ΕΠΛ 674 Ασφάλεια Συστημάτων και Δικτύων **Spring 2011**

Assignment 3

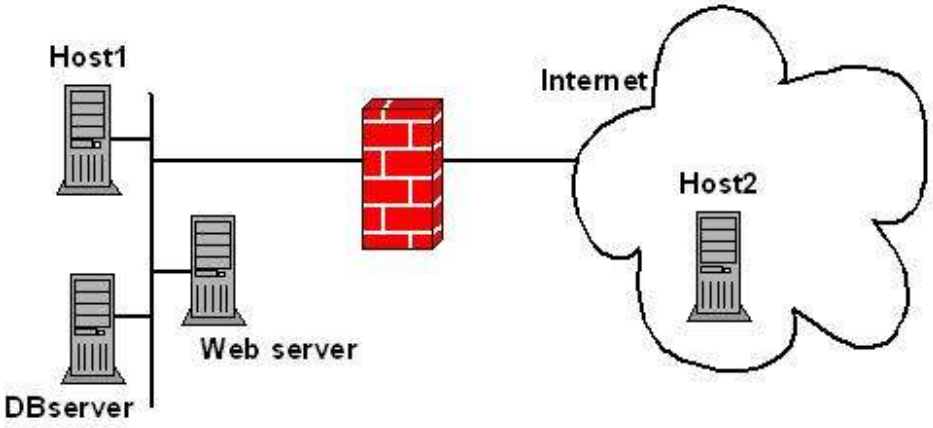
Assigned: 28 February 2011 **Due: 14 March 2011**

Instructions

- All assignments should be submitted typed neatly using a document processing application of your choice. Please make sure to include your name and student number for proper recording of grades.
- Assignment solutions can be written English.
- The assignment is due at the beginning of the lecture at the due date. Late assignments will incur a five-point penalty. Assignments late by more than one day will not be accepted.

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:

_____

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

_____

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

_____

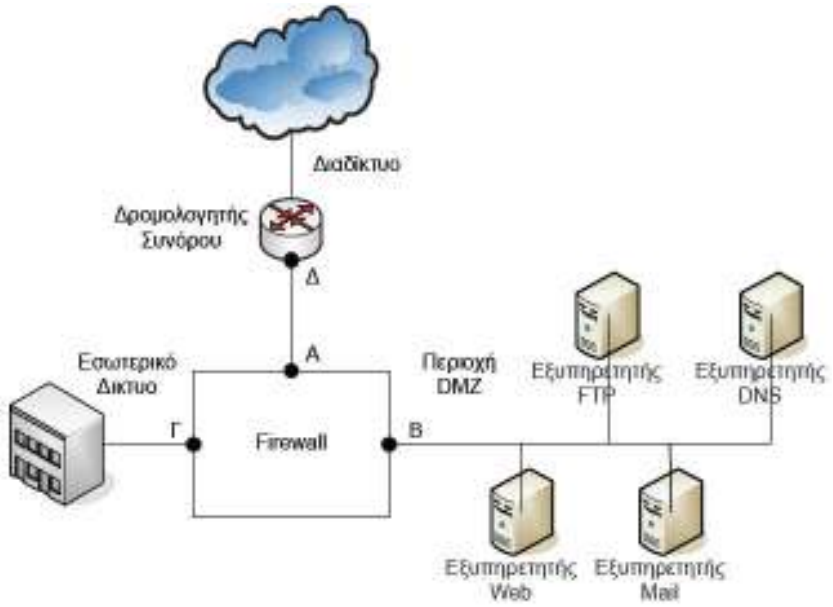
iv. Ένα πακέτο TCP/IP με αίτημα προσπέλασης για SQL από το Internet στον DBserver:

_____

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

_____

[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.

_____

_____

_____

_____

_____

_____

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.

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:

a. 195.209.34.78

b. 195.209.34.89

c. 195.209.34.103

d. 147.47.21.214