

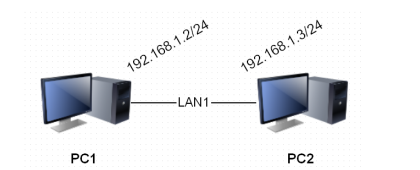
Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή ασκηση 10

Τειχη προστασιας (Firewalls) και NAT

Κουστένης Χρίστος | el20227 | 24/04/2024

# Άσκηση 1: Ένα απλό τείχος προστασίας



### 1.1

**ifconfig em0 192.168.1.2/24** --> PC1

**vi /etc/rc.conf** --> Αλλαγή παραμέτρου hostname

**ifconfig em0 192.168.1.3/24** --> PC2

**vi /etc/rc.conf** --> Αλλαγή παραμέτρου hostname

### 1.2

**kldload ipfw** --> PC1

### 1.3

**kldstat** --> PC1

### 1.4

Όχι δε μπορούμε.



### 1.5

**ipfw list**

### 1.6

**ipfw add 00100 allow all from any to any via lo0**

### 1.7

Ναι.

### 1.8

**ipfw show**

### 1.9

**ipfw zero**

### 1.10

Oχι, « **Permission Denied** ».

### 1.11

**ipfw add allow icmp from any to any**

### 1.12

Έλαβε αριθμό 00200.

### 1.13

Ναι, πετυχαίνουν και τα δυό.

### 1.14

Δε μπορούμε καθώς το traceroute by default χρησιμοποιεί UDP Datagrams, τα οποία και δεν επιτρέπονται να περάσουν από το firewall μας. Αν ωστόσο εκτελέσουμε « **traceroute -I 192.168.1.3** », ώστε να στείλουμε ICMP Echo αντ’ αυτών, τότε πετυχαίνει.

### 1.15

**ipfw add allow udp from me to any 33434-33626**

### 1.16

**ssh lab@192.168.1.3**

Παίρνουμε μήνυμα σφάλματος permission denied

### 1.17

**ipfw add allow tcp from any to any established**

**ipfw add allow tcp from me to any setup**

### 1.18

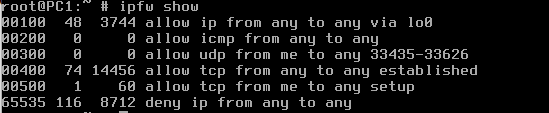
**ipfw zero**

**ssh lab@192.168.1.3** --> σύνδεση με συμπλήρωση κωδικού στο prompt

**ls**

**exit**

### 1.19



Άρα εφαρμόστηκε μία φορά ο κανόνας 00500 (στην τριμερή χειραψία) και 74 φορές ο κανόνας 00400 (κατά τη μεταφορά δεδομένων στη σύνδεση ssh).

### 1.20

Όχι, δεν μπορούμε καθώς έχουμε επιτρέψει μόνο απερχόμενες tcp συνδέσεις από τον PC1.

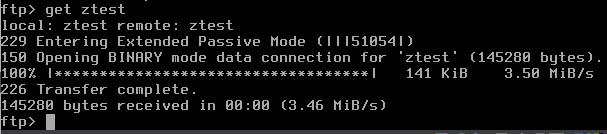
### 1.21

**service ftpd onestart** --> PC2

*(To start service one time, without modifying /etc/rc.conf)*

### 1.22

**ftp lab@192.168.1.3** --> PC1



Βλέπουμε πως το αρχέιο κατέβηκε κανονικά.

# Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

### 2.1

**kldload ipfw**

### 2.2

Όχι, 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

Όχι, αλλά δε λαμβάνουμε Permission Denied αυτή τη φορά.

### 2.6

Μηδενίζουμε τους μετρητές με ipfw zero. Ύστερα εκτελούμε **ping -c 1 192.168.1.2** για να στείλουμε μόνο ένα πακέτο. Με ipfw show βλέπουμε ότι ο κανόνας του 2.4 έχει χρησιμοποιηθεί μία φορά. Δηλαδή, το ICMP reply του PC1 προς το PC2 δεν πέρασε από το firewall του PC2 για αυτό και το ping αποτυγχάνει.

### 2.7

**ipfw delete 00200**

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

### 2.8

Ναι, μπορώ.

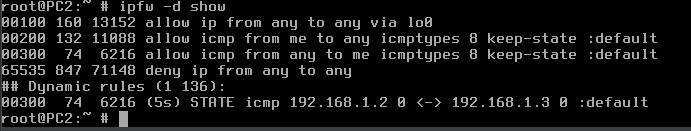
### 2.9

Όχι, πλέον δεν επιτυγχάνει. Όταν υπάρξει ταίριασμα σε κανόνα που λήγει με το keep-state, τότε το τείχος προστασίας λειτουργεί βάσει της κατάστασης (stateful behavior). Δημιουργείται δηλαδή 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.

### 2.10

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

### 2.11





Βλέπουμε τη χρήση ενός δυναμικού κανόνα κατά την επικοινωνία.

### 2.12

**ipfw -d show**

Πλέον βλέπουμε μόνο τους στατικούς κανόνες.

### 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 0,3,11**

0: echo reply , 3 : destination unreachable , 11 : ttl

### 2.15

**ipfw add allow udp from any to me 33435-3626**

### 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** --> μας ζητάει το password

### 2.18

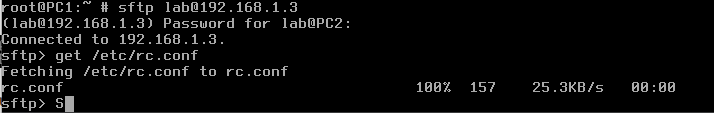
**ipfw add allow tcp from me to any 22 keep-state**

### 2.19

**ipfw add allow tcp from 192.168.1.3 to me 22**

### 2.20

Ναι, αφού το sftp τρέχει πάνω από ssh session.

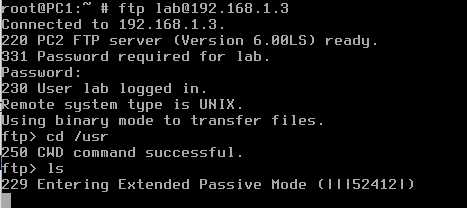


### 2.21

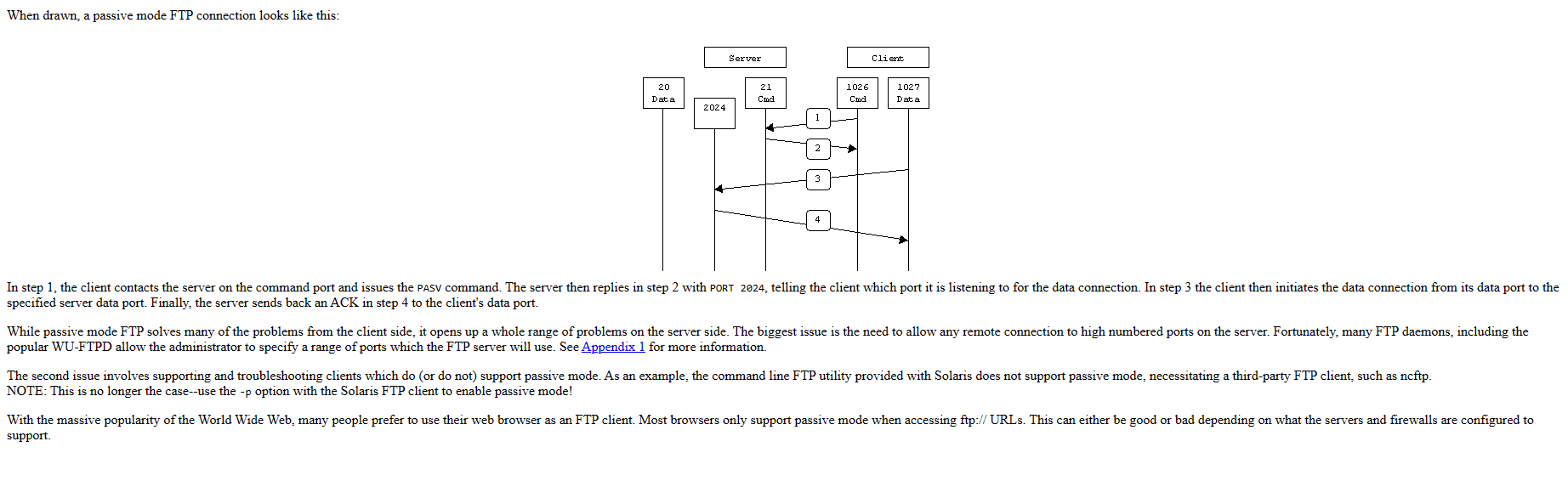
Δε μπορούμε, οπότε εισάγουμε τον παρακάτω κανόνα:

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

### 2.22



### 2.23



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

### 2.24

Ναι.

### 2.25

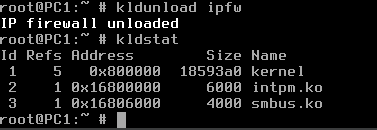
PC2 : **ipfw add allow tcp from me 20 to any 1024-65535 setup keep-state**

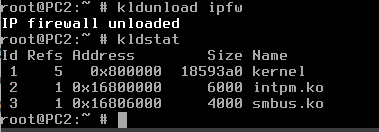
PC1 : **ipfw add allow tcp from any 20 to me 1024-65535 setup**

### 2.26

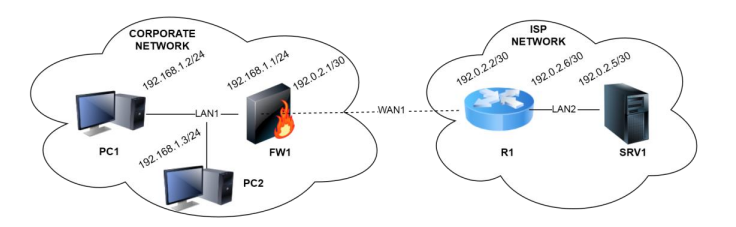
To ftp μπορεί να χρησιμοποιεί πολλές θύρες όπως είδαμε στο ερώτημα 2.23 . Επίσης, ανάλογα με το version του ftp μπορεί ο client να ανοίγει την tcp σύνδεση ή ο server να την ανοίγει. Αυτό προσθέτει δυσκολία στη δημιουργία κανόνων του firewall αφού αναγκαζόμαστε να βάλουμε πολλούς κανόνες ώστε να καλύψουμε όλες τις μορφές του ftp και μπορεί έτσι να μειώσουμε την προστασία του χρήστη έναντι σε κακόβουλους. Από την άλλη, άμα παραλείψουμε κανόνες κάνοντας υποθέσεις για το πως ακριβώς θα λειτουργήσει το ftp κινδυνεύουμε να μην λειτουγεί καθόλου.

### 2.27





# Άσκηση 3: Απλό Network Address Translation



### 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**

### 3.3

**hostname SRV1**

**ifconfig em0 192.0.2.5/30**

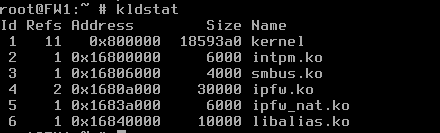
**route add default 192.0.2.6**

### **3.4**

**service ftpd onestart** --> PC2, SRV1

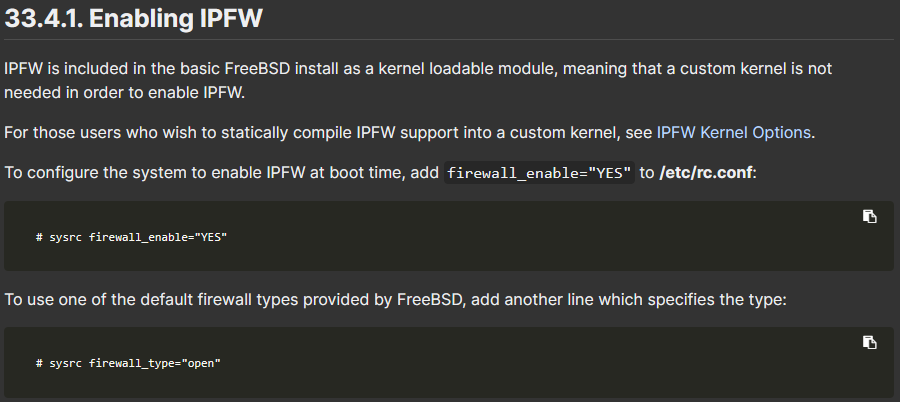
### **3.5**

**kldstat** --> FW1



### **3.6**

Το ipfw.

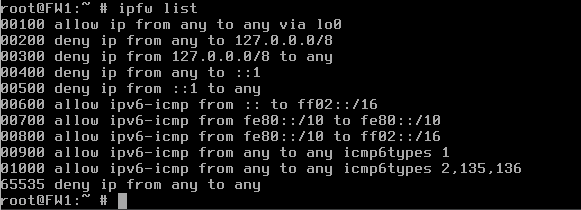


### **3.7**



### 3.8

Βλέπω 11 κανόνες και ο τελευταίος είναι ο προκαθορισμένος κανόνας : **deny ip form any to any**



### 3.9

**ipfw nat show config** --> βλέπουμε πως δεν υπάρχει κανένας πίνακας.

### 3.10

Όχι, σε καμία από τις 2.

### 3.11

Όχι.

### 3.12

**ipfw nat 123 config unreg\_only if em1 reset**

### 3.13

**ipfw add nat 123 ip4 from any to any**

### 3.14

Ναι.

### 3.15

**tcpdump -i em0**

### 3.16

**ipfw show**

**ipfw zero**

### 3.17

**ping -c 3 192.0.2.2**

Πηγή των ICMP Echo requests εμφανίζεται να είναι η 192.0.2.1, δηλαδή η em1FW1.

### 3.18

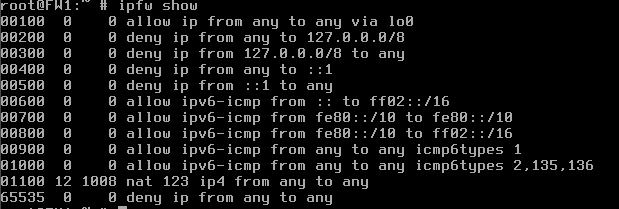
Είναι επίσης 192.0.2.1

### 3.19

Αυτός που πρσθέσαμε στο ερώτημα 3.13 που στέλνει όλα το IPv4 πακέτα για μετάφραση στον πίνακα NAT 123.

### 3.20

Bλέπουμε πως εφαρμόστηκε 12 φορές. Συνολικά πέρασαν από το τείχος 6 πακέτα (3 requests και 3 reply), ωστόσο, το κάθε πακέτο μπήκε για μετάφραση κατά την είσοδο και κατά την έξοδό του από αυτό, οπότε και προκύπτει το 12.



### 3.21

Ναι.

### 3.22

Είναι ο ίδιος κανόνας με παραπάνω, ο οποίος χρησιμοποιήθηκε 2 φορές αυτή τη φορά.

### 3.23

Ωθείται μεν για μετάφραση, αλλά δεν γίνεται μετάφραση γιατί η διεύθυνση 192.0.2.5 δεν είναι ιδιωτική.

### 3.24

Ναι με **ssh lab@192.0.2.5** .

### 3.25

Δεν μπορούμε. Είναι θέμα δρομολόγησης αφού ούτε ping στο PC2 μπορούμε να κάνουμε αλλά ούτε και traceroute. Επίσης, δεν αυξάνεται το πλήθος των εφαρμογών κάποιου κανόνα στο firewall που δείχνει ότι παρεμποδίζει τη διέλευση πακέτων.

### 3.26

**ipfw nat 123 config if em1 unreg\_only reset redirect\_addr 192.168.1.3 192.0.2.1**

### 3.27

**ssh lab@192.0.2.1**

Ναι, είναι επιτυχής. Συνδεθήκαμε στο PC2 όπως διαπιστώνουμε από το hostname.



### 3.28

**ipfw nat 123 config if em1 unreg\_only reset redirect\_addr 192.168.1.3 192.0.2.1 redirect\_port tcp 192.168.1.2:22 192.0.2.1:22**

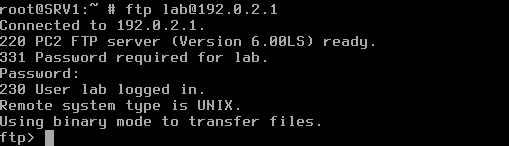
### 3.29

Τώρα συνδεθήκαμε στο PC1 και το βλέπουμε από το prompt.

### 3.30

**ftp lab@192.0.2.1**

Συνδεθήκαμε στο PC2.

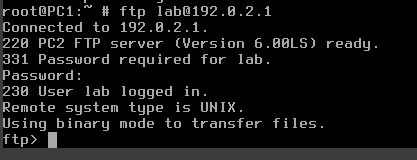


### 3.31

Ναι με ls και ναι με get.

### 3.32

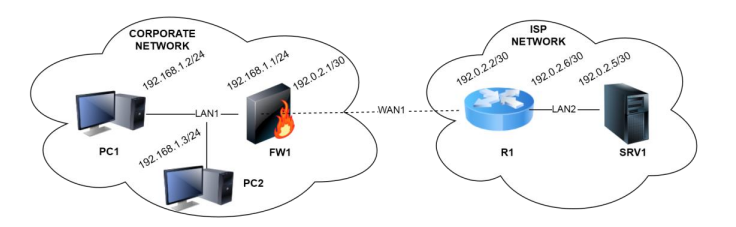
Απαντά το PC2.



### 3.33

Στο PC1, αφού το ssh χρησιμοποιεί την θύρα 22 και στο ερώτημα 3.28 ορίσαμε ότι tcp κίνηση στη διεπαφή του FW1 στο WAN1 με θύρα προορισμού την 22 ανακατευθύνεται στο PC1.

# Άσκηση 4: Τείχος προστασίας και NAT



### 4.1

Όχι, και τα 2 ping αποτυγχάνουν.

### 4.2

Ναι και τα 2 γίνονται αποδεκτά. Αποτυγχάνουν, ωστόσο, αφού απενεργοποιήσαμε το one-pass, οπότε και ελέγχθηκε ο επόμενος κανόνας, ο οποίος εν προκειμένω ήταν ο προκαθορισμένος που απέρριψε τα πακέτα.

### 4.3

**ipfw delete 1100**

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

### 4.4

Ναι είναι επιτυχές.

### 4.5

Συνδεόμαστε στο FW1.

### 4.6

Είναι υπεύθυνοι οι κανόνες 00100 και 01100 δηλαδή ο

« **allow ip from any to any via lo0** » (=100)

και ο « **allow all from any to any via em0** » (=100) .

### 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 PC2. Παρακάτω βλέπουμε το tcpdump στο PC2.

### 4.13

FW1

### 4.14

PC1

### 4.15

PC2

### 4.16

Ναι.

### 4.17

Ναι.

### 4.18

Ναι.

### 4.19

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

### 4.20

Επιτυγχάνουν μόνο τα 4.11 και 4.13, καθώς όλα τα άλλα απαιτούν να εισέλθει κίνηση από το WAN1 μέσω του firewall, πράγμα που απαγορεύσαμε.

### 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

Nαι.

### 4.25

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

### 4.26

Το PC2, όπως βλέπουμε με « **tcpdump -i em0** » στο FW1.

### 4.27

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

### 4.28

Στο PC1.

### 4.29

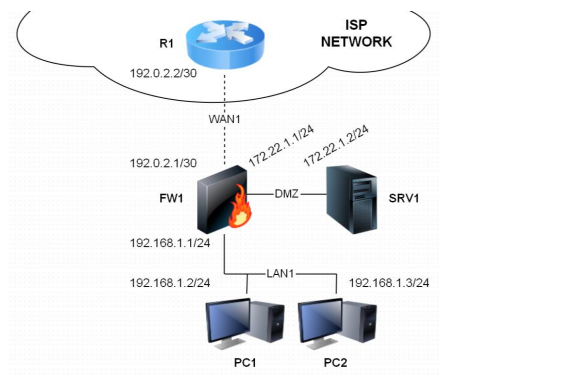
Όχι, καθώς απορρίπτεται από τον κανόνα 2999.

### 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: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης



### 5.1

192.168.1.1/24

### 5.2

10.0.0.1/30

### 5.3



### 5.4

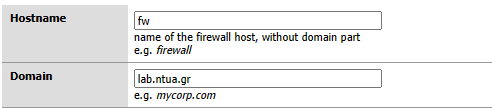
Τις αναμενόμενες 4.

### 5.5

172.22.1.1/24

### 5.6

System -> General setup ->



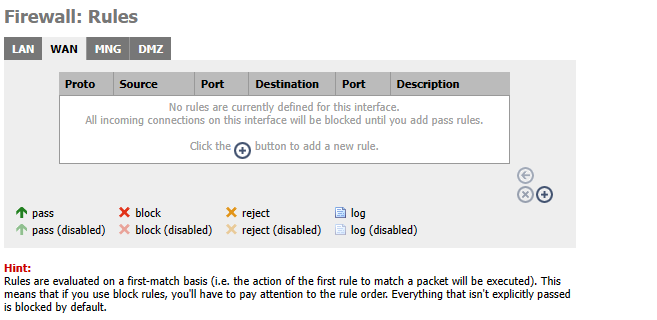
### 5.7



**Save**

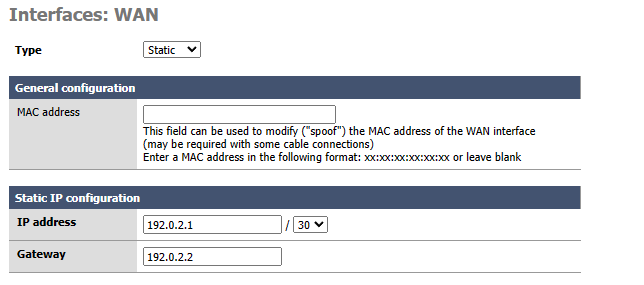
### 5.8

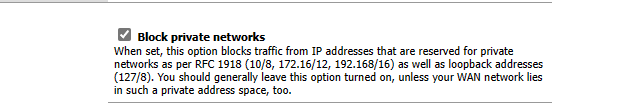
Όχι, δεν υπάρχουν.



### 5.9

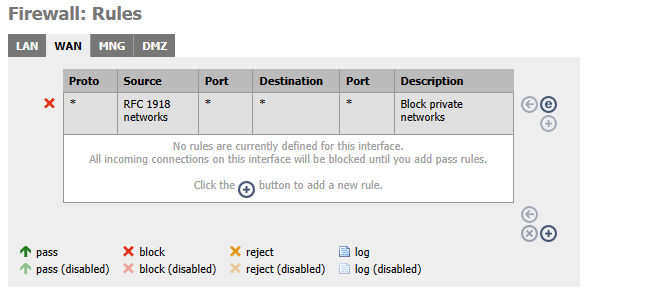
Interfaces -> WAN





### 5.10

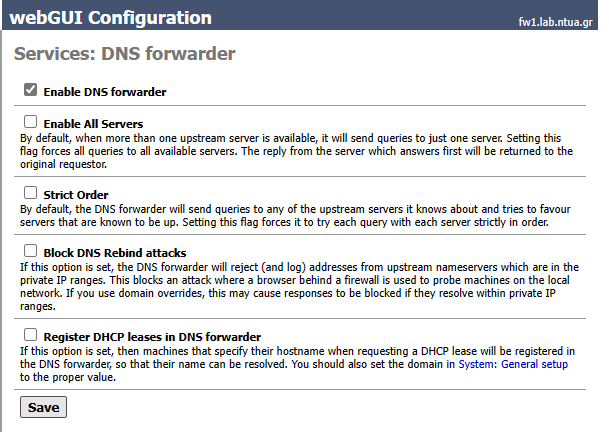
Ναι, υπάρχουν.



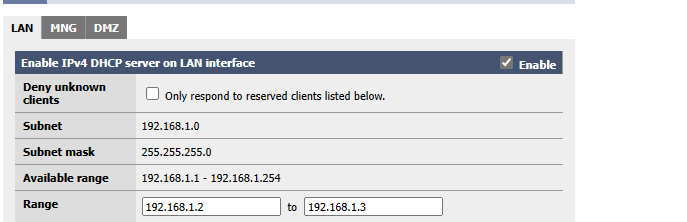
### 5.11

Όχι, καμία.

### 5.12



### 5.13



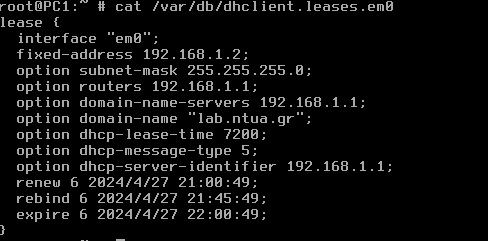
### 5.14

Αποδόθηκε η 192.168.1.2 /24 στο PC1.

**cat /etc/resolv.conf** --> nameserver 192.168.1.1

**netstat -rn** --> default 192.168.1.1

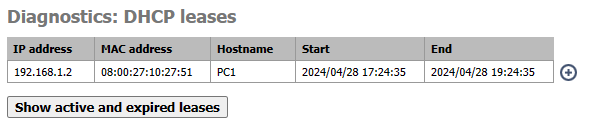
ή απλούστερα cat /var/db/dhclient.leases.em0



### 5.15

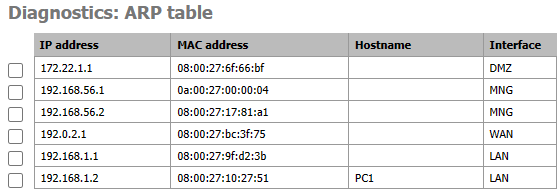
Προκειμένου να χρησιμοποιηθεί η διεπαφή του FW1 στο LAN1 ως DNS για τους πελάτες DHCP.

### 5.16



### 5.17

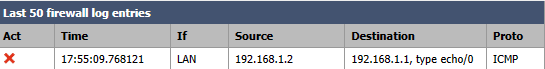
Bλέπουμε 6 εγγραφές.



### 5.18

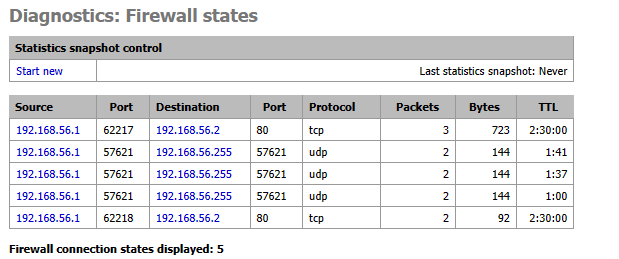
Όχι.

### 5.19



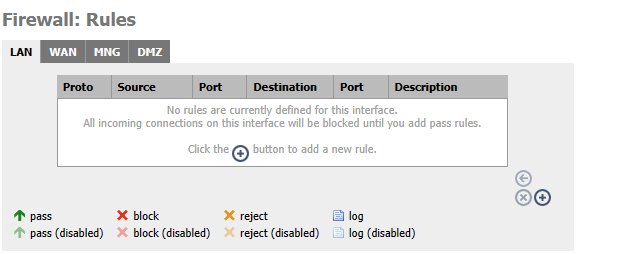
### 5.20

5

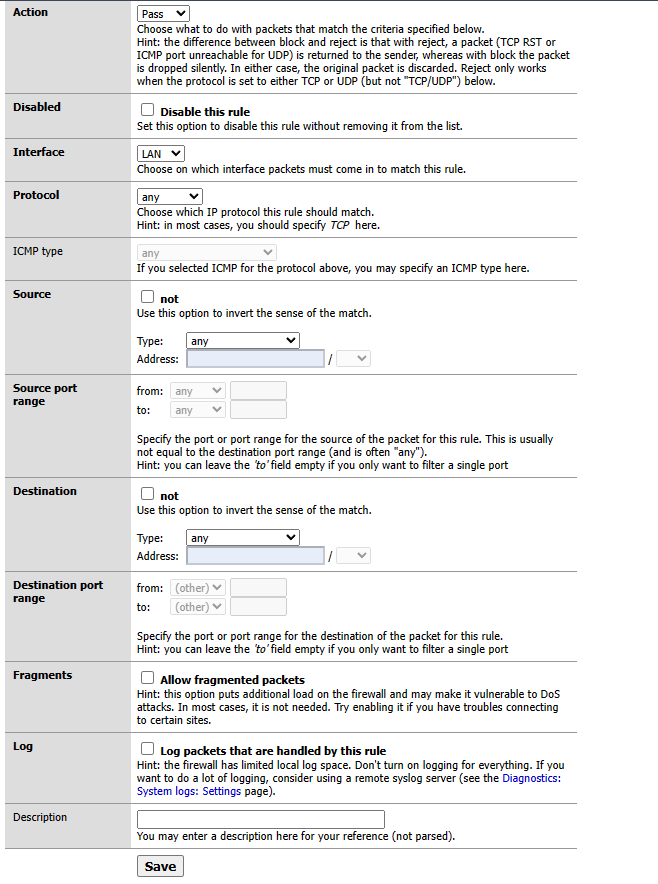


### 5.21

Κανέναν.



### 5.22



### 5.23

Ναι.

### 5.24

Όχι δεν μπορούμε.

### 5.25

**arp -a**

Ναι υπάρχει εγγραφή για τη διεπαφή του FW1 στο WAN1.

### 5.26

Action : Pass

Interface : WAN

Protocol : ICMP

Source : any

Destination : WAN address

### 5.27

Ναι.

### 5.28

Όχι δε μπορούμε, καθώς ο R1 δεν έχει ούτε default gateway, ούτε κατάλληλη εγγραφή για το δίκτυο του PC1.

### 5.29

Ναι μπορούμε, αφού το PC1 έχει default gateway και επιπλέον το NAT είναι by default ενεργοποιημένο, επομένως γίνεται μετάφραση NAT της ιδιωτικής διεύθυνσης του PC1 στη WAN address.

### 5.30

Όχι δεν παίρνουμε απάντηση αφού το SRV1 δεν έχει route to host.

### 5.31

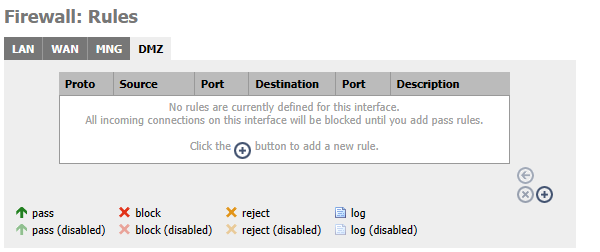
**route add default 172.22.1.1**

### 5.32

Ναι.

### 5.33

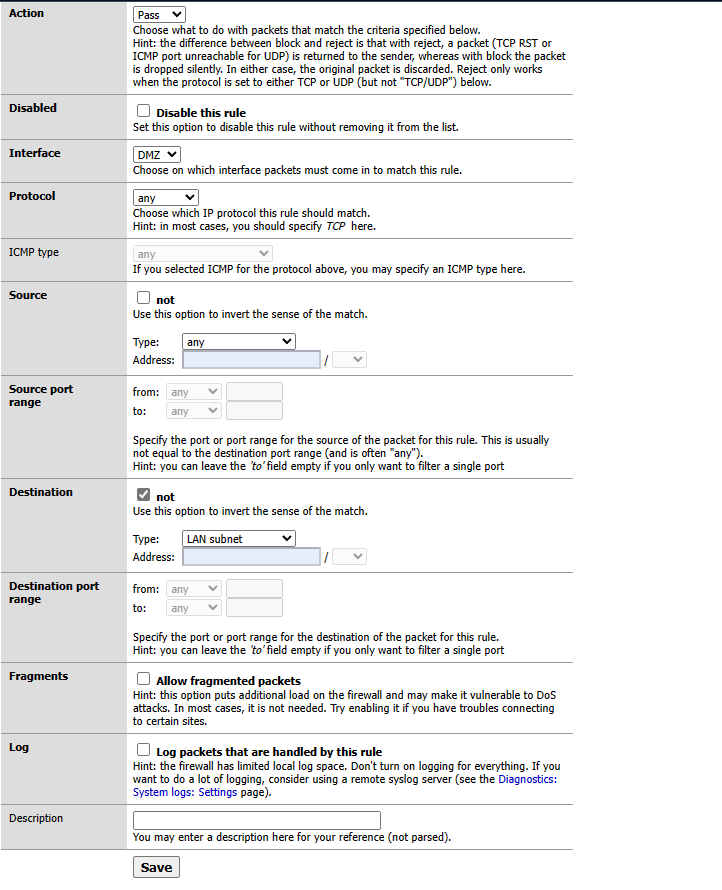
Όχι. Δεδομένου πως δεν έχουμε προσθέσει κανόνες στο firewall για το DMZ, όλα τα πακέτα μπλοκάρονται, ενώ προηγουμένως στο 5.32 μπορούσαμε αφού οι κανόνες είναι stateful, οπότε αφού επιτρεπόταν κίνηση από το PC1 προς τον SRV1, επιτρεπόταν και η αντίστροφη.



### 5.34

Όχι, για τον ίδιο λόγο με το 5.33.

### 5.35



### 5.36

Ναι.

### 5.37

Ναι.

### 5.38

Όχι, καθώς δεν υπάρχει κατάλληλη δρομολόγηση.

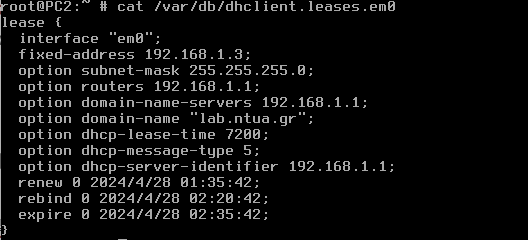
### 5.39

Ναι μπορούμε. Ο SRV1 στέλνει το πακέτο στο default gateway του (FW1), το οποίο και λόγω του firewall rule που βάλαμε γίνεται δεκτό. Στη συνέχεια, ο FW1 εξετάζει τον ARP πίνακά του και δεδομένου ότι το R1 δεν ανήκει στο LAN1 το προωθεί κανονικά, ενώ ο R1 απαντάει στην διεπαφή του FW1 στο WAN1.

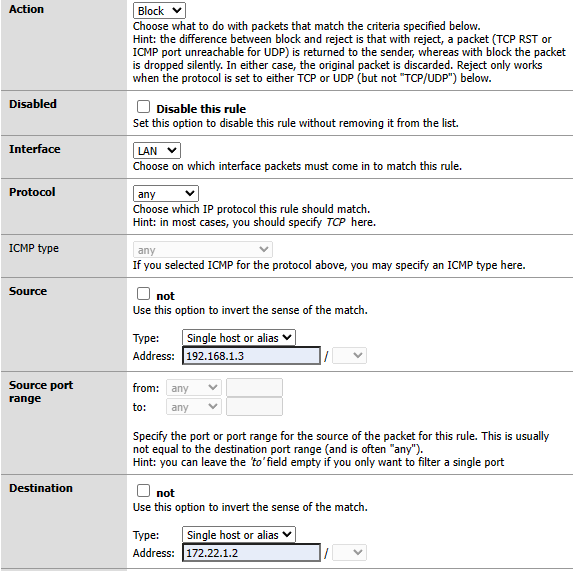
### 5.40

**dhclient em0**

IP = 192.168.1.3, Default Gateway = 192.168.1.1, DNS = 192.168.1.1

****

### 5.41



### 5.42

Πρέπει να τοποθετηθεί πριν, καθώς διαφορετικά γίνεται match πρώτα ο προηγούμενος κανόνας, ο οποίος και επιτρέπει όλη την κίνηση από το LAN1 προς οπουδήποτε.



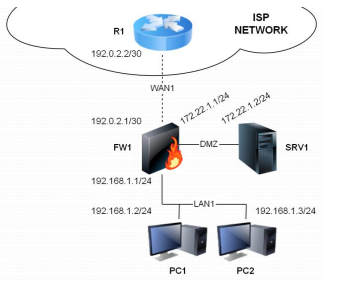
### 5.43

Όχι.

### 5.44

Ναι, καθώς απαγορεύσαμε μόνο τη διέλευση από το PC2 προς το SRV1, όχι προς όλο το DMZ.

# Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT



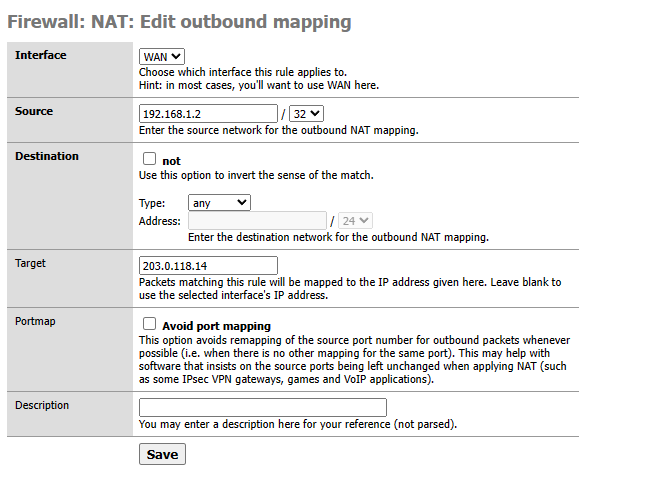
### 6.1

**ip route 203.0.118.0/24 192.0.2.1** --> R1(cli)

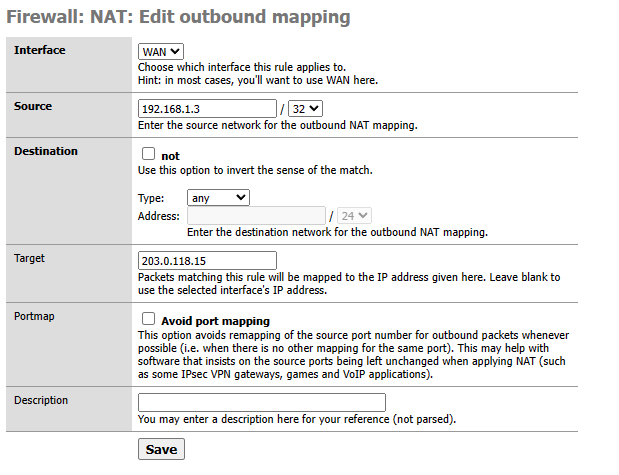
### 6.2

Firewall -> NAT -> Outbound -> Enable advanced outbound NAT

### 6.3



### 6.4



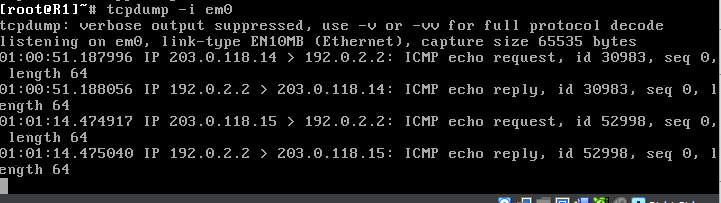
### 6.5

**tcpdump -i em0**

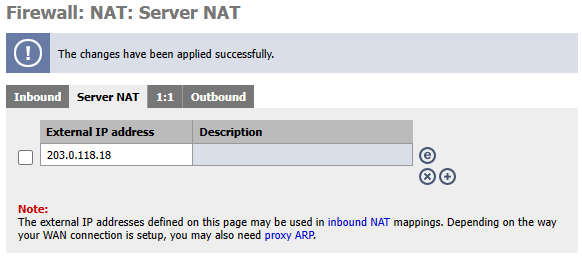
### 6.6

Του PC1 φτάνουν με την IP : 203.0.118.14

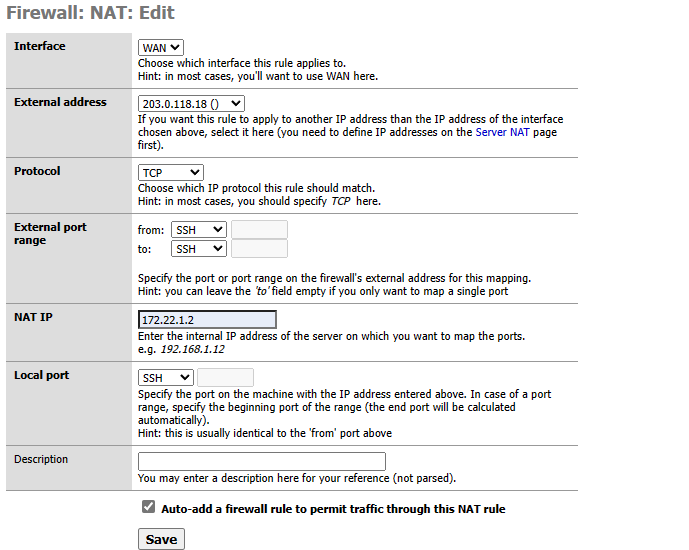
Του PC2 φτάνουν με την IP : 203.0.118.15



### 6.7



### 6.8



### 6.9



Τοποθετήθηκε κανόνας που επιτρέπει την TCP κίνηση προς τη θύρα 22 της διεύθυνσης 172.22.1.2 γιατί επιλέξαμε το «auto-add a firewall rule to permit traffic through this NAT rule».

### 6.10

SRV1

### 6.11

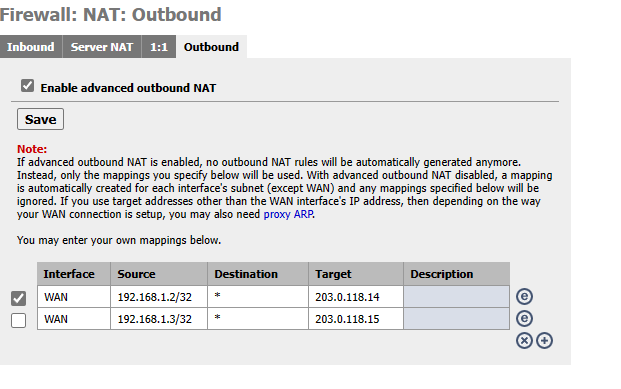
Με ping 203.0.118.18 το ping αποτυγχάνει αφού δεν έχουμε ορίσει κάποιον κανόνα στο WAN που να επιτρέπει την ICMP κίνηση από το R1 προς την 203.0.118.18

### 6.12

Ναι συνδεόμαστε στο SRV1. Τα πακέτα IP από το PC1/PC2 προς το SRV1 πηγαίνουν στο FW1 μετά στο R1, πίσω στο FW1 και φτάνουν στο SRV1.

Με tcpdump στα R1 και SRV1 το αντιλαμβανόμαστε.

### 6.13



Κάνοντας “tcpdump” στον R1 βλέπουμε πως λαμβάνει τα Requests από τη διεύθυνση 192.168.1.2. Ωστόσο, βλέποντας τον πίνακα δρομολόγησής του, βλέπουμε πως δε μπορεί να το δρομολογήσει πίσω στον PC1.

### 6.14

Ναι πλέον είναι επιτυχές γιατί τα icmp echo requests φτάνουν στον R1 με διεύθυνση πηγής 192.0.2.1 που είναι η δημόσια διεύθυνση πηγής IPv4 του FW1.

*«With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN) and any mappings specified below will be ignored.»*

### 6.15

Από τον R1 μπορούμε. Δεν μπορούμε όμως από τα PC1 και PC2.

### 6.16

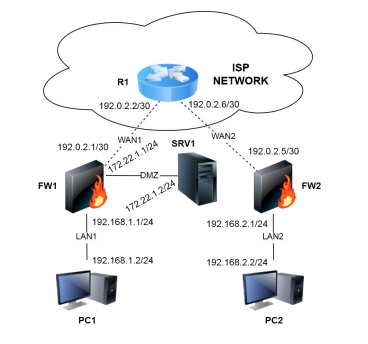
**tcpdump -vvei em0**

Βλέπουμε ότι ενώ ανταλλάσονται τα δύο πρώτα τεμάχια της χειραψίας , μετά γίνεται reset της σύνδεσης.

### 6.17

Η σημείωση στη σελίδα του inbound μας λέει ότι δεν γίνεται να έχουμε πρόσβαση σε NATed services χρησιμοποιώντας την WAN IP address από μέσα από το LAN. Αυτό ακριβώς προσπαθούμε να κάνουμε τώρα αφού τα πακέτα του PC2 έχουν πλεόν μεταφρασμένη διεύθυνση 192.0.2.1 που είναι η WAN address.

# Άσκηση 7: IPSec site-to-site VPN



### 7.1

{Προετοιμασία}

### 7.2

{Προετοιμασία}

### 7.3

{Προετοιμασία}

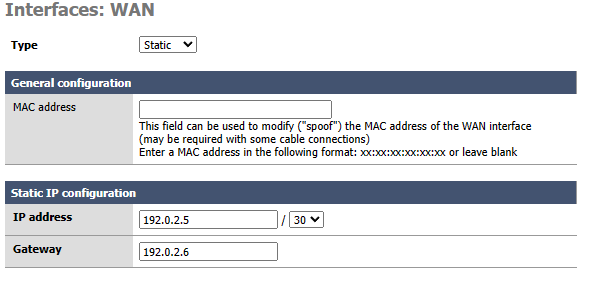
### 7.4

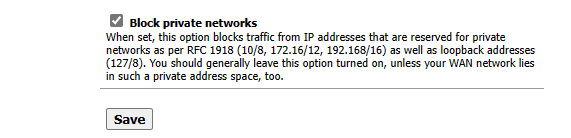
Ναι.

### 7.5



### 7.6





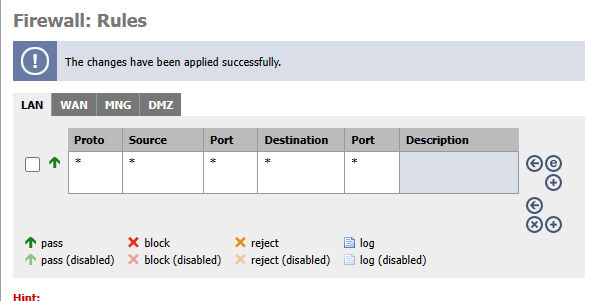
### 7.7

Oρίσαμε 192.168.2.1/24 στο LAN interface.

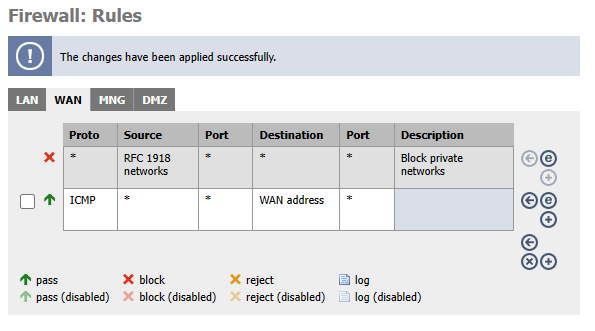
### 7.8

Eπανεκκινήσαμε το firewall.

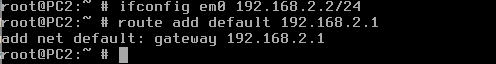
### 7.9



### 7.10



### 7.11



### 7.12

Nαι μπορούμε.

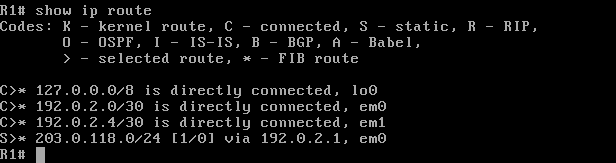
### 7.13

Nαι μπορούμε.

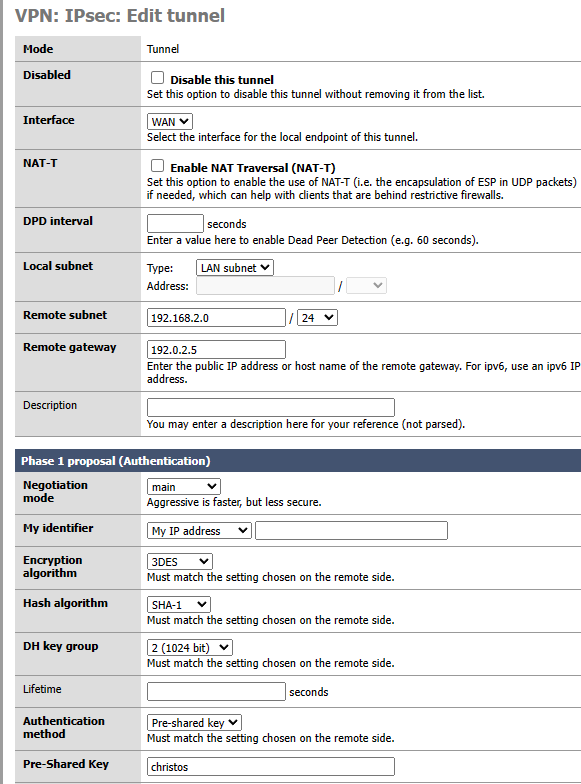
### 7.14

Όχι, δεν μπορούμε.

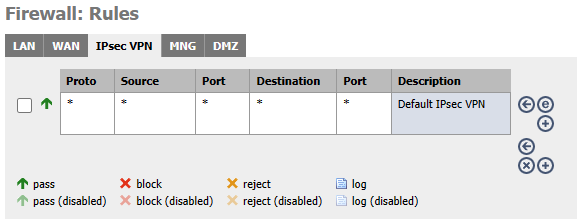
Η επικοινωνία αμφίδρομα είναι αδύνατη, καθώς ο R1 δε μπορεί να δρομολογήσει τα πακέτα. Παρουσιάζουμε τον πίνακα δρομολόγησής του:



### 7.15



### 7.16

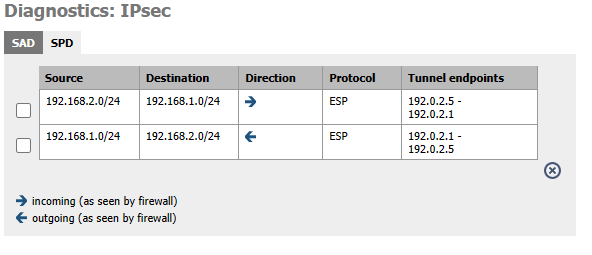


### 7.17

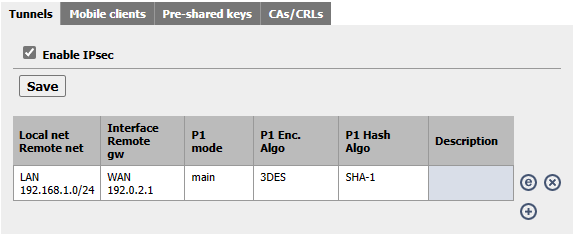
Όχι.

### 7.18

Ναι.

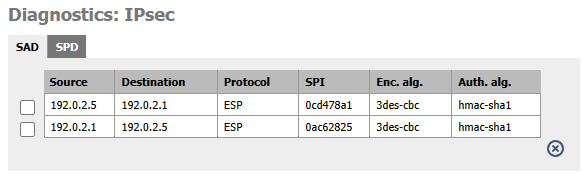


### 7.19



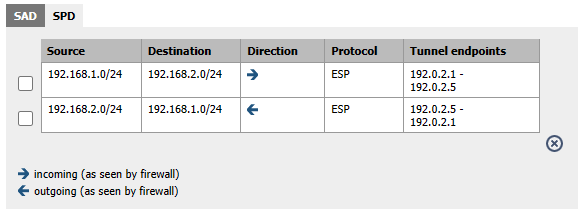
### 7.20

Nαι.(Είχα ξεχάσει ανοικτό ping από PC1 --> PC2). Φυσιολογικά, η απάντηση είναι όχι.



### 7.21

Ναι.



### 7.22

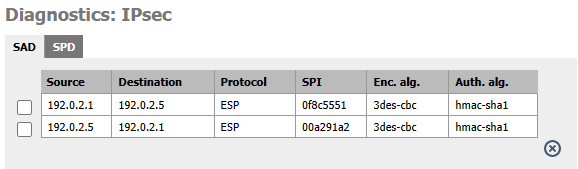
Ναι.

### 7.23

Ναι.

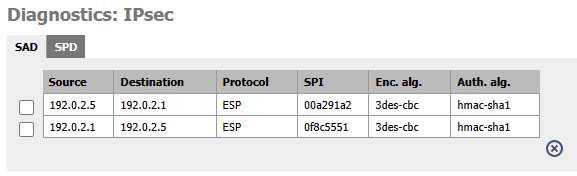
### 7.24

Ναι.



### 7.25

Ναι.



### 7.26

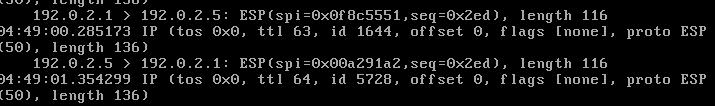
**tcpdump -vvvi em0 -A** --> R1

### 7.27

Όχι.

### 7.28

Εμφανίζονται ESP πακέτα. Τα πακέτα με πηγή το PC1 έχουν διεύθυνση πηγής 192.0.2.1 και διεύθυνση προορισμού 192.0.2.5. Αντίστοιχα, τα πακέτα με πηγή το PC2 έχουν διεύθυνση πηγής 192.0.2.5 και διεύθυνση προορισμού 192.0.2.1 .



### 7.29

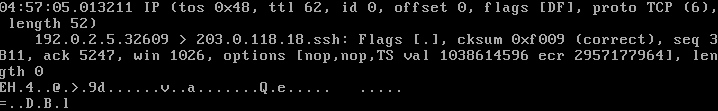
Όχι.

### 7.30

Ναι, μπορούμε.

Πλέον το PC2 δεν έχει το firewall του LAN1 (FW1) αλλά το FW2 και συνεπώς μπορεί να χρησιμοποιήσει τις NATed υπηρεσίες του FW1 αφού χρησιμοποιείται η WAN διεύθυνση του FW2 για τη σύνδεση με το SRV1.

### 7.31

Παρατηρούμε πακέτα TCP. Για τα πακέτα με πηγή το PC2 βλέπουμε διεύθυνση πηγής 192.0.2.5 , θύρα πηγής 32609 και διεύθυνση προορισμού 203.0.118.18 και θύρα προορισμού ssh (=22).

### 7.32

Είναι μεν κρυπτογραφημένα, όχι με το IPsec, αλλά με το SSH.