Προστασία και Ασφάλεια Δικτύων (Εργαστήριο)

Ενότητα 4

OPNET – IP Filter και Firewalls

Σκοπός του εργαστηρίου: η γνωριμία με το λογισμικό σχεδιασμού ανάλυσης και προσομοίωσης δικτύων OPNET IT Guru Academic Edition και η μελέτη της χρησιμότητας των IP Filters και των firewalls στην προστασία του δικτύου.
Στην παρούσα άσκηση θα δημιουργήσετε ένα μοντέλο το οποίο προσομοιάζει την πρόσβαση που έχουν κόμβοι από δύο LANs σε δύο server. Ο ένας server παρέχει υπηρεσίες web ενώ στον άλλο υπάρχει βάση δεδομένων αρχικά προσβάσιμη από όλους. Μέσα από τα σενάρια που θα ακολουθήσουν θα αποτρέψουμε την εξωτερική πρόσβαση στον server όπου τρέχει η βάση χρησιμοποιώντας δύο διαφορετικούς τρόπους.

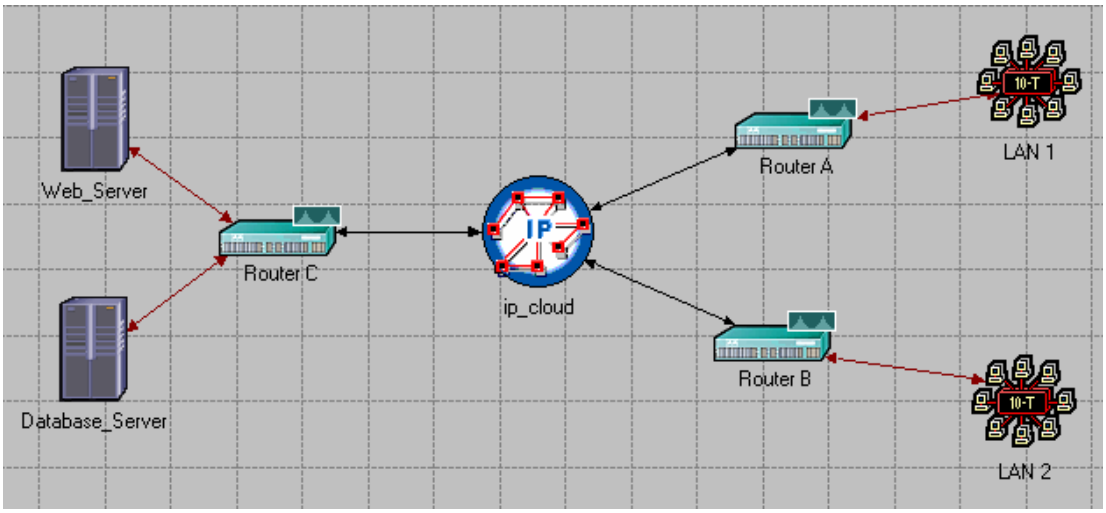
1 Εισαγωγή στο OPNET και δημιουργία δικτύου

Το εργαλείο προσομοίωσης OPNET μας δίνει τη δυνατότητα να σχεδιάσουμε και να παραμετροποιήσουμε το δίκτυο το οποίο θέλουμε να προσομοιώσουμε ώστε να δούμε τη λειτουργία του σε εικονικό περιβάλλον πριν να προχωρήσουμε στην υλοποίηση του. Στο πλαίσιο αυτό θα πρέπει πρώτα να δημιουργηθεί ένα project το οποίο θα περιλαμβάνει το δίκτυο που θα σχεδιάσουμε ακολουθώντας τα παρακάτω βήματα:

1. Δημιουργούμε project με όνομα **<AEM>_Firewall** και όνομα σεναρίου **NoFirewall**
   File → New… → Project
   Project Name : <AEM>_Firewall
   Scenario Name: NoFirewall
   Στο Wizard επιλέγετε **Create Empty Scenario** και στο επόμενο για Network Scale: **Campus**

   Πατήστε Next μέχρι να βγείτε από τον Wizard.

2. Για τη δημιουργία του δικτύου επιλέγουμε από την ομάδα internet_toolbox του Object Palette, το οποίο περιλαμβάνει όλες τις διαθέσιμες δικτυακές συσκευές που υποστηρίζει ο προσομοιωτής τις παρακάτω συσκευές:
   - Δύο **10BaseT_Lan** τα οποία αναπαριστούν τα δύο τοπικά δίκτυα.
   - Δύο εξυπηρετητές **ethernet_server** που θα χρησιμοποιηθούν για να τρέχουν τις εφαρμογές web και database.
   - Ένα **ip32_cloud** το οποίο αναπαριστά το διαδίκτυο και μέσα από το οποίο θα περνάει η κίνηση από τα LANs προς τους servers.
   - Τρεις δρομολογητές **CS_4000_3s_e6_fr2_sl2_tr2** οι οποίοι θα χρησιμοποιηθούν για να συνδέσουν τα δύο τοπικά δίκτυα και τους δύο servers με το ip cloud.
   - Χρησιμοποιήστε **100BaseT** γραμμές, οι οποίες αναπαριστούν συνδέσεις Ethernet στα 100Mbps, για να συνδέσετε τους servers και τα LANs με τους routers, και **PPP_DS1** γραμμές για να συνδέσετε τους routers με το ip cloud.
3. Οι συνδέσεις μεταξύ των συσκευών θα γίνουν όπως φαίνεται στο σχήμα. Επίσης αλλάξτε τα ονόματα σύμφωνα με αυτά που απεικονίζονται.



Σχήμα 1: Αρχικό μοντέλο.

4. Εισάγετε έναν κόμβο **Application Config** (ονομάστε τον Applications) ο οποίος θα χρησιμοποιηθεί για τον ορισμό και την παραμετροποίηση των εφαρμογών οι οποίες θα είναι διαθέσιμες στο διαδίκτυο και έναν κόμβο **Profile Config** (ονομάστε τον Profiles) ο οποίος θα χρησιμοποιηθεί για να οριστούν προφίλ χρήσης εφαρμογών (για αυτές τις εφαρμογές που ορίστηκαν με το Application Config). Τα προφίλ θα υιοθετηθούν από κόμβους έτσι ώστε να δημιουργηθεί η απαιτούμενη κίνηση δεδομένων στο διαδίκτυο.
   - Για το **Application Definitions** του Application Config (Δεξί κλικ → Edit Attributes) επιλέξτε το default ώστε να εμφανιστούν όλες οι εξ'ορισμού εφαρμογές. Για την περιγραφή Database Access (Heavy), ορίστε ότι αφορά High Load χρήση της Database, ενώ για την περιγραφή του Web Browsing (Heavy HTTP1.1), Heavy Browsing για την Http.
   - Για το Profiles ορίστε δύο προφίλ αλλάζοντας τον αριθμό των γραμμών στο Profile Configuration (Δεξί κλικ → Edit Attributes) σε 2 και δώστε τα ονόματα Database Access και Web Access. Τα προφίλ υποστηρίζουν από μια εφαρμογή το καθένα (ο αριθμός γραμμών στο Applications γίνεται 1): το πρώτο την εφαρμογή Database Access (Heavy) και το δεύτερο την εφαρμογή Web Browsing (Heavy HTTP1.1). Και τα δύο προφίλ ξεκινούν 10 sec μετά την έναρξη της προσομοίωσης (**Start Time (seconds) → Distribution Name = constant, Mean Outcome=10**).

5. Στο LAN1 υπάρχουν 30 κόμβοι (Δεξί κλικ → Edit Attributes → **Number of Workstations = 30**) εκ των οποίων οι 20 τρέχουν εφαρμογές Web. Ίδιος αριθμός από κόμβους τρέχει εφαρμογή πρόσβασης στη βάση:
   - **Application: Supported Profiles → rows=2**. Για κάθε μια γραμμή επιλέγουμε το επιθυμητό προφίλ και τον αριθμό των κόμβων που την υποστηρίζουν.

6. Στο LAN2 αντιστοίχως υπάρχουν 50 κόμβοι εκ των οποίων οι 10 τρέχουν εφαρμογές Web και 25 πρόσβασης στη βάση.

7. Κάντε τις απαραίτητες τροποποιήσεις ώστε ο ένας server να παρέχει υπηρεσίες Web και ο άλλος πρόσβασης στη βάση.
   - **Application: Supported Services → Edit, αλλάζουμε τον αριθμό των Rows σε 1 και επιλέγουμε το όνομα της εφαρμογής που θέλουμε να υποστηρίζει ο συγκεκριμένος server.**

8. Η επόμενη επιλογή μας αφορά στο πρωτόκολλο δρομολόγησης το οποίο θα χρησιμοποιηθεί για τη δημιουργία των routing tables των routers της τοπολογίας δακτυλίου (και επομένως και για την εύρεση του μονοπατιού από τον κόμβο Α στον κόμβο Β), και το οποίο θα είναι το RIP (Routing Information Protocol). Από το κυρίως μενού επιλέγουμε
   - **Protocols → IP → Routing → Configure Routing Protocols** επιλέξτε το RIP και πατήστε OK.

2 Ορισμός τιμών παρακολούθησης

Για τις ανάγκες της προσομοίωσης θα προσδιορίσουμε τις παραμέτρους των οποίων τις τιμές θέλουμε να καταγράψουμε κατά τη διαδικασία της προσομοίωσης.

- Από το κυρίως μενού επιλέγουμε: Simulation → Choose Individual Statistics. Από τα Global Statistics επιλέγουμε
  - **HTTP → Page Response Time (sec)** (ορίζει το χρόνο που απαιτείται για την ανάκτηση μιας σελίδας).
- Για τον Database Server με δεξί κλικ και Choose Individual Statistics επιλέγουμε:
  - **Server DB Query → Traffic Received (bytes/sec)**
  - **Server DB Query → Traffic Sent (bytes/sec)**
- Για το LAN1 με δεξί κλικ και Choose Individual Statistics επιλέγουμε:
  - **Client DB → Traffic Received (bytes/sec)**
  - **Client Http → Traffic Received (bytes/sec)**
- Ακολουθούμε την ίδια διαδικασία για το LAN2.

Για να μπορέσουμε να δούμε τις IP διευθύνσεις των δικτυακών συσκευών επιλέγουμε από το κυρίως μενού **Protocols → IP → Addressing → Auto-Assign IP Addresses**. Κατόπιν μπορούμε μέσα από τα Attributes της συσκευής να δούμε την IP που έχει δοθεί σε κάθε συσκευή (IP Host Parameters → Interface Information).

Για να μπορέσουμε να δούμε τις διαδρομές που επιλέγει ο Router C για τη δρομολόγηση δεδομένων επιλέγουμε τον router και από το κυρίως μενού επιλέγουμε το **Protocols → IP → Routing → Export Routing Table for Selected Routers**.

3 Simulation

Για προσομοίωση επιλέγουμε τα παρακάτω.

- **Duration: 5 minutes**
- **Update interval: 1000 Events**
- **Global Attributes → RIP Sim Efficiency: Disable** (RIP messages θα αποστέλλονται καθ'όλη την διάρκεια του simulation)
- **Global Attributes → RIP Stop Time: 1000** (Βάσει των προηγούμενων τιμών που δώσαμε τα Routing Tables θα ανανεώνονται καθ'όλη την διάρκεια του simulation)
- **Global Attributes → IP Routing Table Export / Import: Export** (Στο τέλος του Simulation θα γίνει εξαγωγή των routing table σε ένα αρχείο)

Επιλέξτε **Run** για να ξεκινήσει το simulation.
Με το πέρας της προσομοίωσης μπορείτε να δείτε τα αποτελέσματα της προσομοίωσης με **Results → View Results** και τους πίνακες δρομολόγησης από το Simulation Log.

4 Περιορισμός της κίνησης προς τη βάση δεδομένων

Στα επόμενα βήματα θα αλλάξουμε την πολιτική μας ώστε να αποτρέψουμε στους κόμβους των LANs την πρόσβαση στη βάση δεδομένων καθώς δε θέλουμε κόμβοι εκτός του δικτύου μας να έχουν άμεση πρόσβαση στη βάση δεδομένων. Η υλοποίηση των περιορισμών μπορεί να γίνει με δύο τρόπους:

- με τη χρήση IP Access Lists στον δρομολογητή και
- με τη χρήση firewall

4.1 Με τη χρήση IP Access Lists

Για τον πρώτο τρόπο **εφαρμόζουμε τους περιορισμούς στο επίπεδο δικτύου** και επομένως φιλτράρουμε τα δεδομένα σε επίπεδο IP. Για να το πετύχουμε αυτό δημιουργούμε μια IP Access List την οποία θα εφαρμόζει ο router για τον έλεγχο των δεδομένων που διακινούνται μεταξύ των δικτύων που συνδέει. Για το σκοπό αυτό θα δημιουργήσουμε ένα αντίγραφο του αρχικού σεναρίου με όνομα **IPFirewall (Scenarios → Duplicate Scenario)** .

Στο **IP Routing Parameters** του router και το **Extended ACL Configuration** δίνουμε στην πρώτη λίστα που βρίσκεται στη γραμμή 0 την τιμή 1 και προσθέτουμε στον πίνακα την εγγραφή που απαιτείται ώστε να απαγορεύεται η προώθηση δεδομένων που έχουν ως προορισμό την IP του Database_Server.

Κατόπιν από το Interface Information του IP Routing Parameters για το interface του router που μας οδηγεί στον Database_Server επιλέγουμε για το **Packet Filter → Send Filter** την τιμή 1 η οποία ανταποκρίνεται στην Access List που δημιουργήσαμε. Με αυτόν τον τρόπο ο router για το interface αυτό θα εφαρμόσει τους κανόνες φιλτραρίσματος που ορίσαμε στην λίστα.

4.2 Με τη χρήση Firewall

Ο δεύτερος τρόπος κάνει χρήση ενός firewall το οποίο θα αποτρέπει τη διέλευση των πακέτων που επιχειρούν να αποκτήσουν πρόσβαση στον database server. Για αυτήν την περίπτωση οι περιορισμοί θα εφαρμοστούν σε επίπεδο εφαρμογής και επομένως θα απαγορέψουμε τη διακίνηση δεδομένων που αφορούν πρόσβαση στη βάση δεδομένων. Για το σκοπό αυτό, και **αφού επιστρέψουμε πρώτα στο αρχικό σενάριο**, δημιουργούμε ένα αντίγραφο του αρχικού σεναρίου το οποίο θα ονομάσουμε ProxyFirewall και στο οποίο θα κάνουμε τις ακόλουθες αλλαγές:

1. Αντικαθιστούμε τον δρομολογητή που βρίσκεται πριν από τους servers με ένα firewall του τύπου ethernet2_slip8_firewall (αλλάζοντας το μοντέλο της συσκευής από το Edit Attributes).
2. Από το Proxy Server Information για την Database εφαρμογή επιλέγουμε **Proxy Server Deployed →No.**

Σημείωση: Αν έχετε ακολουθήσει σωστά τα βήματα και δε παίρνετε τα επιθυμητά αποτελέσματα, αντί της αλλαγής του τύπου της συσκευής από το Edit Attributes διαγράψτε την και προσθέστε εκ νέου ένα firewall.

5 Simulation για τα τρία σενάρια

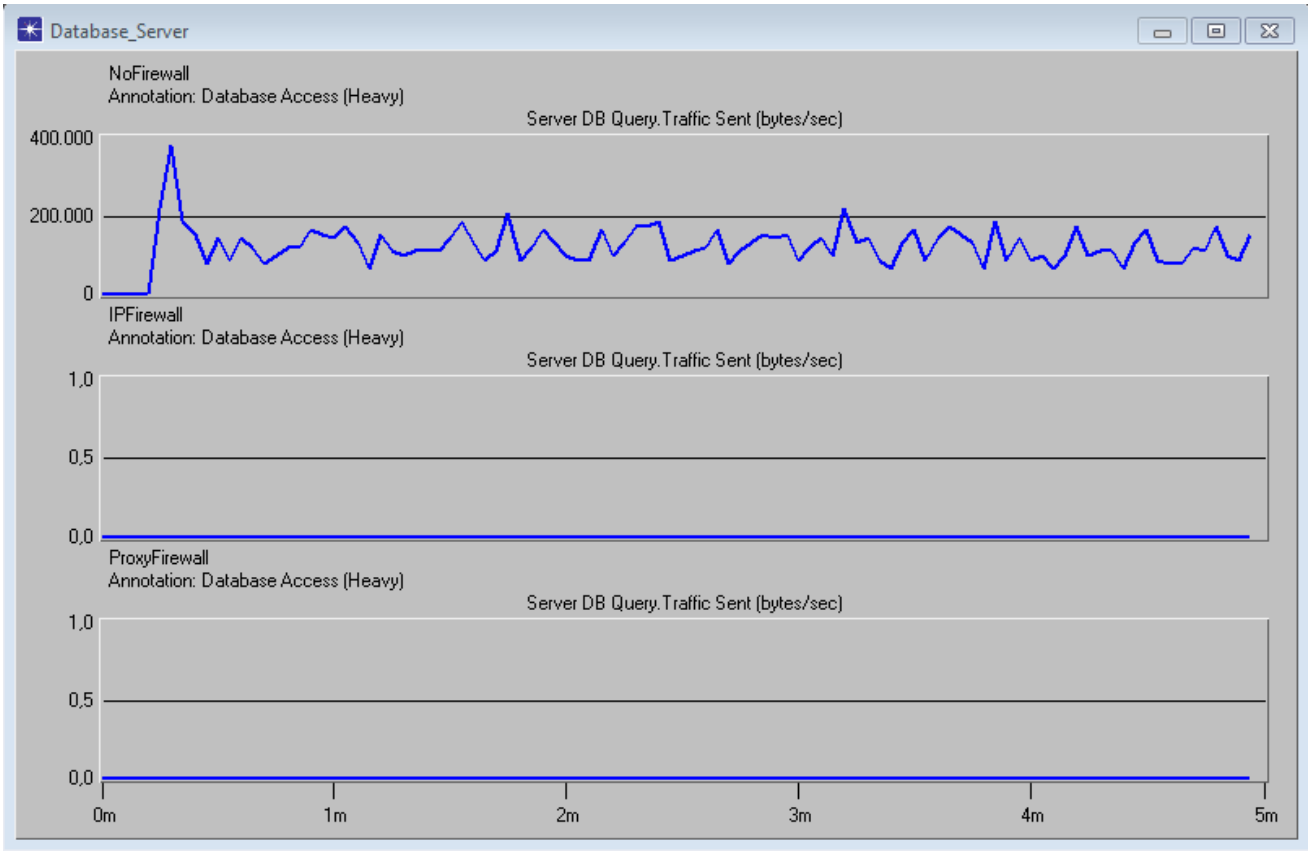
Προκειμένου να προσομοιάσουμε τα τρία σενάρια που δημιουργήσαμε και να συγκρίνουμε τα αποτελέσματα των τριών επιλέγουμε από το κυρίως μενού **Scenarios → Manage Scenarios** και στο πεδίο Results των τριών σεναρίων επιλέγουμε collect και OK.

6 Ανάλυση αποτελεσμάτων

Με το πέρας της προσομοίωσης μπορούμε να δούμε συγκριτικά αποτελέσματα μέσα από το **Results → View Results** και επιλέγουμε να δούμε τα αποτελέσματα από όλα τα σενάρια. Σημειώστε ότι από το **Results → Open Simulation Log** μπορούμε να δούμε αν έχουν γίνει κάποια λάθη κατά την προσομοίωση.

Για την περίπτωση του HTTP δε θα πρέπει να βλέπουμε διαφοροποιήσεις μεταξύ των τριών σεναρίων ενώ για την περίπτωση της βάσης δεδομένων τα αποτελέσματα των δύο τελευταίων σεναρίων θα πρέπει να

είναι ίδια και διαφορετικά από το πρώτο. Στο παρακάτω σχήμα απεικονίζονται τα αναμενόμενα αποτελέσματα για την περίπτωση του **Server DB Query → Traffic Sent (bytes/sec)**



Σχήμα 2: Αναμενόμενα αποτελέσματα για τον database server

1.7 Άσκηση

Σε αντίγραφο του σεναρίου IPFirewall ή ProxyFirewall κάντε τις απαραίτητες αλλαγές ώστε από το LAN1 να επιτρέπεται η πρόσβαση στη βάση δεδομένων ενώ να απαγορεύεται από το LAN2.