



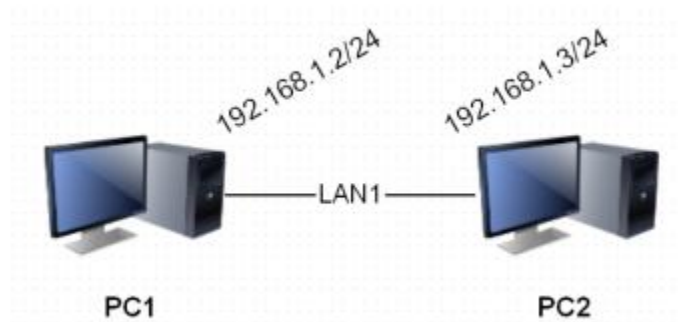
Εργαστήριο Δικτύων Υπολογιστών

ΕΡΓΑΣΤΗΡΙΑΚΗ 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 ipf --> PC1`

1.3

`kldstat --> PC1`

1.4

Όχι δε μπορούμε.

```
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
```

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

Όχι, « **Permission Denied** ».

1.11

`ipfw add allow icmp from any to any`

1.12

Έλαβε αριθμό 00200.

1.13

Ναι, πετυχαίνουν και τα δύο.

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

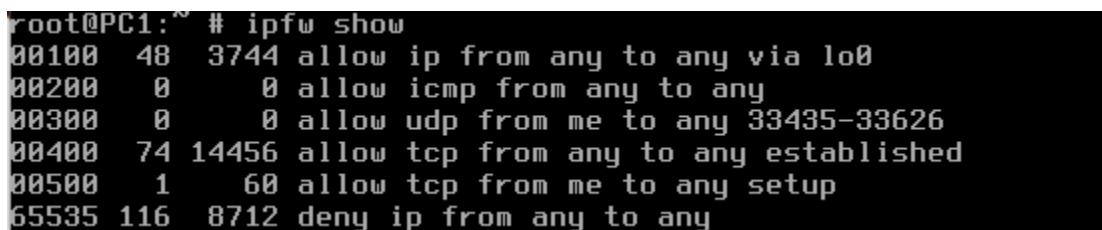
```
ipfw zero
```

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

```
ls
```

```
exit
```

1.19



```
root@PC1:~ # ipfw show
00100  48  3744 allow ip from any to any via lo0
00200   0    0 allow icmp from any to any
00300   0    0 allow udp from me to any 33435-33626
00400  74 14456 allow tcp from any to any established
00500   1   60 allow tcp from me to any setup
65535 116  8712 deny ip from any to any
```

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

```
ftp> get ztest
local: ztest remote: ztest
229 Entering Extended Passive Mode (|||51054|)
150 Opening BINARY mode data connection for 'ztest' (145280 bytes).
100% |*****| 141 KiB 3.50 MiB/s
226 Transfer complete.
145280 bytes received in 00:00 (3.46 MiB/s)
ftp> █
```

Βλέπουμε πως το αρχείο 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

```
root@PC2:~ # ipfw -d show
00100 160 13152 allow ip from any to any via lo0
00200 132 11088 allow icmp from me to any icmptypes 8 keep-state :default
00300 74 6216 allow icmp from any to me icmptypes 8 keep-state :default
65535 847 71148 deny ip from any to any
## Dynamic rules (1 136):
00300 74 6216 (5s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 :default
root@PC2:~ #
```

```
root@PC2:~ # ipfw -D show
## Dynamic rules (1 136):
00300 130 10920 (4s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0 :default
```

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.

```
root@PC1:~ # sftp lab@192.168.1.3
(lab@192.168.1.3) Password for lab@PC2:
Connected to 192.168.1.3.
sftp> get /etc/rc.conf
Fetching /etc/rc.conf to rc.conf
rc.conf                               100% 157    25.3KB/s   00:00
sftp> S
```

2.21

Δε μπορούμε, οπότε εισάγουμε τον παρακάτω κανόνα:

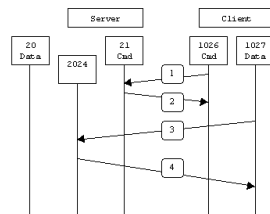
`ipfw add allow tcp from any to me 21 keep-state`

2.22

```
root@PC1:~ # ftp lab@192.168.1.3
Connected to 192.168.1.3.
220 PC2 FTP server (Version 6.00LS) ready.
331 Password required for lab.
Password:
230 User lab logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /usr
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||52412|)
```

2.23

When drawn, a passive mode FTP connection looks like this:



In step 1, the client contacts the server on the command port and issues the `pasv` command. The server then replies in step 2 with `PORT 2024`, telling the client which port it is listening to for the data connection. In step 3 the client then initiates the data connection from its data port to the specified server data port. Finally, the server sends back an ACK in step 4 to the client's data port.

While passive mode FTP solves many of the problems from the client side, it opens up a whole range of problems on the server side. The biggest issue is the need to allow any remote connection to high numbered ports on the server. Fortunately, many FTP daemons, including the popular `WU-FTPD` allow the administrator to specify a range of ports which the FTP server will use. See [Appendix 1](#) for more information.

The second issue involves supporting and troubleshooting clients which do (or do not) support passive mode. As an example, the command line FTP utility provided with Solaris does not support passive mode, necessitating a third-party FTP client, such as `ncftp`.

NOTE: This is no longer the case—use the `-p` option with the Solaris FTP client to enable passive mode!

With the massive popularity of the World Wide Web, many people prefer to use their web browser as an FTP client. Most browsers only support passive mode when accessing `ftp://` URLs. This can either be good or bad depending on what the servers and firewalls are configured to support.

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

Το `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 αναγκάζομαστε 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 λειτουργεί καθόλου.

2.27

```

root@PC1:~ # kldunload ipfw
IP firewall unloaded
root@PC1:~ # kldstat
Id Refs Address      Size Name
 1     5 0x8000000 18593a0 kernel
 2     1 0x16800000    6000 intpm.ko
 3     1 0x16806000    4000 smbush.ko
root@PC1:~ #
  
```

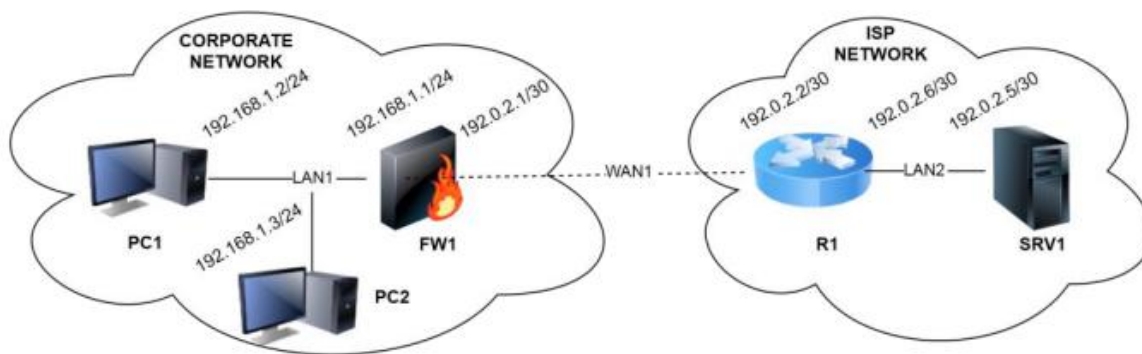


```

root@PC2:~ # kldunload ipfw
IP firewall unloaded
root@PC2:~ # kldstat
Id Refs Address      Size Name
 1    5  0x8000000 18593a0 kernel
 2    1  0x16800000   6000 intpm.ko
 3    1  0x16806000   4000 smbus.ko
root@PC2:~ #

```

Άσκηση 3: Απλό Network Address Translation



3.1

```
route add default 192.168.1.1
```

3.2

```
cli
```

```
hostname R1
```

```
configure terminal
```

```
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

```
root@FW1:~ # kldstat
Id Refs Address      Size Name
 1    11 0x8000000 18593a0 kernel
 2     1 0x16800000    6000 intpm.ko
 3     1 0x16806000    4000 smbus.ko
 4     2 0x1680a000   30000 ipfw.ko
 5     1 0x1683a000    6000 ipfw_nat.ko
 6     1 0x16840000   10000 libalias.ko
```

3.6

To ipfw.

33.4.1. Enabling IPFW

IPFW is included in the basic FreeBSD install as a kernel loadable module, meaning that a custom kernel is not needed in order to enable IPFW.

For those users who wish to statically compile IPFW support into a custom kernel, see [IPFW Kernel Options](#).

To configure the system to enable IPFW at boot time, add `firewall_enable="YES"` to `/etc/rc.conf`:

```
# sysrc firewall_enable="YES"
```

To use one of the default firewall types provided by FreeBSD, add another line which specifies the type:

```
# sysrc firewall_type="open"
```

3.7

```
root@FW1:~ # sysrc firewall_type
firewall_type: UNKNOWN
root@FW1:~ #
```

3.8

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

```
root@FW1:~ # ipfw list
00100 allow ip from any to any via lo0
00200 deny ip from any to 127.0.0.0/8
00300 deny ip from 127.0.0.0/8 to any
00400 deny ip from any to ::1
00500 deny ip from ::1 to any
00600 allow ipv6-icmp from :: to ff02::/16
00700 allow ipv6-icmp from fe80::/10 to fe80::/10
00800 allow ipv6-icmp from fe80::/10 to ff02::/16
00900 allow ipv6-icmp from any to any icmp6types 1
01000 allow ipv6-icmp from any to any icmp6types 2,135,136
65535 deny ip from any to any
root@FW1:~ #
```

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 em1_{FW1}.

3.18

Είναι επίσης 192.0.2.1

3.19

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

3.20

Βλέπουμε 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 έξοδο του από αυτό, οπότε και προκύπτει το 12.

```
root@FW1:~# ipfw show
00100 0 0 allow ip from any to any via lo0
00200 0 0 deny ip from any to 127.0.0.0/8
00300 0 0 deny ip from 127.0.0.0/8 to any
00400 0 0 deny ip from any to ::1
00500 0 0 deny ip from ::1 to any
00600 0 0 allow ipv6-icmp from :: to ff02::/16
00700 0 0 allow ipv6-icmp from fe80::/10 to fe80::/10
00800 0 0 allow ipv6-icmp from fe80::/10 to ff02::/16
00900 0 0 allow ipv6-icmp from any to any icmp6types 1
01000 0 0 allow ipv6-icmp from any to any icmp6types 2,135,136
01100 12 1000 nat 123 ip4 from any to any
65535 0 0 deny ip from any to any
```

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`.

```
lab@PC2:~ % hostname  
PC2  
lab@PC2:~ %
```

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.

```
root@SRV1:~ # ftp lab@192.0.2.1  
Connected to 192.0.2.1.  
220 PC2 FTP server (Version 6.00LS) ready.  
331 Password required for lab.  
Password:  
230 User lab logged in.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

3.31

Ναι με ls και ναι με get.

3.32

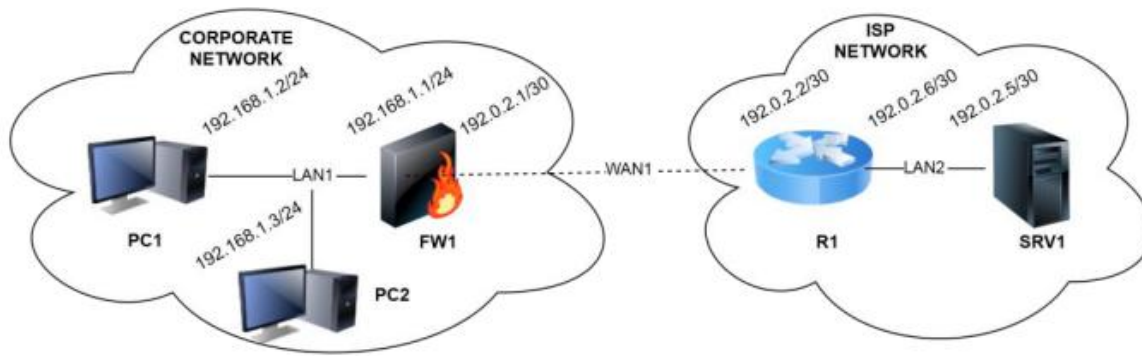
Απαντά το PC2.

```
root@PC1:~ # ftp lab@192.0.2.1  
Connected to 192.0.2.1.  
220 PC2 FTP server (Version 6.00LS) ready.  
331 Password required for lab.  
Password:  
230 User lab logged in.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

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 ring 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

To FW1.

4.12

To 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 em0`

4.20

Επιτυχάνουν 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

Ναι.

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

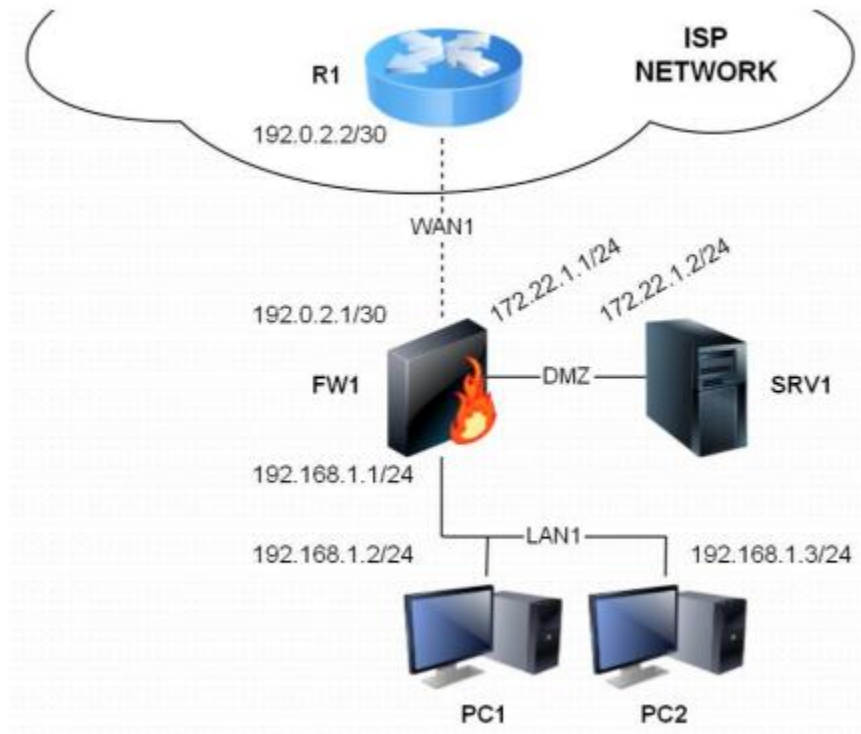
Όχι, καθώς απορρίπτεται από τον κανόνα 2999.

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

Memory usage

33%

5.4

Τις αναμενόμενες 4.

5.5

172.22.1.1/24

5.6

System -> General setup ->

Hostname	<input type="text" value="fw"/> name of the firewall host, without domain part e.g. <i>firewall</i>
Domain	<input type="text" value="lab.ntua.gr"/> e.g. <i>mycorp.com</i>

5.7

Hostname	<input type="text" value="fw1"/> name of the firewall host, without domain part e.g. <i>firewall</i>
----------	--


Save




5.8









Όχι, δεν υπάρχουν.

Firewall: Rules

LAN	WAN	MNG	DMZ
-----	-----	-----	-----

Proto	Source	Port	Destination	Port	Description
No rules are currently defined for this interface. All incoming connections on this interface will be blocked until you add pass rules. Click the  button to add a new rule.					



 pass  block  reject  log
 pass (disabled)  block (disabled)  reject (disabled)  log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

5.9

Interfaces -> WAN

Interfaces: WAN

Type

Static ▼

General configuration

MAC address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

Static IP configuration

IP address

 /

Gateway

☒ **Block private networks**

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.


5.10









Ναι, υπάρχουν.

Firewall: Rules

LAN WAN MNG DMZ

Proto	Source	Port	Destination	Port	Description
*	RFC 1918 networks	*	*	*	Block private networks

No rules are currently defined for this interface.
All incoming connections on this interface will be blocked until you add pass rules.
Click the  button to add a new rule.

 pass  block  reject  log
 pass (disabled)  block (disabled)  reject (disabled)  log (disabled)

5.11

Όχι, καμία.

5.12

webGUI Configuration fw1.lab.ntua.gr

Services: DNS forwarder

☒ **Enable DNS forwarder**

☐ **Enable All Servers**
By default, when more than one upstream server is available, it will send queries to just one server. Setting this flag forces all queries to all available servers. The reply from the server which answers first will be returned to the original requestor.

☐ **Strict Order**
By default, the DNS forwarder will send queries to any of the upstream servers it knows about and tries to favour servers that are known to be up. Setting this flag forces it to try each query with each server strictly in order.

☐ **Block DNS Rebind attacks**
If this option is set, the DNS forwarder will reject (and log) addresses from upstream nameservers which are in the private IP ranges. This blocks an attack where a browser behind a firewall is used to probe machines on the local network. If you use domain overrides, this may cause responses to be blocked if they resolve within private IP ranges.

☐ **Register DHCP leases in DNS forwarder**
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in [System: General setup](#) to the proper value.

Save

5.13

LAN **MNG** **DMZ**

Enable IPv4 DHCP server on LAN interface ☒ **Enable**

Deny unknown clients	<input type="checkbox"/> Only respond to reserved clients listed below.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	<input type="text" value="192.168.1.2"/> to <input type="text" value="192.168.1.3"/>

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`

```
root@PC1:~ # cat /var/db/dhclient.leases.em0
lease {
  interface "em0";
  fixed-address 192.168.1.2;
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.1;
  option domain-name "lab.ntua.gr";
  option dhcp-lease-time 7200;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.1.1;
  renew 6 2024/4/27 21:00:49;
  rebind 6 2024/4/27 21:45:49;
  expire 6 2024/4/27 22:00:49;
}
```

5.15

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

5.16

Diagnostics: DHCP leases

IP address	MAC address	Hostname	Start	End
192.168.1.2	08:00:27:10:27:51	PC1	2024/04/28 17:24:35	2024/04/28 19:24:35



Show active and expired leases

5.17

Βλέπουμε 6 εγγραφές.

Diagnostics: ARP table

	IP address	MAC address	Hostname	Interface
<input type="checkbox"/>	172.22.1.1	08:00:27:6f:66:bf		DMZ
<input type="checkbox"/>	192.168.56.1	0a:00:27:00:00:04		MNG
<input type="checkbox"/>	192.168.56.2	08:00:27:17:81:a1		MNG
<input type="checkbox"/>	192.0.2.1	08:00:27:bc:3f:75		WAN
<input type="checkbox"/>	192.168.1.1	08:00:27:9f:d2:3b		LAN
<input type="checkbox"/>	192.168.1.2	08:00:27:10:27:51	PC1	LAN

5.18

Όχι.

5.19

Last 50 firewall log entries					
Act	Time	If	Source	Destination	Proto
✗	17:55:09.768121	LAN	192.168.1.2	192.168.1.1, type echo/0	ICMP

5.20

5

Diagnostics: Firewall states

Statistics snapshot control							
Start new		Last statistics snapshot: Never					
Source	Port	Destination	Port	Protocol	Packets	Bytes	TTL
192.168.56.1	62217	192.168.56.2	80	tcp	3	723	2:30:00
192.168.56.1	57621	192.168.56.255	57621	udp	2	144	1:41
192.168.56.1	57621	192.168.56.255	57621	udp	2	144	1:37
192.168.56.1	57621	192.168.56.255	57621	udp	2	144	1:00
192.168.56.1	62218	192.168.56.2	80	tcp	2	92	2:30:00


Firewall connection states displayed: 5




5.21









Κανέναν.

Firewall: Rules

LAN
WAN
MNG
DMZ

Proto	Source	Port	Destination	Port	Description
No rules are currently defined for this interface. All incoming connections on this interface will be blocked until you add pass rules. Click the  button to add a new rule.					

 pass
 block
 reject
 log
 pass (disabled)
 block (disabled)
 reject (disabled)
 log (disabled)

5.22

Action	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>LAN</div> <div>Choose on which interface packets must come in to match this rule.</div>
Protocol	<div>any</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</div>
ICMP type	<div>any</div> <div>If you selected ICMP for the protocol above, you may specify an ICMP type here.</div>
Source	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: any</div> <div>Address: /</div>
Source port range	<div>from: any</div> <div>to: any</div> <div>Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port</div>
Destination	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: any</div> <div>Address: /</div>
Destination port range	<div>from: (other)</div> <div>to: (other)</div> <div>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</div>
Fragments	<div><input type="checkbox"/> Allow fragmented packets</div> <div>Hint: this option puts additional load on the firewall and may make it vulnerable to DoS attacks. In most cases, it is not needed. Try enabling it if you have troubles connecting to certain sites.</div>
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>
<div>Save</div>	

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.

Firewall: Rules

LAN **WAN** **MNG** **DMZ**

Proto	Source	Port	Destination	Port	Description
No rules are currently defined for this interface. All incoming connections on this interface will be blocked until you add pass rules. Click the  button to add a new rule.					

 pass  block  reject  log
 pass (disabled)  block (disabled)  reject (disabled)  log (disabled)

5.34

Όχι, για τον ίδιο λόγο με το 5.33.

5.35

Action	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>DMZ</div> <div>Choose on which interface packets must come in to match this rule.</div>
Protocol	<div>any</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</div>
ICMP type	<div>any</div> <div>If you selected ICMP for the protocol above, you may specify an ICMP type here.</div>
Source	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: any</div> <div>Address: /</div>
Source port range	<div>from: any</div> <div>to: any</div> <div>Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port</div>
Destination	<div><input checked="" type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: LAN subnet</div> <div>Address: /</div>
Destination port range	<div>from: any</div> <div>to: any</div> <div>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</div>
Fragments	<div><input type="checkbox"/> Allow fragmented packets</div> <div>Hint: this option puts additional load on the firewall and may make it vulnerable to DoS attacks. In most cases, it is not needed. Try enabling it if you have troubles connecting to certain sites.</div>
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

Save

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

```
root@PC2:~ # cat /var/db/dhclient.leases.em0
lease {
  interface "em0";
  fixed-address 192.168.1.3;
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.1;
  option domain-name "lab.ntua.gr";
  option dhcp-lease-time 7200;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.1.1;
  renew 0 2024/4/28 01:35:42;
  rebind 0 2024/4/28 02:20:42;
  expire 0 2024/4/28 02:35:42;
}
```

5.41

Action	<div>Block ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>any ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
ICMP type	<div>any ▾</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>192.168.1.3</div> / ▾</p>
Source port range	<p>from: <div>any ▾</div></p> <p>to: <div>any ▾</div></p> <p>Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>172.22.1.2</div> / ▾</p>

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.

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

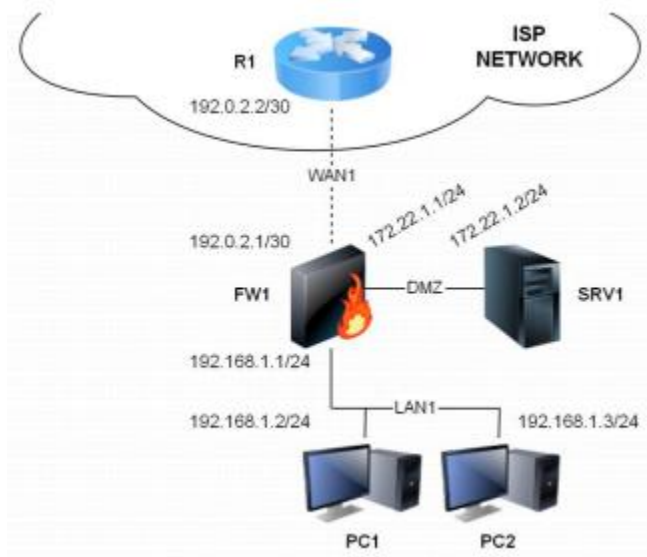
5.43

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

Firewall: NAT: Edit outbound mapping

Interface	<div>WAN ▼</div> <p>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</p>
Source	<div>192.168.1.2 / 32 ▼</div> <p>Enter the source network for the outbound NAT mapping.</p>
Destination	<p><input type="checkbox"/> not</p> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>any ▼</div></p> <p>Address: <div> / 24 ▼</div></p> <p>Enter the destination network for the outbound NAT mapping.</p>
Target	<div>203.0.118.14</div> <p>Packets matching this rule will be mapped to the IP address given here. Leave blank to use the selected interface's IP address.</p>
Portmap	<p><input type="checkbox"/> Avoid port mapping</p> <p>This option avoids remapping of the source port number for outbound packets whenever possible (i.e. when there is no other mapping for the same port). This may help with software that insists on the source ports being left unchanged when applying NAT (such as some IPsec VPN gateways, games and VoIP applications).</p>
Description	<div></div> <p>You may enter a description here for your reference (not parsed).</p>

Save

6.4

Firewall: NAT: Edit outbound mapping

Interface	<div>WAN ▾</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
Source	<div>192.168.1.3 / 32 ▾</div> <div>Enter the source network for the outbound NAT mapping.</div>
Destination	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: any ▾</div> <div>Address: / 24 ▾</div> <div>Enter the destination network for the outbound NAT mapping.</div>
Target	<div>203.0.118.15</div> <div>Packets matching this rule will be mapped to the IP address given here. Leave blank to use the selected interface's IP address.</div>
Portmap	<div><input type="checkbox"/> Avoid port mapping</div> <div>This option avoids remapping of the source port number for outbound packets whenever possible (i.e. when there is no other mapping for the same port). This may help with software that insists on the source ports being left unchanged when applying NAT (such as some IPsec VPN gateways, games and VoIP applications).</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

Save

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

```
[root@R1]~# tcpdump -i em0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 65535 bytes
01:00:51.187996 IP 203.0.118.14 > 192.0.2.2: ICMP echo request, id 30983, seq 0, length 64
01:00:51.188056 IP 192.0.2.2 > 203.0.118.14: ICMP echo reply, id 30983, seq 0, length 64
01:01:14.474917 IP 203.0.118.15 > 192.0.2.2: ICMP echo request, id 52998, seq 0, length 64
01:01:14.475040 IP 192.0.2.2 > 203.0.118.15: ICMP echo reply, id 52998, seq 0, length 64
```

6.7

Firewall: NAT: Server NAT

!

The changes have been applied successfully.

Inbound

Server NAT

1:1

Outbound

External IP address	Description
<input type="checkbox"/> 203.0.118.18	

e

x

+

Note:
The external IP addresses defined on this page may be used in inbound NAT mappings. Depending on the way your WAN connection is setup, you may also need proxy ARP.

6.8

Firewall: NAT: Edit

Interface

WAN

Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

External address

203.0.118.18 ()

If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define IP addresses on the Server NAT page first).

Protocol

TCP

Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

External port range

from: SSH to: SSH

Specify the port or port range on the firewall's external address for this mapping.
Hint: you can leave the 'to' field empty if you only want to map a single port

NAT IP

172.22.1.2

Enter the internal IP address of the server on which you want to map the ports.
e.g. 192.168.1.12

Local port

SSH

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
Hint: this is usually identical to the 'from' port above

Description

You may enter a description here for your reference (not parsed).

☒ Auto-add a firewall rule to permit traffic through this NAT rule

Save

6.9

<input type="checkbox"/>		TCP	*	*	172.22.1.2	22 (SSH)	NAT
--------------------------	--	-----	---	---	------------	----------	-----

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

Firewall: NAT: Outbound

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.

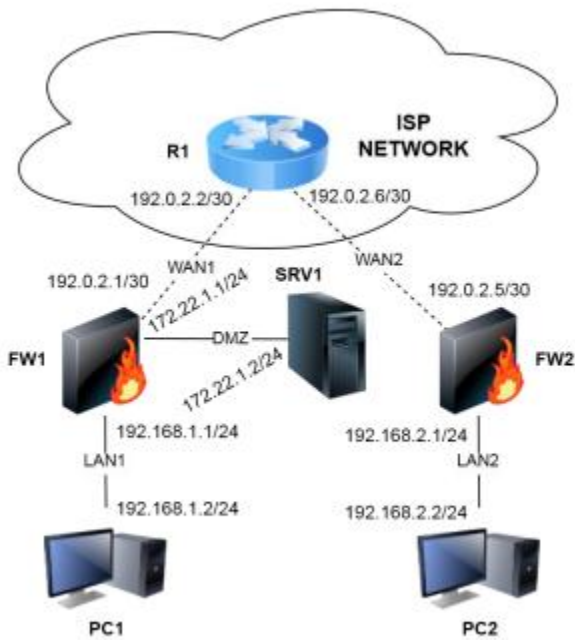
6.16

tcpdump -vvei em0

Βλέπουμε ότι ενώ ανταλλάσσονται 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 πλέον 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

Hostname

fw2

name of the firewall host, without domain part
e.g. *firewall*

7.6

Interfaces: WAN

Type Static ▾

General configuration

MAC address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

Static IP configuration

IP address

 / 30 ▾

Gateway

☒ **Block private networks**

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Save

7.7

Ορίσαμε 192.168.2.1/24 στο LAN interface.

7.8

Επανεκκινήσαμε το firewall.

7.9

Firewall: Rules



The changes have been applied successfully.

LAN

WAN

MNG

DMZ



Proto	Source	Port	Destination	Port	Description
*	*	*	*	*	



pass



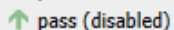
block



reject



log



pass (disabled)



block (disabled)




reject (disabled)





log (disabled)









Hint:

7.10**Firewall: Rules**

 The changes have been applied successfully.

LAN WAN **MNG** DMZ

	Proto	Source	Port	Destination	Port	Description
	*	RFC 1918 networks	*	*	*	Block private networks
<input type="checkbox"/> 	ICMP	*	*	WAN address	*	

 pass
  block
  reject
  log
 pass (disabled)
  block (disabled)
  reject (disabled)
  log (disabled)

7.11

```

root@PC2:~ # ifconfig em0 192.168.2.2/24
root@PC2:~ # route add default 192.168.2.1
add net default: gateway 192.168.2.1
root@PC2:~ #

```

7.12

Ναι μπορούμε.

7.13

Ναι 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:

```

R1# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo0
C>* 192.0.2.0/30 is directly connected, em0
C>* 192.0.2.4/30 is directly connected, em1
S>* 203.0.118.0/24 [1/0] via 192.0.2.1, em0
R1#

```

7.15

VPN: IPsec: Edit tunnel

Mode	Tunnel
Disabled	<input type="checkbox"/> Disable this tunnel Set this option to disable this tunnel without removing it from the list.
Interface	WAN ▼ Select the interface for the local endpoint of this tunnel.
NAT-T	<input type="checkbox"/> Enable NAT Traversal (NAT-T) Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
DPD interval	<input type="text"/> seconds Enter a value here to enable Dead Peer Detection (e.g. 60 seconds).
Local subnet	Type: LAN subnet ▼ Address: <input type="text"/> / <input type="text"/>
Remote subnet	<input type="text"/> / 24 ▼
Remote gateway	<input type="text"/> Enter the public IP address or host name of the remote gateway. For ipv6, use an ipv6 IP address.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

Phase 1 proposal (Authentication)

Negotiation mode	main ▼ Aggressive is faster, but less secure.
My identifier	My IP address ▼ <input type="text"/>
Encryption algorithm	3DES ▼ Must match the setting chosen on the remote side.
Hash algorithm	SHA-1 ▼ Must match the setting chosen on the remote side.
DH key group	2 (1024 bit) ▼ Must match the setting chosen on the remote side.
Lifetime	<input type="text"/> seconds
Authentication method	Pre-shared key ▼ Must match the setting chosen on the remote side.
Pre-Shared Key	<input type="text"/>

7.16

Firewall: Rules

LAN

WAN

IPsec VPN

MNG

DMZ

	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/>	*	*	*	*	*	Default IPsec VPN

pass

pass (disabled)

block

block (disabled)

reject

reject (disabled)

log

log (disabled)

7.17

Όχι.

7.18

Ναι.

Diagnostics: IPsec

SAD

SPD

	Source	Destination	Direction	Protocol	Tunnel endpoints
<input type="checkbox"/>	192.168.2.0/24	192.168.1.0/24		ESP	192.0.2.5 - 192.0.2.1
<input type="checkbox"/>	192.168.1.0/24	192.168.2.0/24		ESP	192.0.2.1 - 192.0.2.5

incoming (as seen by firewall)

outgoing (as seen by firewall)




7.19

Tunnels **Mobile clients** **Pre-shared keys** **CAs/CRLs**

☒ **Enable IPsec**

Save

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

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

Diagnostics: IPsec

SAD **SPD**

	Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
<input type="checkbox"/>	192.0.2.5	192.0.2.1	ESP	0cd478a1	3des-cbc	hmac-sha1
<input type="checkbox"/>	192.0.2.1	192.0.2.5	ESP	0ac62825	3des-cbc	hmac-sha1




7.21

Ναι.

SAD **SPD**

	Source	Destination	Direction	Protocol	Tunnel endpoints
<input type="checkbox"/>	192.168.1.0/24	192.168.2.0/24	➔	ESP	192.0.2.1 - 192.0.2.5
<input type="checkbox"/>	192.168.2.0/24	192.168.1.0/24	➔	ESP	192.0.2.5 - 192.0.2.1



➔ incoming (as seen by firewall)
➔ outgoing (as seen by firewall)

7.22

Ναι.

7.23

Ναι.

7.24

Ναι.

Diagnostics: IPsec

SAD **SPD**

	Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
<input type="checkbox"/>	192.0.2.1	192.0.2.5	ESP	0f8c5551	3des-cbc	hmac-sha1
<input type="checkbox"/>	192.0.2.5	192.0.2.1	ESP	00a291a2	3des-cbc	hmac-sha1

7.25

Ναι.

Diagnostics: IPsec

SAD **SPD**

	Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
<input type="checkbox"/>	192.0.2.5	192.0.2.1	ESP	00a291a2	3des-cbc	hmac-sha1
<input type="checkbox"/>	192.0.2.1	192.0.2.5	ESP	0f8c5551	3des-cbc	hmac-sha1

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 .

```
(50), length 136)
  192.0.2.1 > 192.0.2.5: ESP(spi=0x0f8c5551,seq=0x2ed), length 116
04:49:00.285173 IP (tos 0x0, ttl 63, id 1644, offset 0, flags [none], proto ESP
(50), length 136)
  192.0.2.5 > 192.0.2.1: ESP(spi=0x00a291a2,seq=0x2ed), length 116
04:49:01.354299 IP (tos 0x0, ttl 64, id 5728, offset 0, flags [none], proto ESP
(50), length 136)
```

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).

```
04:57:05.013211 IP (tos 0x48, ttl 62, id 0, offset 0, flags [DF], proto TCP (6),  
length 52)  
192.0.2.5.32609 > 203.0.118.18.ssh: Flags [.] , cksum 0xf009 (correct), seq 3  
811, ack 5247, win 1026, options [nop,nop,TS val 1038614596 ecr 2957177964], len  
gth 0  
EH.4..@.>.9d.....v..a.....Q.e.....  
=..D.B.l
```

7.32

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