



Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή άσκηση 10 (Τείχη προστασίας (Firewalls) και NAT)

Τσάκωνας Παναγιώτης (03119610)

Ομάδα: 2

Ακαδημαϊκό Έτος: 2023-2024

Άσκηση 1: Ένα απλό τείχος προστασίας

- 1.1) (PC1): `ifconfig em0 192.168.1.2/24` και (PC2): `ifconfig em0 192.168.1.3/24`
- 1.2) (PC1): `kldload ipfw`
- 1.3) (PC1): `kldstat`
- 1.4) Όχι δεν μπορώ να κάνω ping στη διεύθυνση IP του βρόχου επιστροφής lo0 ή της διεπαφής em0 μας εμφανίζεται μήνυμα `sendto: permission denied`.
- 1.5) (PC1): `ipfw list`
- 1.6) (PC1): `ipfw add 100 allow all from any to any via lo0`
- 1.7) Ναι είναι επιτυχής.
- 1.8) (PC1): `ipfw show`
- 1.9) (PC1): `ipfw zero`
- 1.10) Όχι δεν μπορώ να κάνω ping από το PC1 στο PC2 και εμφανίζεται μήνυμα `sendto: permission denied`.
- 1.11) (PC1): `ipfw add 200 allow icmp from any to any`
- 1.12) Ο κανόνας έλαβε αύξοντα αριθμό 00200.
- 1.13) Ναι τώρα μπορώ να κάνω ping από το PC1 στο PC2 και αντίστροφα.
- 1.14) Επειδή αντί για icmp το FreeBSD χρησιμοποιεί πακέτα UDP στο traceroute οπότε αρκεί να εκτελέσουμε την εντολή: `traceroute -l 192.168.1.3`
- 1.15) (PC1): `ipfw add 200 allow udp from any to any`
- 1.16) Όχι δεν μπορώ να συνδεθώ από το PC1 με ssh στο PC2, και εμφανίζεται μήνυμα `permission denied`.
- 1.17) (PC1): `ipfw add allow tcp from any to any out → ipfw add allow tcp from any to any in`

1.18) (PC1): ipfw zero → ssh lab@192.168.1.3 → ls → exit

1.19) Ο κανόνας που πρόσθεσα χρησιμοποιήθηκε 32 φορές για τα εξερχόμενα tcp και 29 φορές για τα εισερχόμενα tcp, λόγω του 3-way handshake.

1.20) Ναι μπορώ από το PC2 να συνδεθώ με ssh στο PC1, γιατί επιτρέπουμε και τις δύο (in /out) κατευθύνσεις μηνυμάτων tcp με τον κανόνα που προσθέσαμε στο 1.17.

1.21) (PC2): service ftpd onestart

1.22) (PC1): ftp lab@192.168.1.3 → Ναι μπορώ από το PC1 να συνδεθώ με ftp στο PC2 ως χρήστης lab και να κατεβάσω αρχεία.

Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

2.1) (PC2): kldload ipfw

2.2) Όχι δεν μπορώ να κάνω ping από το PC2 στο PC1 και εμφανίζεται μήνυμα sendto: permission denied.

2.3) (PC2): ipfw add 100 allow all from any to any via lo0

2.4) (PC2): ipfw add allow icmp from me to any

2.5) Όχι δεν μπορώ να κάνω ping από το PC2 στο PC1.

2.6) Περνούν μόνο τα ICMP requests το τείχος προστασίας του PC2, διότι το αντίστοιχο φίλτρο στο PC1 έχει τις διπλάσιες μετρήσεις απ' ότι στο PC2.

2.7) (PC2): ipfw delete 200 → ipfw add allow icmp from me to any keep-state Ναι τώρα μπορώ να κάνω ping από το PC2 στο PC1, διότι λόγω του keep-state το firewall αναγνωρίζει ότι λαμβάνει απάντηση από ένα request που έστειλε το ίδιο το PC2.

2.8) Ναι μπορώ να κάνω ping από το PC1 στο PC2.

2.9) Όχι δεν επιτυγχάνει τώρα το ping από το PC1 στο PC2, διότι ο δυναμικός κανόνας σταμάτησε να ισχύει.

2.10) (PC2): ipfw add allow icmp from any to me icmptypes 8 keep-state

2.11) Έχει προστεθεί ένας δυναμικός κανόνας 'STATE icmp 192.168.1.2 0 < - > 192.168.1.3 0 : default'.

2.12) Ο κανόνας διαγράφηκε.

2.13) (PC2): ipfw add allow udp from any to me → ipfw add allow icmp from me to any icmptypes 3, 11

2.14) (PC2): ipfw add allow udp from me to any → ipfw add allow icmp from any to me icmptypes 3, 11

2.15) (PC1): ipfw add allow icmp from me to any icmptypes 3, 11

2.16) (PC2): ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state

2.17) (PC1): ssh lab@192.168.1.3

2.18) (PC2): ipfw add allow tcp from me to any 22 keep-state

2.19) (PC1): ipfw add allow tcp from 192.168.1.3 to me 22

2.20) Ναι, μπορώ από το PC1 να συνδεθώ με sftp στο PC2 ως χρήστης lab και να κατεβάσω το αρχείο /etc/rc.conf.

2.21) Όχι, δεν μπορώ από το PC1 να συνδεθώ με ftp στο PC2, γιατί το ftp συνδέεται μέσω της πόρτας 21 και όχι της 22 που έχουμε ορίσει πάνω, όποτε πρέπει να ορίσουμε νέο κανόνα στο PC2: ipfw add allow tcp from any to me 21 keep-state

2.22) Η 1^η επιτυγχάνει, διότι χρησιμοποιεί την πόρτα 21, ενώ η 2^η όχι επειδή χρησιμοποιεί τη πόρτα 20.

2.23) (PC2): ipfw add allow tcp from any 21 to me keep-state

2.24) Όχι, δεν μπορώ να κατεβάσω ένα αρχείο από το /usr/bin του PC2 στο PC1.

2.25) (PC2): ipfw add allow tcp from me 20 to any

(PC1): ipfw add allow tcp from any 20 to me

2.26) Το ftp δεν παρέχει κρυπτογράφηση, συνεπώς είναι χρήσιμο να υπάρχει firewall για τέτοια μηνύματα.

2.27) Εφαρμόζουμε τις εντολές: kldunload ipfw → kldstat και στα 2 PC

Άσκηση 3: Απλό Network Address Translation

- 3.1) (PC1): route add default 192.168.1.1 και (PC2): route add default 192.168.1.1
- 3.2) (R1): cli → configure terminal → hostname R1 → interface em0 → ip address 192.0.2.2/30 → interface em1 → ip address 192.0.2.6/30
- 3.3) (SRV1): ifconfig em0 192.0.2.5/30 → route add default 192.0.2.6
- 3.4) (PC2 και SRV1): service ftpd onestart
- 3.5) (FW1): kldstat → Βλέπουμε ότι έχουν φορτωθεί τα εξής modules: kernel, intpm.ko, smbus.ko, ipfw.ko, ipfw_nat.ko και libalias.ko.
- 3.6) Με την εντολή firewall_enable="YES" που έθεσα στο /etc/rc.conf ενεργοποιήθηκε το τείχος προστασίας ipfw.
- 3.7) (FW1): sysrc firewall_type → UNKNOWN
- 3.8) Στο FW1 βλέπω 11 κανόνες, εκ των οποίων ο τελευταίος είναι ο: 'deny ip from any to any'.
- 3.9) (FW1): ipfw nat show config. Δεν βλέπω να έχουν ορισθεί πίνακες in-kernel NAT στο FW1.
- 3.10) Όχι, δεν μπορώ από το PC1 να κάνω ping τη διεπαφή του FW1 στο LAN1 ή στο WAN1.
- 3.11) Όχι δεν μπορώ από το SRV1 να κάνω ping τη διεπαφή του FW1 στο WAN1.
- 3.12) (FW1): ipfw nat 123 config ip 192.0.2.1 reset
- 3.13) (FW1): ipfw add 50 nat 123 ip from any to any
- 3.14) Ναι μπορώ από το PC1 να κάνω ping τη διεπαφή του FW1 στο LAN1.
- 3.15) tcpdump -i em0 -e -vvv
- 3.16) (FW1): ipfw zero
- 3.17) Η IP διεύθυνση πηγής των πακέτων ICMP echo request που βλέπω στην καταγραφή είναι η ip της διεπαφής του firewall στο WAN1.
- 3.18) Η IP διεύθυνση προορισμού των ICMP Echo reply της καταγραφής στον R1 είναι η 192.0.2.1.
- 3.19) Ο κανόνας του τείχους προστασίας που είναι υπεύθυνος για την επιτυχία του ping είναι ο: 'allow ip from any to any'.

- 3.20)** Ο κανόνας εφαρμόστηκε 12 φορές, στάλθηκαν 6 πακέτα και για κάθε πακέτο εφαρμόστηκε 2 φορές.
- 3.21)** Ναι μπορώ από το SRV1 να κάνω ping τη διεπαφή του FW1 στο WAN1.
- 3.22)** Ο κανόνας του τείχους προστασίας που είναι υπεύθυνος για την αποδοχή της προηγούμενης κίνησης είναι ο: 'allow ip from any to any'.
- 3.23)** Ναι ωθείται αυτή στο NAT προς μετάφραση διευθύνσεων, διότι προέρχεται από ιδιωτική διεύθυνση.
- 3.24)** Ναι μπορώ από το PC2 να συνδεθώ με ssh ως χρήστης lab στο SRV1.
- 3.25)** Όταν πάμε να κάνουμε το αντίστροφο και να συνδεθούμε υπάρχει το μήνυμα 'no route to host' αρά είναι πρόβλημα δρομολόγησης, διότι ο R2 δεν ξέρει για την ύπαρξη του LAN1.
- 3.26)** (FW1): ipfw nat 123 if em1 reset redirect_addr 192.168.1.3 192.0.2.1
- 3.27)** Ναι, είναι επιτυχής και το εξακρίβωσα από το hostname.
- 3.28)** (FW1): ipfw nat 123 if em1 reset redirect_addr 192.168.1.3 192.0.2.1 redirect_port 192.168.1.2:22
22
- 3.29)** Συνδεθήκα στο PC1
- 3.30)** Συνδέθηκα στο PC2, γιατί στο PC1 κατευθύνεται μόνο η κίνηση για SSH.
- 3.31)** Ναι μπορώ να δω τα περιεχόμενα του φακέλου /etc και να κατεβάσω το αρχείο rc.conf.
- 3.32)** Εάν από το PC1 κάνω ftp στη διεύθυνση 192.0.2.1 απαντά το PC2.
- 3.33)** Εάν από το PC2 κάνω ssh στη διεύθυνση 192.0.2.1 θα συνδεθώ στο PC1.

Άσκηση 4: Τείχος προστασίας και NAT

- 4.1) (FW1): `ipfw disable one_pass` Όχι τώρα δεν μπορώ να κάνω ping από το PC1 στη διεπαφή του FW1 στο LAN1 ή από το SRV1 στη διεπαφή του FW1 στο WAN1.
- 4.2) Ναι γίνονται δεκτά τα πακέτα από τον κανόνα ώθησης στο NAT της ερώτησης 3.13, αλλά επειδή το μήνυμα πρέπει να περάσει από όλους τους κανόνες, υπάρχει κάποιος που το απορρίπτει.
- 4.3) (FW1): `ipfw delete 50 → ipfw add 1100 allow all from any to any via em0`
- 4.4) Ναι είναι τώρα το ping από το PC1 προς οποιαδήποτε διεπαφή του FW1 επιτυχές.
- 4.5) Εάν από το PC2 κάνω ssh στη διεύθυνση 192.0.2.1 θα συνδεθώ στο FW1, διότι έχουμε διαγράψει το κανόνα προώθησης στο πίνακα του NAT.
- 4.6) Ο κανόνας που προσθέσαμε στο 4.3.
- 4.7) (FW1): `ipfw add 3000 nat 123 ip from any to any xmit em1`
- 4.8) (FW1): `ipfw add 3001 allow all from any to any`
- 4.9) (FW1): `ipfw add 2000 nat 123 ip from any to any recv em1`
- 4.10) (FW1): `ipfw add 2001 check-state`
- 4.11) Εάν κάνω ping από το PC1 στη διεύθυνση 192.0.2.1 απαντά το FW1.
- 4.12) Εάν κάνω ping από το SRV1 στη διεύθυνση 192.0.2.1 απαντά το PC2.
- 4.13) Εάν κάνω ssh από το PC1 στη διεύθυνση 192.0.2.1 θα συνδεθώ στο FW1.
- 4.14) Εάν κάνω ssh από το SRV1 στη διεύθυνση 192.0.2.1 θα συνδεθώ στο PC1.
- 4.15) Εάν κάνω ftp από το SRV1 στη διεύθυνση 192.0.2.1 θα συνδεθώ στο PC2.
- 4.16) Ναι μπορώ να κάνω ping από το PC1 στο SRV1.
- 4.17) Ναι μπορώ να συνδεθώ με ssh από το PC1 στο SRV1.
- 4.18) Ναι μπορώ από το PC1 να συνδεθώ με ftp ως χρήστης lab στο SRV1, να δω τα περιεχόμενα κάποιου φακέλου και να κατεβάσω ένα αρχείο.
- 4.19) (FW1): `ipfw add 2999 deny all from any to any via em1`
- 4.20) Επιτυγχάνουν μόνο οι συνδέσεις στο Firewall που προέρχονται από το LAN1.

- 4.21) (FW1): ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
- 4.22) Ναι μπορώ να κάνω ping από το PC1 στο SRV1.
- 4.23) (FW1): ipfw add 2500 skipto 3000 tcp from any to any 22 out via em1 keep-state
- 4.24) Ναι μπορώ να συνδεθώ με ssh από το PC1 στο SRV1.
- 4.25) (FW1): ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state
- 4.26) Εάν κάνω ping από το SRV1 στη διεύθυνση 192.0.2.1 απαντάει το PC2.
- 4.27) (FW1): ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state
- 4.28) Εάν από το SRV1 κάνετε ssh ως χρήστης lab στη διεύθυνση 192.0.2.1 συνδέομαι στο PC1.
- 4.29) Όχι δεν μπορώ να συνδεθώ από το SRV1 με ftp ως χρήστης lab στη διεύθυνση 192.0.2.1.
- 4.30) (FW1): 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

- 5.1) LAN IP address : 192.168.1.1
- 5.2) WAN IP address : 10.0.0.1
- 5.3) System information → Memory usage 33%
- 5.4) Βλέπουμε 4 διεπαφές δικτύου
- 5.5) DMZ → IP address : 172.22.1.1
- 5.6) General Setup → Hostname : fw
- 5.7) Hostname: fw1 → Save
- 5.8) Όχι δεν υπάρχουν.
- 5.9) WAN → IP address: 192.0.2.1/30, Gateway: 192.0.2.2, Block Private Networks → Save
- 5.10) Ναι υπάρχει κανόνας για το WAN ('Block private networks')
- 5.11) Όχι δεν βλέπω να είναι ενεργοποιημένη κάποια υπηρεσία από τις κατηγορίες "Services" και "VPN".

5.12) DNS forwarder → Enable DNS forwarder

5.13) DHCP server → Enable

5.14) (PC1): dhclient em0 → IP : 192.168.1.2, Gateway : 192.168.1.1, Port : 67

5.15) Χρειάστηκε η ενεργοποίηση της υπηρεσίας DNS forwarder, διότι το firewall λειτουργεί και σαν DNS server.

5.16) Στο DHCP Leases

5.17) 7 εγγραφές

5.18) Όχι δεν μπορώ από το PC1 να κάνω ping τη διεπαφή του FW1 στο LAN1.

5.19) Βλέπουμε ένα error log list με τις τελευταίες 50 καταγραφές → Clear log

5.20) Firewall states → 4 states

5.21) Κανέναν


5.22) Rules → LAN → ‘Add new rule’ → interface LAN from any to any

5.23) Ναι μπορώ τώρα από το PC1 να κάνω ping τις διεπαφές του FW1 στα LAN1, WAN1, DMZ.

5.24) Όχι από τον R1 δεν μπορώ να κάνω ping τη διεπαφή του FW1 στο WAN1.

5.25) (R1): arp -a → Ναι βλέπω εγγραφή για τη διεύθυνση MAC της διεπαφής του FW1 στο WAN1.

5.26)

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

5.27) Ναι μπορώ τώρα από τον R1 να κάνω ping τη διεπαφή του FW1 στο WAN1.

5.28) Όχι δεν μπορώ από τον R1 να κάνω ping το PC1, διότι ο R1 δεν ξέρει για το 192.168.1.0/24.

5.29) Ναι, μπορώ από το PC1 να κάνω ping τον R1. Γίνεται μετάφραση των διευθύνσεων του ιδιωτικού δικτύου με τη διεύθυνση του firewall στο WAN.

5.30) Όχι, δεν μπορώ από το PC1 να κάνω ping τον SRV1, γιατί δεν έχει οριστεί προκαθορισμένη πύλη στο SRV1.


5.31) (SRV1): route add default 172.22.1.1

5.32) Ναι μπορώ τώρα από το PC1 να κάνω ping τον SRV1.

5.33) Όχι δεν μπορώ από τον SRV1 να κάνω ping τη διεπαφή του FW1 στο DMZ, διότι δεν έχει οριστεί εγγραφή στο firewall που να μας το επιτρέπει.

5.34) Όχι δεν μπορώ από τον SRV1 να κάνω ping το PC1 ή το R1, διότι δεν μπορούμε να στείλουμε πακέτο από τη διεπαφή στο DMZ.

5.35)

<input type="checkbox"/>		*	DMZ net	*	! LAN net	*	
--------------------------	---	---	---------	---	-----------	---	--

5.36) Ναι μπορώ τώρα από τον SRV1 να κάνω ping τη διεπαφή του FW1 στο DMZ.


5.37) Ναι μπορώ τώρα από τον SRV1 να κάνω ping τη διεπαφή του FW1 στο WAN1.

5.38) Όχι δεν μπορώ από τον R1 να κάνω ping τον SRV1.

5.39) Ναι μπορώ από τον SRV1 να κάνω ping τον R1, γιατί έχει οριστεί default gateway και στο SRV1 και το FW1 οπότε η κίνηση κατευθύνεται προς το R1.

5.40) (PC2): dhclient em0 → IP : 192.168.1.3, Gateway : 192.168.1.1, Port : 67

5.41)

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

5.42) Πρέπει να τοποθετηθεί πριν τον ήδη υπάρχοντα γιατί αλλιώς θα περνάει όλη η κίνηση

5.43) Όχι δεν μπορώ από το PC2 να κάνω ping τον SRV1.

5.44) Ναι, μπορώ από το PC2 να κάνω ping τη διεπαφή του FW1 στο DMZ, γιατί δεν υπάρχει κάποια εγγραφή που να μου μπλοκάρει αυτή τη διεύθυνση.

Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT

6.1) (R1): ip route 203.0.118.0/24 192.0.2.1

6.2) NAT → Outbound → Enable advanced outbound NAT

6.3) Για το PC1:

Interface	Source	Destination	Target	Description
WAN	192.168.1.2/32	*	203.0.118.14	

6.4) Για το PC2:

WAN	192.168.1.3/32	*	203.0.118.15	
-----	----------------	---	--------------	--

6.5) (R1): tcpdump -i em0 -e -vvv

6.6) Ναι μπορώ να κάνω ping από τα PC1, PC2 στον R1 και φτάνουν με διευθύνσεις 203.0.118.14 και 203.0.118.15 αντίστοιχα.

6.7) NAT → Server NAT → External IP address : 203.0.118.18

6.8)

If	Proto	Ext. port range	NAT IP	Int. port range	Description
WAN	TCP	22 (SSH)	172.22.1.2 (ext.: 203.0.118.18)	22 (SSH)	

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

TCP	*	*	172.22.1.2	22 (SSH)	NAT
-----	---	---	------------	----------	-----

6.10) Ναι, μπορώ από τον R1 να συνδεθώ με ssh στο 203.0.118.18, και απαντάει ο SRV1.

6.11) Όχι δεν μπορώ από τον R1 να κάνω ping το 203.0.118.18, διότι ο κανόνας στο firewall επιτρέπει μόνο πακέτα για ssh.

6.12) Ναι Μπορώ να συνδεθώ με ssh από τα PC1, PC2 στο SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.118. Τα μηνύματα περνάνε από τον R1 όπως φαίνεται και στο tcpdump.

6.13) NAT → Outbound → ‘delete selected mappings’

Όχι, δεν μπορώ να συνδεθώ με ssh από το PC1 στο SRV1, γιατί υπάρχει εγγραφή στο firewall που μπλοκάρει τα private addresses.

6.14) Ναι είναι επιτυχή τα ping από τα PC1, 2 προς τον R1, γιατί πλέον τα μηνύματα στο WAN μεταδίδονται με την ip 192.0.2.1.

6.15) Ναι εξακολουθώ να μπορώ να συνδέομαι από τον R1 στον SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.18. Δεν ισχύει το ίδιο για τα PC1 και PC2.

6.16) Η σύνδεση tcp αποτυγχάνει, διότι 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.

6.17) Για την προηγούμενη συμπεριφορά ευθύνεται ο κανόνας για το DMZ που δεν επιτρέπει επικοινωνία από το DMZ στο LAN1.

Άσκηση 7: IPSec site-to-site VPN

7.1) –

7.2) MNG → ip address : 192.168.56.3

7.3) –

7.4) Ναι μπορώ να συνδεθώ ταυτόχρονα από τον φυλλομετρητή του φιλοξενούντος μηχανήματος στα δύο τείχη προστασίας

7.5) Hostname: fw1 → Save

7.6) WAN → Ip address : 192.0.2.5/30, Gateway : 192.0.2.6

7.7) LAN → Ip address : 192.168.2.1/24

7.8) –

7.9)

Proto	Source	Port	Destination	Port	Description
*	*	*	*	*	Allow all traffic from Lan2

7.10)

Proto	Source	Port	Destination	Port	Description
ICMP	*	*	WAN address	*	Allow all icmp request to WAN destination

7.11) –

7.12) Ναι μπορώ από το PC1 να κάνετε ping τη διεπαφή του FW2 στο WAN2.

7.13) Όχι δεν μπορώ από το PC2 να κάνω ping τη διεπαφή του FW1 στον WAN1.

7.14) Όχι δεν μπορώ από το PC1 να κάνω ping το PC2 ή το αντίστροφο (Destination Host Unreachable). Αυτό συμβαίνει επειδή δεν υπάρχει εγγραφή για το LAN2 στο R1.

7.15) 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 : ‘panagiotistsakonas’

7.16)

Proto	Source	Port	Destination	Port	Description
*	*	*	*	*	Default IPsec VPN

7.17) Όχι δεν βλέπω να έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των 2 υποδικτύων.

7.18) Ναι, έχουν οριστεί 2 πολιτικές προώθησης κίνησης μεταξύ των 2 υποδικτύων.

7.19) 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	

preshared key : 'panagiotistsakonas'

7.20) Όχι δεν βλέπω να έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των 2 υποδικτύων.

7.21) Ναι, έχουν οριστεί 2 πολιτικές προώθησης κίνησης μεταξύ των 2 υποδικτύων.

7.22) Ναι μπορώ από το PC1 να κάνω ping το PC2.

7.23) Ναι μπορώ από το PC2 να κάνω ping το PC1.

7.24) Ναι, προστέθηκαν 2 ακόμη εγγραφές

7.25) Ναι, προστέθηκαν 2 ακόμη εγγραφές

7.26) (R1): tcpdump -i em0 -e -vvv

7.27) Όχι δεν παρατηρώ πακέτα ICMP όταν κάνω ping από ένα PC στο άλλο.

7.28) Παρατηρώ ESP πακέτα, των οποίων η πηγή είναι η διεύθυνση 192.0.2.1 και ο προορισμός τους η διεύθυνση 192.0.2.5.

7.29) Όχι δεν υπάρχει κάπου η πληροφορία για τις διευθύνσεις IP των PC1, PC2'.

7.30) Ναι μπορώ από το PC2 να συνδεθώ με SSH στο SRV1 στη διεύθυνση 203.0.118.18, διότι το PC2 δεν ανήκει πλέον στο LAN1 για το οποίο υπάρχει ξεχωριστός κανόνας στο firewall.

7.31) Παρατηρώ πακέτα TCP με πηγή τη διεύθυνση 192.0.2.5 και προορισμό τη διεύθυνση 203.0.118.18.

7.32) Ναι, είναι κρυπτογραφημένα.