Ονοματεπώνυμο: Ανδρέας Στάμος (03120***)	**Όνομα PC:** linux / Ubuntu 22.04.2 LTS
Ομάδα: 1	**Ημερομηνία:** 16/04/2024

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.

Άσκηση 1

1.1 Στο PC1:

```
hostname PC1
ifconfig em0 192.168.1.2/24
```

Στο PC2:

```
hostname PC2
ifconfig em0 192.168.1.3/24
```

1.2 `kldload ipfw`

1.3 `kldstat`

1.4 Όχι, αποτυγχάνει με μήνυμα λάθους `Permission denied`.

1.5 `ipfw list`

Υπάρχει μόνο ο κανόνας: `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`

Σε κάθε γραμμή δείχνει έναν κανόνας μαζί με τους αντίστοιχους μετρητές. Πιο συγκεκριμένα, μετά τον πρώτο αριθμό, που είναι το rule number, ακολουθεί πρώτα ο μετρητής πακέτων που έχουν κάνει match με τον συγκεκριμένο κανόνα και έπειτα ο μετρητής bytes των πακέτων αυτών.

1.9 `ipfw zero 100`

1.10 Όχι, αποτυγχάνει με μήνυμα λάθους `Permission denied`.

1.11 `ipfw add allow icmp from any to any`

1.12 200

(αριθμός κατά 100 μεγαλύτερος από τον μεγαλύτερο ως τώρα κανόνα, πλήν του προκαθορισμένου, που είναι το 100)

1.13 Ναι επιτυγχάνουν και τα δύο ping.

1.14 Από προεπιλογή το `traceroute` χρησιμοποιεί το πρωτοκόλλο μεταφοράς UDP, η κίνηση του οποίου γίνεται match με τον προεπιλεγμένο κανόνα, οπότε τα σχετικά πακέτα απορρίπτονται.

Θέτοντας το option `-I`, το `traceroute` χρησιμοποιεί πακέτα ICMP αντί UDP, οπότε επιτυγχάνει.

1.15 Γενικά το `traceroute` χρησιμοποιεί από προεπιλογή ως base port το 33434 και σε κάθε πακέτο που αποστέλλει, αυξάνει τον αριθμό θύρας. Με βάση αυτή τη συμπεριφορά, θα πρέπει να επιτρέψουμε την εξερχόμενη UDP κίνηση σε όλες τις UDP θύρες με αριθμό θύρας ≥ 33435. Έτσι εκτελούμε:

```
ipfw add allow udp from me to any 33435-65535 out
```

Πλέον το `traceroute` επιτυγχάνει.

1.16 Όχι.

1.17
```
ipfw add 10 check-state
ipfw add allow tcp from me to any 22 out setup keep-state
```

1.18
```
ipfw zero
ssh lab@192.168.1.3
ls
exit
```

1.19 Ο 2ος κανόνας (για το tcp) εφαρμόστηκε για 80 πακέτα και συνολικά για 14032 bytes.

Ο 1ος κανόνας (για το check-state) για λόγους αποδοτικότητας (στην πραγματικότητα δεν είναι κανόνας, απλά οδηγεί σε άλλους κανόνες) δεν καταγράφεται πλήθος matches.

1.20 Όχι, διότι αφενός δεν έχει γίνει setup σύνδεσης από το PC1, αφετέρου διότι η σύνδεση TCP δεν είναι στην θύρα 22 του PC2, αλλά σε μια τυχαία σύνδεση του PC2.

1.21 `service ftpd onestart`

1.22 Όχι, διότι η κίνηση δεν επιτρέπεται στην TCP θύρα 21 (FTP control θύρα).

Άσκηση 2

2.1 `kldload ipfw`

2.2 Όχι, αποτυγχάνει με μήνυμα λάθους `Permission denied`.

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

2.4 `ipfw add allow icmp from me to any out icmptypes 8`

2.5 Όχι, διότι το Echo Reply που στέλνει πίσω το PC1 προς το PC2 (επιβεβαιώθηκε με tcpdump ότι όντως φθάνει στο PC2), απορρίπτεται από το ipfw.

2.6 Όχι. Παρατηρούμε ότι απορρίπτονται τόσα πακέτα όσα τα Echo Requests που επιτρέπονται. Τα πακέτα που απορρίπτονται είναι τα Echo Replies που στέλνει πίσω το PC1 προς το PC2.

2.7
```
ipfw delete 200
ipfw add allow icmp from me to any out icmptypes 8 keep-state
```

Το ping πλέον επιτυγχάνει.

2.8 Ναι επιτυγχάνει.

2.9 Αποτυγχάνει. Το ipfw μόλις περάσει κάποιος χρόνος από τα τελευταία ping, θεωρεί ότι η "ICMP σύνδεση" έχει λήξει, οπότε διαγράφει τον σχετικό δυναμικό κανόνα που έπετρεπε στα ICMP πακέτα από το PC1 να εισέλθουν στο PC2. Στην συνέχεια, τα Echo Requests του PC1 απορρίπτονται.

2.10 `ipfw add allow icmp from any to me in icmptypes 8 keep-state`

2.11 Με την επιλογή `-d` βλέπουμε και τους δυναμικούς κανόνες, εκτός από τους στατικούς. Με την επιλογή `-D` βλέπουμε μόνο τους δυναμικούς κανόνες.

Εδώ βλέπουμε να υπάρχει δυναμικός κανόνας που επιτρέπει όλη την ICMP κίνηση μεταξύ PC1 και PC2.

2.12 Δεν υπάρχουν δυναμικοί κανόνες.

2.13
```
ipfw add allow udp from any 33435-65535 to me in
ipfw add allow icmp from me to any out icmptypes 3
```

Συμπλήρωση: Εναλλακτικά, για μεγαλύτερη ασφάλεια, ώστε τα UDP πακέτα να μην εισέλθουν προς επεξεργασία στον πυρήνα, μπορούμε να βάλουμε τον κανόνα:

`ipfw add unreach port udp from any 33435-65535 to me in`

Και στις δύο περιπτώσεις επιβεβαιώθηκε ότι το traceroute PC1 → PC2 επιτυγχάνει.

2.14
```
ipfw add allow udp from me 33435-65535 to any out
ipfw add allow icmp from any to me in icmptypes 3,11
```

2.15 `ipfw add unreach port udp from any 33435-65535 to me in`

2.16 `ipfw add allow tcp from 192.168.1.0/24 to me 22 in setup keep-state`

2.17 `ssh lab@192.168.1.3`

2.18 `ipfw add allow tcp from me to any 22 out setup keep-state`

2.19 `ipfw add allow tcp from 192.168.1.3 to me 22 in setup keep-state`

2.20 Ναι.

(σημειώνεται πως πρόκειται για το Secure FTP και όχι για το Simple FTP)

2.21 Όχι δεν μπορούμε, διότι το τοίχος προστασίας απορρίπτει την σχετική κίνηση.

Εκτελούμε στο PC2:

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

Επίσης πρέπει να προσθέσουμε στο PC1 σχετικό κανόνα να για να επιτρέπει την εξερχόμενη κίνηση:

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

2.22 Η 1η εντολή περιλαμβάνει ανταλλαγές μηνυμάτων μόνο στο επίπεδο την FTP σύνδεσης ελέγχου. Αντίθετα, για να φθάσουν τα αποτελέσματα της 2ης εντολής στον πελάτη (PC1), απαιτείται μια FTP σύνδεση δεδομένων.

Από προεπιλογή το ftp λειτουργεί σε Passive Mode. Αυτό σημαίνει ότι ο εξυπηρετητής (το PC2) στέλνει στον πελάτη (PC1), μια θύρα στην οποία θα γίνει η σύνδεση δεδομένων. Την σύνδεση αυτή πρέπει να ξεκινήσει ο πελάτης. Ωστόσο, στον πελάτη (PC1) η εξερχόμενη κίνηση προς αυτή την θύρα απαγορεύεται. Ακόμα, όμως, και αν επιτρέποταν, η αντίστοιχη εισερχόμενη κίνηση στον εξυπηρετητή (PC2) θα απαγορευόταν.

2.23 `ipfw add allow tcp from any to me 1024-65535 in setup keep-state`

Επίσης πρέπει να επιτρέψουμε την σχετική εξερχόμενη κίνηση στο PC1 εκτελώντας σε αυτό:

`ipfw add allow tcp from me to any 1024-65535 out setup keep-state`

2.24 Ναι.

2.25 Στο PC1:

`ipfw add allow tcp from me 20 to any 1024-65535 out setup keep-state`

Στο PC2:

`ipfw add allow tcp from any 20 to me 1024-65535 in setup keep-state`

Η μεταφορά αρχείων σε FTP Active Mode πλέον λειτουργεί.

2.26 Το FTP είναι μια μη ασφαλής υπηρεσία, οπότε γενικά ένας τείχος προστασίας μπορεί να βοηθήσει να γίνει κάπως ασφαλές, επιτρέποντας κίνηση μόνο με συγκεκριμένους hosts.

2.27 Εκτελώ και στο PC1 και στο PC2:

`kldunload ipfw`

Επιβεβαιώνεται ότι απενεργοποιήθηκε με την εντολή:

`kldstat`

Άσκηση 3

3.1 Και στο PC1 και στο PC2:

`route add default 192.168.1.1`

3.2
```
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
```
hostname SRV1
ifconfig em0 192.0.2.5/30
route add default 192.0.2.6
```

3.4 `service ftpd onestart`

3.5 Εκτελώ:

`kldstat`

Έχουν φορτωθεί τα εξής modules:

1. intpm.ko
2. smbus.ko
3. ipfw.ko
4. ipfw_nat.ko
5. libalias.ko

3.6 ipfw

3.7 Εκτελώ:

`sysrc firewall_type`

Η μεταβλητή έχει τιμή `UNKNOWN`, που σημαίνει ότι δεν έχουν φορτωθεί προεπιλεγμένοι κανόνες στο ipfw.

3.8 Υπάρχουν 11 κανόνες.

Ο τελευταίος κανόνας είναι ο προκαθορισμένος: `deny ip from any to any`

3.9 `ipfw nat show config`

Δεν έχουν οριστεί πίνακες NAT.

3.10 Όχι.

3.11 Όχι.

3.12 `ipfw nat 123 config if em1 unreg_only reset`

3.13 `ipfw add nat 123 ip from any to any`

3.14 Ναι επιτυγχάνει και προς την διεπαφή στο LAN1 και προς την διεπαφή στο WAN1.

3.15 `tcpdump -nvi em1`

3.16
```
ipfw show
ipfw zero
```

3.17 `ping -c 192.0.2.2`

Διεύθυνση πηγής είναι η 192.0.2.1, δηλαδή η διεύθυνση του FW1 στο WAN1.

3.18 Διεύθυνση προορισμού είναι η 192.0.2.1, δηλαδή η διεύθυνση του FW1 στο WAN1.

3.19 Βλέποντας τα στατιστικά εκτελώντας `ipfw show`, βλέπουμε ότι υπεύθυνος είναι ο κανόνας:

`nat 123 ip from any to any`

3.20 Εφαρμόστηκε 12 φορές. Από τον FW1 πέρασαν συνολικά 3 Echo Requests και 3 Echo Replies. Κάθε πακέτο παρελήφθηκε και αποστάλθηκε, οπότε πέρασε 2 φορές από το τοίχος προστασίας. Συνολικά, επομένως ο κανόναςν εφαρμόστηκε πράγματι, $2 \cdot (3 + 3) = 12$ φορές.

3.21 Ναι.

3.22 Ο κανόνας για το NAT: `nat 123 ip from any to any`

3.23 Ναι. Εφαρμόζονται διαδοχικά όλοι οι κανόνες του ipfw, και είναι ο 1ος που κάνει match, οπότε εισέρχεται στην μετάφραση διευθύνσεων.

3.24 Ναι.

3.25 Όχι.

Με tcpdump βλέπουμε ότι ο R1 στέλνει στον SRV1 ICMP Host Unreachable. Πράγματι, ο R1 δεν γνωρίζει πώς να δρομολογήσει προς το 192.168.1.3. Συνεπώς, φαινομενικά είναι θέμα δρομολόγησης το γεγονός ότι δεν μπορούμε να στείλουμε πακέτα από το SRV1 προς το PC2.

Όμως, στην πραγματικότητα, το αληθινό πρόβλημα είναι το NAT. Όταν εκκινούμε σύνοδο ssh από το PC2 προς τον SRV1, και πάλι ο SRV1 αποστέλλει πακέτα προς το PC2. Όμως τα πακέτα στέλνονται με διεύθυνση παραλήπτη το FW1, που αναλαμβάνει να αλλάξει τις διευθύνσεις. Εδώ αυτό δεν θα μπορούσε να συμβεί, δηλαδή να εκκινήσουμε σύνοδο ssh με το PC2 στέλνοντας προς τον FW1, διότι στον FW1 δεν υπάρχει εγγραφή μετάφρασης διευθύνσεων, εφόσον η σύνδεση δεν ξεκίνησε πίσω από το NAT.

3.26 `ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1`

3.27 Επιτυγχάνει. Συνδεόμαστε στο PC2. Το διαπιστώνουμε βλέποντας το hostname στο prompt του shell.

3.28 `ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1 redirect_port 192.168.1.2:22 22`

3.29 Συνδεόμαστε στο PC1. Το διαπιστώνουμε βλέποντας το hostname στο prompt του shell.

3.30 Συνδεόμαστε στο PC2. Το διαπιστώνουμε βλέποντας το hostname στην 1η γραμμή που εκτυπώνει το ftp.

3.31 Ναι.

3.32 PC2

3.33 PC1

Άσκηση 4

4.1 (εκτελείται η εντολή)

Τα ping προς τις διεπαφές στο LAN1 και WAN1 αντίστοιχα του FW1 αποτυγχάνουν.

4.2 Γίνονται δεκτά. Ωστόσο, μετά την μετάφραση διευθύνσεων, ακολουθούν τον επόμενο κανόνα, που είναι ο προκαθορισμένος κανόνας 65535, που απορρίπτει όλη την κίνηση.

Αυτό έχει ως αποτέλεσμα να απορρίπτονται τα Echo Requests που στέλνει το PC1, οπότε το ping αποτυγχάνει.

4.3
```
ipfw delete 1100
ipfw add 1100 allow ip from any to any via em0
```

4.4 Ναι.

4.5 Στο FW1.

4.6 Μηδενίσαμε τους μετρήτες, εκτελέσαμε τις εντολές και έπειτα είδαμε τις τιμές τους.

Για το ping απαραίτητος ήταν μόνο ο κανόνας που προστέθηκε πριν.

Όμως, το ssh βρέθηκε πως περνά κάποια αρχική κίνηση από την loopback διεπαφή, οπότε χρησιμοποιείται και ο 1ος κανόνας: `allow ip from any to any via lo0`

4.7 `ipfw add 3000 nat 123 ip from any to any xmit em1`

4.8 `ipfw add 3001 allow ip from any to any`

4.9 `ipfw add 2000 nat 123 ip from any to any recv em1`

4.10 `ipfw add 2001 check-state`

4.11 FW1

4.12 PC2

(τα πακέτα προς την διεύθυνση 192.0.2.1 είχαν γίνει redirect προς το PC2)

4.13 FW1

4.14 PC1

(τα πακέτα προς το port 22 είχαν γίνει redirect προς το PC1)

4.15 PC2

(τα πακέτα προς την διεύθυνση 192.0.2.1 είχαν γίνει redirect προς το PC2)

4.16 Ναι.

4.17 Ναι.

4.18 Ναι.

4.19 `ipfw add 2999 deny ip from any to any via em1`

4.20 Επιτυγχάνουν μόνο τα ping, ftp, ssh μεταξύ hosts του LAN1.

Πιο συγκεκριμένα, δηλαδή, από αυτά που εκτελέστηκαν, επιτυγχάνουν μόνο τα:

- ping PC1 → 192.0.2.1
- ssh PC1 → 192.0.2.1

4.21 `ipfw add 2500 skipto 3000 icmp from any to any xmit em1`

4.22 Ναι.

4.23 `ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 setup keep-state`

4.24 Ναι.

4.25 `ipfw add 2100 skipto 3000 icmp from any to any in via em0`

4.26 PC2. (ελέγχθηκε με tcpdump στο PC2 πως είναι το ίδιο που λαμβάνει τα Echo Requests και που εκπέμπει τα Echo Replies)

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

4.28 PC1

4.29 Όχι, διότι η κίνηση στην θύρα 21 απορρίπτεται από το FW1.

4.30
```
ipfw add 2700 skipto 3000 tcp from any to any 21 recv em1 setup keep-state
ipfw add 2800 skipto 3000 tcp frp any 20 to any recv em0 setup keep-state
```

Ο 1ος κανόνας αφορά στην FTP control σύνδεση που ξεκινά από τον πελάτη και γίνεται στην TCP θύρα 21 του εξυπηρετητή (και σε τυχαία θύρα πελάτη).

Ο 2ος κανόνας αφορά στην FTP δεδομένων σύνδεση που ξεκινά από τον εξυπηρετητή και γίνεται στην TCP θύρα 20 του εξυπηρετητή (η θύρα πελάτη έχει σταλεί πριν στην FTP control σύνδεση).

Επιβεβαιώθηκε ότι η μεταφόρτωση αρχείων σε FTP Active Mode (πελάτης ο SRV1, εξυπηρετητής ο PC2) λειτουργεί.

Άσκηση 5

5.1 Από την κονσόλα βλέπουμε ότι είναι: 192.168.1.1

5.2 Από την κονσόλα βλέπουμε ότι είναι: 10.0.0.1

5.3 Από την landing σελίδα, βλέπουμε ποσοστό χρήσης μνήμης 33%, οπότε το ποσοστό ελεύθερης μνήμης είναι 66%.

5.4 Από την κονσόλα βλέπουμε ότι υπάρχουν 4 διπεαφές δικτύου.

5.5 Interfaces → DMZ.

Η διεύθυνση για την διεπαφή DMZ είναι 172.22.1.1.

5.6 System → General Setup

Hostname: `fw`

DNS περιοχή: `lab.ntua.gr`

5.7 Hostname: `fw1`

Έπειτα πατάω Save.

5.8 Όχι.

5.9 Interfaces → WAN

Θέτω:

IP Address: 192.0.2.1/30

Gateway: 192.0.2.2

Επιλέγω το Block Private Networks.

Πατάω Save.

5.10 Ναι, υπάρχει ο κανόνας που μπλοκάρει την κίνηση που αφορούν σε ιδιωτικές διευθύνσεις.

5.11 Όχι.

5.12 Services → DNS Forwarder → Enable DNS Forwarder → Save

5.13 Services → DHCP Server → LAN → Enable

Range: 192.168.1.2 – 192.168.1.3

Πατάω Save.

5.14 `dhclient em0`

Του αποδόθηκαν:

- IP διεύθυνση: 192.168.1.2/24
- Προεπιλεγμένη πύλη: 192.168.1.1
- DNS εξυπηρετητής: 192.168.1.1

5.15 Προκειμένου ο DHCP εξυπηρετητής του FW1, να διαφημίζει τον εαυτό του ως DNS εξυπηρετητής (που με την σειρά του θα στέλνει τα αιτήματα σε γνωστούς σε αυτόν εξυπηρετητές DNS) στους hosts του LAN, ώστε να έχουν τρόπο να μεταφράσουν domains σε IP διευθύνσεις.

5.16 Diagnostics → DHCP leases

5.17 7

5.18 Όχι.

5.19 Βλέπουμε ότι τα ICMP Echo Requests που στέλνει το PC1 προς το FW1-LAN1 απορρίπτονται.

Καθαρίζουμε το log πατώντας το Clear log.

5.20 25.

5.21 Κανέναν.

5.22 Firewall → Rules → +

Action: Pass

Interface: LAN

Protocol: any

Πατάω Save.

Πατάω Apply Changes.

5.23 Ναι, το ping επιτυγχάνει προς όλες τις διεπαφές του FW1 στα LAN1, WAN1 και DMZ.

5.24 Όχι.

5.25 Ναι, η IP διεύθυνση του FW1 στο WAN1 (192.0.2.1) έχει αντιστοιχηθεί με την σωστή MAC διεύθυνση, δηλαδή με την MAC διεύθυνση της διεπαφής του FW1 στο WAN1.

5.26 Firewall → Rules → +

Action: Pass

Interface: WAN

Protocol: ICMP

Destination → Type: WAN address

Πατάω Save.

Πατάω Apply Changes.

5.27 Ναι.

5.28 Όχι, διότι ο R1 δεν γνωρίζει πως να δρομολογήσει για το 192.168.1.2.

Ακόμα, όμως και αν δρομολογούσε για το 192.168.1.2 προς το FW1, το firewall θα έκοβε την κίνηση προς 192.168.1.3, διότι δεν είναι η "WAN Address".

5.29 Ναι μπορούμε, διότι το NAT μεταφράζει τις ιδιωτικές διεύθυνσεις του LAN στην διεύθυνση του FW1 στο WAN1.

5.30 `ifconfig em0 172.22.1.2/24 up`

Το ping αποτυγχάνει, διότι αν και τα Echo Requests φθάνουν στον SRV1, ο SRV1 δεν γνωρίζει πώς να δρομολογήσει για το PC1, προκειμένου να στείλει το Echo Reply.

5.31 `route add default 172.22.1.1`

5.32 Ναι.

5.33 Όχι, διότι τα ICMP πακέτα με πηγή το DMZ δεν επιτρέπονται από το firewall.

5.34 Όχι, διότι τα ICMP πακέτα με πηγή το DMZ δεν επιτρέπονται από το firewall.

5.35 Firewall → Rules → +

Action: Pass

Interface: DMZ

Protocol: any

Destination → not

Destination → LAN subnet

Πατάω Save.

Πατάω Apply Changes.

5.36 Ναι.

5.37 Ναι.

5.38 Όχι, διότι ο R1 δεν γνωρίζει πως να δρομολογήσει για το 192.168.1.2.

Ακόμα, όμως, και αν δρομολογούσε, τα Echo Requests θα απορρίπτονταν από το firewall, καθώς απορρίπτονται τα πακέτα από το WAN προς ιδιωτικές διευθύνσεις.

5.39 Ναι. Ο FW1 κάνει μετάφραση της διεύθυνσης του SRV1 στου FW1 στα εξερχόμενα προς WAN πακέτα, και μετάφραση της διεύθυνση του FW1 στου SRV1 στα εισερχόμενα από WAN πακέτα.

5.40 `dhclient em0`

Του αποδόθηκαν:

- IP διεύθυνση: 192.168.1.3/24
- Προεπιλεγμένη πύλη: 192.168.1.1
- DNS εξυπηρετητής: 192.168.1.1

5.41 Firewall → Rules → +

Action: Block

Interface: LAN

Protocol: any

Source → Type: Single host or alias

Source → Address: 192.168.1.3

Destination → Type: Single host or alias

Destination → Address: 172.22.1.2

Πατάω Save.

Πατάω Apply Changes.

5.42 Πρέπει να τοποθετηθεί πριν τον υπάρχοντα, διότι διαφορετικά, ο ήδη υπάρχων κανόνας θα επιτρέψει όλη την κίνηση.

Για να γίνει αυτό επιλέγουμε τον νέο κανόνας και πατάμε το "↤" διπλά στον προϋπάρχοντα κανόνα.

Έπειτα πατάω Apply Changes.

5.43 Όχι.

5.44 Ναι, διότι εφαρμόζεται ο 2ος κανόνας του LAN, που επιτρέπει όλη την κίνηση από το LAN.

Άσκηση 6

6.1
```
cli
configure terminal
ip route 203.0.118.0/24 192.0.2.1
```

6.2 (εκτελείται η διαδικασία)

6.3 Firewall → NAT → Outbound → +

Interface: WAN

Source: 192.168.1.2/32

Target: 203.0.118.14

Πατάω Save.

Πατάω Apply Changes.

6.4 Firewall → NAT → Outbound → +

Interface: WAN

Source: 192.168.1.3/32

Target: 203.0.118.15

Πατάω Save.

Πατάω Apply Changes.

6.5 `tcpdump -nvi em0`

6.6 Ναι επιτυγχάνει.

Τα πακέτα από τον PC1 φθάνουν με διεύθυνση πηγής 203.0.118.14.

Τα πακέτα από τον PC2 φθάνουν με διεύθυνση πηγής 203.0.118.15.

6.7 (εκτελείται η διαδικασία)

6.8 (εκτελείται η διαδικασία)

6.9 Κανόνας που επιτρέπει την TCP κίνηση από το WAN προς τον host 172.22.22.1, θύρα 22.

Εισάγεται διότι επιλέξαμε το "Auto-add a firewall rule..." προηγουμένως.

6.10 Ναι επιτυγχάνει.

Συνδεόμαστε στον SRV1.

6.11 Όχι αποτυγχάνει.

Αυτό συμβαίνει διότι το firewall δεν επιτρέπει την ICMP κίνηση από το WAN προς το 172.22.1.2. Ο κανόνας που εισάγαμε προηγουμένως επιτρέπει μόνο κίνηση προς την TCP θύρα 22.

6.12 (εικάζουμε πως υπάρχει τυπογραφικό λάθος και η σωστή διεύθυνση είναι η 203.0.118.18)

Ναι το ssh επιτυγχάνει και από το PC1 και από το PC2 προς τον SRV1.

Ακολοθούν την διαδρομή:

PC1/PC2 ↔ FW1 ↔ R1 ↔ FW1 ↔ SRV1

Τα πακέτα με προορισμό 203.0.118.18 φθάνουν στον FW1, που τα στέλνει προς την προκαθορισμένη πύλη που είναι ο R1. Ο λόγος που συμβαίνει αυτό και δεν στέλνονται απευθείας προς τον SRV1, είναι διότι η μετάφραση Inbound NAT για τον SRV1 γίνεται μόνο όταν πακέτα φθάνουν από το WAN, οπότε εδώ δεν συμβαίνει, αφού ερχόνται από το LAN.

Πριν αποσταλλούν τα πακέτα προς τον FW1, γίνεται η μετάφραση Outbound NAT, που αλλάζει την διεύθυνση πηγής σε δημόσια διεύθυνση (203.0.118.14 αν πρόκειται για το PC1 ή 203.0.118.15 αν πρόκειται για το PC2)

Ο R1 έχει κανόνα δρομολόγησης για το 203.0.118.18 προς τον FW1, οπότε τα πακέτα αποστέλλονται εκ νέου προς τον FW1. Ο FW1 παραλαμβάνοντας, πλέον από το WAN, πακέτα για το 203.0.118.18 εκτελεί την μετάφραση Inbound NAT, τα πακέτα αποκτούν προορισμό 172.22.1.2 και έτσι στέλνονται στον SRV1.

Ωστόσο, δεν εφαρμόζεται η μετάφραση Outbound NAT για το PC1, καθώς αυτή συμβαίνει μόνο στα πακέτα που φεύγουν προς το WAN, ενώ εδώ έρχονται από το WAN και πάνε προς το DMZ. Αυτό έχει ως αποτέλεσμα ο SRV1 να δει ως πηγή την δημόσια διεύθυνση 203.0.118.14 (ή .15).

Στην αντίστροφη πορεία, συμβαίνει η ίδια διαδικασία. Ο SRV1 στέλνει προς την δημόσια διεύθυνση 203.0.118.14 (ή .15), διότι αυτή είδε ως διεύθυνση πηγής πριν. Ο FW1, παραλαμβάνοντας από τον SRV1, δεν εκτελεί την μετάφραση Outbound NAT που αφορά στο PC1(/PC2), διότι δεν είναι στο πεδίο της διεύθυνση πηγής η διεύθυνσή τους. Έτσι, τα πακέτα, όπως πριν, πάνε στον R1, που τα στέλνει πίσω στον FW1. Ο FW1, εκτελεί, όπως πριν, μετάφραση Outbound NAT, οπότε τα πακέτα φθάνουν στο PC1 (/PC2), οπότε το ssh επιτυγχάνει.

Για να το επιβεβαιώσουμε εκτελούμε tcpdump στα PC1, PC2, SRV1 και R1 και επιβεβαιώνουμε ότι πράγματι συμβαίνει η διαδικασία όπως την περιγράφουμε, με τις συγκεκριμένες διεύθυνσεις που περιγράψαμε.

6.13 Firewall → NAT → Outbound

Επιλέγω την εγγραφή με Source 192.168.1.2.

Πατάω το ×.

Η σύνδεση αποτυγχάνει. Αυτό συμβαίνει, διότι, όπως περιγράψαμε στο Ερώτημα 6.12, η σύνδεση ssh από το PC1 προς το 203.0.118.18 περιλαμβάνει αποστολή πακέτων από και προς τον R1, όπου συνέβαινε η Outbound μετάφραση της ιδιωτικής διεύθυνσης του PC1 σε δημόσια διεύθυνση. Αυτό πλέον δεν συμβαίνει, οπότε τα πακέτα φθάνουν στον R1 με διεύθυνση πηγής 192.168.1.2. Ο R1 στέλνει τα πακέτα πίσω στον FW1. Ο FW1 πλέον λαμβάνει πακέτα με διεύθυνση πηγής ιδιωτική διεύθυνση. Όμως υπάρχει κανόνας στο firewall που απαγορεύει αυτή την κίνηση. Έτσι, τελικά, τα πακέτα αυτά απορρίπτονται, και η σύνδεση ssh αποτυγχάνει.

6.14 Firewall → NAT → Outbound

Αποεπιλέγω το Enable advanced outbound NAT.

Πατάω Save.

6.15 Η σύνδεση ssh από τον R1 προς τον SRV1 επιτυγχάνει. Αυτό συμβαίνει, διότι στην επικοινωνία του R1 με τον SRV1, δεν εμπλεκόταν το Outbound NAT, που αφορούσε στα PC1 και PC2, αλλά μόνο το Inbound NAT.

Ωστόσο, η σύνδεση ssh από τα PC1/PC2 αποτυγχάνει. Στο επόμενο ερώτημα (Ερώτημα 6.12) θα εξηγηθεί ο λόγος που συμβαίνει αυτό.

6.16 `tcpdump -envi em0`

Αυτό που συμβαίνει είναι ότι με ανενεργό το Advanced outbound NAT, το FW1 έχει δημιουργήσει αυτόματα ένα mapping διευθύνσεων από όλο το υποδίκτυο του LAN προς την διεύθυνση του WAN, το οποίο όμως εφαρμόζει μόνο κατά την κίνηση μεταξύ LAN και WAN. Έτσι, τα πακέτα πάνε στον R1, επιστρέφουν στον FW1, και τελικά φθάνουν στον SRV1. Ο SRV1 βλέπει πηγή την WAN διεύθυνση του FW1, οπότε στέλνει πακέτα προς αυτή την διεύθυνση, δηλαδή προς τον FW1. Ο FW1, όπως είπαμε πριν, δεν εφαρμόζει μεταφράση διεύθυνσεων αν η κίνηση δεν είναι μεταξύ LAN και WAN, οπότε παραλαμβάνει το πακέτο σαν να ήταν παραλήπτης ο ίδιος, δηλαδή παραδίδει το πακέτο SYNACK του SRV1 στον πυρήνα του, που απαντά με RST, αφού δεν έχει ξεκίνησει καμία σχετική σύνδεση. Τελικά, ο SRV1 παραλαμβάνει ένα RST από τον FW1, ενώ το PC1/PC2 δεν μαθαίνει τίποτα για όσα συνέβησαν.

6.17 Ο κανόνας του ερωτήματος 5.41 δεν έχει σχέση με την προηγούμενη συμπεριφορά, αφού αφορά σε κίνηση από το PC2 προς την διεύθυνση 172.22.1.2, ενώ εδώ, όπως εξηγήσαμε παραπάνω στο ερώτημα 6.16 συμβαίνει ένα διαφορετικό φαινόμενο.

Ο κανόνας για το DMZ (ερώτημα 5.35) δεν έχει κάποια σχέση, αφού επιτρέπει γενικά την εξερχόμενη κίνηση από τον SRV1 προς μηχανήματα εκτός του LAN, και πράγματι αυτό συμβαίνει εδώ: Έχουμε κίνηση από τον SRV1 προς τον FW-WAN1 $\notin$ LAN.

Γενικά ο λόγος που αποτυγχάνει η σύνδεση, είναι το φαινόμενο που περιγράφηκε παραπάνω στο ερώτημα 6.16.

Άσκηση 7

7.1 (αποσυνδέθηκε το καλώδιο)

7.2 Interfaces → MNG

IP address: 192.0.2.1/30

Gateway: 192.0.2.2

Πατάω Save.

7.3 (επανασυνδέθηκε το καλώδιο)

7.4 Ναι.

7.5 System → General Setup

Hostname: fw2

Πατάω Save.

7.6 Interfaces → MNG

IP address: 192.0.2.5/30

Gateway: 192.0.2.6

Επιλέγω Block Private Networks.

Πατάω Save.

7.7 Interfaces → LAN

IP address: 192.168.2.1/24

Πατάω Save.

7.8 Επιλέγω το link για reboot.

Πατάω Yes.

7.9 Firewall → Rules → LAN → +

Action: Pass

Interface: LAN

Protocol: any

Πατάω Save.

Πατάω Apply changes.

7.10 Firewall → Rules → WAN → +

Action: Pass

Interface: WAN

Protocol: ICMP

Destination → Type: WAN address

Πατάω Save.

Πατάω Apply changes.

7.11
```
ifconfig em0 192.168.2.2/24 up
route add default 192.168.2.1
```

7.12 Ναι.

7.13 Ναι.

7.14 Όχι αποτυγχάνει. Ο δρομολογητής R1 στέλνει ICMP Host Unreachable καθώς δεν γνωρίζει πως να δρομολογήσει για το 192.168.1.2 (για ping PC2 → PC1) ή για το 192.168.2.2 (για ping PC1 → PC2).

7.15 VPN → IPsec → Enable IPsec

Πατάω Save.

Πατάω +.

Interface: WAN

Local subnet → Type: LAN subnet

Remote subnet: 192.168.2.0/24

Remote gateway: 192.0.2.5

Pre-Shared Key: thisisakey

Πατάω Save.

Πατάω Apply Changes.

7.16 Κανόνα που επιτρέπει όλη την κίνηση από και προς την διεπαφή IPsec.

7.17 Όχι.

7.18 Ναι, έχουν ορισθεί μία πολιτική για τα πακέτα από το LAN2 και μία για τα πακέτα προς το LAN2.

7.19 VPN → IPsec → Enable IPsec

Πατάω Save.

Πατάω +.

Interface: WAN

Local subnet → Type: LAN subnet

Remote subnet: 192.168.1.0/24

Remote gateway: 192.0.2.1

Pre-Shared Key: thisisakey

Πατάω Save.

Πατάω Apply Changes.

7.20 Όχι.

7.21 Ναι, έχουν ορισθεί μία πολιτική για τα πακέτα από το LAN1 και μία για τα πακέτα προς το LAN1.

7.22 Ναι.

7.23 Ναι.

7.24 Ναι έχουν προστέθει 2 εγγραφές, μία για πακέτα FW1 → FW2 και μία για πακέτα FW2 → FW1.

7.25 Ναι έχουν προστέθει 2 εγγραφές, μία για πακέτα FW2 → FW1 και μία για πακέτα FW1 → FW2.

7.26 `tcpdump -nvi em0`

7.27 Όχι.

7.28 Βλέπουμε πακέτα IP που έχουν επικεφαλίδα με Protocol Number που αντιστοιχεί στο ESP, δηλαδή Encapsulating Security Protocol.

Στα μισά πακέτα IP πηγή είναι η 192.0.2.5 και IP προορισμός ειναι η 192.0.2.1 και στα άλλα μισά πακέτα είναι αντίστροφα.

7.29 Όχι.

7.30 Ναι μπορούμε.

Προηγουμένως τα πακέτα του PC2 έφταναν στον SRV1 με διεύθυνση πηγής 192.0.2.1, που ανήκει στον FW1, οπότε ο PC2 απαντούσε προς διεύθυνση προορισμού 192.0.2.1. Το FW1 λάμβανε από το DMZ, όπου δεν εφάρμοζε την μετάφραση για το PC1, και έτσι θεωρούσε ότι παραλήπτης των πακέτων ήταν το ίδιο μηχάνημα, οπότε η σύνδεση αποτύγχανε.

Αντίθετα, εδώ ο SRV1 λαμβάνει πακέτα με πηγή 192.0.2.5 (η μετάφραση συνέβη στον FW2, τα πακέτα εξήλθαν προς το δημόσιο διαδίκτυο, το IPsec δεν σχετίζεται εδώ), οπότε απαντά με προορισμό το 192.0.2.5. Το FW1 προωθεί αυτά τα πακέτα προς τον R1, που τα προωθεί προς το FW2. Το FW2 λαμβάνει τα πακέτα από το WAN, οπότε εφαρμόζει την μετάφραση διεύθυνσεων, και έτσι, τελικά, η απάντηση του SRV1 φθάνει στο PC2, οπότε η σύνδεση ssh επιτυγχάνει.

7.31 TCP πακέτα μεταξύ των διεύθυνσεων 192.0.2.5 και 203.0.118.18. Η θύρα που αντιστοιχεί σε όποια πλευρά (αποστολέας/παραλήπτης κατά περίπτωση) είναι η 203.0.118.18, είναι η 22 (του ssh). Η άλλη θύρα είναι μια τυχαία θύρα.

7.32 Όχι. Το PC2 συνδέεται προς το 203.0.118.18 που είναι δημόσια διεύθυνση, όποτε τα πακέτα, μετά το FW2, εξέρχονται προς το δημόσιο διαδίκτυο. Το IPsec δεν σχετίζεται με αυτή την σύνοδο ssh.