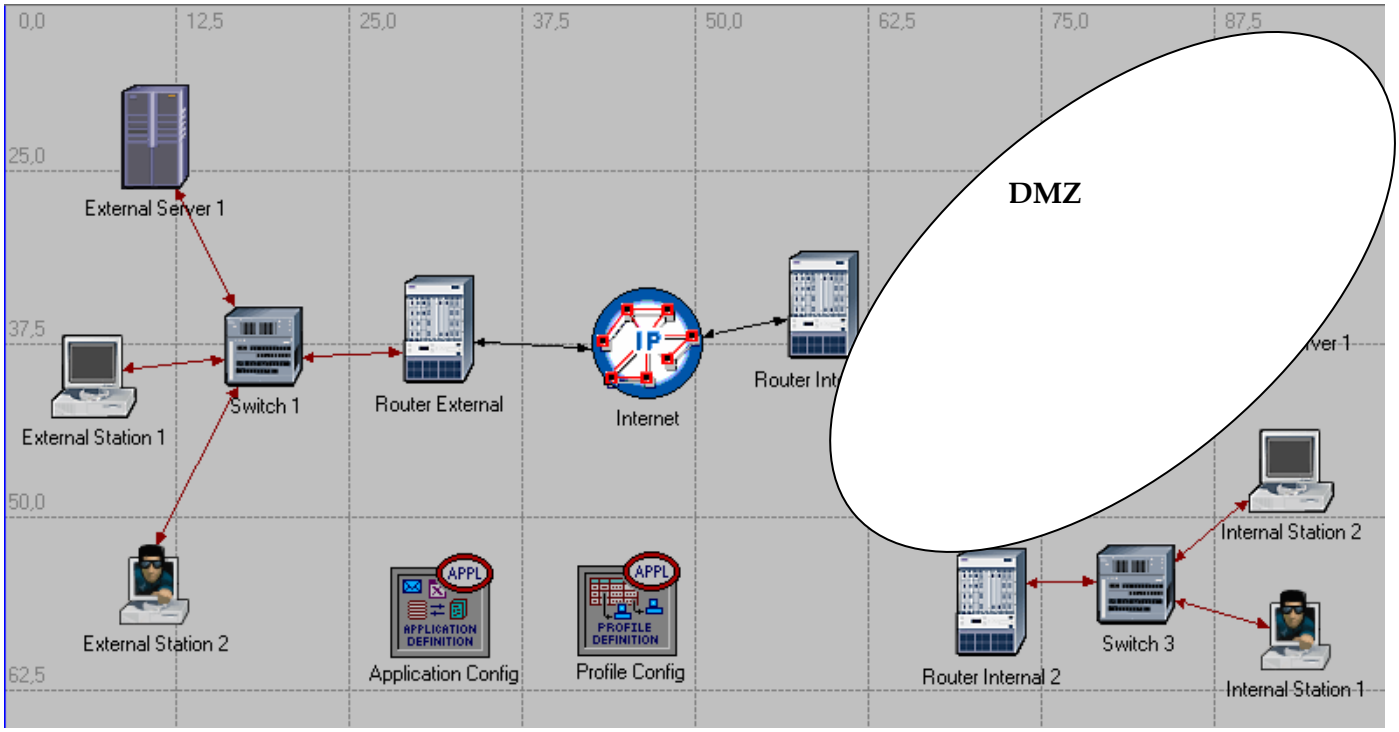
Προστασία και Ασφάλεια Δικτύων (Εργαστήριο)

Ενότητα 6

OPNET – DMZ

Σκοπός του εργαστηρίου: η μελέτη της δημιουργίας και χρήσης αποστρατικοποιημένων ζωνών. Η αποστρατικοποιημένη ζώνη (demilitarized zone – DMZ) αποτελεί ένα ξεχωριστό δίκτυο το οποίο βρίσκεται μεταξύ του ιδιωτικού μας δικτύου και του εξωτερικού (διαδικτύου). Χρησιμοποιείται για να τοποθετούνται οι servers στους οποίους θα πρέπει να υπάρχει πρόσβαση τόσο από το διαδίκτυο όσο και από το εσωτερικό μας δίκτυο.

Για τη δημιουργία μιας DMZ τυπικά χρησιμοποιούνται δύο routers και ένα firewall όπως φαίνεται στο Σχήμα 1. Ο εξωτερικός router (Router Internal 1 στο σχήμα) χρησιμοποιείται για να φιλτράρει αρχικά την κίνηση που εισέρχεται στο δίκτυο, το firewall (Proxy στο Σχήμα) κάνει τον έλεγχο των εισερχόμενων και των εξερχόμενων δεδομένων πριν να τα προωθήσει προς τους εξυπηρετητές, το εσωτερικό ή το εξωτερικό δίκτυο, ενώ ο εσωτερικός router (Router Internal 2) χρησιμοποιείται για να προστατεύει το εσωτερικό δίκτυο από την, ενδεχομένως επιβλαβή, κίνηση που έχει περάσει στην αποστρατικοποιημένη ζώνη.



Σχήμα 1: DMZ

Σημείωση: αυτή δεν είναι η μόνη δυνατή διαμόρφωση μιας DMZ. Ενδεικτικά, ο Internal Server 1 όπου τρέχουν υπηρεσίες στις οποίες δε πρέπει να υπάρχει πρόσβαση από χρήστες μπορεί και αυτός με τη σειρά του να μπει πίσω από ακόμη ένα firewall το οποίο θα βρίσκεται μεταξύ του Internal Server 1 και του Internal Server 2.

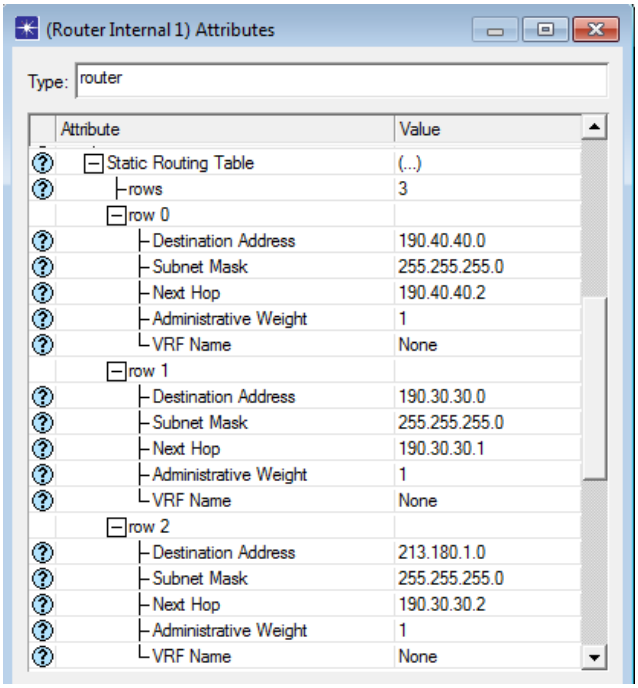
1.1 Δίκτυο

Το δίκτυο που θα χρησιμοποιηθεί για τις ανάγκες αυτού του εργαστηρίου είναι αυτό που φαίνεται στο Σχήμα στο οποίο υπάρχουν οι εξής διαφορές σε σχέση με τα προηγούμενα σενάρια:

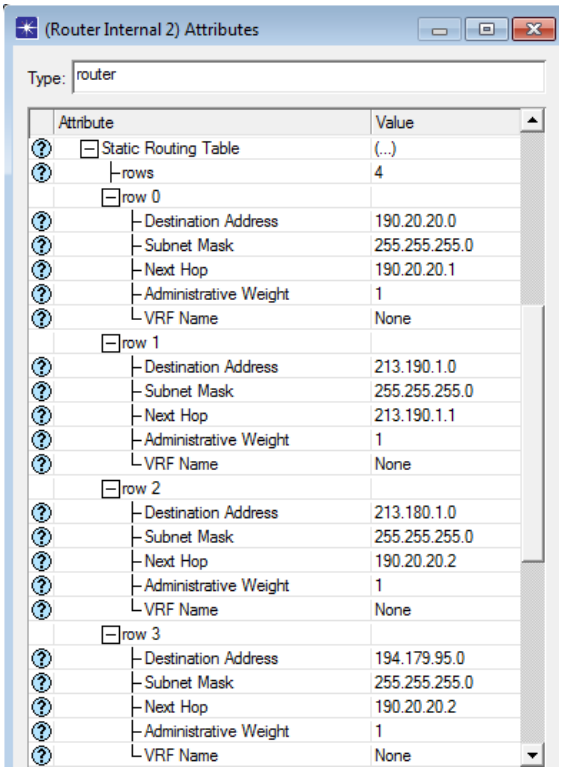
1. Έχουν δοθεί συγκεκριμένες διευθύνσεις στα δίκτυα και δεν έχει χρησιμοποιηθεί το Auto-Assign. Πιο συγκεκριμένα:

Interface	Address/Subnet Mask
External Network	194.179.95.0/24
DMZ	213.180.1.0/24
Internal Network	213.190.1.0/24
Internet – External Network	190.50.50.0/24
Internet – Internal Network	190.40.40.0/24
Router Internal 1 - Proxy	190.30.30.0/24
Proxy – Router Internal 2	190.20.20.0/24

2. Υπάρχει στατική δρομολόγηση των πακέτων σύμφωνα με τα παρακάτω σχήματα (ενδεικτικά απεικονίζονται για τους Router Internal 1 και Router Internal 2):



Σχήμα 2: Router Internal 1 static routing



Σχήμα 3: Router Internal 2 static routing table

Στο δίκτυο υπάρχουν τρία προφίλ εφαρμογών για πρόσβαση σε υπηρεσίες Βάσης Δεδομένων, για File Transfer και για υπηρεσίες ιστού. Οι εξυπηρετητές υποστηρίζουν την παροχή υπηρεσιών σύμφωνα με τον παρακάτω πίνακα:

Server	Υπηρεσίες
External Server	File Transfer (Heavy), Web Browsing (Heavy HTTP 1.1), Database Access (Heavy)
Internal Server 1	Database Access (Heavy), File Transfer (Heavy)
Internal Server 2	Web Browsing (Heavy HTTP 1.1)

Η χρήση των παρεχόμενων υπηρεσιών γίνεται από τους κόμβους ως εξής (ο προτιμώμενος εξυπηρετητής δηλώνεται γιατί υπάρχουν περισσότεροι εκτός ενός εξυπηρετητών που παρέχουν τις ίδιες υπηρεσίες – η δήλωση γίνεται μέσα από το **Edit Attributes → Application: Destination Preferences**):

Server	Profiles	Προτιμώμενος εξυπηρετητής
External Station	DBProfile	SInt1FTPDB (Internal Server 1)
	FTPProfile	SInt1FTPDB (Internal Server 1)
	HTTPProfile	SInt2HTTP (Internal Server 2)
Internal Station 1	DBProfile	SInt1FTPDB (Internal Server 1)
	FTPProfile	SInt1FTPDB (Internal Server 1)
	HTTPProfile	SInt2HTTP (Internal Server 2)
Internal Server 2	HTTPProfile	SExt1HTTPFTPDB (External Server 1)
	FTPProfile	SExt1HTTPFTPDB (External Server 1)

1.1 Άσκηση

Σκοπός της άσκησης είναι να παραμετροποιήσουμε τις δικτυακές συσκευές ώστε να αποκόψουμε τη μη εξουσιοδοτημένη χρήση των εξυπηρετητών από κακόβουλους χρήστες. Πιο συγκεκριμένα, η πολιτική ασφαλείας του οργανισμού μας περιλαμβάνει τις παρακάτω απαιτήσεις αναφορικά με την κίνηση του δικτύου:

1. Δε θα πρέπει να υπάρχει πρόσβαση είτε από το εσωτερικό είτε από το εξωτερικό δίκτυο προς τον Internal Server 1 στον οποίο τρέχουν υπηρεσίες FTP και DB.
2. Θα πρέπει να επιτρέπεται κίνηση προς τον Web Server είτε από το εσωτερικό δίκτυο είτε από το εξωτερικό δίκτυο.
3. Δε θα πρέπει να υπάρχει εξερχόμενη κίνηση από τον Internal Server 1. Οποιαδήποτε άλλη εξερχόμενη από την DMZ κίνηση θα επιτρέπεται.
4. Προς το εσωτερικό δίκτυο θα πρέπει να επιτρέπεται μόνο http κίνηση.

Σημείωση: Αν για τον περιορισμό της κίνησης χρησιμοποιηθούν Access Control Lists οι οποίες έχουν πολλούς κανόνες, υπενθυμίζεται πως εκτελείται ο πρώτος κανόνας ο οποίος βρίσκει εφαρμογή στο συγκεκριμένο πακέτο αγνοώντας τους υπόλοιπους.