



Δημιουργία ασφαλούς περιβάλλοντος, για άσκηση σε θέματα δικτύων και ασφάλειας, με εικονικές μηχανές

Βασιλάκης Βασίλειος

Καθηγητής ΠΕ19, 1^ο ΕΠΑΛ Αργυρούπολης

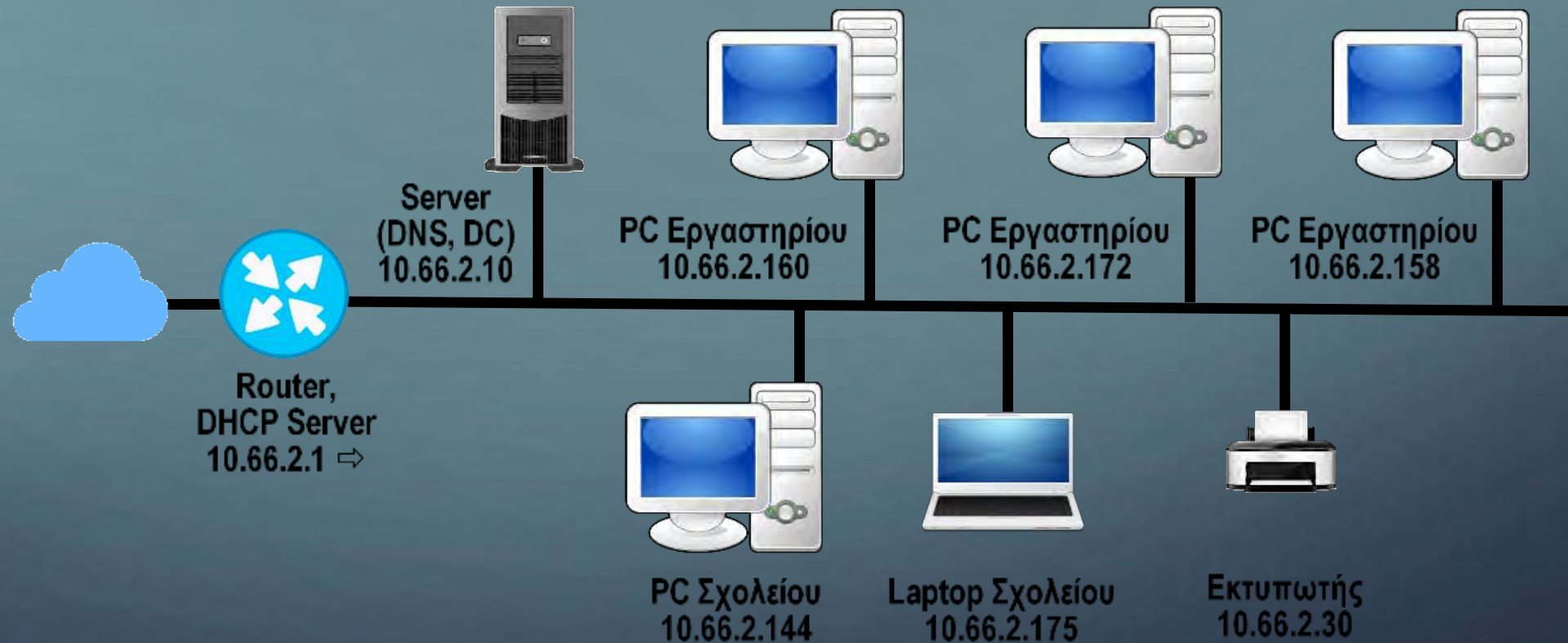
Εισαγωγή

- Τα νέα αναλυτικά προγράμματα των ΕΠΑΛ και οι σύγχρονες ειδικότητες των ΙΕΚ απαιτούν άσκηση σε προχωρημένα θέματα Λ/Σ, Δικτύων & Ασφάλειας
- Αυτό επιτυγχάνεται με τη χρήση Εικονικών Μηχανών (VM)
- Η χρήση τους όμως μπορεί να δημιουργήσει προβλήματα ασφάλειας

Θέματα ασφάλειας

- Οι VM μπορεί να αποκτήσουν πρόσβαση σε υπολογιστές που συνδέονται στο LAN του Σχολείου.
- Αυτοί μπορεί να είναι Η/Υ ή κινητές συσκευές, του Σχολείου ή Καθηγητών διαφόρων ειδικοτήτων χωρίς τις απαραίτητες γνώσεις για προστασία από μη εξουσιοδοτημένη πρόσβαση.
- Χρειάζεται απομόνωση των VM από το υπόλοιπο δίκτυο του Σχολείου.

Τυπική Δομή LAN Σχολείου



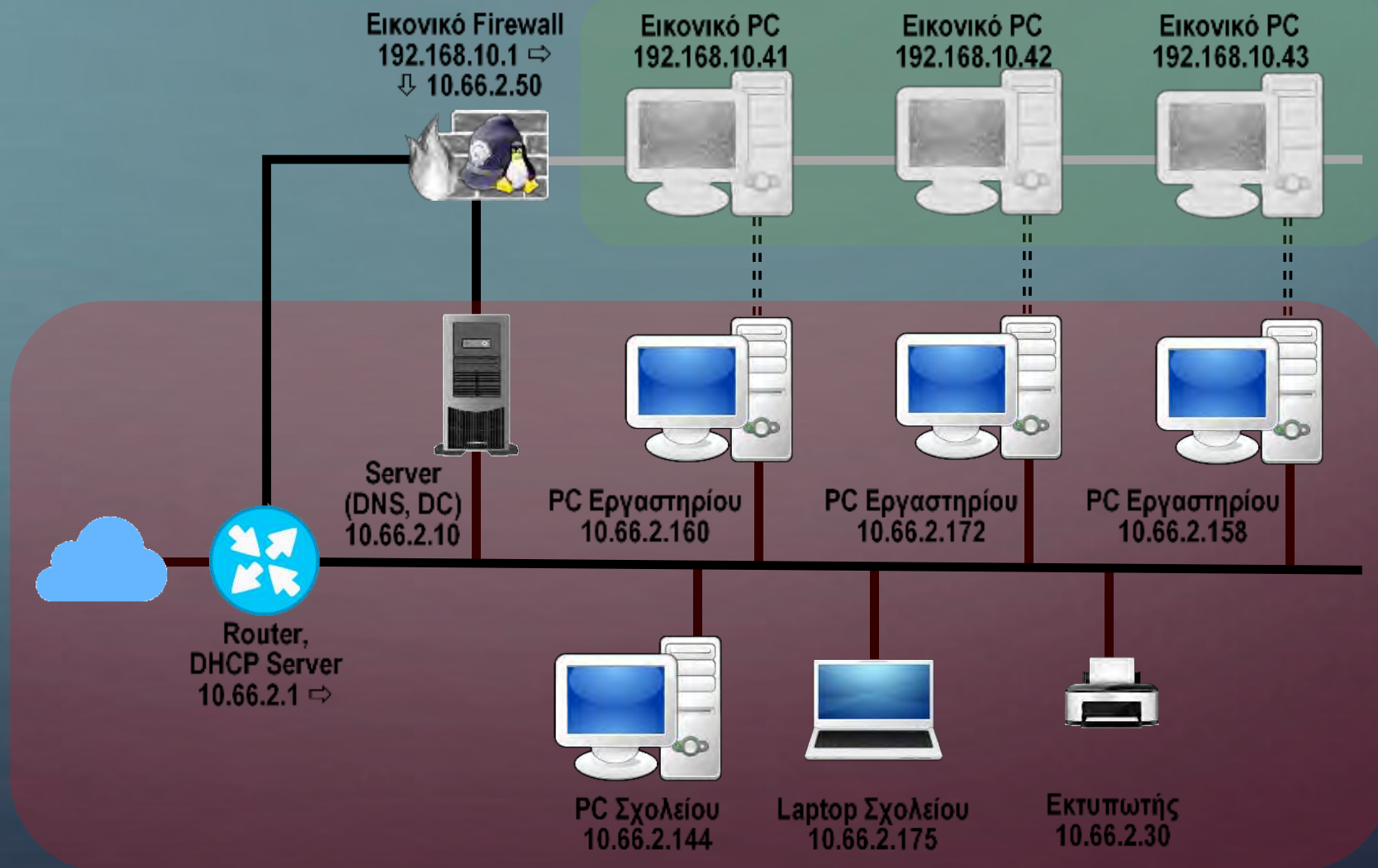
Απαιτήσεις σχήματος ασφάλειας

- Οι VM δεν πρέπει να έχουν πρόσβαση στους Η/Υ του Σχολείου, εκτός από αυτούς που παρέχουν κάποια απαραίτητη υπηρεσία (π.χ. Web Server) και μόνο για τη υπηρεσία αυτή.
- Θα πρέπει να επικοινωνούν μεταξύ τους.
- Θα πρέπει να συνδέονται στο Διαδίκτυο σε επιλεγμένες τοποθεσίες.

Πρόταση υλοποίησης

- Παρεμβολή Τείχους Προστασίας μεταξύ των VM και των φυσικών Η/Υ
- Υλοποίηση με τη διανομή Linux IPCop (<http://www.ipcop.org/>)
- Εγκατάσταση σε παλιό Η/Υ ή σε VM
- Απομόνωση των VM σε δικό τους δίκτυο με διαφορετικές IP διευθύνσεις
- Δημιουργία κανόνων για την παροχή πρόσβασης σε εσωτερικούς Server
- Δημιουργία κανόνων για την απαγόρευση πρόσβασης σε δικτυακούς τόπους

Το δίκτυο μετά την υλοποίηση



Δικτυακές Ρυθμίσεις

IPCor (κατά την εγκατάσταση ή με την εντολή setup)

Διασύνδεση	Διεύθυνση IP	Μάσκα Υποδικτύου	Πρωτεύων DNS	Δευτερεύων DNS	Προεπιλεγμένη Πύλη
RED	10.66.2.50	255.255.255.0	10.66.2.10	194.63.239.164	10.66.2.1
GREEN	192.168.10.1	255.255.255.0			

Εικονικών Μηχανών (χειροκίνητα)

Διεύθυνση IP	Μάσκα Υποδικτύου	Προεπιλεγμένη Πύλη
192.168.10.x	255.255.255.0	192.168.10.1
Απενεργοποίηση IPV6		

Κανόνες Τείχους Προστασίας

Από την ιστοσελίδα ρύθμισης <https://192.168.10.1:8443> (Firewall/Rules/Outgoing Traffic)

Πεδία	Άρνηση Πρόσβασης στο Δίκτυο του Σχολείου	Πρόσβαση σε Web Server
Source	Default Networks: Green Network	Default Networks: Green Network
Destination	Destination IP or Net: 10.66.2.0/24	Destination IP or Net: 10.66.2.5
Use Service	-	http (80)
Additional	Rule Enabled, Rule Action: DROP	Rule Enabled, Rule Action: ACCEPT

❗ Οι κανόνες εφαρμόζονται με τη σειρά, που μπορεί να αλλάξει με τα βέλη ▲ και ▼

Outgoing Traffic:

#	Net Iface	Source		Net Iface	Destination	Remark	Action						
1	GREEN	Green Network	➡➡	Red	10.66.2.5 : http		☒	☒					
2	GREEN	Green Network	✖	Red	10.66.2.0/24		☒	☒					

Άλλες διανομές Firewall

IPFire <http://www.ipfire.org/>



ClearOS <https://www.clearos.com/>



pfSense <https://www.pfsense.org/>

