2; **Ναι**

7.23) Μπορείτε από το PC2 να κάνετε ping το PC1; **Ναι**

7.24) Άλλαξε κάτι στο FW1 -> Diagnostics -> IPSec -> SAD; **Προστέθηκαν 2 εγγραφές**

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.168.1.1	192.0.2.5	ESP	0207c816	3des-cbc	hmac-sha1
192.0.2.5	192.168.1.1	ESP	0b492dd4	3des-cbc	hmac-sha1

7.25) Άλλαξε κάτι στο FW2 -> Diagnostics -> IPSec -> SAD; **Προστέθηκαν 2 εγγραφές**

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.5	192.0.2.1	ESP	0b492dd4	3des-cbc	hmac-sha1
192.0.2.1	192.0.2.5	ESP	0207c816	3des-cbc	hmac-sha1

7.26) Ξεκινήστε μια καταγραφή στον R1 στο WAN1 εμφανίζοντας λεπτομέρειες και το περιεχόμενο των πακέτων και αφήστε την να τρέχει. **tcpdump -i emo -e -vvv**

7.27) Παρατηρείτε πακέτα ICMP όταν κάνετε ping από ένα PC στο άλλο; **Όχι**

7.28) Τι είδους πακέτα εμφανίζονται, ποια είναι η πηγή και ποιος ο προορισμός τους;

Πακέτα ESP, Source: 192.0.2.1, Target: 192.0.2.5

7.29) Υπάρχει κάπου η πληροφορία για τις διευθύνσεις IP των PC1, PC2; **Όχι**

7.30) Μπορείτε από το PC2 να συνδεθείτε με SSH στο SRV1 στη διεύθυνση 203.0.118.18; **Ναι** Εάν ναι, τι άλλαξε σε σχέση με την προηγούμενη άσκηση;

Άλλαξε η διεύθυνση IP του PC2 και συνεπώς ο κανόνας που μπλόκαρε την κίνηση δεν είναι σε ισχύ πλέον.

7.31) Τι πακέτα παρατηρείτε στην καταγραφή, ποιες είναι οι διευθύνσεις IP και θύρες πηγής και προορισμού τους;

TCP, Source: 192.0.2.5 - Port: 60281, Target: 203.0.118.18 - Port: 18

7.32) Είναι κρυπτογραφημένα; Με το IPsec; **Ναι**