|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** Ζευγολατάκος Παναγιώτης | | **Όνομα PC:** panos-PC |
| **Ομάδα:** 1 | **Ημερομηνία:** 11/05/2021 | |

Εργαστηριακή Άσκηση 10

**Τείχη προστασίας (Firewalls) και NAT**

**Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.**

# 1

1.1 kldload ipfw

1.2 kldstat

1.3 Όχι, παίρνω μήνυμα λάθους Permission denied.

1.4 ipfw list

Υπάρχει μόνο ο προεπιλεγμένος κανόνας.

1.5 ipfw show

Εμφανίζει στοιχεία για τη χρήση του κανόνα.

1.6 ipfw zero

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

1.8 Ναι.

1.9 Όχι, παίρνω μήνυμα λάθους Permission denied.

1.10 ipfw add allow icmp from any to any

1.11 200

1.12 Μπορώ να κάνω και τα 2.

1.13 Δεν μπορώ επειδή χρησιμοποιούνται πακέτα UDP. Θα λάβω απάντηση αν βάλω επιλογή -I (ICMP).

1.14 ipfw add allow udp from any to any 33434-33534

1.15 Όχι (Permission denied).

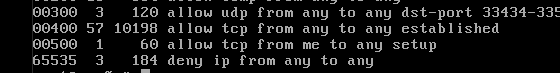
1.16 ipfw add allow tcp from any to any established

ipfw add allow tcp from me to any setup

1.17 ipfw zero

1.18 ipfw show

Χρησιμοποιήθηκε 57 φορές ο κανόνας 00400 και 1 φορά ο κανόνας 00500 (πρώτο πακέτο τριμερούς χειραψίας):



1.19 Όχι, εφόσον έχω ορίσει κανόνες μόνο για απερχόμενες συνδέσεις.

1.20 service ftpd onestart

1.21 Ναι, μπορώ:

ftp 192.168.1.3

cd /usr/bin

ls

get flex++

bye

# 2

2.1 kldload ipfw

2.2 Όχι (Permission denied).

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

2.4 ipfw add allow icmp from me to any icmptypes 8

2.5 Όχι.

2.6 ipfw show

Από τους μετρητές πακέτων παρατηρώ πως περνούν τα requests, αλλά όχι τα replies.

2.7 ipfw delete 200

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

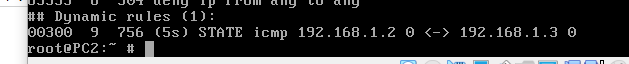
Ναι, μπορώ.

2.8 Ναι, μπορώ.

2.9 Όχι, επειδή ο κανόνας που θέσαμε στο ερώτημα 2.7 είναι δυναμικός κανόνας (keep-state) που επιτρέπει την επικοινωνία μεταξύ των δύο PC (με αυτόν και τα δύο έχουν πλέον κανόνα ‘allow icmp from me to any’), επομένως χωρίς να τρέχει το ping από το PC2 δε θα πετύχει.

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

2.11 Βλέπω το δυναμικό κανόνα που έχει δημιουργηθεί:



2.12 Πλέον εμφανίζονται μόνο οι στατικοί κανόνες.

2.13 ipfw add allow udp from any to me 33434-33534

ipfw add allow icmp from me to any icmptypes 3

2.14 ipfw add allow udp from me to any 33434-33534

ipfw add allow icmp from any to me icmptypes 3

2.15 ipfw add allow icmp from any to any (υπάρχει από την προηγούμενη άσκηση)

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

2.17 ssh lab@192.168.1.3

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

2.19 ipfw add allow tcp from 192.168.1.0/24 to me 22 setup

2.20 Ναι.

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

2.22 Η εντολή cd χρησιμοποιεί TCP control connection, ενώ η εντολή ls χρησιμοποιεί TCP data connection, την οποία δεν επιτρέπει το firewall.

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

2.24 Ναι.

2.25 PC1: ipfw add allow tcp from any 20 to me 1024-65535 setup

PC2: ipfw add allow tcp from me 20 to any 1024-65535 setup keep-state

2.26 Σε FTP Active ο πελάτης πρέπει να δέχεται συνδέσεις σε δυναμικά ports, ενώ σε FTP Passive υπάρχει λιγότερη ασφάλεια, εφόσον χρειάζονται παραπάνω κανόνες που να επιτρέπουν συνδέσεις.

2.27 kldunload ipfw

# 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

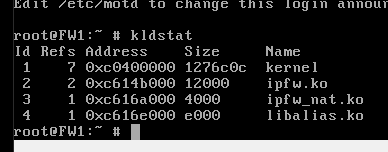
3.3 sysrc hostname=SRV1

ifconfig em0 192.0.2.5/30

route add default 192.0.2.6

3.4 service ftpd onestart

3.5



3.6 Το IPFW.

3.7 UNKNOWN.

3.8 11, ο τελευταίος είναι ο προεπιλεγμένος ‘deny ip from any to any’.

3.9 ipfw nat show config

3.10 Όχι.

3.11 Όχι.

3.12 ipfw nat 123 config ip 192.0.2.1 unreg\_only reset

3.13 ipfw add nat 123 all from any to any

3.14 Ναι.

3.15 ipfw show

Ο κανόνας του ερωτήματος 3.13

3.16 tcpdump -n -i em0

3.17 ipfw show && ipfw zero

3.18 Η διεύθυνση του FW1 στο WAN1.

3.19 Η διεύθυνση του R1 στο WAN1.

3.20 Έχει εφαρμοσθεί ο κανόνας που του ερωτήματος 3.13, 204(=4\*51) φορές, όπου 51 είναι τα πακέτα Echo Request που στάλθηκαν και εφαρμόσθηκε μια φορά πριν τη μετάφραση και μια μετά τη μετάφραση, δύο φορές για το ζεύγος request και reply, άρα 4\*51.

3.21 Ναι.

3.22 Ο κανόνας του ερωτήματος 3.13, αλλά δεν ωθείται προς μετάφραση διευθύνσεων, εφόσον η διεύθυνση των πακέτων δεν είναι private.

3.23 Ναι.

3.24 Ο R1 δεν μπορεί να προωθήσει τα πακέτα στο LAN1, επομένως είναι θέμα δρομολόγησης.

3.25 ipfw nat 123 config 192.0.2.1 unreg\_only reset redirect\_addr 192.168.1.3 192.0.2.1

3.26 Ναι, και έχω συνδεθεί στο PC2 (ifconfig για να δω τη διεύθυνση των καρτών δικτύου).

3.27 ipfw nat 123 config ip 192.0.2.1 unreg\_only reset redirect\_port tcp 192.168.1.3:22 192.0.2.1:22

3.28 Στο PC2 και το εξακριβώνω πάλι κοιτώντας τη διεύθυνση των καρτών δικτύου.

3.29 Στο PC2 και το εξακριβώνω πάλι κοιτώντας τη διεύθυνση των καρτών δικτύου.

3.30 Ναι.

3.31 Το FW1.

3.32 Το PC2.

# 4

4.1 Όχι.

4.2 Γίνονται δεκτά, αλλά συνεχίζουν στη λίστα κανόνων και χρησιμοποιείται ο προεπιλεγμένος κανόνας.

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

4.4 Ναι.

4.5 Το FW1.

4.6 Ο κανόνας του ερωτήματος 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 Το FW1.

4.12 Το FW1.

4.13 Το FW1.

4.14 Το PC2.

4.15 Το FW1.

4.16 Ναι.

4.17 Ναι.

4.18 Ναι.

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

4.20 Κανένα.

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

4.22 Ναι.

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

4.24 Ναι.

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

4.26 Το FW1.

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

4.28 Στο PC2 (και στο FW1 από το PC1).

4.29 Όχι.

# 5

5.1 192.168.1.1/24

5.2 10.0.0.1/30

5.3 97% (έβαλα 1024MB όταν το έφτιαχνα)

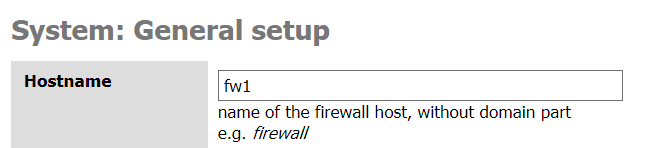


5.4 Παρατηρώ 4 σε σωστή δικτύωση.

5.5 172.22.1.1/24

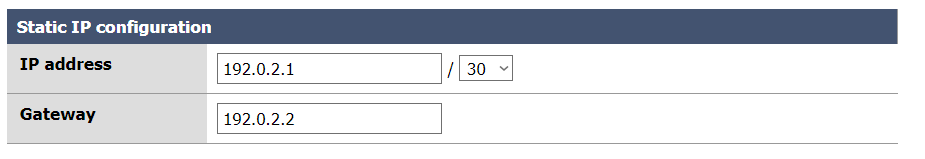
5.6 fw

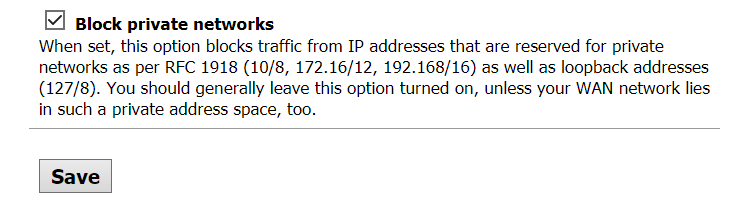
5.7



5.8 Όχι.

5.9 Interfaces/WAN





5.10 Ναι:

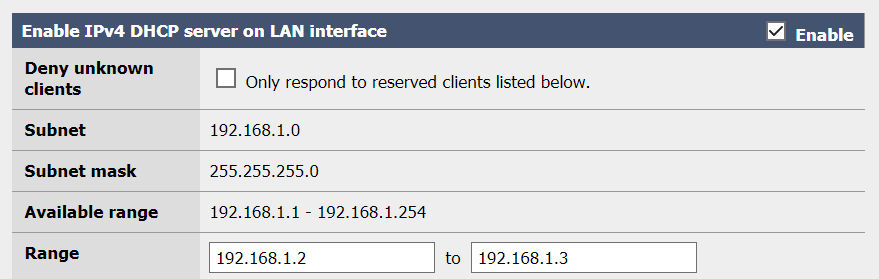


5.11 Όχι.

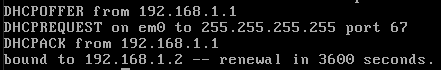
5.12



5.13



5.14 dhclient em0



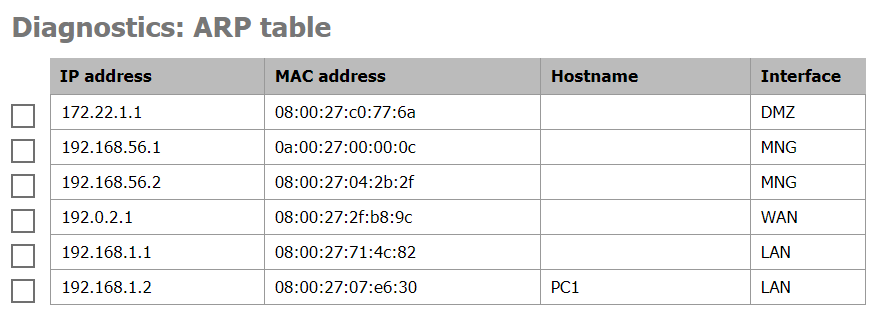
netstat -rn



5.15 Για να μη χρειαστεί να οριστεί DNS Server manually.

5.16 DCHP Leases.

5.17



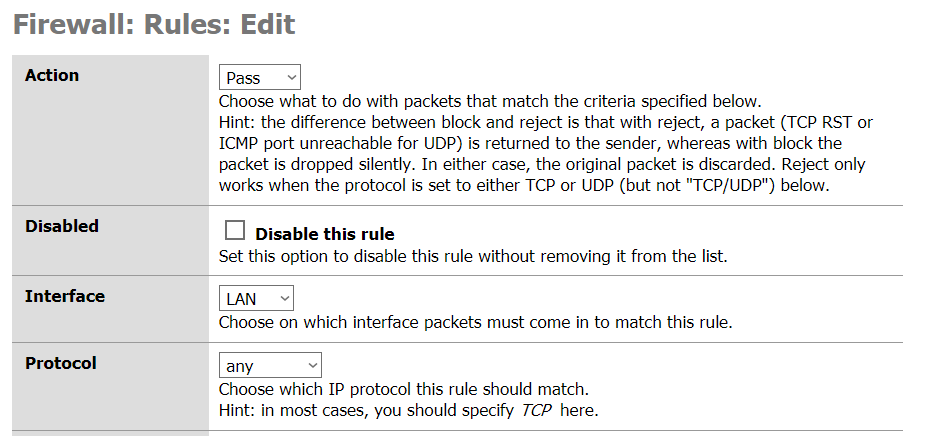
5.18 Όχι.

5.19 Βλέπω log για το ping που έκανα και την απόρριψή του.

5.20 3

5.21 Κανέναν.

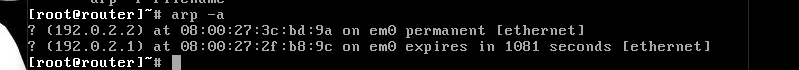
5.22 (τα υπόλοιπα τα άφησα ως έχουν)



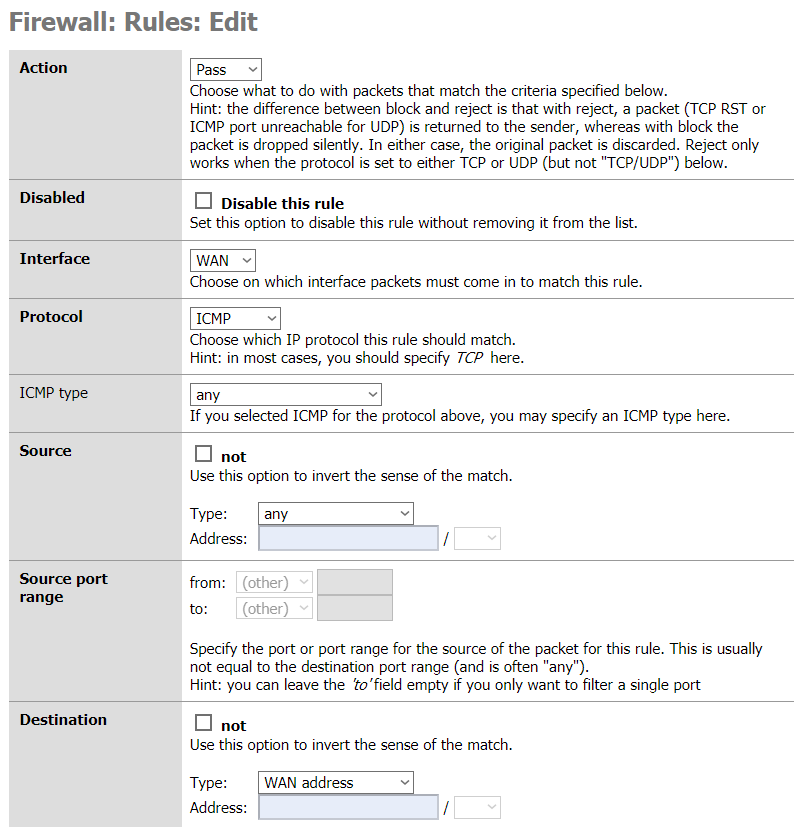
5.23 Ναι.

5.24 Όχι.

5.25 arp -a



5.26



5.27 Ναι.

5.28 Όχι, εφόσον ο R1 δεν ξέρει πως να δρομολογήσει πακέτα στο LAN1.

5.29 Ναι. Επιτρέπει την απερχόμενη κίνηση από τη WAN1 προς την κάρτα δικτύου.

5.30 Όχι, επειδή δεν ξέρει πως να απαντήσει ο SRV1.

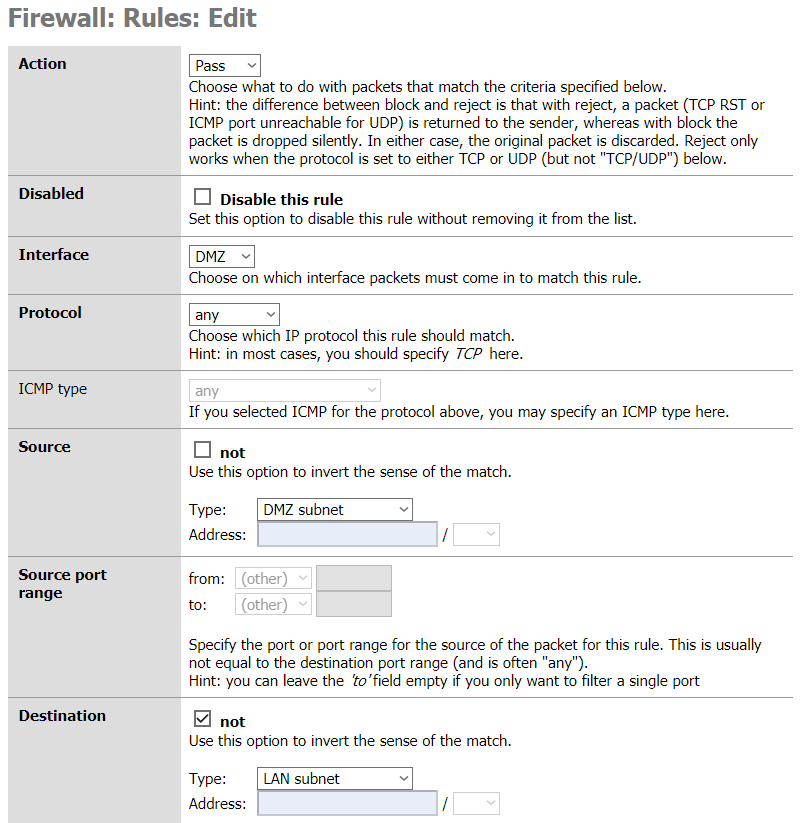
5.31 route add default 172.22.1.1

5.32 Ναι.

5.33 Όχι, εξαιτίας του firewall.

5.34 Όχι, εξαιτίας του firewall.

5.35



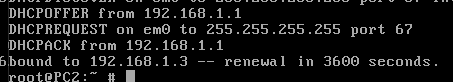
5.36 Ναι.

5.37 Ναι.

5.38 Όχι, επειδή δεν ξέρει πως να το δρομολογήσει.

5.39 Ναι, αφού επιτρέπεται όλη η απερχόμενη κίνηση (πλην του LAN1).

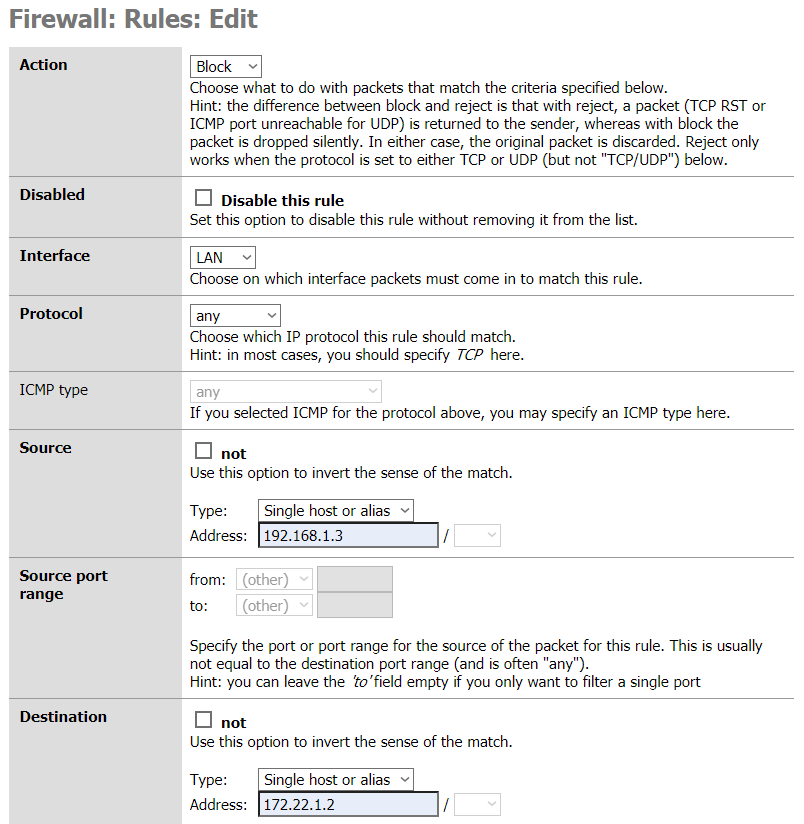
5.40 dhclient em0



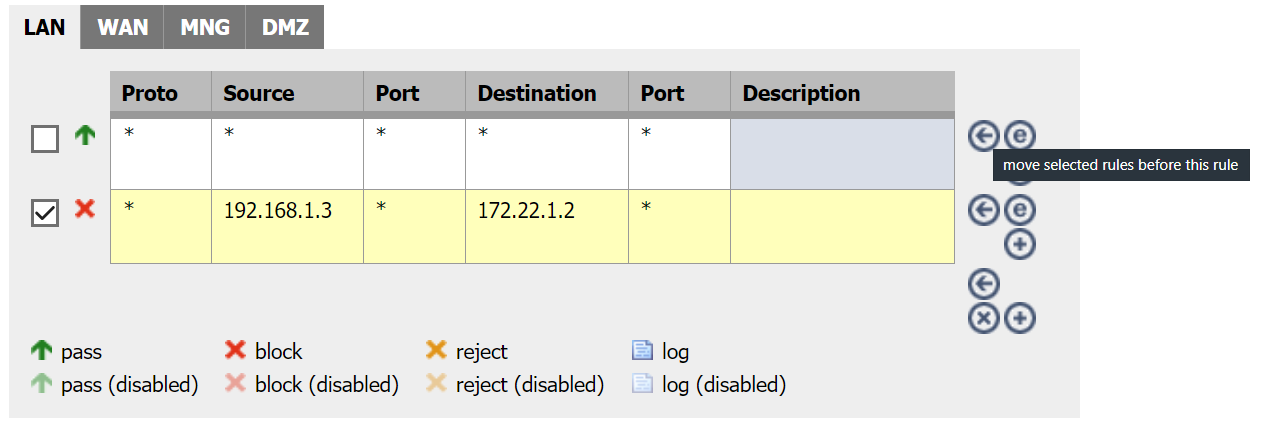
netstat -rn



5.41



5.42 Πριν, για να εκτελείται πρώτος και να γίνει σωστά το φιλτράρισμα:



5.43 Όχι.

5.44 Ναι, εφόσον ο κανόνας απαγορεύει μόνο την διεύθυνση IP του SRV1 (172.22.1.1).

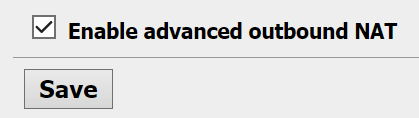
# 6

6.1 cli

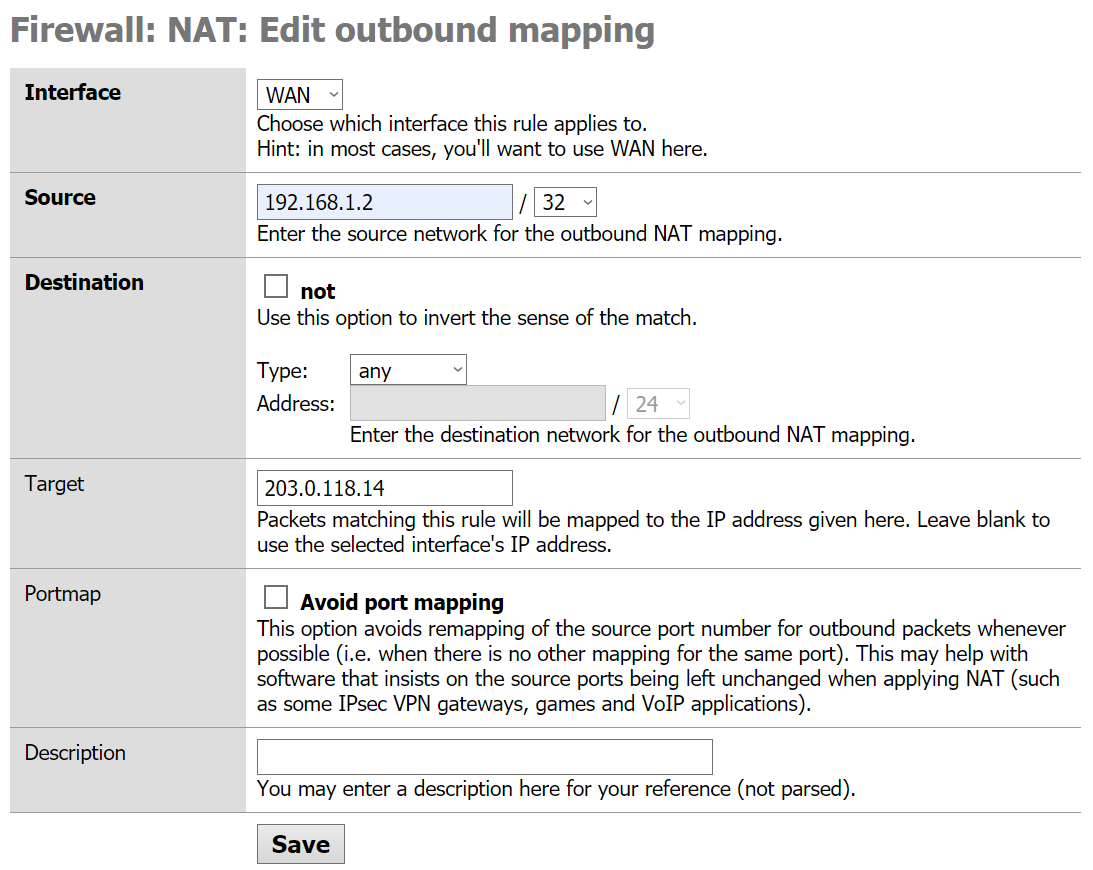
configure terminal

ip route 203.0.118.0/24 192.0.2.1

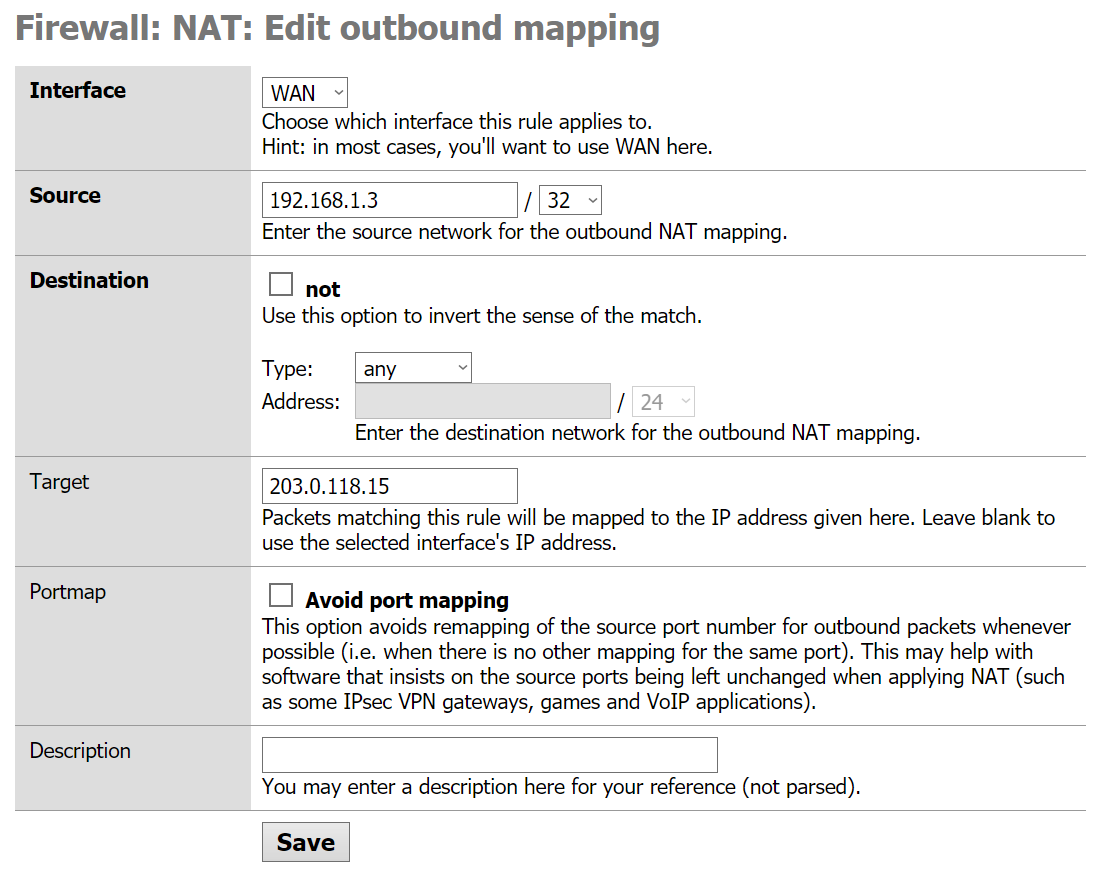
6.2



6.3



6.4



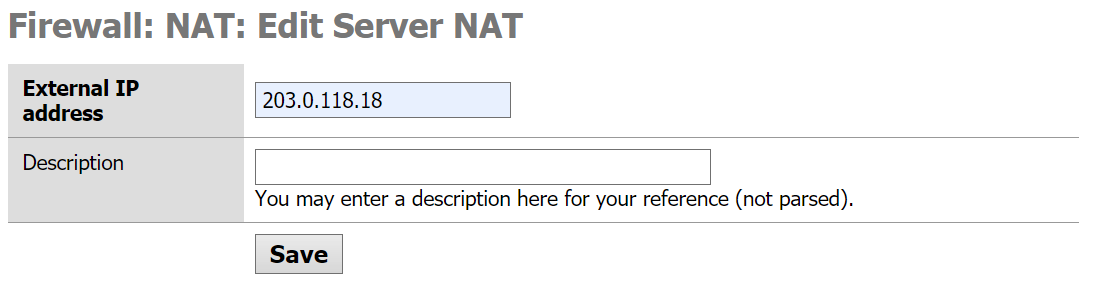
6.5 tcpdump -i em0

6.6 Ναι και φτάνουν με τη διεύθυνση 203.0.118.14

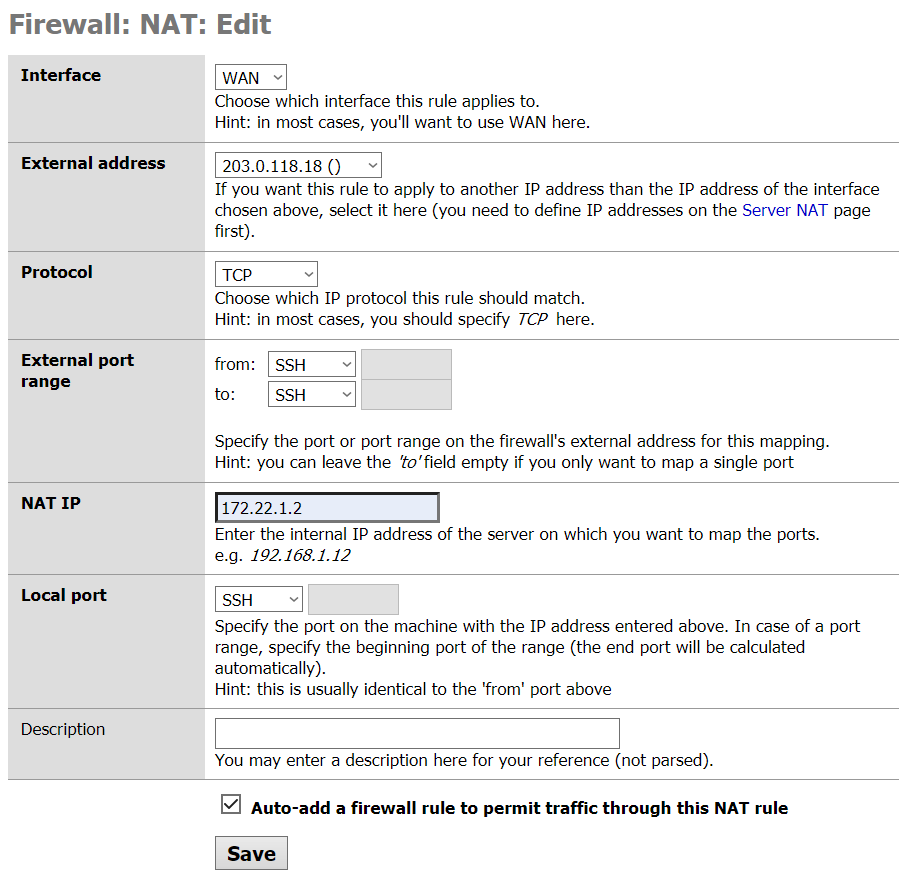
6.7 Ναι και φτάνουν με τη διεύθυνση 203.0.118.15

6.8 Αποτυγχάνει επειδή είναι outbound NAT.

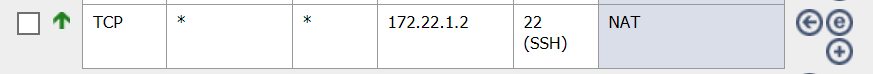
6.9



6.10



6.11 Ο κανόνας που επιτρέπει την κίνηση από any port 22 προς το SRV1:



6.12 Ναι, συνδέομαι στο SRV1.

6.13 Όχι, εφόσον ο κανόνας που όρισα αφορά μόνο το SSH port.

6.14 Ναι και τα πακέτα χρησιμοποιούν τη διαδρομή PC2 🡪 FW1 🡪 R1 🡪 FW1 🡪 SRV1, το οποίο το εξακρίβωσα με την καταγραφή στο R1, όπου επικοινωνεί με τέτοιον τρόπο με τη διεύθυνση 203.1.118.15 (PC2).

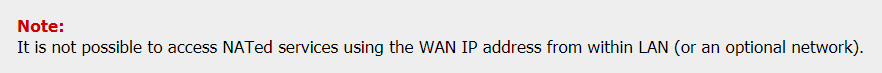
6.15 Όχι, εφόσον στα πακέτα του PC1 δε γίνεται μετάφραση NAT και δεν απαντάει το R1.

6.16 Ναι, εφόσον δημιουργούνται αυτόματα κανόνες NAT για outbound κίνηση και τα πακέτα παίρνουν τη διεύθυνση 192.0.2.1

6.17 Ναι. Όχι.

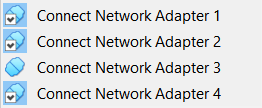
6.18 Αποτυγχάνει επειδή χωρίς το advanced outbound NAT, το FW1 στέλνει στο SRV1 πακέτα με τη δική του διεύθυνση ως source αντί για την 203.0.118.15 (PC2), επομένως όταν το SRV1 στέλνει Syn-Ack, αυτό στέλνει Reset.

6.19 Σύμφωνα με τη σημείωση που βρίσκεται στην καρτέλα Inbound NAT, δεν είναι εφικτό να γίνει πρόσβαση σε υπηρεσίες που χρησιμοποιούν NAT χρησιμοποιώντας τη WAN διεύθυνση IP από κάποιο LAN, για αυτό και αποτυγχάνει το ssh:

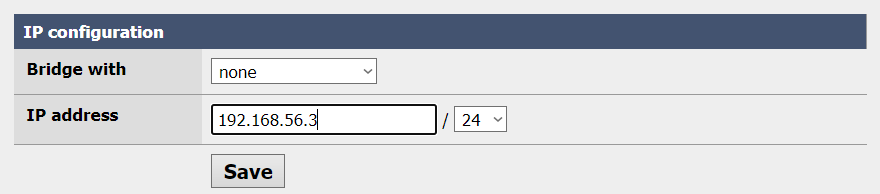


# 7

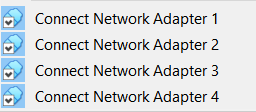
7.1



7.2

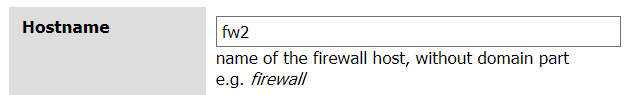


7.3

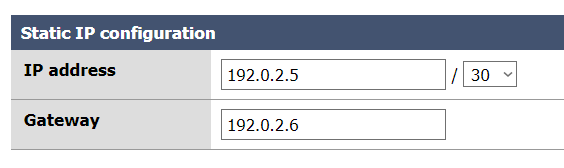


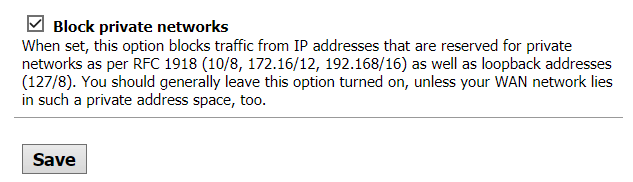
7.4 Ναι.

7.5

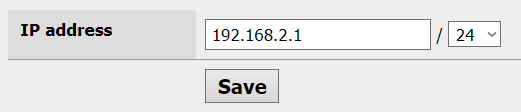


7.6

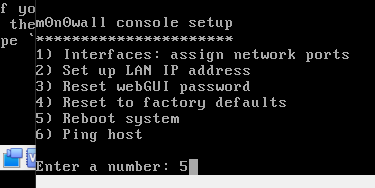




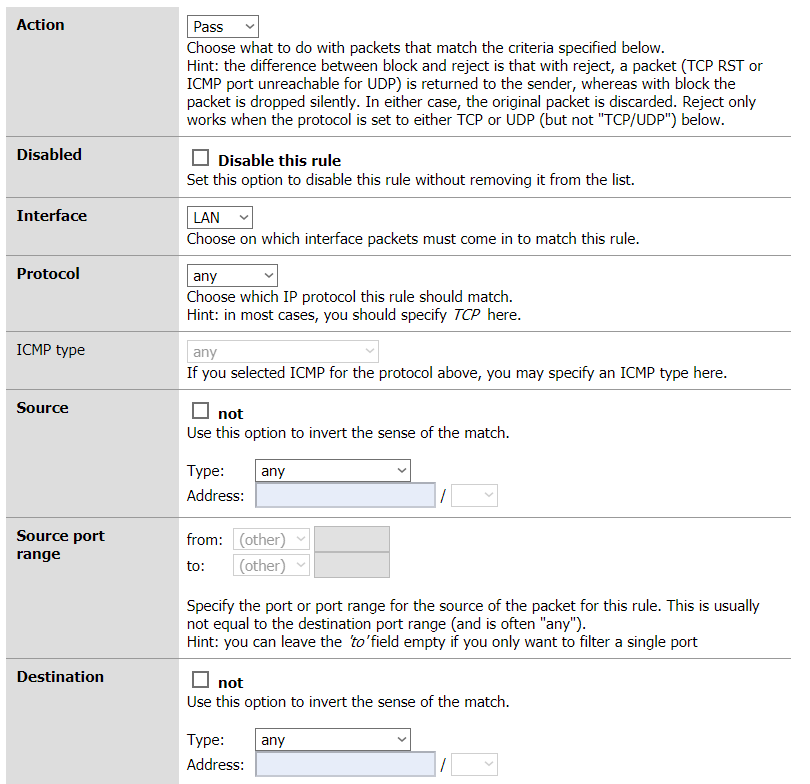
7.7



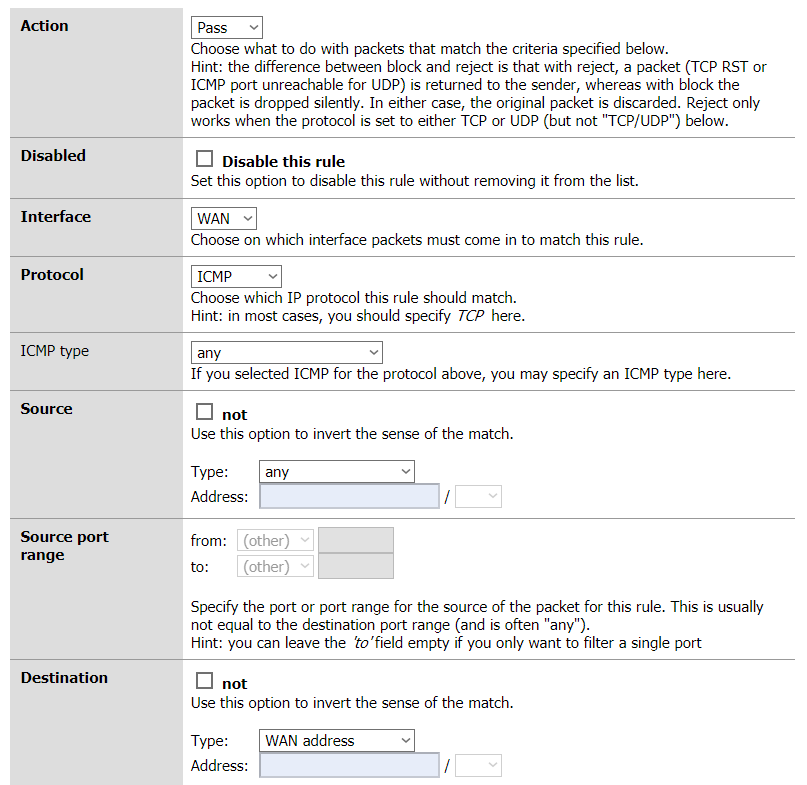
7.8



7.9



7.10



7.11 ifconfig em0 192.168.2.2/24

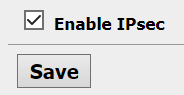
route add default 192.168.2.1

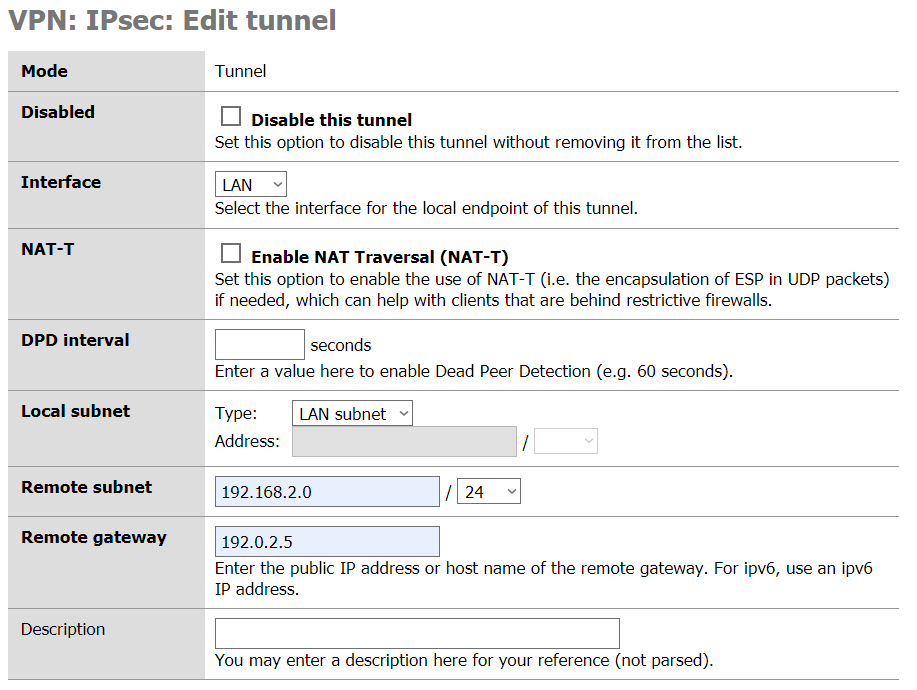
7.12 Ναι.

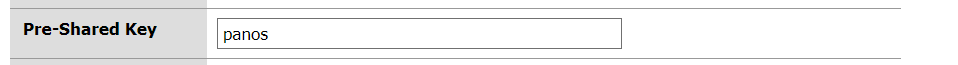
7.13 Ναι.

7.14 Όχι, εφόσον ο R1 δεν ξέρει πως να τα δρομολογήσει.

7.15



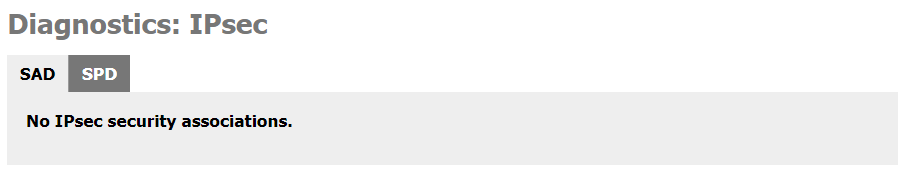




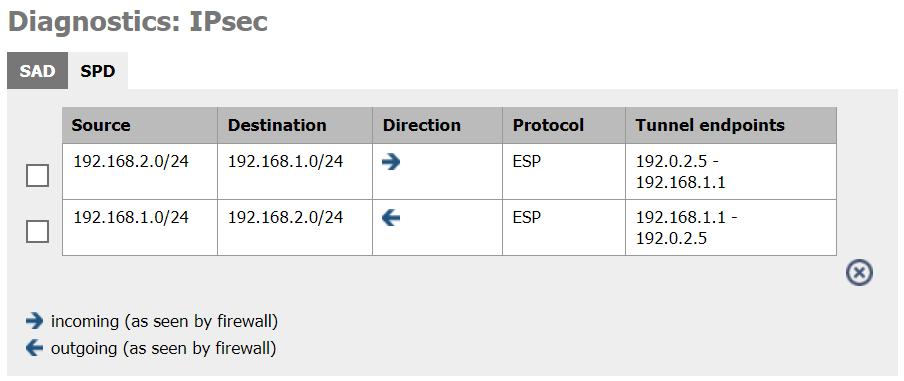
7.16



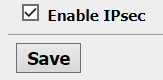
7.17 Όχι:

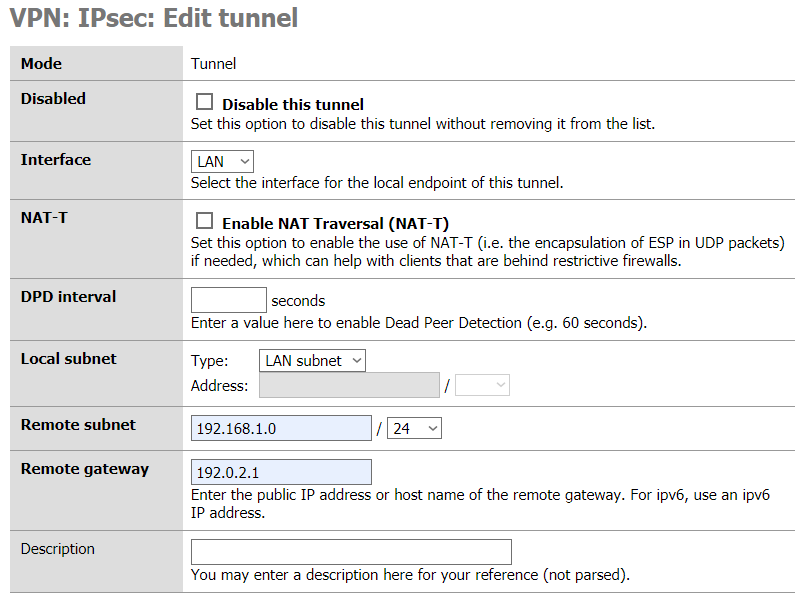


7.18 Ναι:



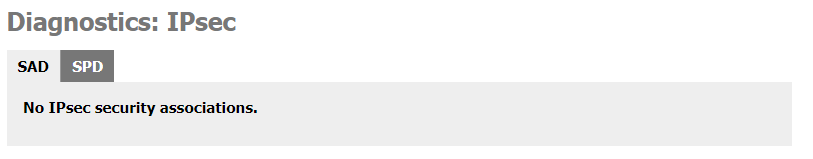
7.19



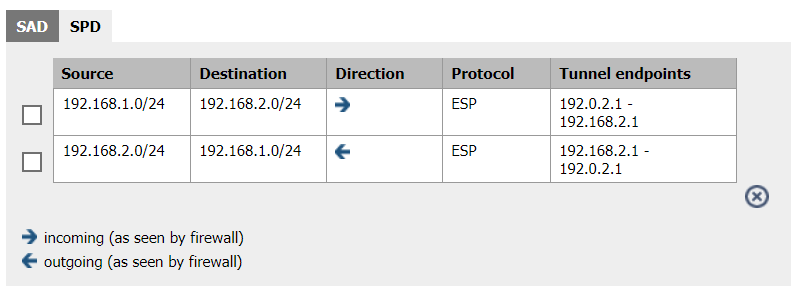




7.20 Όχι:



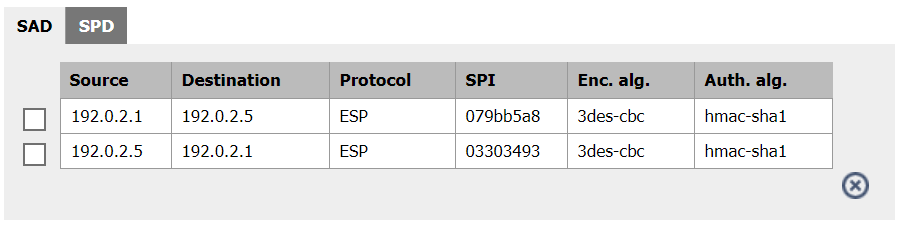
7.21 Ναι:



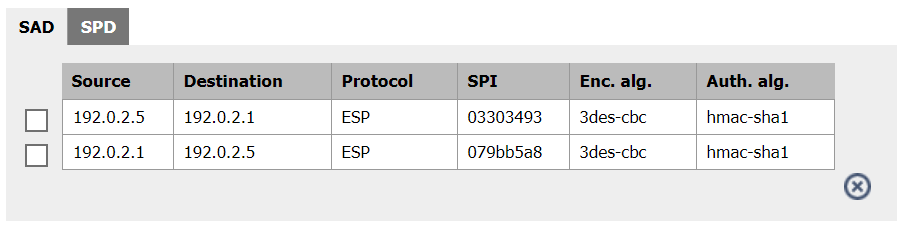
7.22 Ναι.

7.23 Ναι.

7.24 Έχουν προστεθεί 2 σχέσεις:



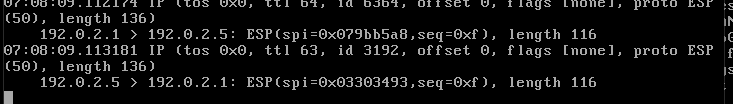
7.25 Έχουν προστεθεί 2 σχέσεις:



7.26 tcpdump -i em0 -vvv

7.27 Όχι.

7.28 Πακέτα ESP, με πηγή και προορισμό τις διεπαφές των FW1, FW2 στα WAN, ενώ δεν υπάρχει πουθενά πληροφορία για τα PC1, PC2:



7.29 Ναι και αυτό που έχει αλλάξει είναι ότι πλέον δρομολογούνται στο FW2 με το σωστό source IP.

7.30 Παρατηρώ πακέτα είδους ssh με πηγή τη διεύθυνση 192.0.2.5 και με προορισμό τη διεύθυνση 203.0.118.18 και δεν είναι κρυπτογραφημένα με IPsec, εφόσον επικοινωνούν υποδίκτυα για τα οποία δεν έχουν οριστεί IPsec:

