

# LAB-10 (Firewalls & NATs)

Όνοματεπώνυμο : Νίκος Μπέλλος (el18183)	Όνομα PC : BELLOS-DELL-G3
Ομάδα : 3	Ημερομηνία : 05/06/2022

## Άσκηση 1: Ένα απλό τείχος προστασίας

1. `kldload ipfw`
2. `kldstat` → εμφανίζεται το ipfw.ko
3. Permission denied
4. `ipfw list`
5. `ipfw show`
6. `ipfw zero`
7. `ipfw add 100 allow all from any to any via lo0`
8. Ναι, είναι
9. Permission denied
10. `ipfw add 200 allow icmp from any to any`
11. Έλαβε α/α 200
12. Ναι και προς τις δύο κατευθύνσεις
13. Επειδή αντί για icmp το freebsd χρησιμοποιεί πακέτα UDP στο traceroute  
`traceroute -I 192.168.1.3`
14. `ipfw add 200 allow udp from any to any`
15. Permission denied
16. `ipfw add allow tcp from any to any out`  
`ipfw add allow tcp from any to any in`
17. `ipfw zero`, `ssh lab@192.168.1.3`
18. 32 για τα εξερχόμενα tcp  
29 για τα εισερχόμενα tcp  
Λόγω του 3-way handshake
19. Ναι μπορούμε, γιατί επιτρέπουμε και τις δύο (in / out) κατευθύνσεις μηνυμάτων tcp
20. `service ftpd onestart`
21. `ftp lab@192.168.1.3` → Ναι μπορούμε να συνδεθούμε και να κατεβάσουμε αρχεία

## Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

1. `kldload ipfw`
2. Όχι, Permission denied
3. `ipfw add 100 allow all from any to any via lo0`

4. `ipfw add allow icmp from me to any`
5. Όχι
6. Περνούν μόνο τα ICMP requests διότι το αντίστοιχο φίλτρο στο PC1 έχει τις διπλάσιες μετρήσεις από τι στο PC2
7. `ipfw delete 200`  
`ipfw add allow icmp from me to any keep-state`  
Ναι, μπορούμε (διότι λόγω του keep-state το firewall αναγνωρίζει ότι λαμβάνει απάντηση από ένα request που έστειλε το ίδιο το PC2)
8. Ναι, μπορώ
9. Όχι, διότι ο δυναμικός κανόνας σταμάτησε να ισχύει
10. `ipfw add allow icmp from any to me icmp types 8 keep-state`
11. Έχει προστεθεί ένας δυναμικός κανόνας (STATE icmp 192.168.1.2 < - > 192.168.1.3 : default)
12. Ο κανόνας διαγράφηκε
13. `ipfw add allow udp from any to me`  
`ipfw add allow icmp from me to any icmp types 3, 11`  
PC1 : `traceroute 192.168.1.3` → Λειτουργεί (παίρνει λίγη ώρα)
14. `ipfw add allow udp from me to any`  
`ipfw add allow icmp from any to me icmp types 3,11`
15. `ipfw add allow icmp from me to any icmp types 3,11`
16. `ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state`
17. Συνδεθήκαμε επιτυχώς με `ssh lab@192.168.1.3`
18. `ipfw add allow tcp from me to any 22 keep-state`
19. `ipfw add allow tcp from 192.168.1.3 to me 22`
20. Ναι, μπορούμε
21. Όχι, δεν μπορούμε, γιατί το ftp συνδέεται μέσω της πόρτας 21 (και όχι της 22 που έχουμε ορίσει πάνω)
22. Γιατί χρησιμοποιεί τη πόρτα 20 (ενώ η πρώτη χρησιμοποιεί την 21)
23. `ipfw add allow tcp from any 21 to me keep-state` (in passive ftp mode the client sends packets from the port 21)
24. Όχι, δεν μπορώ
25. PC2 : `ipfw add allow tcp from me 20 to any`  
PC1 : `ipfw add allow tcp from any 20 to me`
26. Το ftp δεν παρέχει κρυπτογράφηση άρα είναι μία καλή πρακτική να υπάρχει firewall για τέτοια μηνύματα
27. `kldunload ipfw`  
`kldstat`

### Άσκηση 3: Απλό Network Address Translation

- 
1. PC1 : `route add default 192.168.1.1`  
`hostname PC1`  
PC2 : `route add default 192.168.1.1`  
`hostname PC2`
  2. `vtysh`  
`con te`  
`host R1`  
`inte em0`  
`ip add 192.0.2.2/30`  
`exit`  
`inte em1`  
`ip add 192.0.2.6/30`
  3. `ifconfig em0 192.0.2.5/30`  
`route add default 192.0.2.6`  
`hostname SRV1`
  4. `service ftpd onestart`
  5. `kldstat` →
    - kernel
    - ipfw
    - ipfw\_nat
    - libalias
  6. To ipfw
  7. `sysrc firewall_type` → UNKNOWN
  8. 11 κανόνες  
'deny ip from any to any'
  9. `ipfw nat show config`
  10. Όχι, δεν μπορώ
  11. Όχι
  12. `ipfw nat 123 config ip 192.0.2.1 reset`
  13. `ipfw add 50 nat 123 ip from any to any`
  14. Ναι
  15. `tcpdump -i em0 -e -vvv`
  16. `ipfw zero`
  17. Η ip της διεπαφής του firewall στο WAN1
  18. 192.0.2.1
  19. 'allow ip from any to any'
  20. 12 φορές (στάλθηκαν 6 πακέτα και για κάθε πακέτο εφαρμόστηκε 2 φορές)
  21. Ναι
  22. 'allow ip from any to any'

23. Ναι, γιατί προέρχεται απο ιδιωτική διεύθυνση
24. Ναι
25. Όταν πάμε να συνδεθούμε υπάρχει το μήνυμα 'no route to host' αρα είναι πρόβλημα δρομολόγησης. (διότι ο R2 δεν ξέρει για την ύπαρξη του LAN1)
26. `ipfw nat 123 if em1 reset redirect_addr 192.168.1.3 192.0.2.1`
27. Ναι, είναι. Από το hostname
28. `ipfw nat 123 if em1 reset redirect_addr 192.168.1.3 192.0.2.1 redirect_port 192.168.1.2:22 22`
29. Συνδεθήκαμε στο PC1
30. Στο PC2, γιατί στο PC1 κατευθύνεται μόνο η κίνηση για SSH (port 22)
31. Ναι
32. Το PC2
33. Στο PC1

## Άσκηση 4: Τείχος προστασίας και NAT

---

1. `ipfw disable one_pass` → Όχι, δεν γίνεται ping
2. Ναι γίνονται. Αλλά επειδή το μήνυμα πρέπει να περάσει από όλους τους κανόνες, υπάρχει κάποιος που το απορρίπτει
3. `ipfw delete 50`  
`ipfw add 1100 allow all from any to any via em0`
4. Ναι
5. Στο FW1 γιατί έχουμε διαγράψει το κανόνα προώθησης στο πίνακα του NAT
6. Ο κανόνας που προσθέσαμε στο βήμα 3
7. `ipfw add 3000 nat 123 ip from any to any xmit em1`
8. `ipfw add 3001 allow all from any to any`
9. `ipfw add 2000 nat 123 ip from any to any recv em1`
10. `ipfw add 2001 check-state` (ελέγχει αν το μήνυμα είναι απάντηση σε ήδη υπάρχουσα σύνδεση)
11. Το FW1 (λόγω του κανόνα 1100)
12. Το PC2 (λόγω του κανόνα 2000)
13. Στο FW1 (λόγω του κανόνα 1100)
14. Στο PC1 (λόγω του κανόνα 2000)
15. Στο PC2 (λόγω του κανόνα 2000)
16. Ναι
17. Ναι
18. Ναι
19. `ipfw add 2999 deny all from any to any via em1`
20. Επιτυγχάνουν μόνο οι συνδέσεις στο Firewall που προέρχονται από το LAN1

21. `ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state`
22. Ναι
23. `ipfw add 2500 skipto 3000 tcp from any to any 22 out via em1 keep-state`
24. Ναι
25. `ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state`
26. To PC2
27. `ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state`
28. Στο PC1
29. Όχι
30. `ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state`  
`ipfw add 2400 skipto 3000 tcp from any 20 to any setup out via em1 keep-state`

## Άσκηση 5: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

---

1. LAN IP address : 192.168.1.1
2. WAN IP address : 10.0.0.1
3. Status > System → Memory usage 34%
4. Από το CLI 'Port configuration' → 4 δίκτυα
5. Interfaces > DMZ → IP address : 172.22.1.1
6. System > General Setup → Hostname : fw
7. Hostname: fw1 → Save
8. Όχι
9. Interfaces > WAN →
  - IP address: 192.0.2.1/30,
  - Gateway: 192.0.2.2
  - Block Private Networks
  - Save
10. Ναι, υπάρχει (Block private networks)
11. Όχι
12. Services > DNS forwarder
13. Services > DHCP server
14. `dhclient em0` → IP : 192.168.1.2, Gateway : 192.168.1.1, Port : 67
15. Χρειάστηκε γιατί η συσκευή του firewall λειτουργεί και σαν DNS server
16. Diagnostics > DHCP Leases
17. 7 εγγραφές
18. Όχι

19. Diagnostics > Logs → Βλέπουμε έναν error log list με τις τελευταίες 50 καταγραφές  
→ 'Clear log'
20. Diagnostics > Firewall states → 2 states
21. Κανένα
22. Firewall > Rules > LAN > 'Add new rule' → interface LAN from any to any
23. Ναι
24. Όχι
25. `arp -a` → Ναι βλέπουμε
- 26.

<input type="checkbox"/>		ICMP	*	*	WAN address	*	Allow all ICMP request with WAN address destination			
--------------------------	--	------	---	---	-------------	---	---	--	--	--

27. Ναι μπορώ
28. Γιατί δεν αποτελεί WAN address
29. Ναι, μπορούμε. Γίνεται μετάφραση των διευθύνσεων του ιδιωτικού δικτύου με τη διεύθυνση του Firewall στο WAN
30. Όχι, δεν μπορούμε γιατί δεν έχει οριστεί προκαθορισμένη πύλη στο SRV1
31. `route add default 172.22.1.1`
32. Ναι
33. Γιατί δεν έχει οριστεί εγγραφή στο firewall που να μας το επιτρέπει
34. Όχι, γιατί γιατί δεν μπορούμε να στείλουμε πακέτο από τη διεπαφή στο DMZ
- 35.

		Proto	Source	Port	Destination	Port	Description			
<input type="checkbox"/>		*	DMZ net	*	! LAN net	*				

36. Ναι
37. Ναι
38. Όχι, 'No route to host'
39. Ναι, γιατί έχει οριστεί default gateway και στο SRV1 και το FW1 οπότε η κίνηση κατευθύνεται προς το R1
40. `dhclient em0` → IP : 192.168.1.3, Gateway : 192.168.1.1, Port : 67
- 41.

<input type="checkbox"/>		*	192.168.1.3	*	172.22.1.2	*	Block traffic from PC2 to SRV1			
--------------------------	--	---	-------------	---	------------	---	--------------------------------	--	--	--

42. Πρέπει να τοποθετηθεί πριν τον ήδη υπάρχοντα γιατί αλλιώς θα περνάει όλη η κίνηση

	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/>	*	192.168.1.3	*	172.22.1.2	*	Block traffic from PC2 to SRV1
<input type="checkbox"/>	*	*	*	*	*	Allow all traffic from LAN1

43. Όχι δεν μπορώ

44. Ναι, μπορώ γιατί δεν υπάρχει κάποια εγγραφή που να μου μπλοκάρει αυτή τη διεύθυνση

## Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT

1. `route add 203.0.118.0/24 192.0.2.1`

2. Firewall > NAT > Outbound > Enable advanced outbound NAT

3.

	Interface	Source	Destination	Target	Description
<input type="checkbox"/>	WAN	192.168.1.2/32	*	203.0.118.14	

4.

<input type="checkbox"/>	WAN	192.168.1.3/32	*	203.0.118.15	
--------------------------	-----	----------------	---	--------------	--

5. `tcpdump -i em0 -e -vvv`

6. Ναι → 203.0.118.14

7. Ναι → 203.0.118.15

8. Δεν απαντάει, γιατί έχουμε ρυθμίσει μόνο outbound μετάφραση NAT και επίσης το FW1 δεν έχει εγγραφή στο πίνακα δρομολόγησης για το PC1

9. Firewall > NAT > Server NAT > External IP address : 203.0.118.18

10.

	If	Proto	Ext. port range	NAT IP	Int. port range	Description
<input type="checkbox"/>	WAN	TCP	22 (SSH)	172.22.1.2 (ext.: 203.0.118.18)	22 (SSH)	





11. Προστέθηκε ο παρακάτω κανόνας γιατί επιλέξαμε 'Auto-add a firewall rule to permit traffic' και προκειμένου να περνάνε πακέτα tcp για ssh στο DMZ ήταν αναγκαίος

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





12. Ναι, μπορούμε. Απαντάει ο SRV1 λόγω του κανόνα NAT που εισάγαμε προηγουμένως.
13. Όχι, δεν μπορούμε διότι ο κανόνας στο firewall επιτρέπει μόνο πακέτα για ssh
14. Ναι, συνδέεται. Τα μηνύματα περνάνε από το R1 όπως φαίνεται και στο tcpdump
15. Firewall > NAT > Outbound > 'delete selected mappings'.  
Όχι, δεν μπορώ γιατί υπάρχει εγγραφή στο firewall που μπλοκάρει τα private addresses
16. Ναι είναι επιτυχές, γιατί πλέον τα μηνύματα στο WAN μεταδίδονται με την ip 192.0.2.1
17. Ναι, μπορούμε. Από το PC2 δεν μπορούμε.
18. Γιατί η διεύθυνση του PC2 μεταφράζεται σε αυτή του FW1, περνάει από το R1, μετά μεταφράζεται η διεύθυνση του SRV1 στη πραγματική του διεύθυνση, αλλά όταν ο SRV1 απαντάει στέλνει τα μηνύματα στο FW1 και αυτό δεν τα προωθεί ποτέ στο PC2 γιατί δεν υπάρχει εσωτερική μετάφραση διευθύνσεων
19. Ευθύνεται ο κανόνας για το DMZ που δεν επιτρέπει επικοινωνία από το DMZ στο LAN1

## Άσκηση 7: IPSec site-to-site VPN

1. Cable connected turned off
2. Interfaces > MNG > ip address : 192.168.56.3
3. Cable connected turned on
4. Yes
5. System > General Setup > hostname : fw2
6. Interfaces > WAN > ip address : 192.0.2.5/30, Gateway : 192.0.2.6
7. Interfaces > WAN > ip address : 192.168.2.1/24
8. reboot
- 9.



	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> 	*	*	*	*	*	Allow all traffic from LAN2	  

10.

<input type="checkbox"/> 	ICMP	*	*	WAN address	*	Allow all ICMP request with WAN address destination	  
--	------	---	---	-------------	---	---	---


11. `ifconfig em0 192.168.2.2/24`, `route add default 192.168.2.1`
12. Ναι μπορώ
13. Όχι
14. Όχι (Destination Host Unreachable). Δεν υπάρχει εγγραφή για το LAN2 στο R1
15. VPN > IPsec > 'Enable IPsec'



Local net Remote net	Interface Remote gw	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description	
LAN 192.168.2.0/24	WAN 192.0.2.5	main	3DES	SHA-1		 

preshared key : 'nikolasbellos'

16.



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

17. Όχι

18. Ναι, έχουν οριστεί 2

	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

19. VPN > IPsec > 'Enable IPsec'

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		 

20. Όχι

21. Ναι υπάρχουν 2

	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

22. Ναι

23. Ναι

24. Ναι, προστέθηκαν 2 εγγραφές

	Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
<input type="checkbox"/>	192.0.2.1	192.0.2.5	ESP	0c38017e	3des-cbc	hmac-sha1
<input type="checkbox"/>	192.0.2.5	192.0.2.1	ESP	0d0f110c	3des-cbc	hmac-sha1

25. Ναι, προστέθηκαν 2 εγγραφές

	Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
<input type="checkbox"/>	192.0.2.5	192.0.2.1	ESP	0d0f110c	3des-cbc	hmac-sha1
<input type="checkbox"/>	192.0.2.1	192.0.2.5	ESP	0c38017e	3des-cbc	hmac-sha1

26. `tcpdump -i em0 -e -vvv`

27. Όχι

28. Παρατηρούμε ESP πακέτα. Η πηγή είναι η 192.0.2.1 και ο προορισμός η 192.0.2.5

29. Όχι

30. Ναι μπορούμε, γιατί το PC2 δεν ανήκει πλέον στο LAN1 για το οποίο υπάρχει ξεχωριστός κανόνας στο firewall

31. TCP με πηγή το 192.0.2.5 και προορισμό το 203.0.118.18

32. Ναι, είναι κρυπτογραφημένα