Ονοματεπώνυμο: Βασιλάκος Μιχαήλ
Ομάδα: 2
Όνομα PC: laptop
Ημερομηνία: 25/5/22

Άσκηση 1: Ένα απλό τείχος προστασίας

1.1 kldload ipfw
1.2 kldstat
1.3 το ping αποτυγχάνει με μήνυμα λάθους "permission denied"
1.4 ipfw list
1.5 ipfw show
1.6 ipfw zero 65535
1.7 ipfw add 100 allow all from any to any via lo0
1.8 τα ping τώρα λειτουργούν επιτυχώς
1.9 δεν μπορούμε να κάνουμε ping από το PC1 στο PC2 καθώς εμφανίζεται το ίδιο μήνυμα λάθους με πριν - "permission denied"
1.10 ipfw add allow icmp from any to any
1.11 ο κανόνας έλαβε τον αριθμό 200
1.12 το ping λειτουργεί επιτυχώς και από τις δύο πλευρές
1.13 traceroute 192.168.1.3
το traceroute αποτυγχάνει διότι χρησιμοποιεί πακέτα UDP, τα οποία δεν επιτρέπονται από το firewall
για να λάβουμε απάντηση από το PC2 αρκεί να αλλάξουμε τον τύπο των πακέτων σε ICMP αλλάζοντας την εντολή σε *traceroute -I 192.168.1.3*
1.14 ipfw add allow udp from any to any 33434-33523
1.15 ssh 192.168.1.3 -l lab
η σύνδεση αποτυγχάνει με μήνυμα "permission denied"
1.16 ipfw add allow tcp from any to any established
ipfw add allow tcp from me to any
1.17 ipfw zero
ssh 192.168.1.3 -l lab
1.18 ο κανόνας *allow tcp from me to any 22* εφαρμόστηκε μία μόνο φορά κατά τη δημιουργία της σύνδεσης, ενώ ο *allow tcp from any to any established* εφαρμόστηκε 69 φορές, μία φορά για κάθε πακέτο που στάλθηκε ή λήφθηκε κατά τη σύνδεση
1.19 ssh 192.168.1.2 -l lab
δεν μπορούμε να συνδεθούμε γιατί το firewall στο PC1 δεν επιτρέπει τη λήψη πακέτων TCP που δεν βρίσκονται σε ήδη υπάρχουσα σύνδεση και η σύνδεση επιτρέπεται μόνο όταν ξεκινά από τον PC1
1.20 service ftpd onestart
1.21 ftp 192.168.1.3
η σύνδεση είναι επιτυχής

Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

2.1 kldload ipfw
2.2 ping -c 1 192.168.1.2
το ping αποτυγχάνει με μήνυμα λάθους "permission denied"
2.3 ipfw add allow all from any to any via lo0
2.4 ipfw add allow icmp from me to any icmptypes 8
2.5 στο ping δεν εμφανίζεται πλέον το προηγούμενο μήνυμα λάθους, όμως εξακολουθεί να μη λειτουργεί

2.6 τα πακέτα icmp request περνούν από το τείχος προστασίας αφού έχουμε ορίσει τον κατάλληλο κανόνα, όμως τα αντίστοιχα icmp reply δεν περνούν καθώς δεν επιτρέπεται εισερχόμενη κίνηση στο PC2
αυτό μπορούμε να το επιβεβαιώσουμε μηδενίζοντας τους μετρητές των κανόνων και πραγματοποιώντας ping με την εντολή *ping -c 1 192.168.1.2*, αφού θα παρατηρήσουμε πως ο κανόνας *allow icmp from me to any icmptypes 8* έχει μετρητή 1 όπως και ο default κανόνας, δηλαδή η απάντηση απορρίφθηκε σιωπηλά

2.7 ipfw delete 200
ipfw add allow icmp from me to any icmptypes 8 keep-state
το ping τώρα είναι επιτυχές

2.8 το ping από το PC1 στο PC2 επιτυγχάνει όσο τρέχει το ping από το PC2 στο PC1

2.9 το ping από το PC1 στο PC2 δεν επιτυγχάνει διότι πριν είχε ξεκινήσει ping από το PC2 στο PC1 και γίνονταν δεκτά πακέτα ICMP από το PC1, ενώ τώρα η εγγραφή για την ανταλλαγή πακέτων ICMP με το PC1 διαγράφηκε και τα πακέτα απορρίπτονται

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

2.11 ipfw -d show
βλέπουμε πως δημιουργήθηκε δυναμικός κανόνας ο οποίος διατηρεί την κατάσταση της σύνδεσης μεταξύ PC1 και PC2 για την ανταλλαγή πακέτων ICMP

2.12 βλέπουμε πως ο δυναμικός κανόνας διαγράφηκε

2.13 ipfw add allow udp from any to me 33434-33523
ipfw add allow icmp from me to any icmptypes 3

2.14 ipfw add allow udp from me to any 33434-33523
ipfw add allow icmp from any to me icmptypes 3

2.15 ipfw add allow icmp from me to any icmptypes 3

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

2.17 ssh 192.168.1.3 -l lab

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 keep-state

2.20 sftp lab@192.168.1.3
get /etc/rc.conf
καταφέραμε να κατεβάσουμε το αρχείο επιτυχώς

2.21 ftp lab@192.168.1.3
η σύνδεση αποτυγχάνει χωρίς να λάβουμε μήνυμα σφάλματος
για να συνδεθούμε προσθέτουμε τον παρακάτω κανόνα στο PC2
ipfw add allow tcp from any to me 21 keep-state

2.22 ftp lab@192.168.1.3
μέσω του τείχους προστασίας έχουμε επιτρέψει τη σύνδεση και επικοινωνία μόνω μέσω του command port και όχι μέσω του data port, το οποίο και σημαίνει πως επιτρέπουμε την αποστολή εντολών στο PC2 όχι όμως και την ανταλλαγή δεδομένων, οπότε η εντολή ls που επιστρέφει δεδομένα για τα αρχεία του working directory δεν ολοκληρώνεται

2.23 ipfw add allow tcp from any to me 49152-65534

2.24 μπορέσαμε να κατεβάσουμε το αρχείο vi από το /usr/bin του PC2 στο PC1

2.25 στο firewall του PC2 θα προσθέσουμε τον κανόνα
ipfw add allow tcp from me 20 to any keep-state
ενώ στο firewall του PC1 θα πρέπει να επιτρέψουμε τη δημιουργία σύνδεσης από εξωτερική διεύθυνση με τον κανόνα
ipfw add allow tcp from any 20 to me keep-state

2.26 η χρήση των διαφόρων πρωτοκόλλων απαιτεί από τα τείχη προστασίας και των δύο πλευρών της σύνδεσης να έχουν τους κατάλληλους κανόνες για την επιτυχή χρήση τους
το κάθε πρωτόκολλο μπορεί να χρησιμοποιεί πλήθος πρωτοκόλλων μεταφοράς, θυρών πηγής και προορισμού και συνεδριών tcp οπότε απαιτείται ξεχωριστή

φροντίδα από μέρους του διαχειριστή δικτύου για την ικανοποίηση όλων των συνθηκών για τη λειτουργία του
τέλος, παρατηρούμε πως σε πρωτόκολλα όπως το passive ftp δεν γνωρίζουμε εκ των προτέρων τη θύρα προορισμού του πρώτου πακέτου της συνεδρίας tcp, οπότε πρέπει να ανοίξουμε την πρόσβαση σε πολλές θύρες εκθέτοντας τον υπολογιστή σε μεγαλύτερο κίνδυνο

2.27 kldunload ipfw

Άσκηση 3: Απλό Network Address Translation

3.1 PC1:
hostname PC1
ifconfig em0 192.168.1.2/24
route add default 192.168.1.1
PC2:
hostname PC2
ifconfig em0 192.168.1.3/24
route add default 192.168.1.1

3.2 configure terminal
hostname R1
interface em0 -> ip address 192.0.2.6/30
interface em1 -> ip address 192.0.2.2/30

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

3.4 service ftpd onestart

3.5 kldstat
τα modules που έχουν φορτωθεί στον πυρήνα του FW1 είναι τα ipfw, ipfw_nat και libalias

3.6 το firewall που ενεργοποιήθηκε με την εντολή αυτή είναι το ipfw

3.7 sysrc firewall_type
η τιμή της μεταβλητής είναι UNKNOWN

3.8 βλέπουμε 11 κανόνες
ο τελευταίος είναι ο προκαθορισμένος κανόνας για τη σιωπηλή απόρριψη των πακέτων που δεν ταιριάζουν σε κανέναν από τους υπόλοιπους κανόνες

3.9 ipfw nat show config
δεν έχει οριστεί κανένας πίνακας NAT

3.10 το ping και στις δύο διεπαφές αποτυγχάνει χωρίς μήνυμα λάθους

3.11 το ping αποτυγχάνει χωρίς μήνυμα λάθους

3.12 ipfw nat 123 config if em1 reset

3.13 ipfw add nat 123 ipv4 from any to any

3.14 το ping από το PC1 τώρα είναι επιτυχές και προς τις δύο διεπαφές

3.15 tcpdump -i em1

3.16 ipfw show
ο μόνος κανόνας που έχει αυξηθεί ο μετρητής του είναι ο κανόνας προώθησης πακέτων στον πίνακα NAT, ο οποίος έχει 8 εγγραφές
ipfw zero

3.17 ping -c 192.0.2.2
η IP διεύθυνση πηγής στην καταγραφή είναι 192.0.2.1, δηλαδή η IP του FW1 στη διεπαφή WAN1

3.18 η διεύθυνση προορισμού των ICMP echo reply είναι η ίδια με τη διεύθυνση πηγής ICMP echo request, δηλαδή 192.0.2.1

3.19 ο κανόνας που ευθύνεται για την επιτυχία του ping είναι ο κανόνας προώθησης των πακέτων στον πίνακα NAT

3.20 ο κανόνας εφαρμόστηκε 12 φορές, δηλαδή 4 φορές για κάθε ζεύγος ICMP echo request - reply
πρώτα εφαρμόζεται μία φορά για το πακέτο ICMP echo request που έχει ως αφετηρία το PC1 και ως προορισμό το FW1, ύστερα αφού μεταφραστεί η διεύθυνση εφαρμόζεται μία φορά στο νέο echo request που ξεκινά από το FW1 και αποστέλλεται στη διεπαφή WAN1, στη συνέχεια εφαρμόζεται στο echo reply που λαμβάνει ως απάντηση στο προηγούμενο μήνυμα και τέλος εφαρμόζεται μία φορά στο μεταφρασμένο ICMP echo reply που έχει ως προορισμό το PC1

3.21 μπορούμε να κάνουμε ping από το SRV1 στο FW1

3.22 ο υπεύθυνος κανόνας είναι ξανά ο ίδιος που στέλνει τα πακέτα στον πίνακα NAT

3.23 η κίνηση αυτή ωθείται στο NAT για μετάφραση καθώς ο κανόνας του firewall ορίζει πως όλα τα πακέτα ipv4 πρέπει να ωθούνται στο NAT ανεξαρτήτως πηγής και προορισμού

3.24 ssh lab@192.0.2.5
η σύνδεση μέσω ssh είναι επιτυχής

3.25 το αντίστροφο δεν είναι δυνατό λόγω δρομολόγησης, καθώς αν δούμε τον πίνακα δρομολόγησης του R1 με την εντολή *netstat -rn -f inet* θα παρατηρήσουμε πως δεν έχει διαδρομή για το LAN1

3.26 ipfw nat 123 config 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
η σύνδεση γίνεται με το μηχάνημα PC2, όπως φαίνεται και από την εντολή *hostname*, η οποία επιστρέφει το όνομα PC2

3.28 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 ssh lab@192.0.2.1
αυτή τη φορά συνδεθήκαμε στο μηχάνημα PC1 όπως φαίνεται από το prompt όπου αναγράφεται *lab@PC1*

3.30 ftp lab@192.0.2.1
έχουμε συνδεθεί στο PC2 καθώς η υπηρεσία ftp δεν είναι ενεργοποιημένη στο PC1

3.31 cd /etc
get rc.conf
το κατέβασμα του αρχείου ολοκληρώνεται με επιτυχία

3.32 κάνοντας ftp στη διεύθυνση 192.0.2.1 το NAT θα προωθήσει το αίτημα στο PC2, οπότε και θα συνδεθούμε σε αυτό

3.33 κάνοντας ssh στην ίδια διεύθυνση το NAT θα προωθήσει το αίτημα στο PC1 ανεξαρτήτως διεύθυνσης πηγής

Άσκηση 4: Τείχος προστασίας και NAT

4.1 ipfw disable one_pass
τα ping δε λειτουργούν

4.2 μηδενίζοντας τους μετρητές των κανόνων παρατηρούμε πως ο μετρητής του κανόνα προώθησης αυξάνεται, το οποίο σημαίνει πως γίνονται δεκτά, όμως το ping αποτυγχάνει διότι δεν υπάρχει κανόνας στο firewall που να επιτρέπει την κίνηση των πακέτων ICMP

4.3 ipfw add 1100 allow all from any to any via em0

4.4 το ping από το PC1 είναι επιτυχές και στις δύο διεπαφές του FW1

4.5 κάνοντας ssh στη διεύθυνση 192.0.2.1 θα συνδεθούμε στο μηχάνημα FW1

4.6 ο κανόνας που ευθύνεται για τα παραπάνω είναι ο κανόνας που προσθέσαμε στο 4.3

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 απαντά το FW1 καθώς επιτρέπουμε την ανταλλαγή πακέτων εντός του LAN1
4.12 απαντά το PC2 διότι τα εξωτερικά πακέτα περνούν από το NAT, ο οποίος προωθεί τα πακέτα στη διεύθυνση 192.168.1.3
4.13 συνδεόμαστε στο FW1 διότι τα μηνύματα εντός του LAN1 δεν περνάνε από NAT
4.14 κάνοντας ssh από το SRV1 το πακέτο θα περάσει από NAT, οπότε και θα γίνει προώθησή του στο PC1 λόγω του "redirect_port tcp 192.168.1.2:22 22"
4.15 κάνοντας ftp από το εξωτερικό μηχάνημα στη διεύθυνση 192.0.2.1 θα συνδεθούμε στο PC2 λόγω του "redirect_addr 192.168.1.3 192.0.2.1"
4.16 ping 192.0.2.5
το ping είναι επιτυχές
4.17 ssh lab@192.0.2.5
το ssh είναι επιτυχές
4.18 ftp lab@192.0.2.5
cd /usr
cd /bin
ls
get man
οι εντολές επιτυγχάνουν
4.19 ipfw add 2999 deny all from any to any via em1
4.20 αποτυγχάνουν όλα τα ping, ssh και ftp των παραπάνω ερωτημάτων
4.21 ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
4.22 το ping τώρα επιτυγχάνει ξανά
4.23 ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state
4.24 η σύνδεση μέσω ssh από το PC1 στο SRV1 είναι ξανά εφικτή
4.25 ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state
4.26 το μηχάνημα που απαντά στο ping από εξωτερικό του δικτύου LAN1 μηχάνημα είναι το PC2 όπως και πριν
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, καθώς ο NAT προωθεί την κίνηση tcp με προορισμό τη θύρα 22 στο μηχάνημα αυτό
4.29 ftp lab@192.0.2.1
το ftp δεν λειτουργεί
4.30 για να λειτουργήσει το ftp θα πρέπει να προστεθούν οι δύο παρακάτω κανόνες
ipfw add 2300 skipto 3000 tcp from any to any 21 recv em1 keep-state
ipfw add 2400 skipto 3000 tcp from any to any 20 xmit em1 keep-state

Άσκηση 5: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

5.1 192.168.1.1/24
5.2 10.0.0.1/30
5.3 66%
5.4 συνολικά βλέπουμε 4 διεπαφές
5.5 η διεύθυνση της διεπαφής DMZ είναι 172.22.1.1/24
5.6 fw
5.7 fw1 -> 'Save'
5.8 δεν υπάρχουν κανόνες για το WAN1
5.9 IP address 192.0.2.1/30
Gateway 192.0.2.2
5.10 υπάρχει κανόνας Block private networks
5.11 δεν φαίνεται κάποια από τις υπηρεσίες να είναι ενεργοποιημένες
5.12 'Enable DNS forwarder' -> 'Save'
5.13 'Enable' -> 'Range' 192.168.1.2 to 192.168.1.3 -> 'Save'

5.14 dhclient em0
η διεύθυνση IP είναι 192.168.1.2
η προεπιλεγμένη πύλη είναι 192.168.1.1
η διεύθυνση εξυπηρετητή DNS είναι 192.168.1.1
5.15 ενεργοποιώντας την υπηρεσία το μηχάνημα λειτουργεί αυτόματα ως DNS server για τους DHCP clients του LAN1
5.16 στο *DHCP Leases*
5.17 βλέπουμε 7 εγγραφές
5.18 ping 192.168.1.1
όχι
5.19 βλέπουμε πως το ICMP echo request απορρίφθηκε από το firewall
'Clear log'
5.20 βλέπουμε 8 firewall states
5.21 δεν υπάρχει ακόμα κανόνας για το LAN
5.22 προσθέτουμε κανόνα στο LAN ώστε να περνάνε όλα τα πακέτα
5.23 το ping επιτυγχάνει προς όλες τις διεπαφές του FW1
5.24 ping 192.0.2.1
όχι
5.25 arp -a
υπάρχει εγγραφή για τη διεπαφή του FW1 στο WAN1
5.26 Pass
Interface WAN
Protocol ICMP
ICMP type any
Source any
Destination WAN address
'Save' -> 'Apply Changes'
5.27 το ping τώρα είναι επιτυχές
5.28 δεν μπορούμε διότι ο R1 δεν έχει διαδρομή για τη διεύθυνση αυτή
5.29 το ping από το PC1 στον R1 είναι επιτυχές
μπορούμε να συμπεράνουμε πως χάρη στο NAT τα μηχανήματα στο εσωτερικό του δικτύου έχουν πρόσβαση στο διαδίκτυο χωρίς να επιτρέπεται η εξωτερική πρόσβαση σε αυτά
5.30 το ping αποτυγχάνει διότι ο SRV1 δεν έχει διαδρομή για το δίκτυο LAN1
5.31 route add default 172.22.1.1
5.32 το ping τώρα είναι επιτυχές
5.33 το ping αποτυγχάνει διότι δεν έχουμε κανόνα που να επιτρέπει την κίνηση στη διεπαφή DMZ
5.34 για τον ίδιο λόγο με το 5.33
5.35 allow all protocols all sources destination not LAN net
5.36 ping 172.22.1.1
το ping είναι επιτυχές
5.37 ping 192.0.2.1
το ping είναι επιτυχές
5.38 ping 172.22.1.2
το ping αποτυγχάνει με μήνυμα 'No route to host'
5.39 ping 192.0.2.2
το ping είναι επιτυχές καθώς γίνεται μετάφραση της διεύθυνσης του SRV1 μέσω NAT και έτσι ο R1 έχει διαδρομή για να απαντήσει
5.40 dhclient em0
διεύθυνση IP 192.168.1.3
default gateway 192.168.1.1
DNS server 192.168.1.1
5.41 block from 192.168.1.3 to 172.22.1.2

5.42 ο κανόνας πρέπει να τοποθετηθεί πριν τον ήδη υπάρχον, καθώς εκτελείται ο πρώτος κανόνας που ταιριάζει στο κάθε πακέτο
5.43 ping 172.22.1.2
όχι
5.44 ping 172.22.1.1
ναι, γιατί το μπλοκάρισμα των πακέτων γίνεται μόνο σε αυτά που έχουν ως προορισμό τη διεπαφή του SRV1 οπότε δεν επηρεάζεται το ping προς το FW1

Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT

6.1 ip route 203.0.118.0/24 192.0.2.1
6.2 Enable advanced outbound NAT
6.3 interface WAN
source 192.168.1.2/32
destination any
target 203.0.118.14
6.4 interface WAN
source 192.168.1.3/32
destination any
target 203.0.118.15
6.5 tcpdump -i em0
6.6 ping 192.0.2.2
το ping είναι επιτυχές
η διεύθυνση IP πηγής των πακέτων που φτάνουν είναι 203.0.118.14
6.7 ping 192.0.2.2
και αυτό το ping είναι επιτυχές
η διεύθυνση IP πηγής των πακέτων που φτάνουν είναι 203.0.118.15
6.8 ping 203.0.118.14
το ping αποτυγχάνει διότι στους κανόνες του firewall δεν επιτρέπουμε τη διέλευση πακέτων ICMP από εξωτερικά μηχανήματα
6.9 έγινε
6.10 έγινε
6.11 προστέθηκε αυτόματα ο κανόνας που επιτρέπει τη διέλευση κίνησης με πρωτόκολλο TCP, οποιαδήποτε πηγή, διεύθυνση προορισμού 172.22.1.2 και πύλη προορισμού 22 ώστε να επιτρέπεται η σύνδεση εξωτερικών μηχανημάτων με τον SRV1 μέσω ssh
6.12 ssh lab@203.0.118.18
η σύνδεση ήταν επιτυχής και το μηχάνημα στο οποίο συνδεθήκαμε είναι το SRV1
6.13 ping 203.0.118.18
το ping αποτυγχάνει καθώς η μόνη εξωτερική κίνηση που επιτρέπεται είναι η σύνδεση μέσω ssh
6.14 η σύνδεση μέσω ssh είναι επιτυχής
η διαδρομή που ακολουθείται είναι
PC1 -> FW1 -> R1 -> FW1 -> SRV1
το οποίο επιβεβαιώνουμε αφού φαίνονται τα πακέτα ssh στη διεπαφή του R1 όπου κάνουμε την καταγραφή
6.15 ping 192.0.2.2
το ping αποτυγχάνει
το PC1 στέλνει ICMP echo request στον R1, όμως αυτός δεν γνωρίζει διαδρομή προς το PC1 οπότε και δεν μπορεί να απαντήσει στο αίτημά του
6.16 καταργώντας το advanced outbound NAT το ping προς τον R1 είναι επιτυχές καθώς δεν χρειάζεται να προσθέσουμε αντιστοίχιση εμείς για το PC1 στο NAT αφού αυτό γίνεται αυτόματα

6.17 η σύνδεση μέσω ssh από τον R1 στη διεύθυνση 203.0.118.18 εξακολουθεί να λειτουργεί, όμως η σύνδεση από το PC2 όχι
6.18 tcpdump -i em0 -e
παρατηρούμε πως το πακέτο για τη δημιουργία της σύνδεσης περνά από το FW1 στον R1 και από εκεί προωθείται πίσω στο FW1 για να φτάσει στον SRV1, όμως η απάντηση του FW1 δεν εμφανίζεται στην καταγραφή του R1 λόγω αποτυχίας μετάφρασης στη NAT
6.19 ο λόγος που δεν λειτουργεί το ssh είναι πως δεν μπορούμε να κάνουμε χρήση NAT υπηρεσίας χρησιμοποιώντας την εξωτερική της διεύθυνση από μηχανήματα εντός του LAN

Άσκηση 7: IPSec site-to-site VPN

7.1 έγινε
7.2 έγινε
7.3 έγινε
7.4 ναι, συνδεόμαστε μέσω 192.168.56.2 στο fw1 και μέσω 192.168.56.3 στο fw2
7.5 καρτέλα *System > General Setup*
7.6 καρτέλα *Interfaces > WAN*
7.7 καρτέλα *Interfaces > LAN*
7.8 έγινε
7.9 Allow
Interface: LAN
Protocol: any
Source: any
Destination: any
7.10 Allow
Interface: WAN
Protocol: ICMP
Source: any
Destination: WAN address
7.11 ifconfig em0 192.168.2.2/24
route add default 192.168.2.1
7.12 ping 192.0.2.5
το ping είναι επιτυχές
7.13 ping 192.0.2.1
το ping είναι επιτυχές
7.14 δεν μπορούμε να κάνουμε ping από το ένα μηχάνημα στο άλλο αφού για να γίνει αυτό πρέπει να γίνει το ping από το ένα μηχάνημα να περάσει στο εξωτερικό δίκτυο και από εκεί να συνεχίσει η προώθηση του πακέτου στο άλλο δίκτυο, όμως τα πακέτα ICMP δεν επιτρέπονται στο εσωτερικό δίκτυο όταν προέρχονται από το εξωτερικό δίκτυο
7.15 έγινε
7.16 βλέπουμε πως δημιουργήθηκε κανόνας με τα εξής χαρακτηριστικά:
pass
Protocol: any
Source: any
Port: any
Destination: any
Port: any
7.17 δεν έχουν οριστεί σχέσεις
7.18 έχουν οριστεί πολιτικές προώθησης μεταξύ των υποδικτύων
7.19 έγινε
7.20 όχι

7.21 βλέπουμε να έχουν οριστεί πολιτικές προώθησης μεταξύ των υποδικτύων
7.22 το ping λειτουργεί
7.23 το ping λειτουργεί ξανά
7.24 βλέπουμε πως στο SAD έχουν οριστεί τώρα σχέσεις μεταξύ των υποδικτύων
7.25 και σε αυτή τη SAD έχουν οριστεί σχέσεις
7.26 tcpdump -i em0 -nvvv
7.27 στην καταγραφή δεν εμφανίζονται πακέτα ICMP
7.28 τα πακέτα που εμφανίζονται είναι τύπου ESP και έχουν διεύθυνση πηγής και προορισμού 192.0.2.1 και 192.0.2.5 εναλλάξ, δηλαδή από το FW1 στο FW2 και αντίστροφα
7.29 δεν εμφανίζεται κάπου στην καταγραφή πληροφορία για τις διευθύνσεις των PC
7.30 η σύνδεση μέσω ssh είναι επιτυχής
αυτό οφείλεται στο γεγονός πως το PC2 δεν βρίσκεται στην πραγματικότητα στο ίδιο εσωτερικό LAN που βρίσκεται και ο SRV1
7.31 στην καταγραφή παρατηρούνται πακέτα TCP με διευθύνσεις προορισμού και πηγής 192.0.2.5 και 203.0.118.18 και αντίστροφα
7.32 το περιεχόμενο των πακέτων είναι κρυπτογραφημένο καθώς ανήκουν στο πρωτόκολλο SSH, όμως δεν κάνουν χρήση του IPsec αφού σε κανένα από τα δύο firewall δεν έχουμε διεύθυνση προορισμού από ένα LAN και διεύθυνση πηγής από το άλλο λόγω της μετάφρασης NAT των διευθύνσεών τους