

# Εργαστήριο Δικτύων Υπολογιστών

Όνοματεπώνυμο: Παναγιώτης Σταματόπουλος	Όνομα PC: TakisAsus
Ομάδα: 2	Ημερομηνία: 12/5/2024

## Εργαστηριακή Άσκηση 10

### Τείχη προστασίας (Firewalls) και NAT

#### Άσκηση 1:

- 1.1: sysrc hostname="PC1"  
ifconfig em0 192.168.1.2/24  
sysrc hostname="PC2"  
ifconfig em0 192.168.1.3/24
- 1.2: kldload ipfw
- 1.3: kldstat
- 1.4: Όχι, permission denied
- 1.5: ipfw list  
65535 deny ip from any to any
- 1.6: ipfw add 100 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 icmp from any to any
- 1.12: 200 ( Previous + 100 )
- 1.13: Ναι
- 1.14: Το traceroute χρησιμοποιεί UDP αντί για ICMP επομένως  
δεν μπορεί να στείλει το μήνυμα
- 1.15: traceroute -I 192.168.1.3
- 1.16: Όχι
- 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

ls

exit

1.19: allow tcp from any to any established: 64

allow tcp from me to any setup: 1

1 φορά για την εγκατάσταση της σύνδεσης και 64 φορές  
για τη μεταφορά των δεδομένων (ls και αποτελέσματα  
κλπ)

1.20: Όχι, γιατί έχουμε επιτρέψει μόνο απερχόμενες συνδέσεις  
από τον PC1

1.21: service ftpd onestart

1.22: Ναι

## **Άσκηση 2:**

2.1: `kldload ipfw`

2.2: Όχι

2.3: `ipfw add allow all from any to any via lo0`

2.4: `ipfw add allow icmp from me to any icmp types 8`

2.5: Όχι

2.6: `ipfw zero`

`ping -c 1 192.168.1.2`

`ipfw show`

Ο μετρητής του κανόνα που προσθέσαμε αυξήθηκε,  
επομένως το πακέτο έφυγε από το firewall

2.7: `ipfw delete 00200`

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

Το ping πετυχαίνει

2.8: Ναι

2.9: Όχι, γιατί η επιλογή keep-state κάνει τη σύνδεση stateful και τα ping από το PC1 πετυχαίνουν όσο στέλνει ping ο PC2

2.10: `ipfw add allow icmp from any to me icmp types 8 keep-state`

2.11: Με την πρώτη εντολή βλέπουμε όλους τους τρέχοντες κανόνες, στατικούς και δυναμικούς

Με τη δεύτερη βλέπουμε μόνο το δυναμικό

2.12: Δεν υπάρχει πια δυναμικός κανόνας

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

`ipfw add allow icmp from me to any icmp types 3`

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

`ipfw add allow icmp from any to me icmp types 3`

2.15: `ipfw add allow udp from any to me 33434-33534`

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`

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

2.21: Δεν μπορούμε

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

2.22: Προσθέσαμε τη θύρα 21 για το Control FTP και όχι την 20 για το FTP Data Transfer

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: Το FTP χρησιμοποιεί μεγάλο εύρος θυρών το οποίο μπορεί να προκαλέσει προβλήματα ασφαλείας όταν ορίζουμε τους κανόνες του firewall

2.27: kldunload ipfw

### **Άσκηση 3:**

- 3.1: route add default 192.168.1.1
- 3.2: configure terminal
  - hostname R1
  - interface em0
  - ip address 192.0.2.2/30
  - exit
  - 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
- 3.5: kernel
  - intpm.ko
  - smbus.ko
  - ipfw.ko
  - ipfw\_nat.ko
  - libalias.ko
- 3.6: ipfw
- 3.7: Unknown
- 3.8: 11 κανόνες και τελευταίος ο default
- 3.9: ipfw nat show config
  - Κανένας
- 3.10: Όχι
- 3.11: Όχι
- 3.12: ipfw nat 123 config if em1 unreg\_only reset
- 3.13: ipfw add nat 123 all from any to any
- 3.14: Ναι
- 3.15: tcpdump -vvvni em0
- 3.16: ipfw show
  - ipfw zero
- 3.17: 192.0.2.1 (FW1)
- 3.18: 192.0.2.2 (R1)
- 3.19: nat 123 ip from any to any

- 3.20: 12: 3 Request και 3 Reply που επεξεργάζονται κατά την είσοδο και την έξοδο από το firewall το καθένα, δηλαδή 6 + 6
- 3.21: Ναι
- 3.22: Επίσης ο nat 123 ip from any to any
- 3.23: Ωθείται αλλά δεν μεταφράζεται
- 3.24: Ναι
- 3.25: Είναι θέμα δρομολόγησης, καθώς λαμβάνουμε μήνυμα No route to host και στον πίνακα δρομολόγησης του R1 δεν υπάρχει εγγραφή για το PC2
- 3.26: ipfw nat 123 config if em1 unreg\_only reset redirect\_addr 192.168.1.3 192.0.2.1
- 3.27: Ναι, συνδεθήκαμε στο PC2 όπως φαίνεται από το hostname ή εκτελούμε ifconfig και βλέπουμε ότι η IP address αντιστοιχεί στο 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: Αυτή τη φορά στο PC1 και το καταλαβαίνουμε με τον ίδιο τρόπο όπως πριν
- 3.30: Εκτελούμε netstat -a στα PC1 και PC2, παρατηρούμε λοιπόν έχουμε ενεργή ftp σύνδεση στο PC2
- 3.31: Ναι
- 3.32: Το PC2
- 3.33: Στο PC1

#### **Άσκηση 4:**

- 4.1: Όχι
- 4.2: Γίνονται αποδεκτά αλλά χωρίς το one-pass εκτελείται ο επόμενος κανόνας, ο default, με αποτέλεσμα να μην πετυχαίνει το ping
- 4.3: ipfw delete 01100  
ipfw add 1100 allow all from any to any via em0
- 4.4: Ναι
- 4.5: FW1
- 4.6: Ο κανόνας που προσθέσαμε στο 4.3
- 4.7: ipfw add 3000 nat 123 all from any to any xmit em1
- 4.8: ipfw add 3001 allow all from any to any
- 4.9: ipfw add 2000 nat 123 all from any to any recv em1
- 4.10: ipfw add 2001 check-state
- 4.11: FW1
- 4.12: ping -c 1 -R 192.0.2.1  
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: 4.11 και 4.13 δηλαδή PC1 ping 192.0.2.1 και PC1 ssh lab@192.0.2.1
- 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: PC2

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

4.28: PC1

4.29: O<sub>χ</sub>

4.30: 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  
xmit em1 keep-state



### **Άσκηση 5:**

5.1: 192.168.1.1/24

5.2: 10.0.0.1/30

5.3: 66%

5.4: 4 όλες είναι σωστές

5.5: 172.22.1.1/24

5.6: Hostname: fw

DNS: lab.ntua.gr

5.7: Hostname: fw1 → Save

5.8: Όχι

5.9: IP: 192.0.2.1/30

Default Gateway: 192.0.2.2

5.10: Ναι, ο block private networks

5.11: Όχι

5.12: Enable DNS forwarder

5.13: Enable

Range: 192.168.1.2 to 192.168.1.3

5.14: dhclient em0

IP address: 192.168.1.2

Default Gateway: 192.168.1.1

DNS: 192.168.1.1

5.15: Η διεπαφή του FW1 στο LAN1 αποτελεί DNS για τους  
DHCP clients

5.16: DHCP Leases

5.17: 5

5.18: Όχι

5.19: Βλέπουμε το αποτυχημένο ping

5.20: 1

5.21: Κανέναν

5.22: Protocol: any

5.23: Ναι

5.24: Όχι

5.25: Ναι

5.26:

### Firewall: Rules: Edit

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"/> <b>Disable this rule</b></div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>WAN ▾</div> <div>Choose on which interface packets must come in to match this rule.</div>
Protocol	<div>ICMP ▾</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"/> <b>not</b></div> <div>Use this option to invert the sense of the match.</div> <div>Type: any ▾</div> <div>Address: <input type="text"/> / ▾</div>
Source port range	<div>from: (other) ▾ <input type="text"/></div> <div>to: (other) ▾ <input type="text"/></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"/> <b>not</b></div> <div>Use this option to invert the sense of the match.</div> <div>Type: WAN address ▾</div> <div>Address: <input type="text"/> / ▾</div>
Destination port	<div>from: (other) ▾ <input type="text"/></div>

5.27: Ναι

5.28: Όχι γιατί ο R2 δεν έχει εγγραφή για το PC1 ούτε default gateway

5.29: Ναι, το NAT είναι ενεργοποιημένο αφού λόγω των stateful κανόνων το R1 επιστρέφει απάντηση στο PC1

5.30: `ifconfig em0 172.22.1.2/24`

Όχι γιατί ο SRV1 δεν έχει εγγραφή ή default gateway για να στείλει απάντηση

5.31: `route add default 172.22.1.1`

5.32: Ναι

5.33: Όχι, γιατί εκτελείται ο default κανόνας στο DMZ και το πακέτο του ping απορρίπτεται

- 5.34: Όχι, γιατί και πάλι εκτελείται μόνο ο default κανόνας απόρριψης
- 5.35: Destination: not LAN subnet
- 5.36: Ναι
- 5.37: Ναι
- 5.38: Όχι γιατί δεν έχει εγγραφή ή default gateway
- 5.39: Ναι, γιατί ο R1 στέλνει την απάντηση στη διεπαφή του FW1 στο WAN1
- 5.40: IP address: 192.168.1.3  
Default Gateway: 192.168.1.1  
DNS: 192.168.1.1
- 5.41: Block, Interface: LAN, Protocol: any, Source: Single host 192.168.1.3, Destination: Single host 172.22.1.2
- 5.42: Πριν, αλλιώς θα εκτελεστεί ο πρώτος που επιτρέπει όλη την κίνηση μέσα από το LAN
- 5.43: Όχι
- 5.44: Ναι, γιατί η διέλευση δεν απαγορεύεται σε όλο το DMZ δίκτυο αλλά μόνο στη διεύθυνση του SRV1

## Άσκηση 6:

- 6.1: `ip route 203.0.118.0/24 192.0.2.1`
- 6.2: Enable advanced outbound NAT → Save
- 6.3: Interface: WAN, Source: 192.168.1.2/32, Type: any, Target: 203.0.118.14
- 6.4: Interface: WAN, Source: 192.168.1.3/32, Type: any, Target: 203.0.118.15
- 6.5: `tcpdump -vvnvi em0`
- 6.6: Ναι, και τα 2 φτάνουν με τη δημόσια IP
- 6.7: Εκτελούμε την αλλαγή
- 6.8:

### Firewall: NAT: Edit

Interface	<div>WAN ▾</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
External address	<div>203.0.118.18 () ▾</div> <div>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 <a href="#">Server NAT</a> page first).</div>
Protocol	<div>TCP ▾</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</div>
External port range	<div>from: SSH ▾ <input type="text"/></div> <div>to: SSH ▾ <input type="text"/></div> <div>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</div>
NAT IP	<div>172.22.1.2 <input type="text"/></div> <div>Enter the internal IP address of the server on which you want to map the ports. e.g. 192.168.1.12</div>
Local port	<div>SSH ▾ <input type="text"/></div> <div>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</div>
Description	<div><input type="text"/></div> <div>You may enter a description here for your reference (not parsed).</div>

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

Save

- 6.9: `Pass TCP * * 172.22.1.2 22`
- 6.10: Ναι, στο SRV1
- 6.11: Όχι, γιατί δεν έχουμε ορίσει δρομολόγηση IP πακέτων προς τον SRV1

- 6.12: Ναι, τα πακέτα IP βρίσκονται σε loop μεταξύ του R1 και του FW1 μέχρι να μηδενιστεί το TTL τους, καθώς ο καθένας το δρομολογεί μέσω της default gateway στον άλλο  
Μπορούμε να το επιβεβαιώσουμε με traceroute
- 6.13: Όχι, γιατί πλέον ο R1 λαμβάνει τα μηνύματα του PC1 από τη διεύθυνση 192.168.1.2 την οποία δεν έχει στον πίνακα δρομολόγησης για να επιστρέψει την απάντηση
- 6.14: Ναι
- 6.15: Μπορούμε να συνδεθούμε μόνο από τον R1 γιατί η δρομολόγηση των πακέτων από και προς τον R1 δεν επηρεάστηκε από τις αλλαγές
- 6.16: Παρατηρούμε ότι στέλνονται από τον R1 στον SRV1 TCP [S] μηνύματα για την εγκατάσταση της σύνδεσης  
Ο SRV1 στέλνει στον R2 TCP [S,.] και περιμένει απάντηση [.] για να εγκατασταθεί η σύνδεση μάταια, οπότε και στέλνει TCP [R] για να τερματιστεί  
Όμως δεν παρατηρούμε κίνηση από τον R1 προς το WAN1 γιατί δεν έχει στον πίνακα δρομολόγησης για την 192.168.1.2 ή 192.168.1.3 με αποτέλεσμα τα πακέτα που λαμβάνει να χάνονται και η προσπάθεια σύνδεσης να τερματίζει από την πλευρά του PC1/2 λόγω timed out
- 6.17: Δεν είναι σφάλμα κάποιου από αυτούς τους 2, αλλά δρομολόγησης

## **Άσκηση 7:**

- 7.1: Αποσυνδέουμε το καλώδιο
- 7.2: 192.168.56.3 FW2
- 7.3: Επανασυνδέουμε το καλώδιο
- 7.4: Ναι
- 7.5: System → General setup → Hostname
- 7.6: IP: 192.0.2.5/30  
Default Gateway: 192.0.2.6
- 7.7: 192.168.2.1/24
- 7.8: Reboot
- 7.9: Action: Pass, Interface: LAN, Protocol: any
- 7.10: Type: ICMP, Interface: WAN
- 7.11: ifconfig em0 192.168.2.2/24  
route add default 192.168.2.1
- 7.12: Ναι
- 7.13: Ναι
- 7.14: Όχι γιατί ο R1 δεν μπορεί να δρομολογήσει τα πακέτα
- 7.15: Εκτελούμε τις αλλαγές με Pre-Shared Key: panagiotis
- 7.16: Default IPsec VPN
- 7.17: No IPsec security associations
- 7.18: Ναι
- 7.19: Εκτελούμε τις αλλαγές με Pre-Shared Key: panagiotis
- 7.20: Όχι
- 7.21: Ναι
- 7.22: Ναι
- 7.23: Ναι
- 7.24: Ναι
- 7.25: Ναι
- 7.26: tcpdump -vnni em0
- 7.27: Όχι
- 7.28: ESP με πηγή και προορισμό τις διεπαφές στα WAN των 2 firewalls
- 7.29: Όχι
- 7.30: Ναι, μπορούμε να συνδεθούμε χωρίς να χρειαστεί να αλλάξουμε την IP του PC2

7.31: TCP, IP addresses: 192.0.2.5 και 203.0.118.18, Ports: 3268  
και 22 αντίστοιχα

7.32: Είναι κρυπτογραφημένα μέσω του ssh