# Προστασία και Ασφάλεια Δικτύων (Εργαστήριο)

## Ενότητα 5

## OPNET – VPN

**Σκοπός του εργαστηρίου:** η μελέτη των ιδιωτικών εικονικών δικτύων (virtual private networks) και ο τρόπος με τον οποίον ένα δίκτυο μπορεί να επεκταθεί ώστε να συμπεριλάβει δύο ή περισσότερα φυσικά απομακρυσμένα δίκτυα επιτρέποντας την ασφαλή διακίνηση δεδομένων μέσα στο νέο δίκτυο ακόμη και όταν αυτή γίνεται μέσω του ανασφαλούς δημόσιου δικτύου. Στην πράξη οι απομακρυσμένοι κόμβοι μπορούν να λογίζονται ως τμήματα του ίδιου δικτύου.

Η τεχνική των VPNs χρησιμοποιεί την έννοια της IP σήραγγας, μια εικονική σύνδεση σημείου προς σημείο μεταξύ δύο απομακρυσμένων κόμβων. Η εικονική σύνδεση δημιουργείται με την ενθυλάκωση των δεδομένων εντός ενός νέου δεδομενογραφήματος το οποίο δημιουργεί ο κόμβος που βρίσκεται στην αρχή της σήραγγας και στο οποίο ως διεύθυνση προορισμού χρησιμοποιείται η διεύθυνση του άλλου άκρου της σήραγγας. Η διεύθυνση πηγής είναι η διεύθυνση του δρομολογητή στην αρχή της σήραγγας. Τα δεδομένα προστατεύονται εξασφαλίζοντας τόσο την εμπιστευτικότητα όσο και την ακεραιότητας τους.

Το αποτέλεσμα είναι η δυνατότητα να προστατέψουμε ευαίσθητα δεδομένα τα οποία διακινούνται μέσω ενός αφιλόξενου δικτύου (όπως είναι το δημόσιο) αλλά και, εσκεμμένα, να παρακάμψουμε τυχόν περιορισμούς που θέτει η χρήση firewall, όπως είναι στο παρόν σενάριο.

## 1.1 Δημιουργία δικτύου

Στο project της προηγούμενης ενότητας με όνομα <AEM>_Firewall δημιουργούμε ένα αντίγραφο του σεναρίου ProxyFirewall το οποίο ονομάζουμε VPN.
Στο νέο σενάριο μεταξύ του Router C και του Database Server θα μεσολαβεί ένας δρομολογητής **CS_4000_3s_e6_fr2_sl2_tr2** τον οποίο και μετονομάζουμε σε **Router D**.

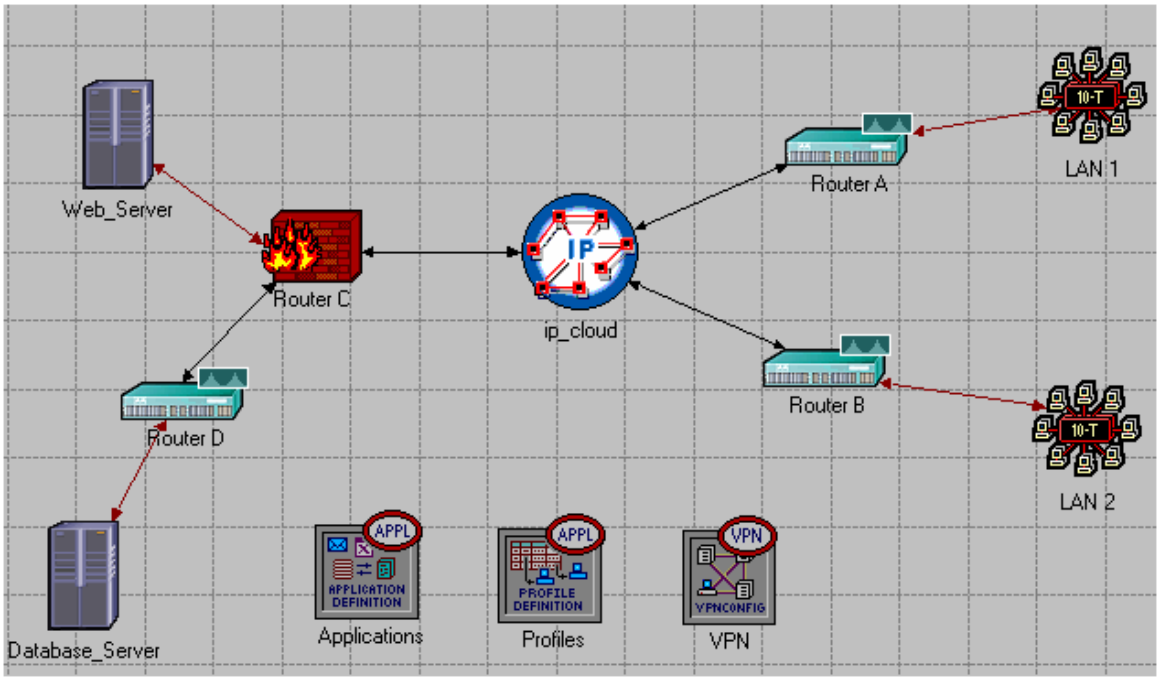
Για τη σύνδεση του νέου δρομολογητή:

- Αφαιρούμε την υπάρχουσα σύνδεση μεταξύ του Router C και του Database Server και
- Χρησιμοποιούμε μια **10BaseT** γραμμή για να συνδέσουμε τον Router D με τον database server και μια **PPP_DS1** γραμμή για να συνδέσουμε Router D με τον Router C.

Για τη δρομολόγηση επιλέγουμε το πρωτόκολλο RIP.

Επίσης προσθέτουμε έναν κόμβο IP VPN Config, τον οποίο ονομάζουμε VPN και ο οποίος θα μας επιτρέψει να ορίσουμε τις απαιτούμενες παραμέτρους για τη δημιουργία ενός εικονικού ιδιωτικού δικτύου.

Το νέο δίκτυο απεικονίζεται στο Σχήμα 1.




**Σχήμα 1: Σενάριο VPN.**

Το επόμενο βήμα αφορά τη δημιουργία ενός IP tunnel μεταξύ του Router A και του Router D το οποίο στην ουσία δημιουργεί ένα εικονικό ιδιωτικό δίκτυο επιτρέποντας στους κόμβους του LAN 1 να έχουν πρόσβαση στον Database Server μέσω του δημοσίου δικτύου παρακάμπτοντας τους περιορισμούς του Firewall. Η κίνηση μεταξύ του Router A και του Router D προστατεύεται και επομένως και τα δεδομένα μεταξύ των κόμβων του LAN και της database.

Από τις ιδιότητες του VPN προσθέτουμε μια ρύθμιση την οποία παραμετροποιούμε ως εξής:

1. Ως Tunnel Source βάζουμε το ακριβές όνομα του Router A.
2. Ως Tunnel Destination ορίζουμε τον Router D.
3. Ως απομακρυσμένους πελάτες οι οποίοι συνδέονται απευθείας με την πηγή του tunnel ορίζουμε το LAN 1.

## 1.5 Simulation για όλα τα σενάρια

Για το simulation επιλέγουμε τη συλλογή τιμών για όλα τα σενάρια και παρατηρούμε αν τα αποτελέσματα είναι σύμφωνα με τα αναμενόμενα αναφορικά με την κίνηση από και προς τη βάση δεδομένων.

**ΣΗΜΕΙΩΣΗ**: Αν δεν έχετε τα αναμενόμενα αποτελέσματα, θεωρώντας ωστόσο ότι έχετε ακολουθήσει σωστά όλες τις παραπάνω κατευθύνσεις, δοκιμάστε να διαγράψετε τον Router C και να τον εισάγεται ξανά (κάνοντας παράλληλα όλες τις απαραίτητες ρυθμίσεις όπως αυτές περιγράφονται στην προηγούμενη ενότητα) έτσι ώστε να διαγραφεί η όποια προηγούμενη παραμετροποίηση του που οδηγεί σε εσφαλμένα αποτελέσματα.