|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** | | **Όνομα PC:** |
| **Ομάδα:** | **Ημερομηνία:** | |

# 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 δεν μπορούμε, βλέπουμε permission denied.

1.4 ipfw list



1.5 ipfw show



1.6 ipfw zero

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

1.8 Ναι τώρα είναι επιτυχή.

1.9 Όχι. Permission denied.

1.10 ipfw add allow icmp from any to any

1.11 200



1.12 Ναι μπορούμε. Από το PC2 στο PC1 πάλι μπορούμε.

1.13 Γιατί by default η Traceroute χρησιμοποιεί πακέτα UDP στο FreeBSD τα οποία δεν ταιριάζουν στον κανόνα που προσθέσαμε και απορρίπτονται βάσει του default κανόνα. Για να λάβουμε απάντηση traceroute -I 192.168.1.3

1.14 ipfw add allow udp from me 33434-50000 to any 33434-50000

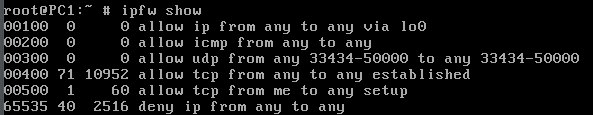
1.15 Όχι δεν μπορούμε.

1.16 ipfw add allow tcp from any to any established

ipfw add allow tcp from me to any setup

1.17 ssh lab@192.168.1.3

1.18 Εφαρμόσθηκε 1 φορά ο κανόνας για το setup της TCP σύνδεσης και 71 φορές ο κανόνας για τις ανοιχτές TCP συνδέσεις (τεμάχια που περιέχουν ACK ή RST) για την ανταλλαγή των άλλων δύο πακέτων της χειραψίας αλλά και των χαρακτήρων.



1.19 Όχι δεν μπορούμε γιατί το τεμάχιο TCP με σημαία SYN για εκκίνηση της TCP σύνδεσης δεν ταιριάζει με κάνεναν από τους κανόνες που ορίσαμε και απορρίπτεται

1.20 service ftpd onestart

1.21 Ναι μπορούμε.

***2***

2.1 kldload ipfw

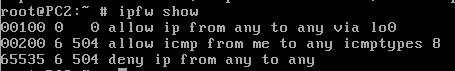
2.2 Όχι δεν μπορούμε.

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 δεν μπορούμε.

2.6 Ναι τα περνούν αλλά απορρίπτονται οι απαντήσεις.



2.7 Ναι τώρα μπορούμε.

2.8 Ναι μπορούμε.

2.9 Όχι τώρα δεν επιτυγχάνει διότι πέρασε ο χρόνος ζωής του δυναμικού κανόνα επειδή δεν υπήρξε κίνηση που να ταιριάζει με αυτόν (icmp μηνύματα μεταξύ PC1 και PC2).

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

2.11 Βλέπουμε έναν δυναμικό κανόνα για μία σύνδεση μεταξύ PC1 και PC2.



2.12 Ότι πλέον δεν υπάρχει αυτός ο δυναμικός κανόνας.

2.13 ipfw add allow udp from any to me

ipfw add allow icmp from me to any icmptypes 3

2.14 ipfw add allow udp from me to any

ipfw add allow icmp from any to me icmptypes 3

2.15 ipfw add allow udp from any to me

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 192.168.1.3 22 to me 22 setup keep-state

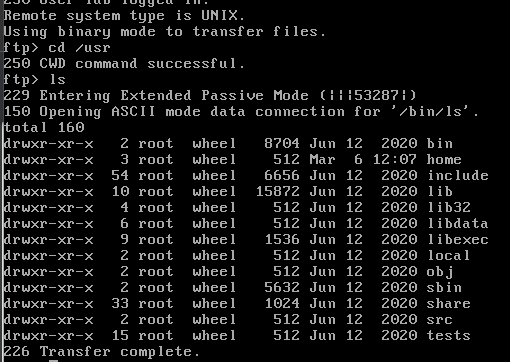
2.20 Ναι μπορούμε.

2.21 Όχι δεν μπορούμε.

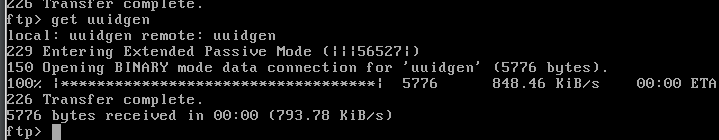
ipfw add allow tcp from any to me 21 setup keep-state

2.22 Γιατί η πρώτη εκτελείται χρησιμοποιώντας τη θύρα 21 του PC2 ενώ η δεύτερη προσπαθεί να το θέσει σε passive mode όπου ο server θα ανοίξει ένα άλλο τυχαίο port για το οποίο δεν υπάρχει κανόνας στο firewall.

2.23 ipfw add allow tcp from any to me 1024-65000 setup keep-state



2.24 Ναι μπορούμε.



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

PC1: ipfw add allow tcp from any 20 to me setup keep-state

2.26 Η χρήση πρωτοκόλλων όπως το ftp μεταξύ υπολογιστών που χρησιμοποιούν τείχη προστασίας είναι ιδιαίτερα περίπλοκη και απαιτεί πολύ ειδική ρύθμιση των τειχών προστασίας για να λειτουργούν οι διάφορες υπηρεσίες που προσφέρει το πρωτόκολλο.

2.27 kldunload ipfw

kldstat

##### 3

3.1 ifconfig em0 192.168.1.2/24

route add default 192.168.1.1

Αντίστοιχα για PC2.

3.2 interface em0

ip address 192.0.2.2/30

interface em1

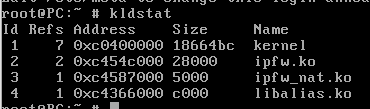
ip address 192.0.2.6/30

3.3 interface em0 192.0.2.5/30

route add default 192.0.2.6/30

3.4 service ftpd onestart

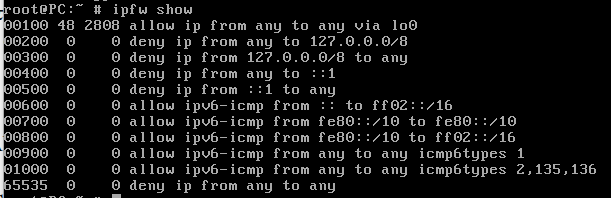
3.5 ipfw, ipfw\_nat, libalias



3.6 Το IPFW.

3.7 UNKNOWN

3.8 11 κανόνες. Ο τελευταίος είναι deny ip from any to any.



3.9 ipfw nat show config

3.10 Όχι δε μπορούμε

3.11 Όχι δε μπορούμε

3.12 ipfw nat 123 config ip 192.0.2.1 unreg\_only reset

3.13 ipfw add nat 123 ip4 from any to any

3.14 Ναι μπορούμε.

3.15 tcpdump -i em0

3.16 ipfw show

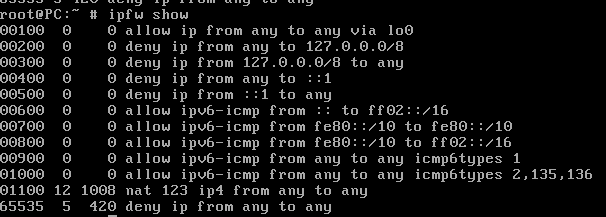
ipfw zero

3.17 192.0.2.1 (της διεπαφής του FW1 στο WAN1)

3.18 192.0.2.1

3.19 Ο nat 123 ip4 from any to any.

3.20 Εφαρμόστηκε 12 φορές, μία για κάθε εισερχόμενο ICMP request και το αντίστοιχο εξερχόμενο και ύστερα για κάθε εισερχόμενο ICMP reply από το WAN1 και κάθε εξερχόμενο στο LAN1. Συνολικά 3+3+3+3=12.



3.21 Ναι μπορούμε.

3.22 Ο ίδιος με πριν (nat 123 ip4 from any to any).

3.23 Όχι δεν ωθείτε διότι δεν πρόκειται για ιδιωτική διεύθυνση.

3.24 Ναι μπορούμε.

3.25 Δεν μπορούμε γιατί ο R1 δεν έχει διαδρομή προς το LAN1. Πρόκειται για θέμα δρομολόγησης και το καταλαβαίνουμε γιατί αν κάνουμε ping από τον SRV1 στο PC2 λαμβάνουμε destination host unreachable από τον R1.

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

3.27 Είναι επιτυχής. Συνδεθήκαμε στο PC2. Το καταλαβαίνουμε από το prompt και με την εντολή who.

3.28 ipfw nat 123 config ip 192.0.2.1 unreg\_only reset redirect\_addr 192.168.1.3 192.0.2.1 redirect\_port tcp 192.168.1.2:22 22

3.29 Στο PC1. Το εξακριβώνουμε από το prompt και με την εντολή who.

3.30 Στο PC2 Το καταλαβαίνουμε εκτελώντας sockstat -P tcp στα υποψήφια μηχανήματα.

3.31 Ναι μπορούμε.

3.32 Στο PC2.

3.33 Στο PC1.

##### 4

4.1 Όχι δεν μπορούμε.

4.2 Ναι γίνονται αποδεκτά. Αποτυγχάνει γιατί η επεξεργασία των πακέτων συνεχίζει με τον επόμενο κανόνα του τείχους προστασίας που είναι ο default και απορρίπτει τα πακέτα.

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

4.4 Ναι είναι

4.5 Στο FW1.

4.6 allow ip from any to any via lo0

allow ip from any to any via em0

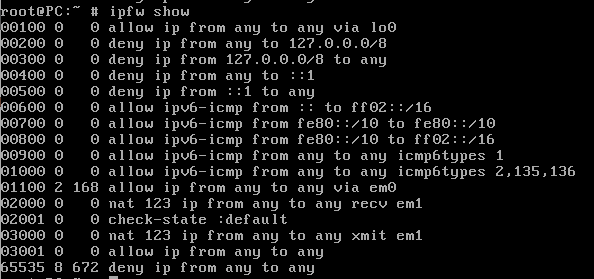
4.7 ipfw add 3000 nat 123 all from any to any xmit em1

4.8 ipfw add 3001 allow all from any to any

4.9 ipfw add 2000 nat 123 all from any to any recv em1

4.10 ipfw add 2001 check-state

4.11 Το FW1 διότι τα πακέτα γίνονται αποδεκτά από τον κανόνα 1100.



4.12 Το PC2.

4.13 Στο FW1.

4.14 Στο PC1.

4.15 Στο PC2.

4.16 Ναι μπορούμε.

4.17 Ναι μπορούμε.

4.18 Ναι μπορούμε.

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

4.20 ping 192.0.2.1 από το PC1.

ssh lab@192.0.2.1 από το PC1.

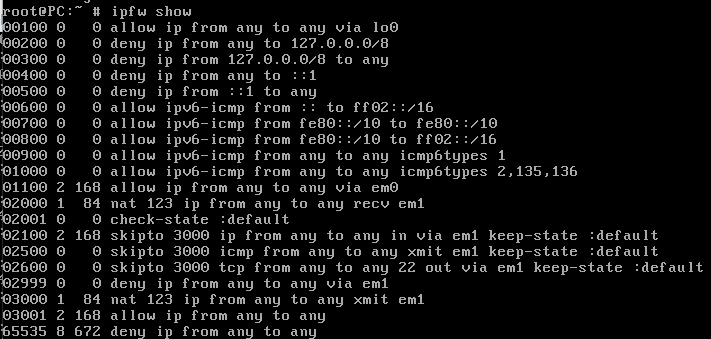
4.21 ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state

4.22 Ναι μπορούμε.

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

4.24 Ναι μπορούμε.

4.25 ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state. (Note to self: Χρησιμεύει επειδή είναι stateful ώστε η μετάφραση να εφαρμόζεται στα εξερχόμενα πακέτα. Αποτελέσματα μετά από Ping ενός πακέτου από SRV1 προς 192.0.2.1)



4.26 Το PC2.

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

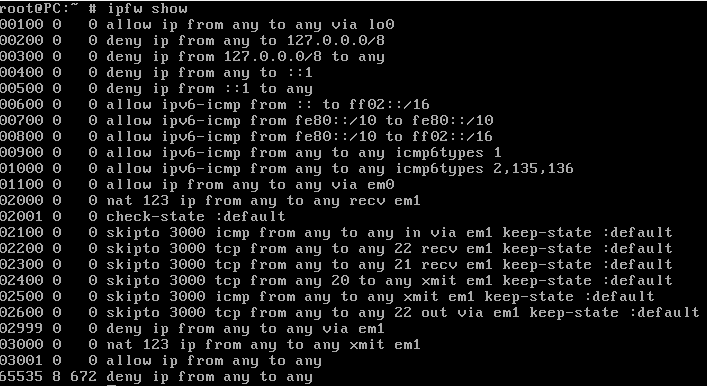
4.28 Στο PC1.

4.29 Όχι δεν επιτυγχάνει

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

ipfw add 2400 skipto 3000 tcp from any 20 to any xmit em1 keep-state

Συνολικά οι κανόνες:

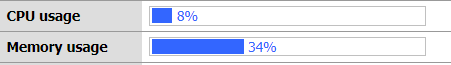


##### 5

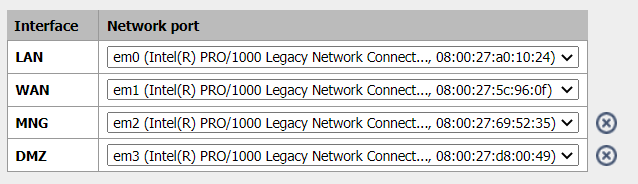
5.1 192.168.1.1/24

5.2 10.0.0.1/30

5.3 66%

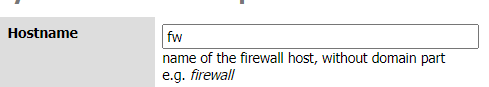


5.4 Τέσσερις

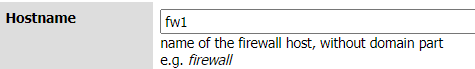


5.5 172.22.1.1/24

5.6 fw

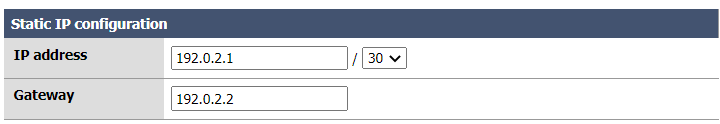


5.7



5.8 Όχι δεν υπάρχουν.

5.9



5.10 Ναι υπάρχει ένας κανόνας

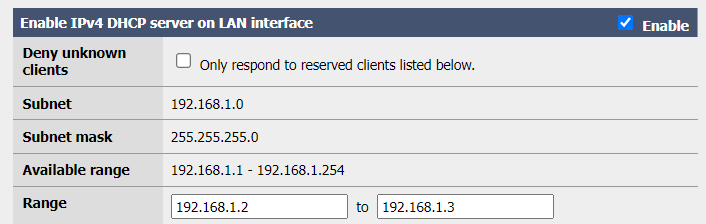


5.11 Όχι δεν είναι.

5.12



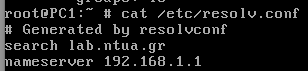
5.13



5.14 Διεύθυνση IP: 192.168.1.2

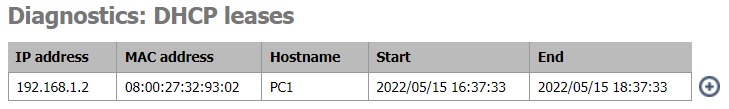
Default Gateway 192.168.1.1

DNS Server 192.168.1.1

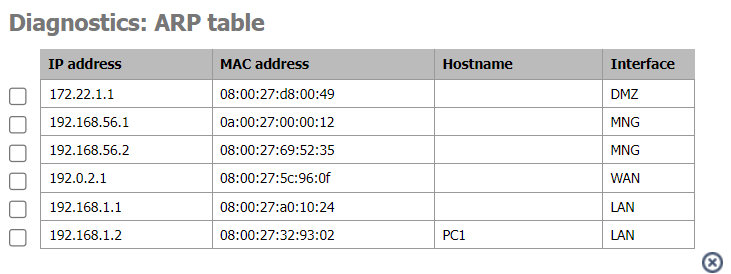


5.15 Γιατί οι clients θα έχουν ως DNS Sever το FW1 το οποίο όμως δεν γνωρίζει πολλά ονόματα οπότε πρέπει τα αιτήματα DNS που θα λαμβάνει από τους clients να τα προωθεί σε έναν DNS Forwarder ο οποίος θα μπορεί να απαντά.

5.16 DHCP leases.

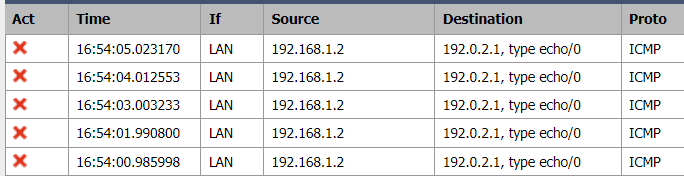


5.17 6

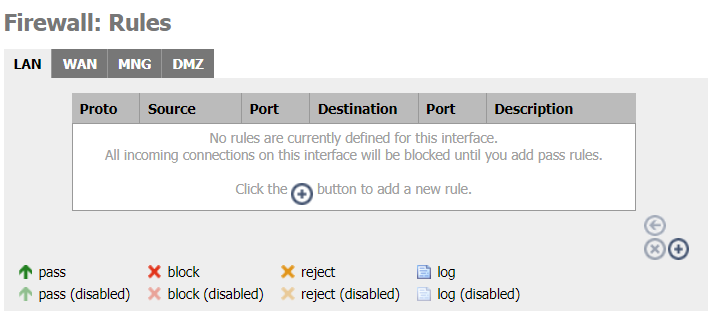


5.18 Όχι δεν μπορούμε.

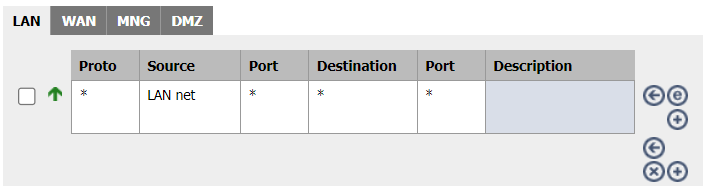
5.19 Βλέπουμε τα πακέτα του Ping που απορρίφθηκαν.

5.20 34

5.21 Κανέναν.



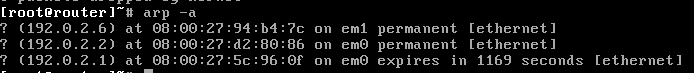
5.22



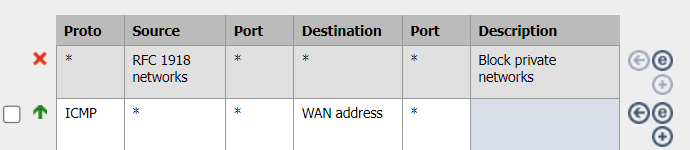
5.23 Ναι μπορούμε.

5.24 Όχι δεν μπορούμε.

5.25 Ναι βλέπουμε.



5.26



5.27 Ναι μπορούμε.

5.28 Όχι δεν μπορούμε διότι πακέτα με προορισμό το LAN1 στη διεπαφή του WAN1 απορρίπτονται.

5.29 Ναι μπορούμε. Ότι υπάρχει NAT ενεργοποιημένο by default για την εξερχόμενη κίνηση.

5.30 Όχι διότι ο SRV1 δεν έχει διαδρομή προς το LAN1.

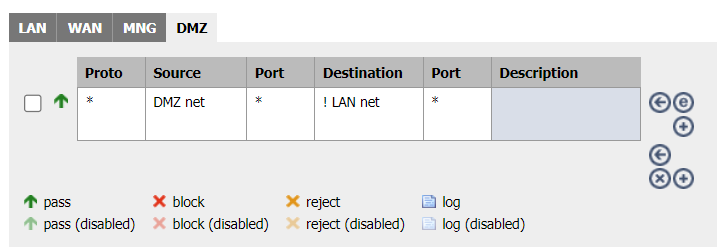
5.31 route add default 172.22.1.1

5.32 Ναι μπορούμε.

5.33 Όχι διότι το firewall μπλοκάρει τις εισερχόμενες συνδέσεις στο DMZ αφού δεν έχουμε προσθέσει κανόνα για pass.

5.34 Όχι για τον ίδιο λόγο με πριν.

5.35



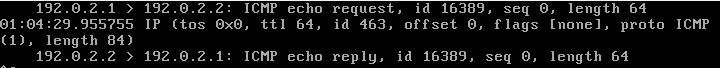
5.36 Ναι μπορούμε.

5.37 Ναι μπορούμε.

5.38 Όχι δεν μπορούμε. Αυτό συμβαίνει επειδή τα πακέτα request έχουν διεύθυνση προορισμού αυτήν του SRV1 και όχι του WAN οπότε δεν ταιριάζουν με κάποιον κανόνα και απρρίπτονται.



5.39 Ναι μπορούμε. Αυτό συμβαίνει επειδή τα requests που στέλνει ο server μεταφράζονται από το NAT και φτάνουν στον R1 με διεύθυνση πηγής αυτή του WAN, οπότε ο R1 απαντά εκεί και υπάρχει κανόνας που επιτρέπει πακέτα με προορισμό αυτή τη διεύθυνση.

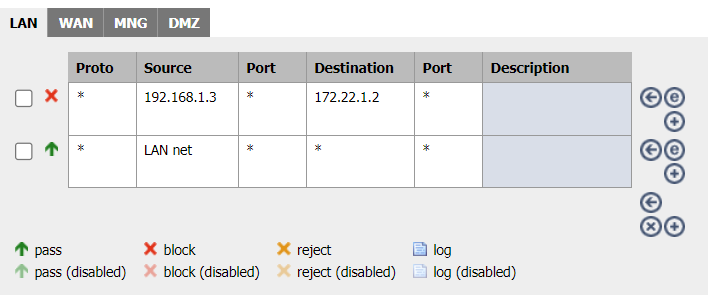


5.40 Διεύθυνση IP: 192.168.1.3

Default Gateway 192.168.1.1

DNS Server 192.168.1.1

5.41



5.42 Πριν διότι εξετάζονται με τη σειρά και ο πρώτος θα επιτρέψει όλη την κίνηση από το LAN1.

5.43 Όχι δεν μπορούμε.

5.44 Ναι μπορούμε διότι ο κανόνας που εισαγάγαμε απαγορεύει την κίνηση από το PC2 Μόνο προς τον SRV1.

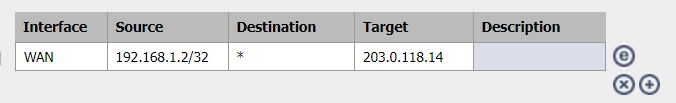
##### 6

6.1 ip route 203.0.118.0/24 192.0.2.1

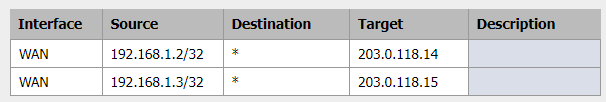
6.2



6.3

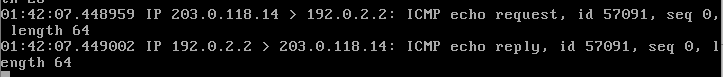


6.4

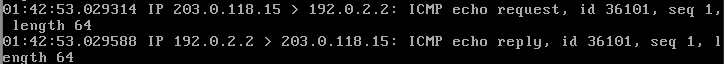


6.5 tcpdump -i em0

6.6 Ναι μπορούμε. Τα πακέτα φτάνουν με διεύθυνση 203.0.118.14

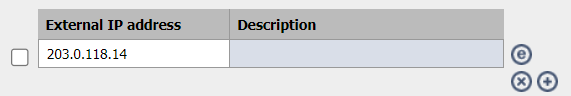


6.7 Ναι μπορούμε. Τα πακέτα φτάνουν με διεύθυνση 203.0.118.15

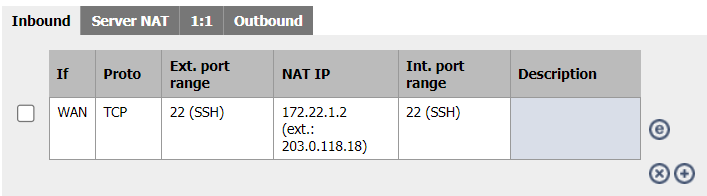


6.8 Διότι δεν υπάρχει κανόνας που να επιτρέπει εξερχόμενη κίνηση από το WAN1 και διότι δεν υπάρχει μετάφραση για εισερχόμενη κίνηση με διεύθυνση 203.0.118.14. Οι προηγούμενοι κανόνες είναι keep-state οπότε πρέπει η κίνηση να ξεκινά από το LAN προς το WAN για να μπορεί αυτό να απαντήσει.

6.9



6.10



6.11



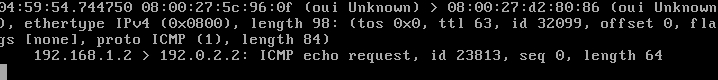
Αυτός διότι επιλέξαμε “Auto-add a firewall rule to permit traffic through this NAT rule” και πρέπει ο SRV1 να είναι προσβάσιμος από το WAN1.

6.12 Ναι μπορούμε. Στον SRV1.

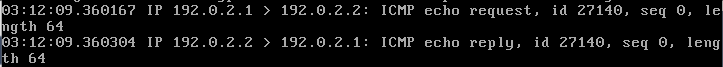
6.13 Όχι δεν μπορούμε διότι ούτε υπάρχει μετάφραση NAT για θύρες εκτός της 22 (που δεν χρησιμοποιεί το Ping) ούτε και κανόνας που να επιτρέπει την κίνηση από τον SRV1 στο LAN1.

6.14 Ναι μπορούμε. Ακολουθούν τη διαδρομή PC2, FW1, R1, FW1, SRV1, FW1, R1, FW1, PC2. Το βλέπουμε κάνοντας tcpdump στον R1.

6.15 Όχι δεν μπορούμε διότι τώρα η διεύθυνση του αποστολέα δεν μεταφράζεται από το NAT και τα πακέτα φτάνουν στον R1 με διεύθυνση πηγής την 192.168.1.2 για την οποία δε γνωρίζει κάποια διαδρομή.



6.16 Ναι είναι επιτυχές και τώρα βλέπουμε ως διεύθυνση πηγής και προορισμού τη NAT διεύθυνση 192.0.2.1.



6.17 Ναι εξακολουθούμε να μπορούμε. Από το PC2 πλέον δεν μπορούμε.

6.18 Γιατί το FW1 προωθεί το πακέτο με τη σημαία SYN στον R1, το οποίο το επιστρέφει στο FW1 όπου δε μεταφράζεται η διεύθυνση 192.0.2.1 οπότε το πακέτο στέλνεται στον SRV1 με αυτήν ως διεύθυνση πηγής οπότε απάντα σε αυτήν με SYN, ACK και το FW μη επιτρέποντας χρήση NATed υπηρεσιών χρησιμοποιώντας τη WAN IP διεύθυνση από εντός του LAN ή ενός optional network απαντά με Reset τερματίζοντας τη σύνδεση TCP.

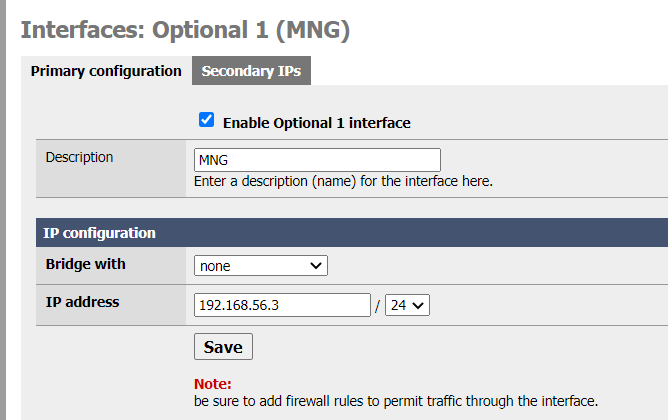
6.19 Όχι δεν ευθύνεται κανένας από τους δύο κανόνες. Ο λόγος είναι ότι δεν μπορούμε να χρησιμοποιήσουμε υπηρεσίες του NAT όπως το Port Forwarding που επιχειρούμε να χρησιμοποιήσουμε εδώ στέλνοντας κίνηση προς τη θύρα 22 στον SRV1 χρησιμοποιώντας τη WAN IP από το LAN ή ένα optional network όπως το DMZ.



##### 7

7.1 Το αποσυνδέουμε από το γραφικό περιβάλλον του Virtual Box.

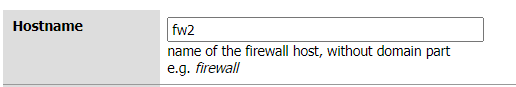
7.2 Μενού Interfaces->MNG.



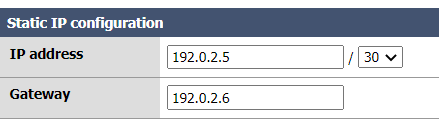
7.3 Το ξανασυνδέουμε από το γραφικό περιβάλλον του Virtual Box.

7.4 Ναι μπορούμε.

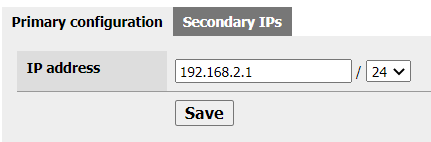
7.5 General setup -> Hostname



7.6 Interfaces->WAN



7.7 Interfaces->LAN

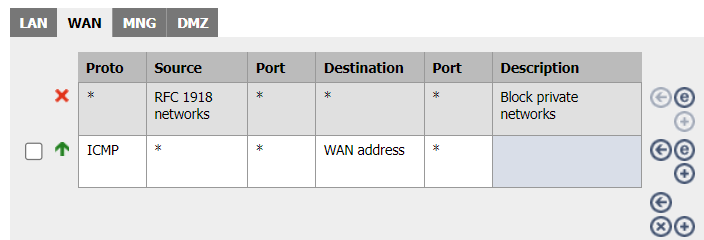


7.8 reboot από το Prompt που εμφανίστηκε.

7.9 Rules->LAN->+



7.10 Rules->WAN->+



7.11 ifconfig em0 192.168.2.2/24

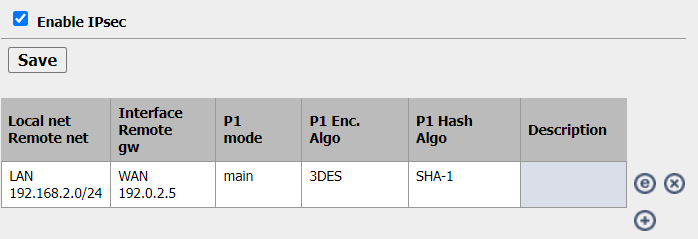
route add default 192.168.2.1

7.12 Ναι μπορούμε.

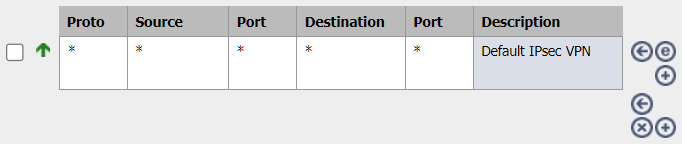
7.13 Ναι μπορούμε.

7.14 Όχι δεν μπορούμε γιατί αυτά είναι ιδιωτικά δίκτυα για τα οποία ο R1 δεν έχει διαδρομές.

7.15 VPN->IPsec->+



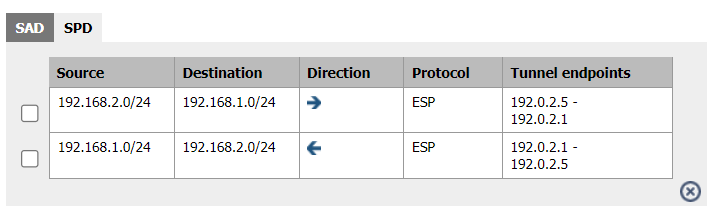
7.16



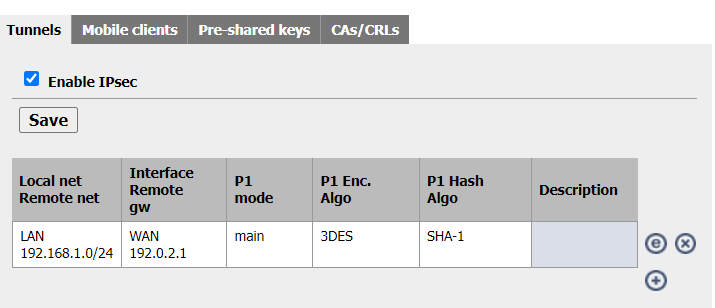
7.17 Όχι δε βλέπουμε να έχουν οριστεί.



7.18 Ναι έχουν ορισθεί πολιτικές προώθησης μεταξύ των δύο υποδικτύων.

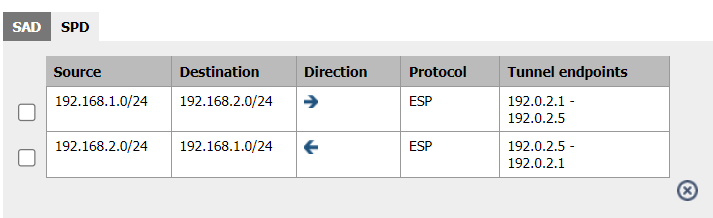


7.19 VPN->IPsec->+



7.20 Όχι δεν έχουν οριστεί σχέσεις μεταξύ των δύο υποδικτύων.

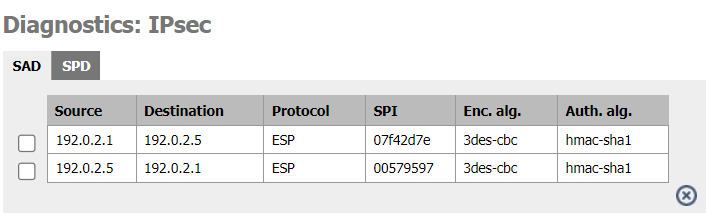
7.21 Ναι έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων.



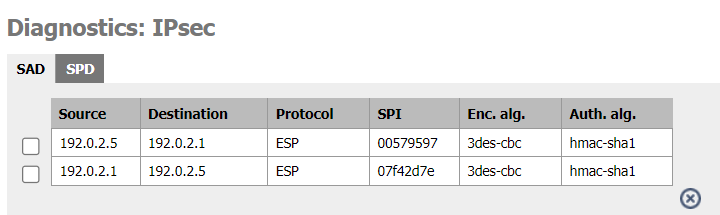
7.22 Ναι μπορούμε.

7.23 Ναι μπορούμε.

7.24 Ναι τώρα έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων.

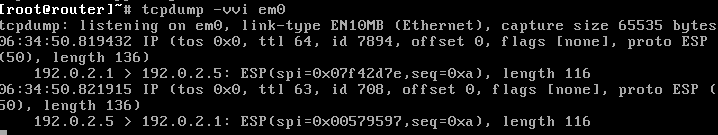


7.25 Ναι τώρα έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων.



7.26 tcpdump -vvi em0

7.27 Όχι δεν παρατηρούμε.



7.28 Εμφανίζονται πακέτα ESP με πηγή τη διεύθυνση του FW1 στο WAN1 και προορισμό τη διεύθυνση του FW2 στο WAN2 στο πακέτο που αντιστοιχεί στο request και αντίστροφα στο πεδίο που αντιστοιχεί στο reply.

7.29 Όχι δεν υπάρχει.

7.30 Ναι μπορούμε. Τι άλλαξε?

7.31 Παρατηρούμε πακέτα TCP με πηγή τη διεύθυνση του FW2 στο WAN2 (NAT address) και προορισμό την Public IP address του SRV1 (203.0.118.18).

7.32 Ναι είναι κρυπτογραφημένα αλλά όχι με το IPsec.