9. Firewalls

9.1 Εισαγωγή

Αντικείμενο της παρούσας άσκησης είναι η μελέτη του ρόλου των τοίχων προστασίας Firewalls στην προστασία των κοινόχρηστων δικτύων.

Στην επιστήμη των υπολογιστών ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό-εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης.

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου. Ένα firewall μπορεί να αποτρέψει την είσοδο σε μια IP ή σε κάποια υπηρεσία (FTP, DataBase, e-mail).

Σκοπός της άσκησης είναι η εξοικείωση του σπουδαστή με το ρόλο των firewall τα οποία προστατεύουν την πληροφορία στους εξυπηρετητές παρέχοντας πρόσβαση σε πελάτες με τα κατάλληλα δικαιώματα.

9.2 Διαδικασία Εργαστηρίου

9.2.1 Δημιουργία νέου έργου (project)

1. Τρέξτε το Riverbed Modeler Academic Edition 17.5 ⇒ File ⇒**New**
2. Επιλέξτε **Project** ⇒ **OK** ⇒ Ονομάστε το project <**τα αρχικά σας**>**_Firewall**, και το σενάριο **No_Firewall** ⇒ **OK**.
3. Πατήστε Quit στον Startup Wizard.
4. Για να αφαιρέσετε τον παγκόσμιο χάρτη από το φόντο επιλέξτε το μενού View⇒ **Background** ⇒ **Set Border Map** ⇒ επιλέξτε **NONE** από το μενού ⇒ πατήστε **OK**.

9.2.2 Δημιουργία ενός δικτύου

1. Το πλαίσιο διαλόγου *Object Palette* πρέπει να είναι ανοικτό πάνω από τον χώρο του project. Αν δεν είναι πατήστε το κουμπί  για να το ανοίξετε. Βεβαιωθείτε ότι είναι επιλεγμένο το **internet_toolbox**.
2. Στον χώρο εργασίας του προσομοιωτής προσθέστε τα εξής αντικείμενα: **Application Config**, **Profile Config**, ένα **ip32_cloud**, έναν **ppp_server**, τρεις δρομολογητές **ethernet4_slip8_gtwy**, και δύο υπολογιστές **ppp_wkstn**. Συνδέστε τις συσκευές με αμφίδρομες ζεύξεις τύπου **ppp_DS1**.

α. Για να προσθέσετε ένα αντικείμενο από την παλέτα, πατήστε στην εικόνα του που βρίσκετε στην παλέτα ⇒ μετακινήστε το ποντίκι στο χώρο εργασίας ⇒ κάντε αριστερό κλικ για να αφήσετε το αντικείμενο. Δεξί κλικ όταν τελειώσετε.

3. Μετονομάστε τα αντικείμενα όπως φαίνεται στην εικόνα και σώστε τη δουλειά σας.

Σχήμα 9.1 Στιγμιότυπο με τα αντικείμενα από το σενάριο No_Firewall ολοκληρωμένο.

4. Κλείστε την παλέτα αντικειμένων και σώστε τη δουλειά σας.

9.2.3 Ρύθμιση των κόμβων

1. Κάντε δεξί κλικ στον κόμβο **Applications** ⇒ **Edit Attributes** ⇒ Δώστε στην ιδιότητα **Application Definitions** την τιμή **Default** ⇒ Πατήστε **OK**.
2. Κάντε δεξί κλικ στον κόμβο **Profiles** ⇒ **Edit Attributes** ⇒ Δώστε στην ιδιότητα **Profile Configuration** την τιμή **Sample Profiles** ⇒ Πατήστε **OK**.
3. Κάντε δεξί κλικ στον κόμβο **Server** ⇒ **Edit Attributes** ⇒ Δώστε στην ιδιότητα **Application: Supported Services** την τιμή **All** ⇒ Πατήστε **OK**.
4. Κάντε δεξί κλικ στον κόμβο **Sales A** ⇒ **Select Similar Nodes** (βεβαιωθείτε ότι επιλέχθηκαν και οι δύο κόμβοι Sales A και Sales B).

α. Κάντε δεξί κλικ στον κόμβο **Sales A** ⇒ **Edit Attributes** ⇒ Επιλέξτε το κουτάκι **Apply Changes to Selected Objects**.

β. Επεκτείνετε την ιδιότητα **Application: Supported Profiles** ορίστε την τιμή του **rows** σε **1** ⇒ Επεκτείνετε την ιεραρχία **row 0** ⇒ **Profile Name = Sales Person** (είναι ένα από τα έτοιμα προφίλ – δείγματα που ορίσαμε στον κόμβο **Profiles**).

γ. Πατήστε **OK**.

5. Σώστε τη δουλειά σας.

9.2.4 Επιλέξτε τα στατιστικά

1. Κάντε δεξί κλικ οπουδήποτε πάνω στο χώρο εργασίας κι επιλέξτε το μενού **Choose Individual Des Statistics**.
2. Στο πλαίσιο διαλόγου *Choose Results* επιλέξτε τα στατιστικά:

α. **Global Statistics ⇒ DB Query ⇒ Response Time (sec)**

β. **Global Statistics ⇒ HTTP ⇒ Page Response Time (seconds)**

3. Πατήστε **OK**.
4. Κάντε δεξί κλικ στον κόμβο Sales A κι επιλέξτε **Choose Individual Des Statistics**.
5. Στο πλαίσιο διαλόγου *Choose Results* επιλέξτε τα στατιστικά:

α. **Client DB ⇒ Traffic Received (bytes/sec)**.

β. **Client HTTP ⇒ Traffic Received (bytes/sec)**.

6. Πατήστε OK.
7. Κάντε δεξί κλικ στον κόμβο Sales B κι επιλέξτε **Choose Individual Statistics**.
8. Στο πλαίσιο διαλόγου *Choose Results* επιλέξτε τα στατιστικά:

α. **Client DB ⇒ Traffic Received (bytes/sec)**.

β. **Client HTTP ⇒ Traffic Received (bytes/sec)**.

9. Πατήστε OK και σώστε τη δουλειά σας.

9.2.5 Τρέξτε την προσομοίωση

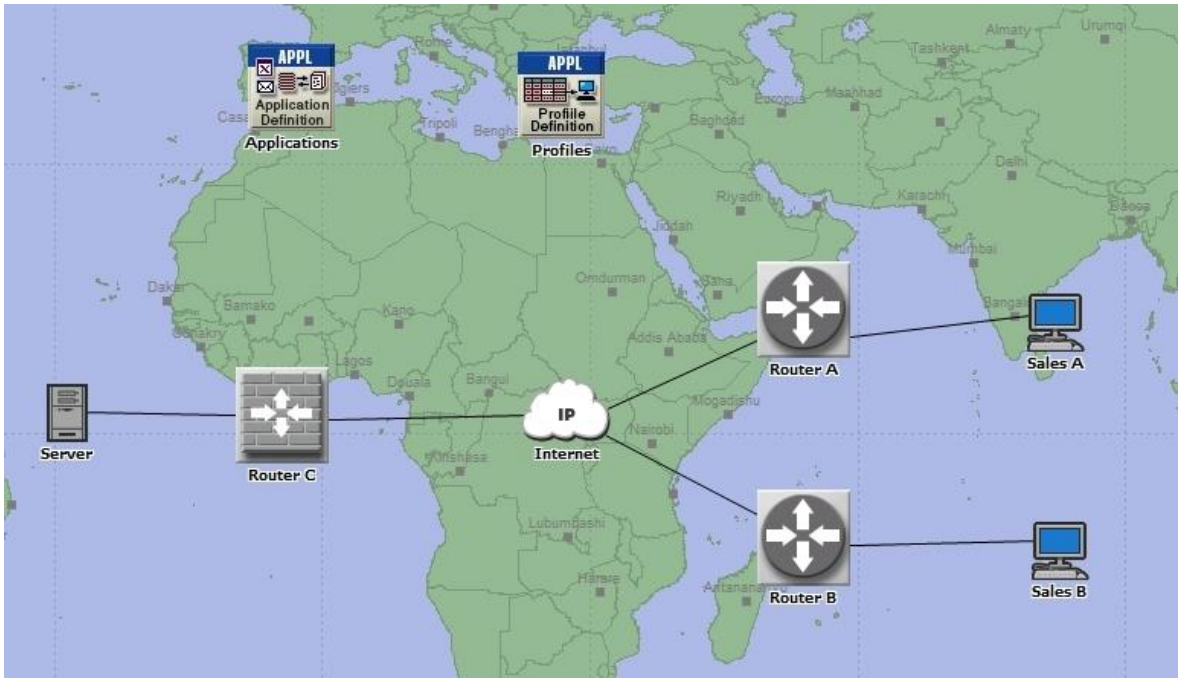
1. Πατήστε το κουμπί **Configure/Run Discrete Event Simulation (DES)**  .
2. Βεβαιωθείτε ότι το **Duration** είναι **1 hours**.

9.3 Σενάριο με τοίχο προστασίας (Firewall)

Στο δίκτυο που μόλις κατασκευάσαμε, το πορτραίτο Sales Person επιτρέπει και στα δύο σημεία πωλήσεων να έχουν πρόσβαση σε εφαρμογές που παρέχονται από τον εξυπηρετητή, όπως το e-mail, οι βάσεις δεδομένων και η περιήγηση στον ιστό, (ελέγξτε και το Profile Configuration στον κόμβο Profiles). Υποθέστε ότι θέλουμε να προστατέψουμε τη βάση δεδομένων που βρίσκεται στον εξυπηρετητή από εξωτερική πρόσβαση μεταξύ της οποίας είναι και η πρόσβαση του προσωπικού πωλήσεων. Ένας τρόπος να το πετύχουμε αυτό είναι αντικαθιστώντας το δρομολογητή Router C με ένα firewall, όπως παρακάτω:

1. Από το μενού **Scenarios** επιλέξτε **Duplicate Scenario** και δώστε του το όνομα **Firewall_DB** ⇒ Πατήστε **OK**.
2. Στο νέο σενάριο κάντε δεξί κλικ στο **Router C** ⇒ **Edit Attributes**
3. Θέστε την τιμή **ethernet2_slip8_firewall** στην ιδιότητα **model**.
4. Επεκτείνετε την ιεραρχία **Proxy Server Information** ⇒ επεκτείνετε την ιεραρχία **row 1** που αντιστοιχεί στις εφαρμογές βάσεων δεδομένων ⇒ Ορίστε την τιμή **No** στην ιδιότητα **Proxy Server Deployed**.
5. Πατήστε **OK** και σώστε τη δουλειά σας.

Η ρύθμιση του Firewall δεν επιτρέπει κίνηση που σχετίζεται με βάσεις δεδομένων να διέρθει μέσω αυτού (φιλτράρει δηλαδή τέτοια πακέτα, απορρίπτοντάς τα). Με τον τρόπο αυτό προστατεύονται οι βάσεις δεδομένων του εξυπηρετητή από εξωτερική πρόσβαση. Το σενάριο με το firewall πρέπει να μοιάζει με το παρακάτω:



Σχήμα 9.2 Στιγμιότυπο με τα αντικείμενα από το σενάριο Firewall ολοκληρωμένο.

9.3.1 Δείτε τα αποτελέσματα

1. Πηγαίνετε στο μενού **DES ⇒ Results** και επιλέξτε **View Results**.
2. Στην καρτέλα **DES Graphs**, στο *Results for* επιλέξτε **Current Project**.
3. Επεκτείνετε την ιεραρχία **Object Statistics ⇒ Sales A ⇒ Client DB** και επιλέξτε **Traffic Received**.
4. Στο *Presentation* που βρίσκεται στο κάτω δεξί μέρος βεβαιωθείτε ότι είναι επιλεγμένο το **Overlaid Statistics** και **time_average**.
5. Πατήστε **Show**, το γράφημα θα πρέπει να μοιάζει με το παρακάτω.

Σχήμα 9.3 Traffic Received (bytes/sec) του πελάτη DataBase για τον κόμβο A.

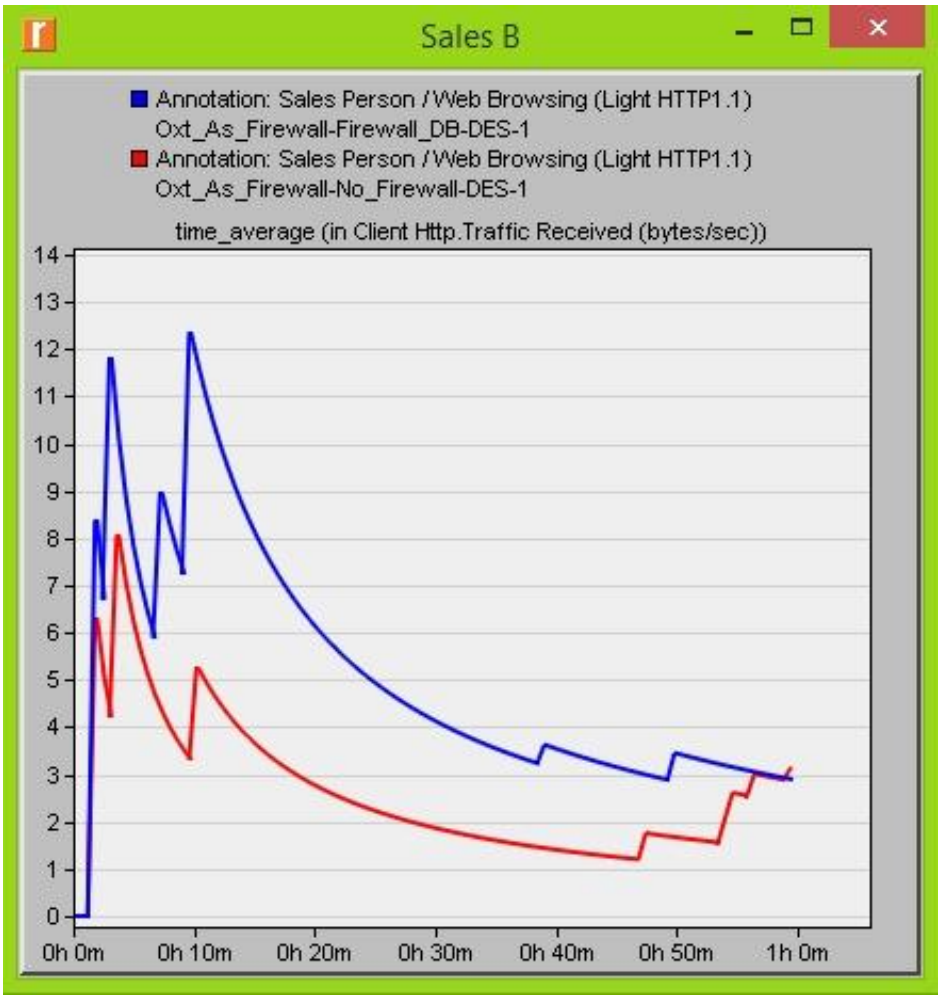
6. Με τον ίδιο τρόπο φτιάξτε ένα γράφημα για το Sales B.

Σχήμα 9.4 Traffic Received (bytes/sec) του πελάτη DataBase για τον κόμβο B.

7. Δημιουργείστε δύο γραφήματα ίδια με τα προηγούμενα για να παρουσιάσετε τα στατιστικά **Traffic Received** από τον πελάτη **Client HTTP** τόσο για το **Sales A** όσο για το **Sales B**.

Σημείωση: Τα αποτελέσματα μπορεί να διαφέρουν ελαφρά λόγω διαφορών στην τοποθέτηση των κόμβων.

Σχήμα 9.5 Traffic Received (bytes/sec) του πελάτη Http για τον κόμβο A.



Σχήμα 9.6 Traffic Received (bytes/sec) του πελάτη Http για τον κόμβο B.

9.4 Ερωτήσεις

9.4.1 Ερώτηση 1η

Εξηγείστε, χρησιμοποιώντας τα γραφήματα, την επίδραση του firewall στην κίνηση της εφαρμογής των βάσεων δεδομένων.

9.4.2 Ερώτηση 2η

Συγκρίνετε τα γραφήματα που δείχνουν τη λαμβανόμενη κίνηση HTTP με εκείνα που δείχνουν τη λαμβανόμενη κίνηση βάσεων δεδομένων.

9.4.3 Ερώτηση 3η

Δημιουργείστε και αναλύστε τα γραφήματα που δείχνουν την επίδραση του firewall στο χρόνο απόκρισης (delay) των σελίδων HTTP και των ερωτημάτων βάσεων δεδομένων.

9.4.4 Ερώτηση 4η

Δημιουργείστε ένα αντίγραφο του σεναρίου Firewall_DB και ονομάστε το Firewall_FTP. Το νέο σενάριο δεν θα επιτρέπει στα δύο σημεία πωλήσεων να έχουν πρόσβαση σε εφαρμογές που έχουν σχέση μόνο με FTP. Δημιουργείστε τα γραφήματα που δείχνουν την λαμβανόμενη κίνηση FTP και για τους δυο πωλητές και συγκρίνετέ τα με εκείνα που δείχνουν την λαμβανόμενη κίνηση HTTP και DB. Τα γραφήματα θα πρέπει να περιέχουν τα σενάρια No_Firewall και Firewall_FTP. Για να δείτε κίνηση στα δυο σενάρια θα πρέπει να τρέξετε τα σενάρια επιλέγοντας τα κατάλληλα στατιστικά.

9.4.5 Ερώτηση 5η

Δημιουργείστε ένα αντίγραφο του σεναρίου Firewall_FTP και ονομάστε το Firewall_DB and FTP και κάντε τις κατάλληλες αλλαγές ώστε να μην επιτρέπει ταυτόχρονα κίνηση DB και FTP. α) Τι περιμένουμε να δούμε στο χρόνο απόκρισης delay; β) Δημιουργείστε ένα γράφημα για το συγκεκριμένο σενάριο το οποίο θα παρουσιάζει τη λαμβανόμενη κίνηση DB, FTP και HTTP για τον Sales A.