Ονοματεπώνυμο: Περόγαμβρος Γεώργιος	**Όνομα PC:**
Ομάδα: 2	**Ημερομηνία: 25/5/2022**

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

1.1Χρησιμοποίησα την εντολή kldload ifpw.

1.2 Με την εντολή kldstat βλέπουμε πως έχει φορτωθεί το αρχείο ipfw.ko.

1.3 Όχι, δεν είναι εφικτό. Εμφανίζεται το μήνυμα λάθους ping: send to: permission denied.

1.4 Χρησιμοποίησα την εντολή ipfw list. Υπάρχει ο κανόνας 65535 deny ip from any to any.

1.5 Χρησιμοποίησα την εντολή ipfw show. 65535 10 840 deny ip from any to any.

1.6 Με την εντολή ipfw zero.

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

1.8 Ναι, είναι και τα δύο επιτυχή.

1.9 Όχι, εμφανίζεται το μήνυμα ping: send to: permission denied.

1.10 Χρησιμοποίησα την εντολή ipfw add allow icmp from any to any.

1.11 Έλαβε τον αύξοντα αριθμό 200.

1.12 Ναι, το ping λειτουργεί και προς τις δύο κατευθύνσεις.

1.13 Γιατί το traceroute από default χρησιμοποιεί διαγράμματα udp που εμείς δεν έχουμε επιτρέψει. Μπορούμε να χρησιμοποιήσουμε τη σημαία -I (traceroute -I 192.168.1.3) για να χρησιμοποιήσει icmp πακέτα που επιτρέπονται.

1.14 Χρησιμοποίησα την εντολή ipfw add allow udp from me to any 33434-33534.

1.15 Όχι, λαμβάνουμε το μήνυμα σφάλματος ssh: connect to host 192.168.1.3 port 22: Permission denied.

1.16 Χρησιμοποίησα τις εντολές ipfw add allow tcp from any to any established και ipfw add allow tcp from me to any setup.

1.17 Χρησιμοποίησα τις εντολές ipfw zero, ssh lab@192.168.1.3, έβαλα κωδικό, ls, exit.

1.18 Ο δεύτερος κανόνας (setup) εφαρμόστηκε 1 φορά, επειδή αναφέρεται στο πρώτο μήνυμα της τριμερούς χειραψίας. Ο πρώτος κανόνας (established) εφαρμόστηκε 68 φορές, μία για κάθε πακέτο που ανταλλάχθηκε κατά την εγκατεστημένη σύνδεση.

1.19 Όχι, καθώς βάσει του δεύτερου κανόνα που εφαρμόσαμε (setup) ο PC1 μπορεί να στείλει αλλά όχι να λάβει το πρώτο μέρος της τριμερούς χειραψίας.

1.20 Χρησιμοποίησα τις εντολές sysrc ftpd_enable=”YES” και service ftpd start.

1.21 Ναι μπορούμε, επειδή το ftp χρησιμοποιεί tcp για τη σύνδεση και τη μεταφορά δεδομένων.

2.1 Χρησιμοποίησα την εντολή kldload ipfw.

2.2 Όχι.

2.3 Χρησιμοποίησα την εντολή ipfw add allow all from any to any via lo0.

2.4 Χρησιμοποίησα την εντολή ipfw add allow icmp from me to any icmptypes 8.

2.5 Όχι, δεν λαμβάνουμε απάντηση στο ping.

2.6 Τα πακέτα δεν icmp echo request που στέλνει ο PC2 περνούν το τείχος λόγω του κανόνα που μόλις εισάγαμε. Παρόλα αυτά οι απαντήσεις icmp echo replies που στέλνει ο PC1 δεν περνούν.

2.7 Χρησιμοποίησα τις εντολές ipfw delete 200, ipfw add allow icmp from me to any icmptypes 8 keep state. Ναι, τώρα το ping είναι επιτυχές.

2.8 Ναι το ping από τον PC1 στον PC2 είναι επιτυχές.

2.9 Όχι, γιατί έπαψε να ισχύει ο δυναμικός κανόνας που ορίσαμε και έτσι τα icmp echo requests του PC1 δεν περνάνε το τείχος του PC2.

2.10 Χρησιμοποίησα την εντολή ipfw add allow icmp from any to me icmptypes 8 keep-state.

2.11 Με την εντολή ipfw -d show βλέπουμε τους κανόες και τους μετρητές και τους δυναμικούς κανόνες που υπάρχουν αυτή τη στιγμή. Στην προκειμένη περίπτωση έχουμε τον δυναμικό κανόνα STATE που επιτρέπει την icmp κίνηση μεταξύ 192.168.1.2 και 192.168.1.3 με χρόνο ζωής 4 sec.

2.12 Ο δυναμικός κανόνας διαγράφεται αφού λήγει ο χρόνος ζωής του.

2.13 Χρησιμοποίησα τις εντολές ipfw add allow udp from any to me 33434-33534 και ipfw add allow icmp from me to any icmptypes 3.

2.14 Χρησιμοποίησα τις εντολές ipfw add allow udp from me to any 33434-33534, ipfw add allow icmp from any to me icmptypes 3.

2.15 Χρησιμοποίησα την εντολή ipfw add allow udp from any to me 33434-33534.

2.16 Χρησιμοποίησα την εντολή ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state.

2.17 Με την εντολή ssh lab@192.168.1.3 συνδεόμαστε με ssh από το PC1 και στο PC2 με την εντολή ipfw -d show βλέπουμε τη δημιουργία του αντίστοιχου δυναμικού κανόνα.

2.18 Χρησιμοποίησα την εντολή ipfw add allow tcp from me to any 22 keep-state.

2.19 Χρησιμοποίησα την εντολή ipfw add allow tcp from 192.168.1.3 to me 22.

2.20 Ναι μπορώ.

2.21 Χρησιμοποίησα την εντολή ipfw add allow tcp from any to me 21 keep-state.

2.22 Το ls αποτυγχάνει καθώς στο passive mode χρησιμοποιούνται τυχαίες θύρες και εμείς έχουμε επιτρέψει την κίνηση μέσω της 21.

2.23 Προσθέτουμε τον κανόνα ipfw add allow tcp from any to me setup keep-state.

2.24 Ναι, μπορούμε.

2.25 Στον PC2 πρέπει να εφαρμόσουμε τον κανόνα ipfw add allow tcp from me 20 to any setup keep-state και στον PC1 τον κανόνα ipfw add allow tcp from any 20 to me setup keep-state.

2.26 Επειδή το ftp χρησιμοποιεί πολλές θύρες είναι αρκετά δύσκολο να το περιορίσουμε στο τείχος προστασίας με κανόνες αποκλειστικούς για αυτό.

2.27 Χρησιμοποίησα τις εντολές kldunload ipfw και kldstat.

3

3.1 Χρησιμοποίησα την εντολή route add default 192.168.1.1 στα PC1 PC2(οι ip και τα ονόματα είχαν οριστεί από το πρώτο μέρος.

3.2 Χρησιμοποίησα τις εντολές cli, configure terminal, hostname R1, interface em0, ip address 192.0.2.2/30, exit, interface em1, ip address 192.0.2.6/30.

3.3 Χρησιμοποίησα τις εντολές hostname SRV1, ifconfig em0 192.0.2.5/30, route add default 192.0.2.6.

3.4 Χρησιμοποίησα τις εντολές sysrc ftpd_enable=”YES” και service ftpd start.

3.5 Χρησιμοποίησα την εντολή kldstat. Είναι φορτωμένα τα kernel, ipfw.ko, ipfw_nat.ko, libalias.ko

3.6 Έχει φορτωθεί το ipfw.

3.7 Χρησιμοποίησα την εντολή sysrc -A | grep firewall_type. Είναι τύπου UNKNOWN.

3.8 Με την εντολή ipfw list βλέπω 11 κανόνες με τελευταίο τον 65535 deny ip from any to any.

3.9 Με την εντολή ipfw nat show config βλέπουμε πως δεν έχει ορισθεί κάποιος πίνακας in-kernel NAT.

3.10 Όχι δεν μπορώ σε καμία από τις δύο.

3.11 Όχι δεν μπορώ.

3.12 Χρησιμοποίησα την εντολή ipfw nat 123 config if em1 unreg_only reset.

3.13 Χρησιμοποίησα την εντολή ipfw add nat 123 ip4 from any to any.

3.14 Ναι, μπορούμε να κάνουμε ping και στις δύο.

3.15 Χρησιμοποίησα την εντολή tcpdump -i em0.

3.16 Χρησιμοποίησα τις εντολές ipfw show και ipfw zero.

3.17 Χρησιμοποίησα την εντολή ping -c 3 192.0.2.2. Η η IP διεύθυνση πηγής των πακέτων ICMP echo request που βλέπουμε στην καταγραφή είναι 192.0.2.1, δηλαδή η ip της διεπαφής του FW1 στο WAN1.

3.18 Ίδια με την διεύθυνση πηγής των echo requests, δηλαδή η 192.0.2.1.

3.19 Κάνοντας ipfw show στον FW1 βλέπουμε πως μη μηδενικό counter έχει ο κανόνας nat 123 ip4 from any to any και άρα αυτός είναι υπεύθυνος για την επιτυχία του ping.

3.20 Με την εντολή ipfw show βλέπουμε πως ο κανόνας έχει εφαρμοστεί 12 φορές. Για κάθε echo request και echo reply ο κανόνας εφαρμόζεται από 2 φορές στο καθένα (το πακέτο εισέρχεται στο FW1 και εξέρχεται από αυτόν). Συνολικά στάλθηκαν 3 echo requests και 3 echo reply * 2 εφαρμογές του κανόνα, σύνολο 12.

3.21 Ναι, μπορώ.

3.22 Ο ίδιος με το 3.20 (nat 123 ip4 from any to any)

3.23 Ωθείται καθώς πληρή τον κανόνα nat 123 ip4 from any to any.

3.24 Ναι, μπορώ.

3.25 Το ssh από τον PC2 προς τον SRV1 είναι επιτυχές καθώς η δημόσια διεύθυνση του PC2 μεταφράζεται σε 192.0.2.1 μέσω του NAT και έτσι μετά ο R1 μπορεί να απαντήσει (δηλαδή να προωθήσει την απάντηση του SRV1). Όταν ο SRV1 προσπαθήσει να συνδεθεί με ssh στον PC2, προωθεί το μήνυμα στον R1 ο οποίος όμως δεν έχει στον πίνακα δρομολόγησης πληροφορία για την διεύθυνση του PC2 και έτσι δεν μπορεί να προωθήσει κάπου το μήνυμα.

3.26 Χρησιμοποίησα την εντολή ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1.

3.27 Η προσπάθεια είναι επιτυχής. Συνδεθήκαμε στον PC2. Μπορούμε να το καταλάβουμε αν κάνουμε who στον PC2 (βλέπουμε τον 10.0.2.5 συνδεδεμένο ως lab).

3.28 Χρησιμοποίησα την εντολή 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 22.

3.29 Τώρα συνδεθήκαμε στο PC1, καθώς το ssh χρησιμοποιεί tcp στην θύρα 22, οπότε έχει προτεραιότητα ο κανόνας redirect_port. Το κατάλαβα με who στον PC1.

3.30 Συνδεθήκαμε στο PC2 καθώς εφαρμόστηκε ο κανόνας redirect_addr (ο κανόνας redirect_port δεν εφαρμόστηκε αφού η 22 δεν είναι ftp port). Το καταλάβαμε με netstat -a στον PC2.

3.31 Ναι, μπορώ να κάνω και τα δύο.

3.32 Απαντά το PC2 λόγω του redirect_addr.

3.33 Απαντά το PC1 λόγω του redirect_port.

4

4.1 Και τα 2 ping αποτυγχάνουν.

4.2 Τα πακέτα γίνονται αποδεχτά από τον κανόνα ώθησης στο NAT, αλλά μετά απορρίπτονται καθώς ο μόνος κανόνας που ταιριάζει είναι ο deny ip from any to any.

4.3 Χρησιμοποίησα τις εντολές ipfw delete 1100 και ipfw add 1100 allow all from any to any via 192.168.1.1.

4.4 Ναι, είναι.

4.5 Θα συνδεθώ στο FW1.

4.6 Ο κανόνας allow ip from any to any via 192.168.1.1 που προσθέσαμε στο 4.2.

4.7 Χρησιμοποίησα την εντολή ipfw add 3000 nat 123 all from any to any out xmit em1.

4.8 Χρησιμοποίησα την εντολή ipfw add 3001 allow all from any to any.

4.9 Χρησιμοποίησα την εντολή ipfw add 2000 nat 123 all from any to any in recv em1.

4.10 Χρησιμοποίησα την εντολή ipfw add 2001 check-state.

4.11 Απαντά ο FW1.

4.12 Απαντά ο PC2.

4.13 Συνδεόμαστε στο FW1.

4.14 Στο PC1.

4.15 Στο PC2.

4.16 Ναι, μπορούμε.

4.17 Ναι, μπορούμε.

4.18 Όλα γίνονται επιτυχώς.

4.19 Χρησιμοποίησα την εντολή ipfw add 2999 deny all from any to any via em1.

4.20 Επιτυγχάνουν πλέον μόνο το ping του 4.11 και το ssh του 4.13.

4.21 Χρησιμοποίησα την εντολή ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state.

4.22 Ναι, μπορούμε.

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

4.24 Ναι, μπορούμε.

4.25 Χρησιμοποίησα την εντολή ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state.

4.26 Απαντά το PC2.

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

4.28 Στο PC1.

4.29 Όχι, καθώς ο κανόνας που προσθέσαμε αφορά την κίνηση με προορισμό τη θύρα 22, που δεν χρησιμοποιείται από το ftp.

4.30 Πρέπει να προσθέσουμε τους κανόνες ipfw add 2300 skipto 3000 tcp from any to any 21 recv em1 keep-state και ipfw add 2400 skipto 3000 tcp from any 20 to any xmit em1 keep-state.

5

5.1 Η διεπαφή του FW1 στο LAN1 έχει διεύθυνση 192.168.1.1/24. Το βλέπουμε στο Interfaces → LAN → Primary Configuration IP address στο GUI.

5.2 Η διεπαφή του FW1 στο WAN1 έχει διεύθυνση 10.0.0.1/30. Το βλέπουμε στο Interfaces → WAN → Static IP configuration στο GUI.

5.3 Είναι ελεύθερο το 66% της μνήμης του FW1. Το βλέπουμε στο Status → System στο GUI.

5.4 Βλέπουμε συνολικά 4 διεπαφές στο Status → Interfaces. Συμφωνούν με αυτές του Virtual Box.

5.5 Η διεπαφή του FW1 στο DMZ έχει διεύθυνση 172.22.1.1/24. Το βλέπουμε στο Interfaces → DMZ → IP configuration → IP address στο GUI.

5.6 Το hostname του FW1 είναι fw. Το βλέπουμε στο System → General Setup → Hostname.

5.7 Το άλλαξα από το System → General Setup → Hostname.

5.8 Όχι, δεν υπάρχουν.

5.9 Οι αλλαγές έγιναν στο Interfaces → WAN → Static IP configuration και το checkbox στο κάτω μέρος.

5.10 Υπάρχει ένας κανόνας που μπλοκάρει τα ιδιωτικά δίκτυα.

5.11 Όχι, δεν είναι ενεργοποιημένη καμία υπηρεσία από αυτές των κατηγοριών “Services” και “VPN”.

5.12 Ενεργοποίησα το checkbox Enable DNS Forwarder στο Services → DNS forwarder.

5.13 Ενεργοποίησα το checkbox Enable στο Services → DHCP server → LAN και άλλαξα τις περιοχές στο Range στις ζητούμενες.`

5.14 Χρησιμοποίησα την εντολή dhclient em0. Αποδόθηκε η διεύθυνση 192.168.1.2/24, η προεπιλεγμένη πύλη 192.168.1.1 και ο DNS εξυπηρετητής 192.168.1.1.

5.15 Με αυτήν την επιλογή το DHCP service εξυπηρετεί αυτόματα τα ip addresses του LAN ως ένας DNS server χωρίς να χρειάζεται εμείς να ορίσουμε χειροκίνητα DNS servers.

5.16 Το βλέπουμε από το υπομενού DHCP Leases.

5.17 Συνολικά βλέπουμε 7 εγγραφές.

5.18 Όχι δεν μπορούμε.

5.19 Βλέπουμε τις απορρίψεις των icmp echo requests που στάλθηκαν από τον PC1. Καθαρίσαμε τα logs με το Clear Logs.

5.20 Βλέπουμε 6 firewall states.

5.21 Δεν βλέπουμε κανέναν κανόνα.

5.22 Προσθέσαμε τον κανόνα από το Menu Firewall → Rules → LAN κλικ στο + Action: Pass, Interface: LAN, Protocol: Any, Source: Any, Destination: Any.

5.23 Το ping είναι επιτυχές σε όλες τις διεπαφές.

5.24 Όχι, το ping είναι ανεπιτυχές.

5.25 Χρησιμοποίησα την εντολή arp -a. Ναι υπάρχει εγγραφή για την MAC της διεπαφής του FW1 στο WAN1

5.26 Προσθέσαμε τον κανόνα από το Menu Firewall → Rules → WAN κλικ στο + Action: Pass, Interface: WAN, Protocol: ICMP, Source: Any, Destination: WAN address.

5.27 Ναι, μπορούμε.

5.28 Το R1 δεν έχει διαδρομή προς το υποδίκτυο του PC1 ούτε default gateway και έτσι έχουμε μήνυμα σφάλματος No route to host.

5.29 Το ping είναι επιτυχές. Καταλαβαίνουμε πως το FW1 περνάει τις διευθύνσεις από πίνακα NAT και μεταφράζει την ιδιωτική διεύθυνση του PC1 στη δημόσια 192.0.2.1 (FW1) και έτσι ο R1 μπορεί να απαντήσει.

5.30 Όχι, το ping δεν είναι επιτυχές καθώς ο SRV1 δεν έχει διαδρομή για το PC1 ή default gateway και δεν ξέρει που να στείλει τα πακέτα.

5.31 Χρησιμοποίησα την εντολή route add default 172.22.1.1.

5.32 Ναι, τώρα το ping είναι επιτυχές.

5.33 Το ping είναι ανεπιτυχές. Τα πακέτα απορρίπτονται από το firewall καθώς δεν υπάρχει κατάλληλος κανόνας. Το ping από το PC1 προηγουμένως ήταν επιτυχές επειδή μάλλον ο κανόνας προστίθεται με keep-state.

5.34 Όχι καθώς δεν επιτρέπεται η διερχόμενη κίνηση από τη διεπαφή του WAN1 στο DMZ.

5.35 Προσθέσαμε τον κανόνα από το Menu Firewall → Rules → DMZ κλικ στο + Action: Pass, Interface: DMZ, Protocol: any, Source: DMZ net, Destination: not LAN net.

5.36 Ναι, μπορώ.

5.37 Ναι, μπορώ.

5.38 Όχι, δεν μπορούμε καθώς το R1 δεν έχει διαδρομή για το SRV1 ή default gateway και έτσι έχουμε μήνυμα σφάλματος No Route to Host.

5.39 Γίνεται καθώς με τον τελευταίο κανόνα που προσθέσαμε στο 5.35 επιτρέπεται εξερχόμενη κίνηση από το DMZ προς το WAN1. Το FW1 μεταφράζει την διεύθυνση του SRV1 στην 192.0.2.1 και έτσι ο R1 ξέρει που να απαντήσει. Επειδή οι κανόνες είναι δυναμικοί η απάντηση του R1 φτάνει στον SRV1.

5.40 Χρησιμοποίησα την εντολή dhclient em0. Αποδόθηκε η διεύθυνση 192.168.1.3/24, η προεπιλεγμένη πύλη 192.168.1.1 και ο DNS εξυπηρετητής 192.168.1.1

5.41 Προσθέσαμε τον κανόνα από το Menu Firewall → Rules → LAN κλικ στο + Action: Block, Interface: LAN, Protocol: any, Source: 192.168.1.3, Destination: 172.22.1.2.

5.42 Πρέπει να τοποθετηθεί πριν από αυτόν που υπάρχει καθώς εκτελείται το action του πρώτου κανόνα που ταιριάζει.

5.43 Όχι, δεν μπορούμε.

5.44 Ναι μπορούμε, καθώς ο κανόνας που προσθέσαμε αφορά μόνο τον SRV1.

6

6.1 Χρησιμοποίησα την εντολή route add 203.0.118.0/24 192.0.2.1.

6.2 Ενεργοποίησα το checkbox Enable advanced outbound NAT στο υπομενού Outbound.

6.3 Προσθέσαμε mapping από το Menu Firewall → NAT → Outbound κλικ στο +, Interface: WAN, Source: 192.168.1.2/32, Destination: any, Target 203.0.118.114.

6.4 Προσθέσαμε mapping από το Menu Firewall → NAT → Outbound κλικ στο +, Interface: WAN, Source: 192.168.1.3/32, Destination: any, Target 203.0.118.115.

6.5 Χρησιμοποίησα την εντολή tcpdump.

6.6 Το ping είναι επιτυχές. Τα πακέτα φτάνουν με διεύθυνση πηγής την 203.0.118.14 που ορίσαμε.

6.7 Το ping είναι επιτυχές. Τα πακέτα φτάνουν με διεύθυνση πηγής την 203.0.118.15 που ορίσαμε.

6.8 Το ping αποτυγχάνει επειδή η διεύθυνση 203.0.118.14 χρησιμοποιείται για το PC1 μόνο στην εξερχόμενη κίνηση. Το ping πριν ήταν επιτυχές επειδή ξεκινούσε από το PC1.

6.9 Πρόσθεσα νέα εγγραφή με External IP address 203.0.118.18.

6.10 Συμπλήρωσα τα ζητούμενα πεδία.

6.11 Προστέθηκε κανόνας με Proto: TCP, Source: Any, Destination: 172.22.1.2:22 και Description: NAT.

6.12 Μπορούμε. Συνδεόμαστε στον SRV1.

6.13 Το ping αποτυγχάνει καθώς η αντιστοίχηση που προσθέσαμε αφορούσε μόνο TCP πρωτόκολλο.

6.14 Η σύνδεση με ssh είναι επιτυχής. Τα πακέτα ακολουθούν τη διαδρομή PC2 → FW1 → R1 → FW1 → R1 → SRV1 και τη συμμετρική στον γυρισμό. Τη διαδρομή την επιβεβαιώνουμε αν κάνουμε tcpdump στον R1 καθώς βλέπουμε τα διερχόμενα πακέτα με τις αντίστοιχες διευθύνσεις προορισμού και πηγής. Η διαδρομή είναι λογική καθώς αρχικά όταν ο FW1 πρωτολαμβάνει τα πακέτα δεν τα απορρίπτει (δεν υπάρχει κανόνας απόρριψης) και από τον πίνακα δρομολόγησής του τα προωθεί στο R1. Ο R1 τα στέλνει πίσω λόγω της στατικής διαδρομής που βάλαμε νωρίτερα και τότε ενεργοποιούνται οι κανόνες του WAN που προσθέσαμε πριν λίγο με Inbound και Outbound NAT.
6.15 Διαγράψαμε τον κανόνα από το Menu Firewall → NAT → Outbound. Το ping δεν είναι επιτυχές. Από την καταγραφή βλέπουμε πως πλέον δεν μεταφράζεται η διεύθυνση του PC1 και έτσι ο R1 δεν ξέρει που να απαντήσει.

6.16 Κάνουμε κλικ στο επιλεγμένο checkbox Enable advanced outbound NAT στο Menu Firewall → NAT → Outbound. Το ping τώρα είναι επιτυχές καθώς οι διευθύνσεις πλέον μεταφράζονται αυτόματα και έτσι το PC1 εμφανίζεται στο R1 με την διεύθυνση 192.0.2.1.

6.17 Από τον R1 συνδεόμαστε επιτυχώς, από τον PC2 όμως όχι.

6.18 Βλέπουμε πως στο τελευταίο μέρος της τριμερούς χειραψίας ο 192.0.2.1 απαντάει με R (Reset) και έτσι το ssh αποτυγχάνει.

6.19 Δεν φταίει κανένας από τους 2 κανόνες. Όπως βλέπουμε και από την υπόδειξη οι NATed υπηρεσίες δεν είναι προσβάσιμες όταν χρησιμοποιείται η WAN IP address από δίκτυο LAN.

7

7.1 Αποσυνδέσαμε το καλώδιο.

7.2 Άλλαξα το πεδίο IP address στο Interfaces → MNG → Primary Configuration. Τώρα συνδέομαι στη διεύθυνση 192.168.56.3.

7.3 Συνδέσαμε το καλώδιο.

7.4 Συνδεόμαστε ταυτόχρονα στην 192.168.56.2 για το FW1 και 192.168.56.3 για το FW3.

7.5 Άλλαξα το πεδίο hostname στο System → General Setup.

7.6 Στο Interfaces → WAN άλλαξα τα πεδία IP addresses (192.0.2.5) και Gateway (192.0.2.6) και ενεργοποίησα το checkbox Block private networks.

7.7 Άλλαξα το πεδίο IP address σε 192.168.2.1 στο Interfaces → LAN → Primary Configuration.

7.8 Το επανεκκίνησα.

7.9 Προσθέσαμε τον κανόνα από το Menu Firewall → Rules → LAN κλικ στο + Action: Pass, Interface: LAN, Protocol: any, Source: LAN subnet, Destination: any.

7.10 Προσθέσαμε τον κανόνα από το Menu Firewall → Rules → WAN κλικ στο + Action: Pass, Interface: WAN, Protocol: ICMP, Source: any, Destination: WAN address.

7.11 Χρησιμοποίησα τις εντολές /etc/rc.d/netif restart, ifconfig em0 192.168.2.2, route add default 192.168.2.1. Είχα αλλάξει ήδη το PC2 στο LAN2 από το Virtual Box.

7.12 Το ping είναι επιτυχές.

7.13 Το ping είναι επιτυχές.

7.14 Το ping δεν είναι επιτυχές και παίρνουμε μήνυμα σφάλματος Destination Host Unreachable, καθώς το R1 δεν γνωρίζει για τις διευθύνσεις των LAN.

7.15 Ενεργοποίησα το checkbox στο VPN → IPsec → Tunnels. Από το ίδιο υπομενού πρόσθεσα έναν νέο κανόνα με Interface: WAN, Local Subnet Type: LAN subnet, Remote Subnet: 192.168.2.0/24, Remote Gateway: 192.0.2.5, Pre-Shared Key: key.

7.16 Βλέπουμε κανόνα που επιτρέπει όλη την κίνηση από όλους προς όλους με περιγραφή “Default IPsec VPN”.

7.17 Δεν υπάρχει τίποτα.

7.18 Έχουν ορισθεί 2 πολιτικές μία για τα εισερχόμενα και μία για τα εξερχόμενα.

7.19 Ενεργοποίησα το checkbox στο VPN → IPsec → Tunnels. Από το ίδιο υπομενού πρόσθεσα έναν νέο κανόνα με Interface: WAN, Local Subnet Type: LAN subnet, Remote Subnet: 192.168.1.0/24, Remote Gateway: 192.0.2.1, Pre-Shared Key: key.

7.20 Δεν υπάρχει τίποτα.

7.21 Έχουν ορισθεί 2 πολιτικές μία για τα εισερχόμενα και μία για τα εξερχόμενα.

7.22 Ναι, μπορούμε.

7.23 Ναι, μπορούμε.

7.24 Ναι, προστέθηκαν 2 εγγραφές μία από το 192.0.2.5 προς το 192.0.2.1 και μία για το αντίστροφο.

7.25 Ναι, προστέθηκαν 2 εγγραφές μία από το 192.0.2.5 προς το 192.0.2.1 και μία για το αντίστροφο.

7.26 Χρησιμοποίησα την εντολή tcpdump -i em0 -vvv.

7.27 Δεν καταγράφονται πακέτα icmp.

7.28 Βλέπουμε πακέτα esp. Διευθύνσεις πηγής και προορισμού είναι οι διεπαφές των firewalls στα WAN.

7.29 Δεν βλέπουμε να εμφανίζεται κάπου πληροφορία για τις IP των PC1 και PC2.

7.30 Μπορούμε να συνδεθούμε. Αυτό που άλλαξε σε σχέση με την προηγούμενη άσκηση είναι πως τα μηνύματα που στέλνονται από το PC2 έχουν διεύθυνση πηγής την 192.0.2.5 και για αυτό μπορούμε να χρησιμοποιήσουμε τις NATed υπηρεσίες.

7.31 Βλέπουμε πακέτα tcp με πηγές πηγής και προορισμού τις διευθύνσεις 192.0.2.5 και 203.0.118.18.

7.32 Τα μηνύματα είναι κρυπτογραφημένα. Δεν είναι κρυπτογραφημένα με IPsec αλλά με SSH.