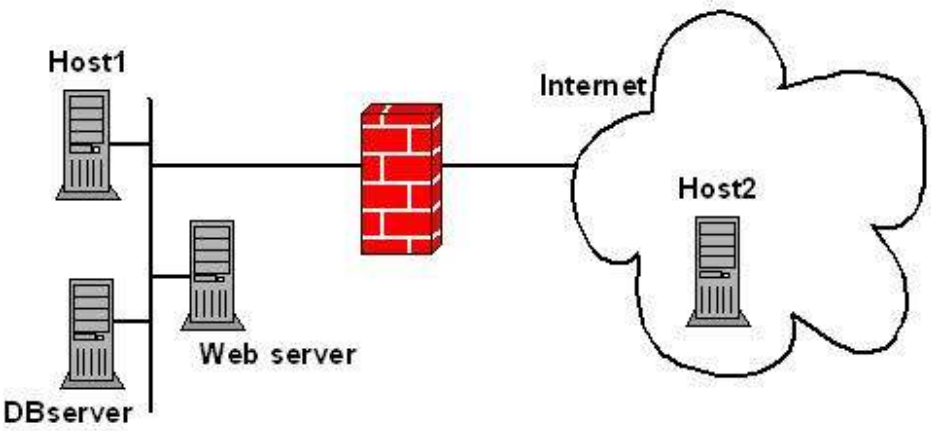
ΛΥΣΕΙΣ

Αναχώματα ασφαλείας – Firewalls

[1] Θεωρείστε την ακόλουθη τοπολογία δικτύου:



Το Firewall έχει πολιτική ασφάλειας που περιγράφεται με τους παρακάτω κανόνες:

Α/Α	Προέλευση	Προορισμός	Υπηρεσία	Ενέργεια
1	Εσωτερικό δίκτυο	Οπουδήποτε	όλες	επιτρέπεται
2	Host2	DBserver	SQL	επιτρέπεται
3	Οπουδήποτε	Web server	HTTP	επιτρέπεται
4	Οπουδήποτε	Οπουδήποτε	όλες	απαγορεύεται

Απαντήστε **ποιος** και **γιατί** από τους παραπάνω κανόνες ενεργοποιείται για να γίνει ο έλεγχος στα παρακάτω αιτήματα:

i. Ένα πακέτο TCP/IP με αίτημα προσπέλασης από το Internet στον Web server για http: (10)

Ενεργοποιείται ο κανόνας 3 → το πακέτο επιτρέπεται να περάσει το firewall. Το Internet ως προέλευση εμπίπτει στο «Οπουδήποτε» του κανόνα 3, ενώ προορισμός είναι ο Web server.

ii. Ένα πακέτο TCP/IP με αίτημα προσπέλασης από το Host2 στον Host1 για http: (10)

Ενεργοποιείται ο κανόνας 4 → το πακέτο απορρίπτεται από το firewall. Ο Host2 ως προέλευση εμπίπτει στο «Οπουδήποτε» του κανόνα 4, ενώ και ο Host1 ως προορισμός εμπίπτει στο «Οπουδήποτε» του ίδιου κανόνα. Τέλος, η υπηρεσία http εμπεριέχεται στην περιγραφή «όλες» του κανόνα 4.

iii. Ένα πακέτο TCP/IP με αίτημα προσπέλασης από το DBserver στον Web server για http: (10)

Ενεργοποιείται ο κανόνας 1 → το πακέτο επιτρέπεται να περάσει το firewall. Ο DBserver ως προέλευση εμπίπτει στο «Εσωτερικό δίκτυο» του κανόνα 1, ενώ και ο Web server ως προορισμός εμπίπτει στο «Οπουδήποτε» του ίδιου κανόνα. Τέλος, η υπηρεσία http εμπεριέχεται στην περιγραφή «όλες» του κανόνα 1.

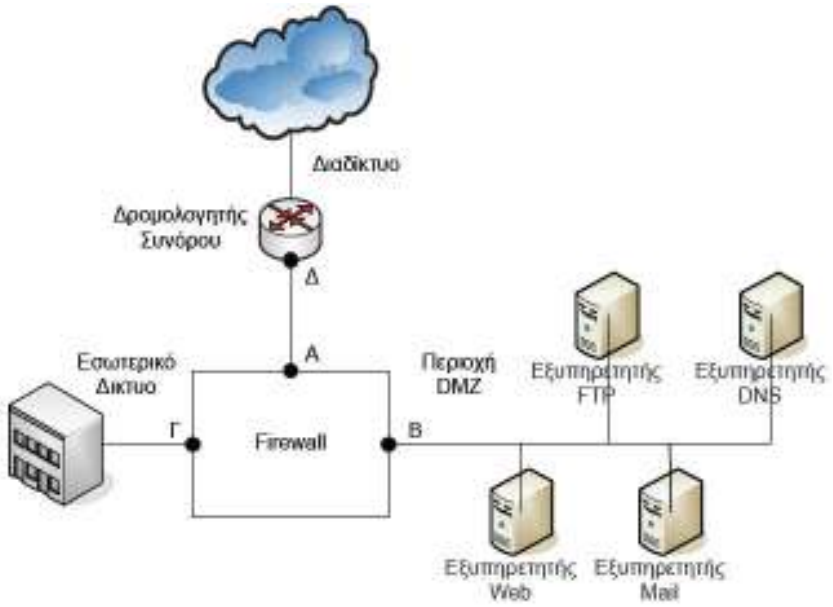
iv. Ένα πακέτο TCP/IP με αίτημα προσπέλασης για SQL από το Internet στον DBserver: (10)

Ενεργοποιείται ο κανόνας 4 → το πακέτο απορρίπτεται από το firewall. Το Internet ως προέλευση εμπίπτει στο «Οπουδήποτε» του κανόνα 4, ενώ και ο DBserver ως προορισμός εμπίπτει στο «Οπουδήποτε» του ίδιου κανόνα. Τέλος, η υπηρεσία SQL εμπεριέχεται στην περιγραφή «όλες» του κανόνα 4.

v. Ένα πακέτο TCP/IP με αίτημα προσπέλασης από το Host2 στον DBserver για SQL ως εισερχόμενη κυκλοφορία από το Internet: (10)

Ενεργοποιείται ο κανόνας 2 → το πακέτο επιτρέπεται να περάσει το firewall. Ο Host2 ταυτίζεται με την προέλευση που περιγράφει ο κανόνας 2 και ο DBserver ταυτίζεται με τον προορισμό που περιγράφει ο ίδιος κανόνας.

[2] Στο δίκτυο του σχήματος χρησιμοποιείται ένα σύστημα Firewall για να προστατεύει την περιοχή των εξυπηρετητών (Demilitarized Zone – DMZ) και να απομονώνει το εσωτερικό δίκτυο ενός οργανισμού από απειλές που προέρχονται από το χώρο του Διαδικτύου.



i. Ο διαχειριστής του οργανισμού έχει στη διάθεσή του το πεδίο διευθύνσεων **193.29.12.0/24**, το οποίο διαχωρίζει σε **3 υποδίκτυα** (**Α-Δ**, **DMZ**, **Εσωτερικό Δίκτυο**) και έχει αποδώσει τις εξής διευθύνσεις IP στα διάφορα στοιχεία του δικτύου του:
Interfaces του firewall: **Α: 193.29.12.45**, **Β: 193.29.12.86**, **Γ: 193.29.12.196**
Στους εξυπηρετητές στην περιοχή DMZ: **Web: 193.29.12.82**, **Mail: 193.29.12.83**, **FTP: 193.29.12.84**, **DNS: 193.29.12.85**

a. Ποια **διεύθυνση IP** πρέπει να αποδώσουμε στο Interface του δρομολογητή, **Δ**, ώστε μεταξύ Δρομολογητή – Firewall να δημιουργηθεί το μικρότερο δυνατό υποδίκτυο που θα λειτουργεί σωστά; Ποιο είναι το **υποδίκτυο** που δημιουργείται; Δώστε τη **μάσκα** και τις **διευθύνσεις** που περιλαμβάνει. (15)

Interface του firewall: A: 193.29.12.45 → 45: 00101101
Το μικρότερο δυνατό υποδίκτυο μεταξύ Δρομολογητή – Firewall προκύπτει με αλλαγή του τελευταίου bit, άρα η διεύθυνση IP που μπορούμε να αποδώσουμε στο Interface του δρομολογητή Δ είναι η 193.29.12.44, όπου το 44 προκύπτει από το 45 με αλλαγή του τελευταίου bit από 1 σε 0 → 44: 00101100.
Υποδίκτυο: 193.29.12.44/31 (εφόσον 31 bits είναι σταθερά και μόνο 1, το τελευταίο, διαφοροποιείται).
Μάσκα: 255.255.255.254 εφόσον τα σταθερά bits είναι 31, δηλ. 11111111.11111111.11111111.11111110
Διευθύνσεις που περιλαμβάνει: 193.29.12.44, 193.29.12.45.

b. Ποιο είναι το μικρότερο δυνατό **υποδίκτυο** που μπορεί να οριστεί στην περιοχή DMZ με βάση την IP διεύθυνση που έχουμε αποδώσει στο Interface B του firewall; Δώστε τη **μάσκα** που θα χρησιμοποιηθεί και τις **διευθύνσεις** Δικτύου. (15)

Interface του firewall: B: 193.29.12.86 → 86: 01010110
Το μικρότερο δυνατό υποδίκτυο που μπορεί να οριστεί στην περιοχή DMZ προκύπτει με αλλαγή στα τελευταία 3 bits της παραπάνω διεύθυνσης, εφόσον με 3 bits προκύπτουν 2^3=8 συνδυασμοί που καλύπτουν τις ανάγκες απόδοσης 5 IPs στην περιοχή DMZ. Οι διευθύνσεις που μπορούμε να πάρουμε είναι από 01010000 έως 01010111 δηλ. από 193.29.12.80 έως 193.29.12.87.
Υποδίκτυο: 193.29.12.80/29 (εφόσον 29 bits είναι σταθερά και 3, το τελευταία, διαφοροποιούνται).
Μάσκα: 255.255.255.248 εφόσον τα σταθερά bits είναι 29, δηλ. 11111111.11111111.11111111.11111000
Διευθύνσεις που περιλαμβάνει: 193.29.12.80, 193.29.12.81, 193.29.12.82, 193.29.12.83, 193.29.12.84, 193.29.12.85, 193.29.12.86, 193.29.12.87.

ii. Το Firewall έχει τους παρακάτω κανόνες ελέγχου της κίνησης για τα εισερχόμενα από το Διαδίκτυο πακέτα με βάση τη διεύθυνση IP προέλευσης (source):
Deny from 195.209.34.64/28
Deny from 195.209.34.96/29
Deny from 147.32.0.0/12
Allow from any
Για κάθε ένα από τα εισερχόμενα πακέτα με τις παρακάτω διευθύνσεις προέλευσης, περιγράψτε αν θα περάσει ή θα απορριφθεί από το firewall και γιατί:

Κανόνας 1: με CIDR 28 σημαίνει ότι στην IP έχω 28 σταθερά bits και 4 που μπορεί να αλλάζουν, συνεπώς το τμήμα της IP που διαφοροποιείται είναι η τελευταία 8άδα. Το 64 → 01000000 όπου τα υπογραμμισμένα bits μπορεί να αλλάζουν και έτσι να προκύπτει το διάστημα 01000000 έως 01001111, δηλ. από 195.209.34.64 έως 195.209.34.79. Ο Κανόνας 1 λοιπόν ορίζει ότι το firewall θα απορρίψει πακέτα με διευθύνσεις προέλευσης από 195.209.34.64 έως και 195.209.34.79.

Κανόνας 2: με CIDR 29 σημαίνει ότι στην IP έχω 29 σταθερά bits και 3 που μπορεί να αλλάζουν, συνεπώς το τμήμα της IP που διαφοροποιείται είναι η τελευταία 8άδα. Το 96 → 01100000 όπου τα υπογραμμισμένα bits μπορεί να αλλάζουν και έτσι να προκύπτει το διάστημα 01100000 έως 01100111, δηλ. από 195.209.34.96 έως 195.209.34.103. Ο Κανόνας 2 λοιπόν ορίζει ότι το firewall θα απορρίψει πακέτα με διευθύνσεις προέλευσης από 195.209.34.96 έως και 195.209.34.103.

Κανόνας 3: με CIDR 12 σημαίνει ότι στην IP έχω 12 σταθερά bits και 20 που μπορεί να αλλάζουν, συνεπώς το τμήμα της IP που διαφοροποιείται είναι η 2η 8άδα. Σε αυτήν την 2η 8άδα έχω 4 σταθερά bits και 4 που μπορεί να αλλάζουν. Το 32 → 00100000 όπου τα υπογραμμισμένα bits μπορεί να αλλάζουν και έτσι να προκύπτει το διάστημα 00100000 έως 00101111, δηλ. από 147.32.0.0 έως 147.47.255.255. Ο Κανόνας 3 λοιπόν ορίζει ότι το firewall θα απορρίψει πακέτα με διευθύνσεις προέλευσης από 147.32.0.0 έως και 147.47.255.255.

a. 195.209.34.78 (5)
Το πακέτο με διεύθυνση προέλευσης 195.209.34.78 θα **απορριφθεί** από το firewall λόγω του Κανόνα 1, καθώς εμπίπτει στο διάστημα από 195.209.34.64 έως και 195.209.34.79.

b. 195.209.34.89 (5)

Το πακέτο με διεύθυνση προέλευσης 195.209.34.89 θα **περάσει** από το firewall, καθώς είναι εκτός τόσο του διαστήματος από 195.209.34.64 έως και 195.209.34.79 που ορίζει ο Κανόνας 1, όσο και του διαστήματος από 195.209.34.96 έως και 195.209.34.103 που ορίζει ο Κανόνας 2.

c. 195.209.34.103 (5)

Το πακέτο με διεύθυνση προέλευσης 195.209.34.89 θα **απορριφθεί** από το firewall λόγω του Κανόνα 2, καθώς εμπίπτει στο διάστημα από 195.209.34.96 έως και 195.209.34.103.

d. 147.47.21.214 (5)

Το πακέτο με διεύθυνση προέλευσης 147.47.21.214 θα **απορριφθεί** από το firewall λόγω του Κανόνα 3, καθώς εμπίπτει στο διάστημα από 147.32.0.0 έως και 147.47.255.255.