ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΘΕΜΑ: ‘ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΣΕ ΔΙΚΤΥΑ ΚΟΡΜΟΥ ΒΑΣΙΣΜΕΝΗ ΣΕ ΤΕΧΝΟΛΟΓΙΕΣ CISCO SYSTEMS’

ΙΑΤΡΟΥ ΕΥΑΓΓΕΛΟΣ
ΑΜ 2113159

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ
ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ
Καθηγητής

ΣΥΝΕΠΙΒΛΕΠΩΝ
ΞΕΝΑΚΗΣ ΑΠΟΣΤΟΛΟΣ
Πανεπιστημιακός Υπότροφος

Λαμία 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΘΕΜΑ: ‘ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΣΕ ΔΙΚΤΥΑ ΚΟΡΜΟΥ ΒΑΣΙΣΜΕΝΗ ΣΕ ΤΕΧΝΟΛΟΓΙΕΣ CISCO SYSTEMS’

ΙΑΤΡΟΥ ΕΥΑΓΓΕΛΟΣ
ΑΜ 2113159

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ
ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ
Καθηγητής

ΣΥΝΕΠΙΒΛΕΠΩΝ
ΞΕΝΑΚΗΣ ΑΠΟΣΤΟΛΟΣ
Πανεπιστημιακός Υπότροφος

Λαμία 2020

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

THESIS TITLE: 'DESIGN AND SIMULATION OF SECURITY POLICIES IN BACKBONE TECHNOLOGY BASED ON CISCO SYSTEMS TECHNOLOGIES'

IATROU EVANGELOS

FINAL THESIS

ADVISOR
STAMOULIS GEORGIOS
Professor

CO ADVISOR
XENAKIS APOSTOLOS
University Scholar (Grant holder)

Lamia 2020

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από τις διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά, χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια.

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: ……/..…/20……

Ο – Η Δηλ.

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Οι ηλεκτρονικοί υπολογιστές είναι πλέον αναπόσπαστο κομμάτι της καθημερινότητάς μας τις τελευταίες δεκαετίες. Άνθρωποι όλων των ηλικιών εξυπηρετούν μεγάλο μέρος των αναγκών τους χρησιμοποιώντας το μέσο αυτό. Πέραν όμως από τη χρησιμότητά του ως μέσο πλέον έχει παγιωθεί ακόμη και στους πιο δύσπιστους η ανάγκη για προστασία, τόσο των ίδιων των υπολογιστικών συστημάτων όσο και των χρηστών τους. Τα στοιχεία είναι ιδιαίτερα ανησυχητικά καθώς αποκαλύπτουν ότι οι επιθέσεις με σκοπό είτε την πρόσβαση στα δεδομένα των υπολογιστικών συστημάτων (αριθμούς πιστωτικών καρτών, κωδικούς τραπεζικών λογαριασμών κ.α.), είτε την ίδια τη διακοπή της λειτουργίας τους αυξάνονται καταιγιστικά.

Στην παρούσα πτυχιακή εργασία γίνεται μια προσπάθεια να παρουσιαστούν κάποιες από τις βασικότερες προσεγγίσεις που έχουν προταθεί και χρησιμοποιούνται προς την κατεύθυνση της προστασίας των ευαίσθητων αυτών συστημάτων καθώς και των χρηστών τους με έμφαση στα δίκτυα κορμού τα οποία αποτελούν τις λεγόμενες ‘λεωφόρους της πληροφορίας’. Πιο συγκεκριμένα, θα περιγραφούν συστήματα αποτροπής άλλα και εντοπισμού επιθέσεων εστιάζοντας στον τρόπο λειτουργίας τους, τους κινδύνους από τους οποίους μας προστατεύουν καθώς και πώς θα πρέπει να συνδυαστούν προκειμένου να καλύπτει η μία υπηρεσία την άλλη στους τομείς που η άλλη υστερεί. Ακολούθως, θα εξετάσουμε τον τρόπο με τον οποίο λειτουργούν τα συστήματα από την οπτική της Cisco, μιας από τις πιο καταξιωμένες εταιρίες στο χώρο άλλα και έτερου ανταγωνιστού, που αρχίζει να ξεχωρίζει, του Fortinet.

Το εργαστηριακό κομμάτι της πτυχιακής εργασίας έχει υλοποιηθεί με τη χρήση του προγράμματος GNS3.

Λέξεις κλειδιά: δίκτυο υπολογιστών, ασφάλεια, τοίχος προστασίας, Cisco systems

ABSTRACT

Computers have been an integral part of our daily lives for the last decades. People of all ages use computers for their needs. But beyond that, even the most skeptical ones have become entrenched in the need to protect both the computer systems themselves and their users. The data are particularly alarming as they reveal that attacks aimed at either accessing computer system data (credit card numbers, bank account codes, etc.) or shutting them down are on the rise.

In this thesis we present some of the key approaches that have been proposed and used to protect these sensitive systems as well as their users with an emphasis on the backbone networks which are the so-called 'information boulevards' (data bus). More specifically, we will describe other deterrence and attack detection systems focusing on how they work, the risks they protect us from and how they should be combined in order to cover one service over another. Moreover, we will look at how systems work from the perspective of Cisco which is one of the most reputable companies as well as Fortinet, Cisco's main competitor.

The laboratory part of this thesis has been implemented using the GNS3 program.

Keywords: computer network, security, firewall, Cisco systems

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Ο ηλεκτρονικός υπολογιστής μέσα σε πολύ σύντομο χρονικό διάστημα, έχει παρουσιάσει πολύ μεγάλη εξέλιξη. Ο πρώτος ηλεκτρονικός υπολογιστής κατασκευάστηκε για στρατιωτικούς σκοπούς των Η.Π.Α. κατά το Β' Παγκόσμιο πόλεμο και καταλάμβανε ένα ολόκληρο δωμάτιο. Σήμερα, οι υπολογιστές αποτελούν σχεδόν αναπόσπαστο κομμάτι της καθημερινότητας των ανθρώπων, τόσο για επαγγελματική όσο και για προσωπική χρήση. Αξιοσημείωτο φαντάζει το γεγονός πως ένας υπολογιστής μπορεί να ζυγίζει ακόμα και λιγότερο από ένα κιλό χωρίς να υστερεί βέβαια σε δυνατότητες.

Τα υπολογιστικά συστήματα, δηλαδή μία πλήρης υπολογιστική συσκευή, δε λειτουργούν πλέον αυτόνομα αλλά είναι μονίμως συνδεμένα σε ένα δίκτυο μέσω του οποίου επικοινωνούν προκειμένου να εξυπηρετήσουν τις ανάγκες των χρηστών τους. Το δίκτυο αυτό όμως πέραν από μια κοινωνία πληροφορίας αποτελεί και ένα πεδίο απειλών και κινδύνων. Κρίνεται λοιπόν απαραίτητο να αναζητηθούν μέθοδοι που να προστατεύουν τα συστήματα και τους χρήστες τους από τους κινδύνους αυτούς. Η πρόκληση αυτή αντιμετωπίζεται σε πολυστρωματικό επίπεδο, τόσο από τα ίδια τα μηχανήματα με τη χρήση ειδικού λογισμικού όσο και περιμετρικά των μηχανημάτων με εξειδικευμένο εξοπλισμό εγκατεστημένο σε καίριες θέσεις επί των διαφόρων δικτύων μέσω των οποίων συνδέονται τα μηχανήματα αυτά. [6]

Από την όλη αυτή προσέγγιση θα ήταν λάθος να μην εξετάζαμε την πιο ευαίσθητη και σύνθετη οντότητα, τον ίδιο το χρήστη του υπολογιστικού συστήματος. Ο χρήστης που μπορεί να ανήκει σε οποιαδήποτε ηλικιακή ομάδα, οποιαδήποτε κοινωνική, οικονομική, θρησκευτική και με οποιοδήποτε μορφωτικό επίπεδό αποτελεί ίσως τον πιο αδύναμο κρίκο στην όλη προσπάθεια προστασίας τόσο του ίδιου όσο και των υπολογιστικών συστημάτων. Για το λόγο αυτό κρίνεται αναγκαία η επιβολή κανόνων καλής χρήσης των συστημάτων τόσο σε ατομικό επίπεδο όσο και σε ευρύτερο. Αξίζει να σημειωθεί ότι στην όλη προσπάθεια δεν θα πρέπει να ξεχνάμε ότι η τεχνολογία είναι το μέσο που φτιάχτηκε για να εξυπηρετεί τον άνθρωπο, όχι για να τον εξουσιάζει ούτε για να τον ελέγχει.

Σκοπός της παρούσας πτυχιακής εργασίας είναι ο σχεδιασμός πολιτικών ασφάλειας σε δίκτυα κορμού και η προσομοίωσή τους χρησιμοποιώντας τεχνολογίες CISCO. Για την υλοποίηση χρησιμοποιήθηκε το πρόγραμμα GNS3καθώς και η εικονική μηχανή VMware Workstation. Πιο συγκεκριμένα, η πτυχιακή χωρίζεται σε δύο μέρη, το θεωρητικό και το εργαστηριακό. Τα Κεφάλαια 2 και 3 ανήκουν στο θεωρητικό μέρος και περιλαμβάνουν βασικές έννοιες όπως δίκτυα υπολογιστών, πολιτικές ασφάλειας καθώς και επιθέσεις στα δίκτυα Η/Υ και στις επικοινωνίες. Το εργαστηριακό μέρος αποτελείται από το Κεφάλαιο 4 όπου γίνεται ανάλυση και σύγκριση των σεναρίων ασφάλειας. Τέλος, στο Κεφάλαιο 5 αποτυπώνονται τα συμπεράσματα της παρούσας πτυχιακής εργασίας.

ΚΕΦΑΛΑΙΟ 2 Ανασκόπηση πολιτικών ασφάλειας σε Δίκτυα Η/Υ και Επικοινωνιών

2.1 Δίκτυα Η/Υ και Δίκτυα Κορμού

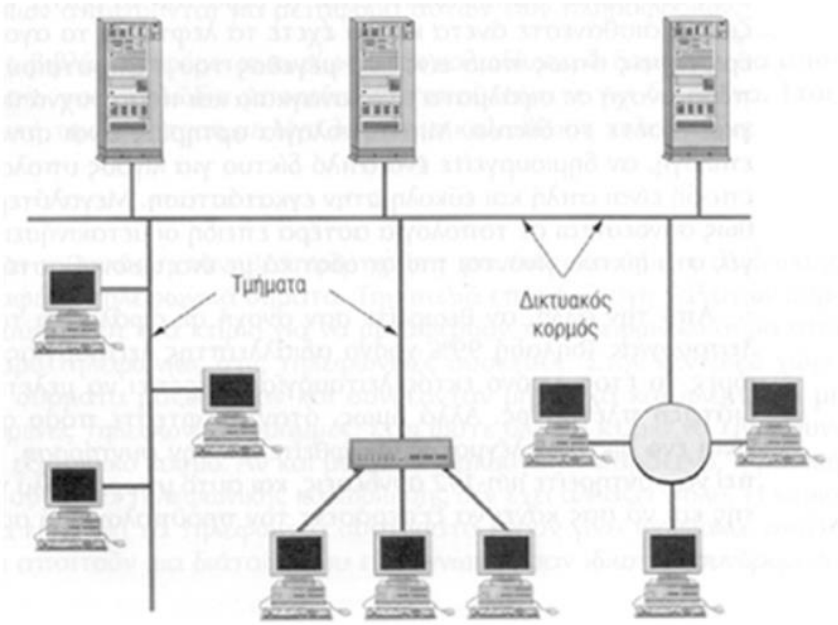
Ο ηλεκτρονικός υπολογιστής, σε οποιαδήποτε μορφή του (Desktop, Laptop, Tablet, κινητό τηλέφωνο, Smartwatch) αδιαμφισβήτητα αποτελεί από μόνο του ένα ιδιαίτερα χρήσιμο εργαλείο. Η χρησιμότητά του όμως πραγματικά εκτοξεύεται όταν συνδέεται σε ένα δίκτυο. Μέσω του δικτύου αποκτά σχεδόν άπειρες δυνατότητες και μετατρέπεται σε μέσω επικοινωνίας, αναζήτησης πληροφοριών, εργασίας κ.α. Καθίσταται λοιπόν προφανές ότι είναι απαραίτητη η σύνδεση του στο δίκτυο.

Δίκτυο υπολογιστών καλείται ένα τηλεπικοινωνιακό σύστημα αποτελούμενο από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές ή αλλιώς κόμβοι θεωρούνται διασυνδεδεμένοι όταν γίνεται ανταλλαγή πληροφορίας μεταξύ τους, ενώ αυτόνομοι όταν δεν καθίσταται δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία κάποιου άλλου(π.χ. εκκίνηση ή τερματισμό). [1]

Εικόνα 1 Δίκτυο Υπολογιστών

Ο τύπος του δικτύου χαρακτηρίζεται από τον τρόπο με τον οποίο τα συστήματα συνδέονται στο δίκτυο καθώς και ο αριθμός τους. Ξεκινώντας από το δίκτυο του σπιτιού μας, ή του τμήματος ενός πανεπιστήμιου - οργανισμού έχουμε το **τοπικό δίκτυο** το οποίο αποτελείται από υπολογιστές που ανήκουν σε μια ομάδα. Πολλά τοπικά δίκτυα συνδέονται μεταξύ τους μέσω ενός δικτύου κορμού και αποτελούν ένα **μητροπολιτικό δίκτυο**(metropolitan area network ή MAN) το οποίο καλύπτει μια πόλη η μία πανεπιστημιούπολη. Η κλιμάκωση αυτή ολοκληρώνεται με τα **δίκτυα ευρείας περιοχής** όπου εδώ πλέον καλύπτονται μεγάλες γεωγραφικές περιοχές όπως χώρες. Τέλος, τα **«διαδίκτυα»** είναι δίκτυα ευρείας περιοχής τα οποία όμως καλύπτουν γεωγραφικές περιοχές μίας ή περισσοτέρων ηπείρων διασυνδέοντας έτσι επιμέρους δίκτυα. Σε ένα διαδίκτυο είναι δυνατό να συνυπάρχουν διασυνδεδεμένοι

υπολογιστές και δίκτυα που χρησιμοποιούν διαφορετικές τεχνολογίες αλλά και λειτουργικά συστήματα. Το Διαδίκτυο (Internet) είναι το μεγαλύτερο τέτοιου είδους δίκτυο. [1][2]



Εικόνα 2 Δίκτυο Κορμού

Επιπλέον, η ταξινόμηση των δικτύων γίνεται και ως εξής:

- Χαρακτηρίζονται ως «ενσύρματα» ή «ασύρματα» αναλόγως το φυσικό μέσο διασύνδεσης τους και
- «Δημόσια» ή «ιδιωτικά» αναλόγως τον τρόπο πρόσβασης σε αυτά [1]

Κάθε τύπος δικτύου αποτελεί μια ξεχωριστή οντότητα με ιδιαίτερα χαρακτηριστικά, δεν απουσιάζουν όμως και τα κοινά στοιχεία μεταξύ των διαφορετικών τύπων δικτύων. Κατά συνέπεια τα συστήματα που συνδέονται σε αυτά δεν μπορούν να αποδώσουν το μέγιστο δυνατόν εάν περιορίζονται μόνο σε έναν τύπο δικτύου. Τα δίκτυα επικοινωνούν μεταξύ τους με αποτέλεσμα να ‘εισάγουν’ και να διακινούν κινδύνους που ενδεχομένως με την πρώτη ματιά να μην απειλούν το ίδιο το δίκτυο στο οποίο κινούνται άλλα κάποιο απομακρυσμένο τμήμα του. Είναι προφανές, λοιπόν, ότι εάν θέλουμε να μεγιστοποιήσουμε την αποτελεσματικότητα των μεθόδων ασφάλειας που θα εφαρμόσουμε θα πρέπει να αντιμετωπίσουμε το σύνολο των δικτύων, των υπολογιστών που συνδέονται σε αυτό άλλα και των χρηστών ακόμη σαν ένα ενιαίο σύνολο. [1]

2.2 Ασφάλεια Δικτύου Υπολογιστών

Η έννοια της ασφάλειας Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Εκτός αυτού, θεωρείται η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί, καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών. [4] [8]

Προκειμένου να ασφαλίσουμε τα δίκτυα των υπολογιστικών συστημάτων σαν πρώτη γραμμή άμυνας χρησιμοποιούμε τα λεγόμενα **συστήματα αποτροπής μη εξουσιοδοτημένης εισόδου (Intrusion Prevention Systems)** και ακολούθως τα **συστήματα εντοπισμού μη εξουσιοδοτημένης εισόδου (Intrusion Detection Systems)**.

Η βασικότερη διαφορά τους είναι, όπως μαρτυρά και η ονομασία τους, ότι τα πρώτα έχουν ενεργό ρόλο στη διαχείριση του δικτύου στερώντας ή επιτρέποντας ανάλογα με τους κανόνες που τους έχουν δοθεί την είσοδο στο δίκτυο, ενώ τα δευτέρα 'περιορίζονται' σε ένα ρόλο παθητικό. Παρακολουθούν, δηλαδή, αδιάκοπα την κάθε κίνηση στο δίκτυο και όταν εντοπίσουν κάποια ύποπτη δραστηριότητα ενημερώνουν το διαχειριστή του δικτύου ώστε αυτός να αποφασίσει για τις περαιτέρω ενέργειες. Στις αρχικές τους εκδόσεις τα συστήματα αυτά λειτουργούσαν σε ξεχωριστές συσκευές, στο πέρασμα του χρόνου όμως εξελίχθηκαν και πλέον τα συναντάμε να λειτουργούν αλληλοσυμπληρωμένα και στην ίδια συσκευή.[7] [8]

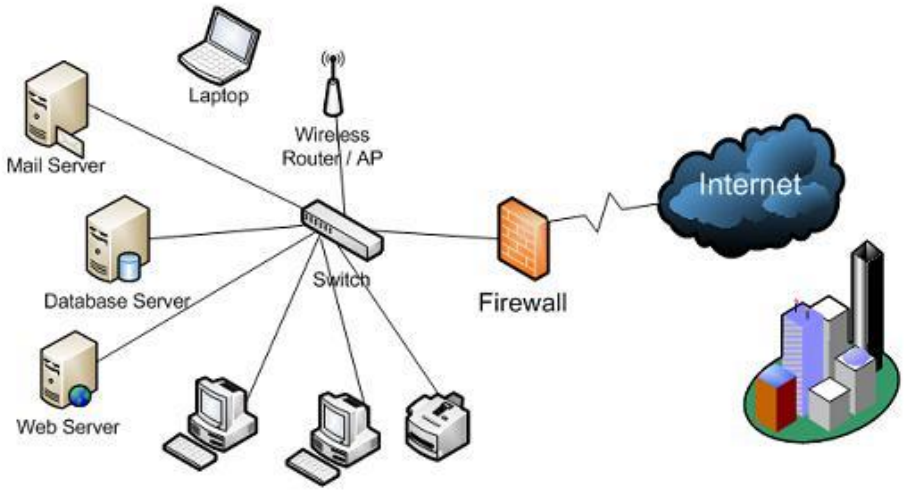
Εικόνα 3 Ασφάλεια Δικτύου

2.2.1 Συστήματα Αποτροπής Εισόδου

Τείχος προστασίας ή αλλιώς Firewall καλείτε η συσκευή ή το λογισμικό που χρησιμοποιούμε προκειμένου να ελέγξουμε την κίνηση, τόσο την εισερχόμενη όσο και την εξερχόμενη σε ένα συγκεκριμένο δίκτυο. Ο Abid (2018) περιέγραψε το τείχος προστασίας ως μια συσκευή εγκατεστημένη μεταξύ του εσωτερικού δικτύου ενός οργανισμού και του υπολοίπου δικτύου η οποία είναι κατάλληλα παραμετροποιημένη ώστε να προωθεί στον προορισμό τους τα εγκεκριμένα πακέτα, ενώ δύναται να απορρίψει αυτά που έχει οδηγίες να απορρίψει. Η

παραμετροποίηση αυτή βασίζεται σε δύο διαφορετικές μεθοδολογίες όπου είτε θα επιτρέπει την οποιαδήποτε κίνηση έκτος από αυτή που ρητά απαγορεύεται, είτε θα τερματίζει την κίνηση που δεν πληρεί ορισμένα κριτήρια που βασίζονται στον τύπο δικτύου τον οποίο το firewall διαχειρίζεται. Η κίνηση αυτή ελέγχεται τόσο για το είδος της όσο και για τον προορισμό και την αφετηρία της. Πιο συγκεκριμένα το Firewall μπορεί να δεχθεί και να εφαρμόσει κανόνες, όπως να επιτρέψει μονάχα την κίνηση του πρωτοκόλλου TCP σε ένα εξυπηρετητή που βρίσκεται στην IP 192.168.1.240 στη θύρα 80 ή να απαγορεύσει κάθε εξερχόμενη κίνηση στο υποδίκτυο 10.0.0.1/28.

Υπάρχουν διαφόρων ειδών Firewalls ανάλογα με το πώς είναι φτιαγμένα αλλά και τον τρόπο λειτουργίας τους. Μπορούν να αποτελούν μεμονωμένες - ανεξάρτητες συσκευές ή λογισμικό που εκτελείται πάνω σε κάποιο υπολογιστή. Τα Firewalls που δρουν ως ανεξάρτητες συσκευές είναι προτιμητέα σε δίκτυα με πολλούς υπολογιστές, ενώ τα λογισμικού τύπου συνηθίζονται σε μεμονωμένα συστήματα όπου το κάθε λογισμικό αναλαμβάνει να προστατεύει το σύστημα το οποίο το φιλοξένει. Γίνεται εύκολα αντιληπτό στον αναγνώστη ότι η κάθε προσέγγιση έχει πλεονεκτήματα και μειονεκτήματα. Η πρώτη προσέγγιση εισάγει ένα επιπλέον επίπεδο ασφάλειας στο δίκτυο και κατά συνέπεια μια κεντρικοποιημένη διαχείριση με μειονέκτημα ότι σε περίπτωση αστοχίας όλο το δίκτυο μένει απροστάτευτο. Έτερος διαχωρισμός των ειδών βασίζεται στο τμήμα του πακέτου του TCP όπου αυτά που ελέγχουν την επικεφαλίδα ομαδοποιούνται σε ελεγκτές πακέτων (Packet-Filtering Firewall) ενώ αυτά που ελέγχουν το σώμα σε διαμεσολαβητές (Proxy Firewall).[3][8]



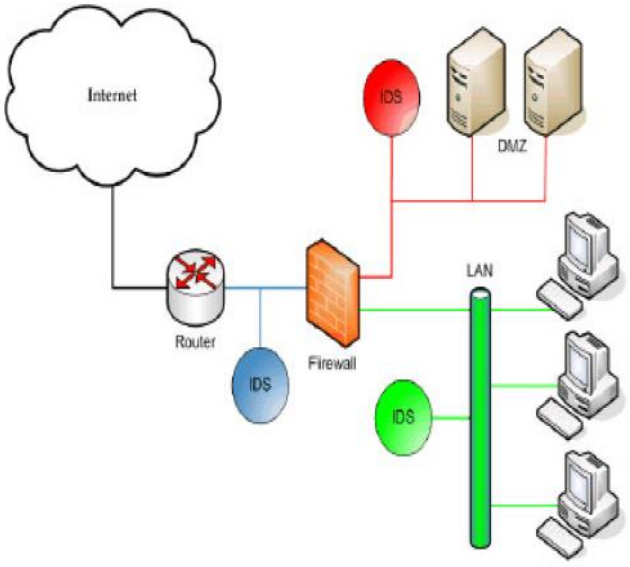
Εικόνα 4Τοίχος προστασίας (Firewall)

2.2.2 Συστήματα Εντοπισμού Εισόδου

Τα συστήματα αυτά συγκεντρώνουν και αναλύουν τα πακέτα από τις διαφορετικές τοποθεσίες του δικτύου αναζητώντας ίχνη παραβιάσεων ασφαλείας. Σε αντίθεση με τα Firewalls τα συστήματα αυτά δεν περιορίζονται στον έλεγχο πρόσβασης αλλά στη γενικότερη κίνηση. Αποτέλεσμα αυτού είναι να είναι σε θέση να εντοπίσουν όχι μόνο εισερχόμενους κινδύνους αλλά και αυτούς που προέρχονται από το εσωτερικό του δικτύου. Με τον τρόπο αυτό ο φορέας είναι προστατευμένος και από τον εσωτερικό «υπάλληλο» (client) ο όποιος (ενσυνείδητα ή όχι) προβαίνει σε ενέργειες που μπορεί να τον βλάψουν αφού το σύστημα θα εντοπίσει αυτή

την επικίνδυνη συμπεριφορά και θα ενημερώσει το διαχειριστή του δικτύου. Ο τελευταίος θα εκτιμήσει το μέγεθος του κινδύνου και θα λάβει τα κατάλληλα μέτρα.

Τα συστήματα αυτά, από την οπτική ενός διαχειριστή δικτύου, διακρίνονται σε 4 βασικές κατηγορίες ανάλογα με τον τρόπο δράσης. Αρχικά, έχουμε τα λεγόμενα δικτυακά τα οποία αποτελούν ανεξάρτητες πλατφόρμες, οι οποίες ελέγχουν γενικά το δίκτυο και παρακολουθούν με τον τρόπο αυτό πολλαπλούς σταθμούς. Είναι τοποθετημένα σε στρατηγικά σημεία ώστε να ελέγχουν το σύνολο της κίνησης του δικτύου και να αναζητούν επικίνδυνες τάσεις. Πέραν από τα κεντρικοποιημένα δικτυακά υπάρχουν και αυτά που εκτελούνται στους επιμέρους υπολογιστές του δικτύου. Τα συστήματα αυτής της κατηγορίας παρακολουθούν διάφορες ενέργειες του υπολογιστή όπως κλήσεις του συστήματος, αρχεία εγγραφής συμβάντων, αλλαγές σε αρχεία καθώς και άλλες προκειμένου να εντοπίσουν ύποπτες ενέργειες. Ακολούθως υπάρχουν τα λεγόμενα περιμετρικά τα οποία εστιάζουν την εποπτεία σε συγκεκριμένα σημεία περιμετρικά του δικτύου και τέλος τα βασιζόμενα σε εικονικές μηχανές όπου το σύστημα εποπτεύει μια εικονική μηχανή. [8] [9] [10]



Εικόνα 5Δίκτυο Υπολογιστή με χρήση IDS

2.3 Σύγχρονες Πολιτικές Ασφάλειας

Τέλος, θα αναφερθούμε στον πιο πολύπλοκο και ευαίσθητο παράγοντα των συστημάτων ασφαλείας, τον ίδιο τον άνθρωπο. Όσο δυνατό και έξυπνο να είναι ένα σύστημα ασφάλειας για να λειτουργήσει τα μέγιστα θα πρέπει να πλαισιώνεται από χρήστες οι οποίοι να διαθέτουν μια κατάρτιση, ώστε να μπορούν να ξεχωρίσουν τον κίνδυνο και να μειώσουν το φόρτο εργασίας των συστημάτων ασφαλείας. Μελέτες δείχνουν ότι ένα πολύ μεγάλο ποσοστό των ενεργειών που μπορούν να βλάψουν τον οργανισμό προκαλούνται από την αμέλεια των χρηστών. Για το λόγο αυτό κρίνεται απαραίτητη η σύνταξη ενός συνόλου απλών κανόνων, εύκολων στην εφαρμογή τους οποίους θα πρέπει να τηρούν όλοι, ανεξαιρέτως, οι χρήστες του συστήματος. Το σύνολο αυτό το ονομάζουμε Πολιτική Ασφάλειας. Στόχος της είναι να

προστατέψει τις ευαίσθητες πληροφορίες του οργανισμού καθώς και τον εξοπλισμό του παρεμβαίνοντας το ελάχιστο δυνατόν στην αδιάκοπη λειτουργία τόσο των πληροφοριακών συστημάτων όσο και στις εργασίες των χρηστών. Μια πολιτική ασφάλειας συνοδεύεται από ένα σύνολο μέτρων προστασίας (security measures, security controls), ή αντιμέτρων (counter measures) ή μέτρων ασφάλειας (security measures, security controls). [12]

Κατά καιρούς έχουν προταθεί διάφορες προσεγγίσεις με βασικό πρόβλημα την έλλειψη ενδιαφέροντος των χρηστών με αποτέλεσμα την ελλιπή εφαρμογή τους. Οι χρήστες είτε λόγω άγνοιας του κινδύνου, είτε λόγω αυξημένου φόρτου εργασίας, είτε επειδή αντιλαμβάνονται ότι ένα τέτοιο σύνολο κανόνων τους εξουσιάζει και τους περιορίζει δε δίνουν την πρέπουσα προσοχή με αποτέλεσμα η εφαρμογή των κανόνων να εξασθενεί με τον καιρό η ακόμα και να μην εφαρμόζεται καθόλου.

Για την αντιμετώπιση του μεγάλου αυτού προβλήματος οι Gokce και Dogerlioglu (2019) μελέτησαν τη λύση του να χρησιμοποιούν οι χρήστες το δικό τους ιδιωτικό εξοπλισμό στην εργασία τους (Bring Your Own Device). Με τον τρόπο αυτό αντιμετωπίζουν την ασφάλεια από εντελώς διαφορετική σκοπιά, μιας και τώρα δεν προσέχουν απλώς τα δεδομένα και τον εξοπλισμό του οργανισμού στον οποίο εργάζονται αλλά και τα ίδια τα δικά τους δεδομένα και το δικό τους εξοπλισμό. Έτσι οι χρήστες έχουν αυξημένο ενδιαφέρον να μάθουν πώς μπορούν να προστατευθούν από τους γνωστούς κινδύνους και είναι πολύ πιο προσεκτικοί στην εφαρμογή των κανόνων αυτών. Πέραν αυτού του πολύ σημαντικού πλεονεκτήματος η μέθοδος εμφανίζει και άλλα σημαντικά οφέλη για τον οργανισμό. Οι χρήστες είναι πιο ευτυχισμένοι μιας και αισθάνονται πιο οικεία στην εργασία τους, αφού χρησιμοποιούν τον προσωπικό τους εξοπλισμό με αποτέλεσμα να είναι πιο αποδοτικοί. Επιπλέον μαζί με τον εξοπλισμό τους συχνά φεύγοντας από την εργασία τους παίρνουν μαζί τους και δουλειά την οποία συνεχίζουν στον προσωπικό τους χρόνο χωρίς να ενοχλούνται από αυτό με άμεση συνέπεια την ακόμη μεγαλύτερη αύξηση της απόδοσης. Από πλευρά κόστους οι οργανισμοί δεν έχουν πλέον τα έξοδα της αγοράς, συντήρησης, υποστήριξης και λειτουργίας του εξοπλισμού αυτού αφού τα αναλαμβάνουν οι χρήστες έναντι ενός πολύ μικρότερου κόστους. [5]

Η μέθοδος εμφανίζει και μειονεκτήματα όπως η δυσκολότερη διαχείριση από πλευράς τμήματος πληροφορικής λόγω της ανομοιογένειας των συστημάτων και θέματα ασφάλειας όπως η σύνδεση μέσω δικτύου. Θεωρούμε όμως πως βρίσκεται προς τη σωστή κατεύθυνση και, μιας και πρόκειται για μια νέα προσέγγιση, υπάρχουν μεγάλα περιθώρια βελτίωσης.

ΚΕΦΑΛΑΙΟ 3 Επιθέσεις σε Δίκτυα Η/Υ και Επικοινωνιών

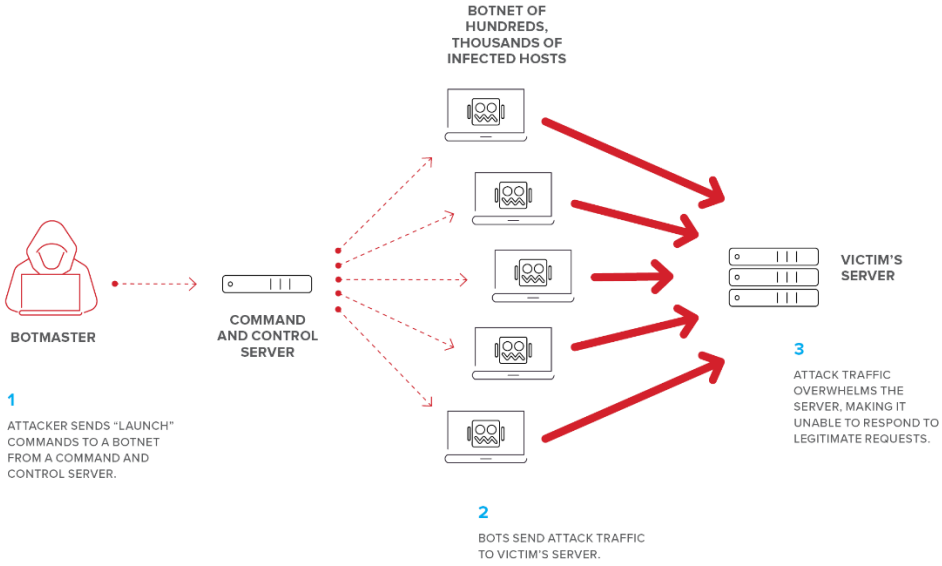
3.1 Τύποι Επιθέσεων

Προκειμένου να αντιληφθεί καλύτερα ο αναγνώστης, στο σημείο αυτό θα κάνουμε μια αναφορά σε κάποια από τα σημαντικότερα είδη επιθέσεων που έχουν κατά καιρούς καταγραφεί. Οι διάφορες επιθέσεις αυτές μπορούν να κατηγοριοποιηθούν και με βάση το αποτέλεσμα που επιφέρουν αφού ολοκληρώσουν με επιτυχία την αποστολή τους. Αρχικά, θα αναφέρουμε τις επιθέσεις τύπου 'KOD' (Kiss Of Death), όπου ο επιτιθέμενος αποστέλλει τροποποιημένα IGMP πακέτα που προκαλούν την κατάρρευση της TCP/IP στοίβας με συνέπεια τη γνωστή μπλε οθόνη.

Ακολούθως η 'DOS attack' επίθεση η οποία ομοίως στοχεύει στο να θέσει εκτός υπηρεσίας το επιτιθέμενο σύστημα είτε υποχρεώνοντας το σε επανεκκίνηση είτε καταναλώνοντας όλους τους πόρους του, με αποτέλεσμα να μην είναι σε θέση να διεκπεραιώσει νέες κλήσεις. Ομοίως και η 'DOS conseal' η οποία όμως στοχεύει σε Firewall συσκευές τις οποίες θέτει εκτός υπηρεσίας αποστέλλοντας μεγάλο αριθμό παραποιημένων IP διευθύνσεων. Τα Firewalls αδυνατώντας να ανταποκριθούν στο φόρτο εργασίας που προκαλεί είτε η καταγραφή κανόνων δρομολόγησης είτε η καταγραφή στατιστικών καταρρέουν.

Στη συνέχεια θα αναφερθούμε στην 'DOS Bloop' η οποία στοχεύει κυρίως σε εξυπηρετητές ιστοσελίδων τους οποίους θέτει εκτός υπηρεσίας αποστέλλοντας μαζικά ICMP πακέτα. Οι εξυπηρετητές είναι υποχρεωμένοι να απαντήσουν σε κάθε ένα από αυτά με αποτέλεσμα να μην μπορούν να ανταποκριθούν και να καταρρέουν.

Καθίσταται σαφές ότι κατόπιν προσεκτικής μελέτης των επιθέσεων είναι εφικτό να κατατάξουμε ενέργειες σε ύποπτες αλλά και σε επικίνδυνες. Βασισμένοι στα στοιχεία αυτά μπορούμε να παραμετροποιήσουμε τόσο τα συστήματα αποτροπής όσο και εντοπισμού κινδύνων ώστε να είναι σε θέση να εντοπίσουν τους κινδύνους και να προβαίνουν στις κατάλληλες ενέργειες για την αποτροπή τους.[10] [13]



Εικόνα 6 Dos Attack

3.2 Ευπάθειες Συστημάτων και Δικτύων

Κάθε σύστημα όπως και κάθε δίκτυο είναι ευπαθές σε επιθέσεις. Για τη μείωση των πιθανοτήτων ώστε οι επιθέσεις να μη διαπεράσουν τις άμυνες του συστήματος χρειάζονται προϊόντα και πολιτικές ασφάλειας. Φυσικά, κανένα σύστημα ή δίκτυο δεν μπορεί να χαρακτηριστεί τελείως ασφαλές.

Οι κατηγορίες των σημείων ευπάθειας σε ένα πληροφοριακό σύστημα είναι οι εξής:

- **Φυσικές Ευπάθειες (Physical).** Αφορούν το φυσικό περιβάλλον (π.χ. κτήρια). Σε επιθέσεις κατά των δικτύων η πρώτη άμυνα παρέχεται από τους φύλακες, τις βιομετρικές συσκευές, τους αντικλεπτικούς συναγερμούς και τους ελέγχους της φυσικής προσπέλασης.

- **Εκ Φύσεως Ευπάθειες (Natural).** Οι πυρκαγιές, οι πλημμύρες, οι κεραυνοί, ακόμα και οι διακοπές ρεύματος ‘απειλούν’ τους υπολογιστές. Όπως επίσης η σκόνη, η υγρασία και οι ακραίες θερμοκρασίες.

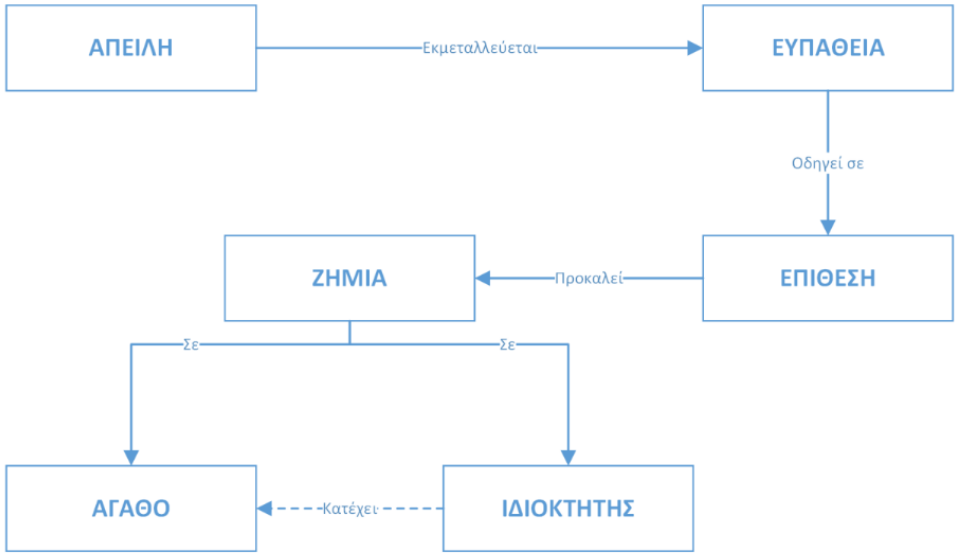
- **Ευπάθειες Υλικού και Λογισμικού (Hardware and Software).** Ένα πληροφοριακό σύστημα μπορεί να αντιμετωπίσει δυσλειτουργίες στο υλικό ή στο λογισμικό είτε λόγω εσωτερικών σφαλμάτων είτε λόγω εσφαλμένης εγκατάστασης των συστατικών μερών του.

- **Ευπάθειες Μέσων (Media).**Η διαρροή ευαίσθητων δεδομένων μπορεί να προκληθεί από την κλοπή ή από την καταστροφή μαγνητικών μέσων.

- **Ευπάθειες Εκπομπών (Emanation).** Εφόσον όλες οι ηλεκτρονικές συσκευές εκπέμπουν ηλεκτρομαγνητική ακτινοβολία, έχοντας τον κατάλληλο εξοπλισμό μπορεί εύκολα κάποιος να υποκλέψει τα εκπεμπόμενα σήματα από ένα σύστημα ή ένα δίκτυο υπολογιστών με σκοπό την πρόσβαση σε κρίσιμες πληροφορίες.

- **Ευπάθειες Επικοινωνιών (Communications).** Ένας υπολογιστής όταν συνδεθεί σε ένα ανοικτό δίκτυο γίνεται αυτομάτως ευάλωτος και αυξάνεται ο κίνδυνος διείσδυσης από τρίτους. Με αυτό τον τρόπο μπορούν να υποκλαπούν μηνύματα.

- **Ανθρώπινες Ευπάθειες (Human).** Η μεγαλύτερη πηγή ευπαθειών είναι οι άνθρωποι. Η ασφάλεια ενός συστήματος εξαρτάται κατά κύριο λόγο από τους ανθρώπους. [11]



Εικόνα 7Σχεδιάγραμμα Ευπαθειών

3.3 Τρόποι Αντιμετώπισης Ευπάθειας

Για να αντιμετωπίσουμε τις ευπάθειες ενός πληροφοριακού συστήματος, θα πρέπει να λάβουμε τα κατάλληλα μέτρα προστασίας ή αλλιώς αντίμετρα. Οι διαφορετικοί τύποι αντιμέτρων έχουν ως αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας πληροφοριακών συστημάτων στις ακόλουθες συνιστώσες:

- **Φυσική ασφάλεια συστήματος (physical security).** Αφορά την προστασία ολόκληρου του εξοπλισμού του υπολογιστή από φυσικές καταστροφές όπως πλημμύρες, φωτιά κλπ.

- **Ασφάλεια υπολογιστικού συστήματος (computer security).** Αφορά την προστασία των δεδομένων του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (αρχεία δεδομένων, εφαρμογές). Στοχεύει κυρίως στις συγκεκριμένες υπηρεσίες των λειτουργικών συστημάτων που καθορίζουν ποιος και πως θα δικαιούται να προσπελάσει τα δεδομένα και τις εφαρμογές του λειτουργικού συστήματος.

- **Ασφάλεια βάσεων δεδομένων (database security).** Κάθε σύστημα θα πρέπει να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, στην οποία αναφέρεται ποιοι εξουσιοδοτούνται να δουν αλλά και να τροποποιήσουν τα προστατευμένα δεδομένα.

- **Ασφάλεια δικτύων επικοινωνιών (network security).** Κάθε πληροφορία που μεταδίδεται μέσω των τηλεφωνικών, δορυφορικών ή άλλων δικτύων όπως τα τοπικά δίκτυα, θα πρέπει να προστατεύεται. [11]

ΚΕΦΑΛΑΙΟ 4 Σύγκριση Πολιτικών Ασφάλειας

4.1 Το περιβάλλον GNS3

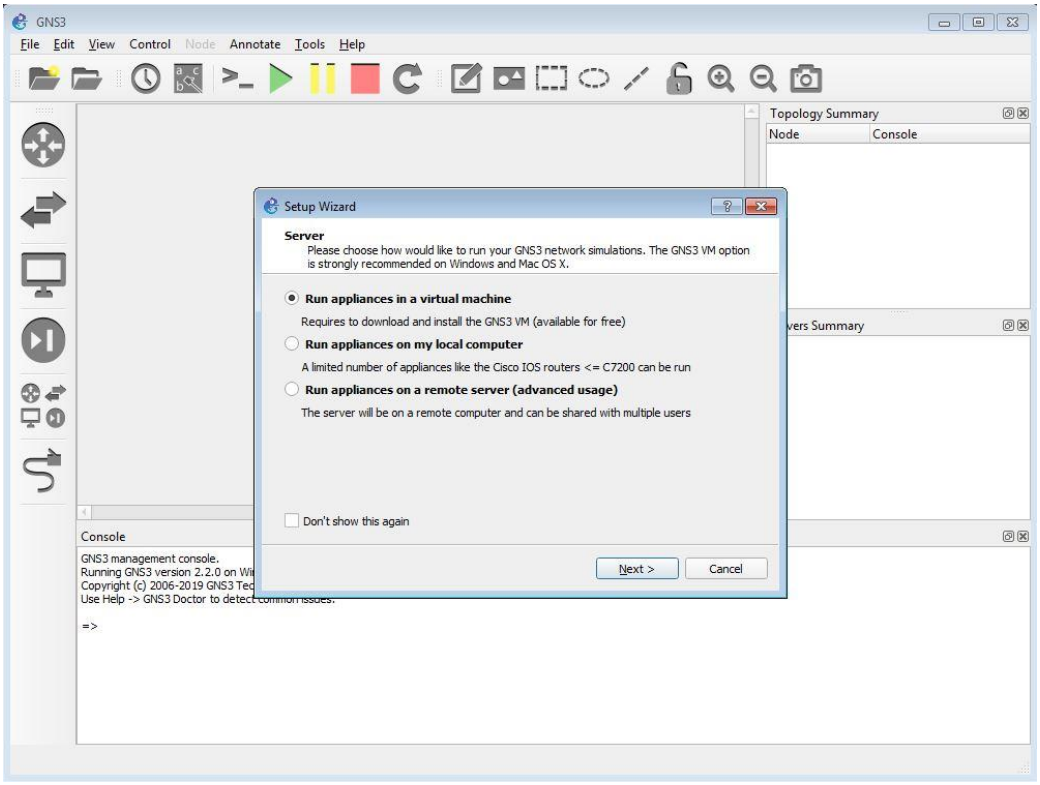
4.1.1 Λήψη & Εγκατάσταση του λογισμικού

Κατά το εργαστηριακό μέρος της πτυχιακής εργασίας είναι απαραίτητη η λήψη και εγκατάσταση της εφαρμογής GNS3.Το αρχείο είναι διαθέσιμο για λήψη από τον επίσημο ιστότοπο της εταιρίας και συγκεκριμένα στη διεύθυνση www.gns3.com/software/download. Ο ιστότοπος ζητά από το χρήστη, πριν του διαθέσει το λογισμικό, να δημιουργήσει δωρεάν ένα λογαριασμό. Το λογισμικό ανήκει στη κατηγορία των λογισμικών ανοιχτού κώδικα, διατίθεται στο κοινό δωρεάν με μοναδική υποχρέωση τη δημιουργία λογαριασμού από πλευράς του χρήστη. Αφού ολοκληρωθεί η διαδικασία της εγγραφής, ο χρήστης χρησιμοποιεί τα στοιχεία που δήλωσε για να ταυτοποιηθεί. Ακολούθως τα απαιτούμενα αρχεία της εφαρμογής είναι διαθέσιμα για λήψη.

4.1.2 Παραμετροποίηση της εφαρμογής

Την πρώτη φορά που θα εκτελεστεί η εφαρμογή θα πρέπει να ορίσουμε κάποιες παραμέτρους που έχουν να κάνουν με τον τρόπο που θα λειτουργεί η εφαρμογή. Ειδικότερα, θα πρέπει να ορίσουμε το περιβάλλον στο οποίο θα εκτελούνται οι διάφορες συσκευές της κάθε διάταξης που χρησιμοποιούμε. Ο λόγος για τον οποίο συμβαίνει αυτό είναι ότι το GNS χρησιμοποιεί τα ίδια αρχεία εικόνας που χρησιμοποιούν οι συσκευές. Αυτό πρακτικά σημαίνει ότι ο χρήστης έχει τη δυνατότητα να διαμορφώσει ένα δρομολογητή (Router) μέσα στο περιβάλλον και κατόπιν να μεταφέρει το αρχείο εικόνας του σε ένα πραγματικό δρομολογητή μεταφέροντας έτσι την παραμετροποίηση χωρίς καμιά περαιτέρω ενέργεια. Δίδεται, με τον τρόπο αυτό, η δυνατότητα στο χρήστη να διαμορφώσει μια συσκευή στο ασφαλές περιβάλλον του GNS και κατόπιν να το περάσει στο πραγματικό περιβάλλον ελαχιστοποιώντας το χρόνο που το δίκτυο δεν θα είναι διαθέσιμο καθώς και τους κινδύνους των λαθών.

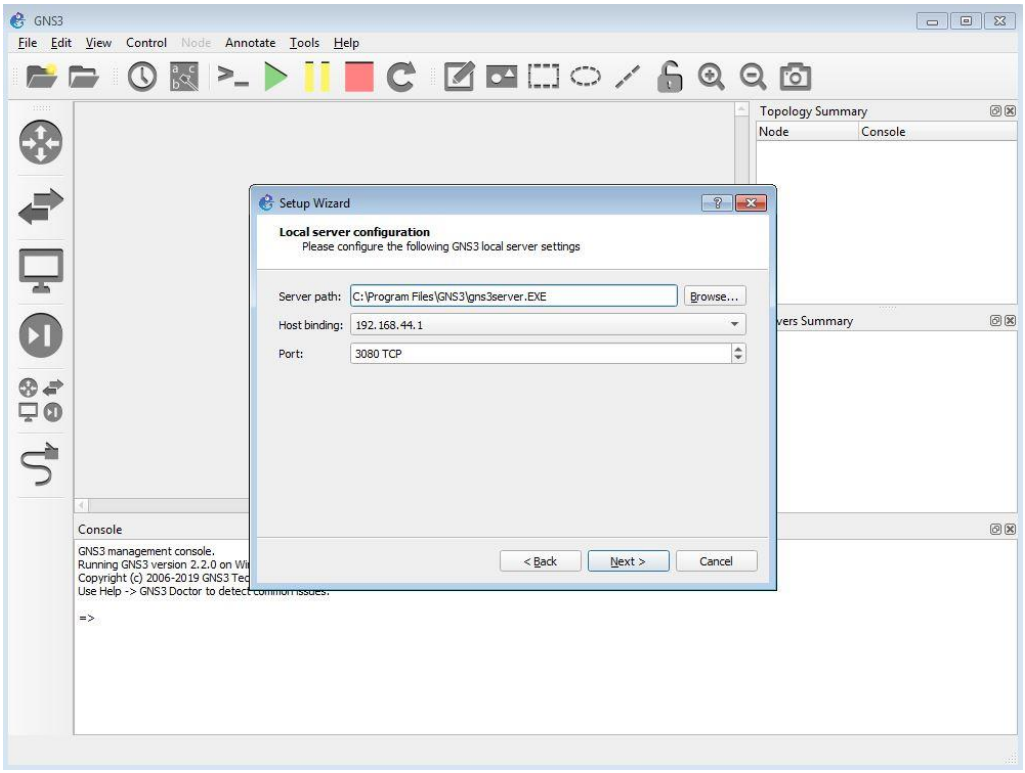
Για να το πετύχει αυτό το GNS θα πρέπει να δημιουργήσει ένα περιβάλλον μέσα στο οποίο θα εκτελούνται οι συσκευές αυτές. Διαθέτει τρεις διαθέσιμες τοποθεσίες, είτε στον ίδιο τον υπολογιστή όπου εκτελείται το GNS, είτε σε κάποιο άλλο υπολογιστή και τέλος σε ένα εικονικό μηχάνημα. Η επιλογή δίδεται την πρώτη φορά που θα εκτελεστεί η εφαρμογή μέσω ενός παράθυρου που μας ζητά να ορίσουμε που θα εκτελούνται οι συσκευές.



Εικόνα 8 Πρώτη εκτέλεση της εφαρμογής

Η κατασκευάστρια εταιρία συνιστά να επιλέγεται η πρώτη επιλογή η οποία αποτελείται από ένα εικονικό μηχάνημα το οποίο ονομάζει GNS3 VM και αποτελείται από ένα Ubuntu έκδοσης 18 το διάστημα που γραφόταν η παρούσα εργασία. Το μηχάνημα αυτό είναι κατάλληλα διαμορφωμένο για να μπορεί να φιλοξενήσει τις συσκευές που θα χρησιμοποιήσει ο χρήστης στην κάθε διάταξη που θα δημιουργήσει. Η λειτουργία των συσκευών στην εικονική αυτή μηχανή εκμεταλλεύεται πλήρως τις δυνατότητες του GNS3, παρέχοντάς μας μεγαλύτερο σύνολο επιλογών καθώς και διατάξεων. Επιπλέον στο μέλλον, μόνο αυτή η επιλογή θα είναι διαθέσιμη.

Παράλληλα όμως με το εικονικό μηχάνημα η εφαρμογή απαιτεί την ύπαρξη ενός εξυπηρετητή τοπικά στον ίδιο υπολογιστή που εκτελείται το GNS. Αυτό γίνεται για να έχει τη δυνατότητα ο χρήστης να τρέξει συσκευές και στον τοπικό υπολογιστή. Για την παραμετροποίησή του οι προεπιλεγμένες τιμές είναι αρκετές, δεδομένου ότι τόσο η διεύθυνση IP όσο και η πόρτα δεν είναι δεσμευμένες από άλλη υπηρεσία.

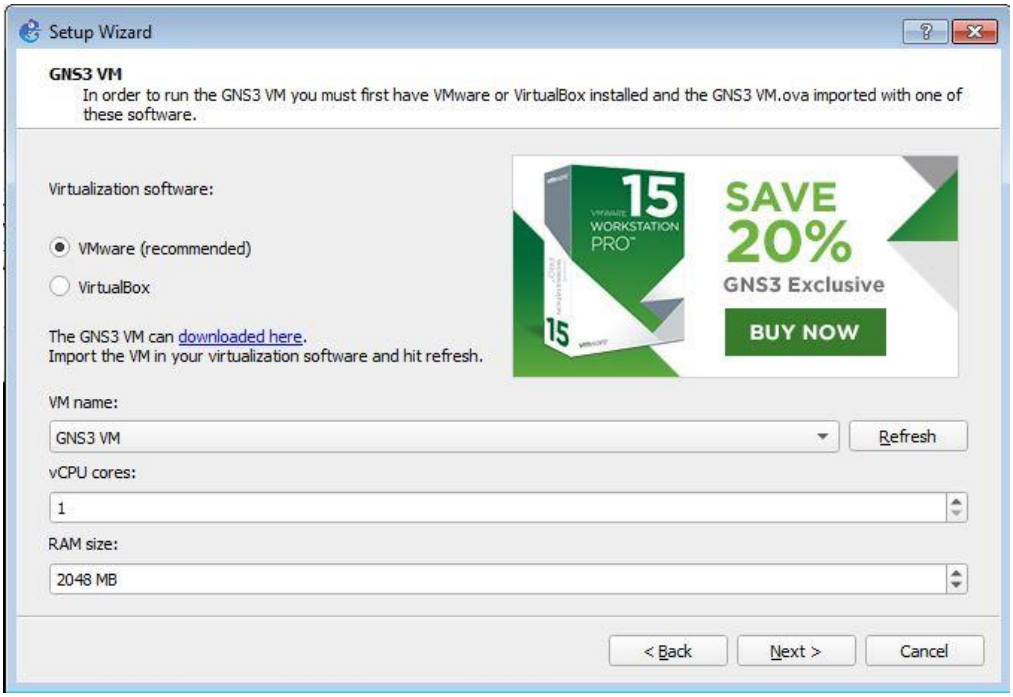


Εικόνα 9 Παραμετροποίηση του τοπικού εξυπηρετητή

Επιλέγοντας το κουμπί Next η εφαρμογή ελέγχει για τη διαθεσιμότητα των επιλογών και ακολούθως ξεκινά τον εξυπηρετητή. Η διαδικασία συνεχίζει με την εγκατάσταση του εξυπηρετητή του GNS3.

4.1.3 Δημιουργία εικονικής μηχανής GNS3 VM

Για τη δημιουργία της εικονικής μηχανής απαιτείται η χρήση κάποιας εφαρμογής διαχείρισης εικονικών μηχανών. Οι προτεινόμενες είναι δύο, της VMware και της Oracle. Από την εταιρία προτείνεται η χρήση της VMware αν και θα μπορούσε να χρησιμοποιηθεί και αυτή της Oracle με τον περιορισμό όμως ότι η έκδοση θα πρέπει να είναι 6.0 ή νεότερη και ο επεξεργαστής του υπολογιστή να ανήκει στην οικογένεια AMD. Αυτό διότι η εφαρμογή της Oracle υποστηρίζει εμφωλευμένη εικονοποίηση από την έκδοση 6 και μετά και μόνο για AMD επεξεργαστές. Η παρούσα εργασία υλοποιήθηκε πάνω σε VMware.



Εικόνα 10: Επιλογή του είδους της Εικονικής Μηχανής που θα φιλοξενήσει τις διάφορες συσκευές. Η λήψη του αρχείου εικόνας του GNS3 VM γίνεται επιλέγοντας το σύνδεσμο.

Από το σημείο αυτό ο χρήστης ορίζει και τις διάφορες παραμέτρους της εικονικής μηχανής όπως το όνομα της, τον αριθμό των εικονικών πυρήνων που θα διαθέτει και το σύνολο της μνήμης που θα της ανατεθεί.

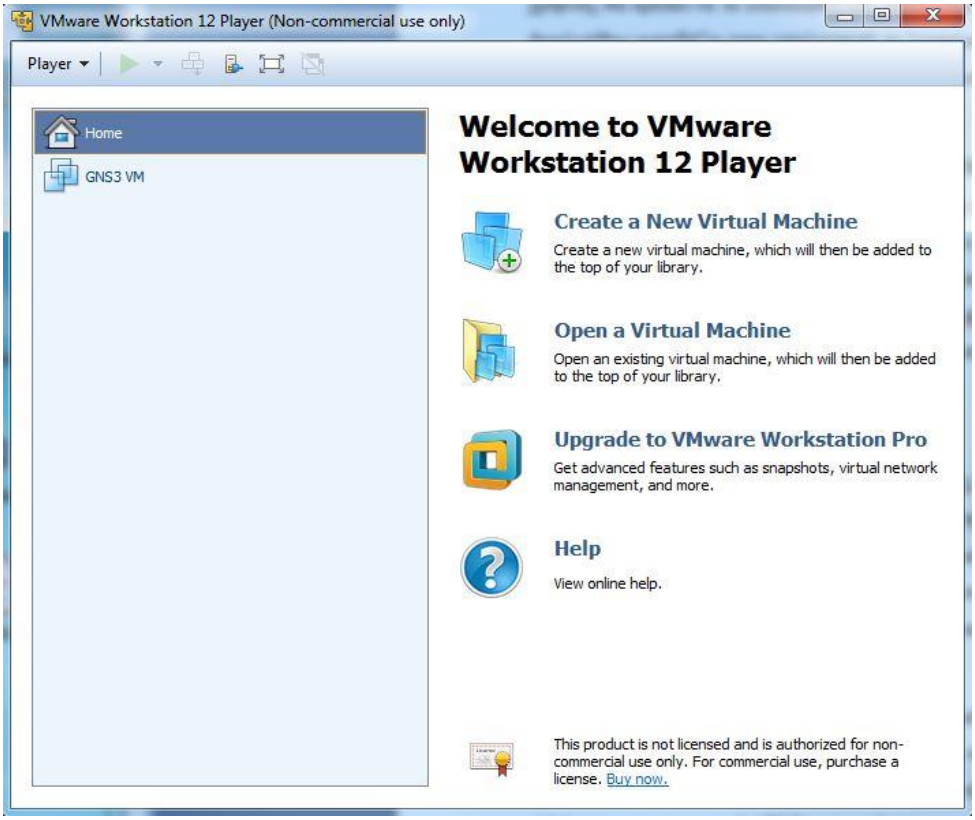
4.1.3.1 Εγκατάσταση VMware Workstation

Η έκδοση που θα πρέπει να χρησιμοποιηθεί είναι η 12.5. Νεότερες από αυτή δεν είναι συμβατές την παρούσα χρονική περίοδο και μπορεί να χρησιμοποιηθεί η δωρεάν έκδοση. Το απαιτούμενο αρχείο διατίθεται από τον επίσημο ιστότοπο στη διεύθυνση https://my.vmware.com/web/vmware/info?slug=desktop_end_user_computing/vmware_workstation_pro/12_0. Όπως και το GNS3,το οποίο διατίθεται δωρεάν, απαιτεί όμως πρώτα τη δημιουργία ενός δωρεάν λογαριασμού. Μετά τη δημιουργία του λογαριασμού ο χρήστης λαμβάνει ένα email το οποίο περιέχει ένα σύνδεσμο ενεργοποίησης του λογαριασμού. Ο χρήστης θα πρέπει να το επισκεφθεί και αυτομάτως ο λογαριασμός ενεργοποιείται. Ακολούθως κατεβάζει στον υπολογιστή το λογισμικό και στη συνέχεια το εγκαθιστά. Η εγκατάσταση δεν παρουσιάζει κάποια δυσκολία και οι προεπιλεγμένες παράμετροι είναι αρκετοί για να ολοκληρωθεί η εγκατάσταση.

4.1.3.2 Εισαγωγή του αρχείου εικόνας GNS3 VM στο VMware Workstation

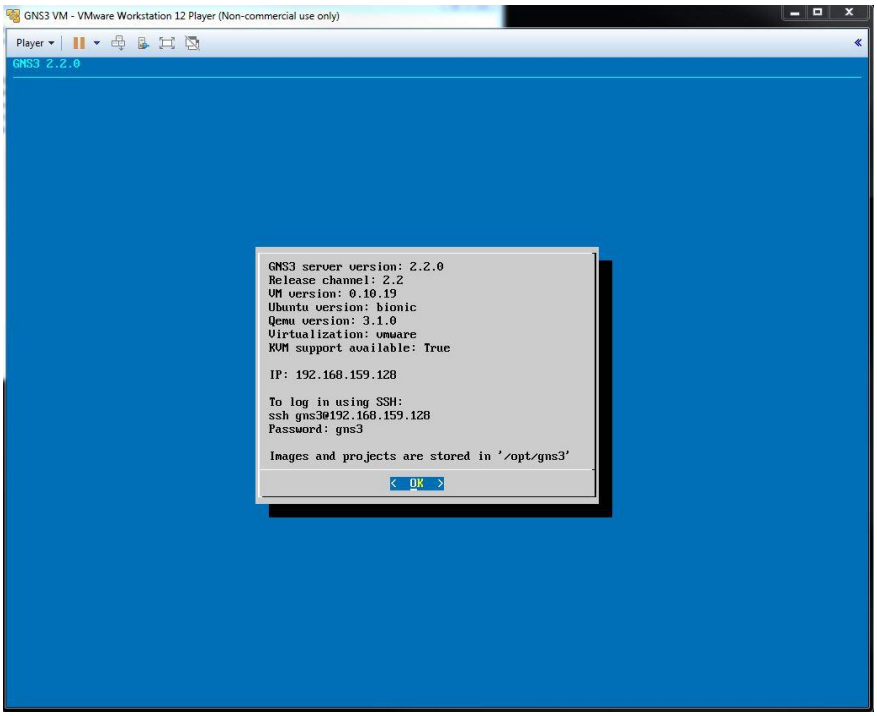
Το αρχείο είναι διαθέσιμο από το σύνδεσμο που παρέχει το GNS3. Πατώντας ο χρήστης ανοίγει το παράθυρο στον προεπιλεγμένο φυλλομετρητή και αρχίζει η λήψη του αρχείου μέσω του github. Μόλις η λήψη ολοκληρωθεί το αρχείο θα πρέπει να αποσυμπιεσθεί και κατόπιν θα εισαχθεί στο VMware Workstation επιλέγοντας Άνοιγμα μιας εικονικής Μηχανής. Για την ολοκλήρωση την εισαγωγής επιλέγουμε το αρχείο με κατάληξη OVA.

Η εφαρμογή διαβάζει το αρχείο εικόνας και εφόσον δεν εντοπίσει κάποιο σφάλμα που να οφείλεται στη μεταφορά η οπουδήποτε αλλού, η εισαγωγή ολοκληρώνεται. Στη συνέχεια ο χρήστης επιστρέφει στην εφαρμογή GNS3 και επιλέγοντας το πλήκτρο Επαναφόρτιση η εφαρμογή εντοπίζει την εικονική μηχανή που έχει εισαχθεί στο VMware Workstation. Πατώντας το πλήκτρο Επόμενο η εφαρμογή εμφανίζει μια σύνοψη της δοσμένης παραμετροποίησης και η διαδικασία ολοκληρώνεται. Στη συνέχεια η εφαρμογή GNS3 αναλαμβάνει να εκκινήσει την εικονική μηχανή GNS3 VM. Η διαδικασία τόσο της ενεργοποίησης όσο και του τερματισμού της εικονικής μηχανής γίνεται αυτόματα κατά την έναρξη και τον τερματισμό της εφαρμογής GNS3. Η ρύθμιση αυτή δύναται να τροποποιηθεί μέσω της εφαρμογής GNS3.



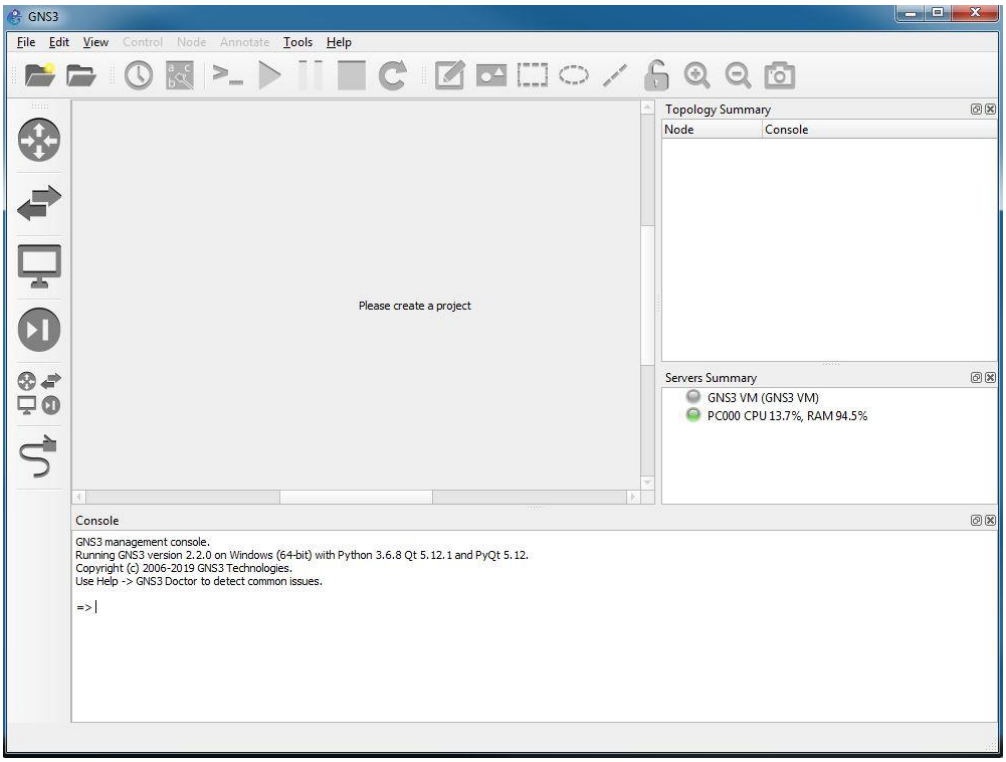
Εικόνα 11: Ο VMware Workstation με την GNS3 VM.

Εικόνα 12: Η μηχανή GNS3 VM κατά την εκκίνηση



Εικόνα 13: Η εικονική μηχανή έτοιμη να δεχθεί συσκευές.

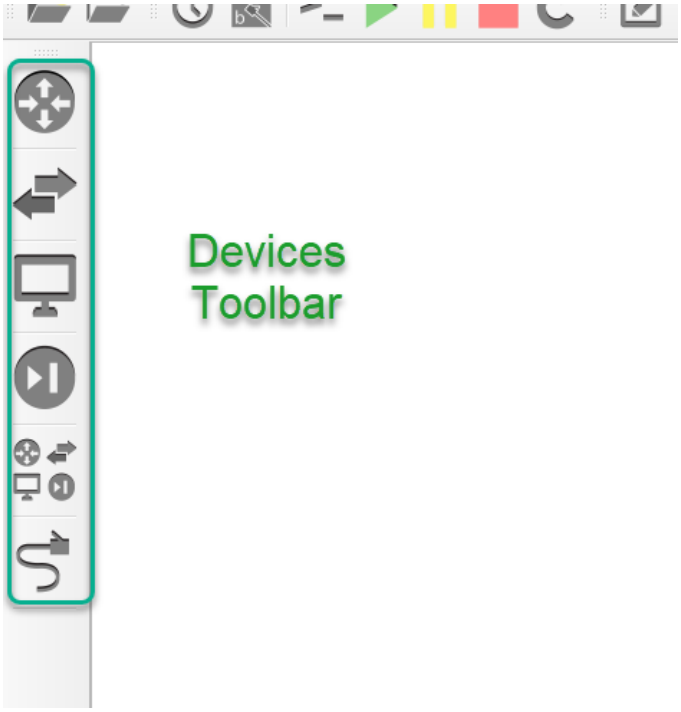
4.1.4 Εξοικείωση με το περιβάλλον GNS3



Εικόνα 14: Το περιβάλλον του GNS3

Όπως αναφέρει η εφαρμογή το πρώτο πράγμα που θα πρέπει να γίνει από πλευράς του χρήστη είναι η δημιουργία μιας νέας διάταξης. Αυτό επιτυγχάνεται μέσω του File / New Blank Project. Στο νέο παράθυρο που θα ανοίξει ο χρήστης θα ορίσει τη διαδρομή που θα αποθηκευτεί η νέα αυτή διάταξη.

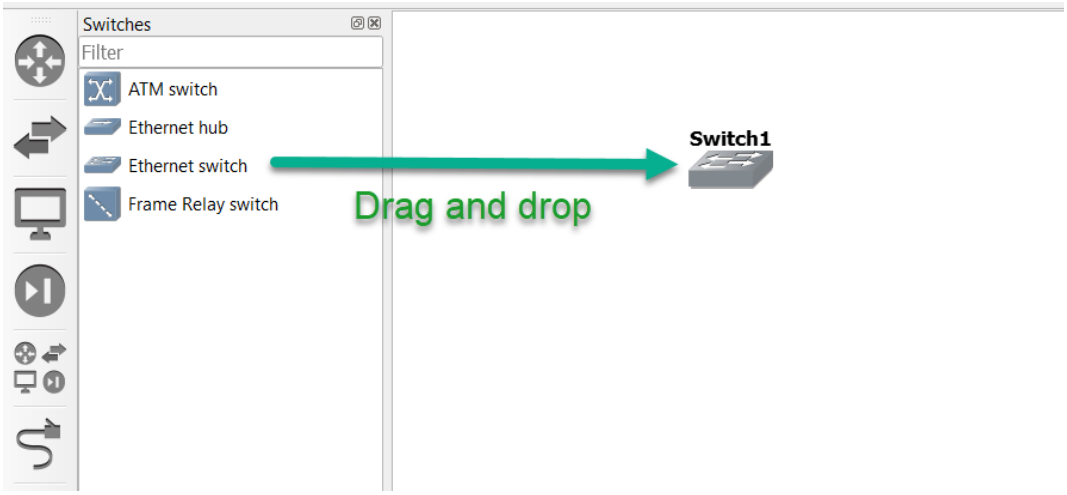
Όπως έχει προαναφερθεί η εφαρμογή GNS3 διακρίνεται λόγω της ικανότητας της να χρησιμοποιεί τα αρχεία εικόνας των ίδιων συσκευών που θα χρησιμοποιηθούν σε μια πραγματική διάταξη δικτύου. Τα αρχεία αυτά δεν διατίθενται εξ αρχής στην εφαρμογή άρα για να χρησιμοποιήσουμε οποιαδήποτε συσκευή θα πρέπει να εισάγουμε στην εφαρμογή το αντίστοιχο αρχείο εικόνας της (Image). Για το λόγο αυτό, την πρώτη φορά που θα εκτελέσουμε την εφαρμογή στον υπολογιστή μας δεν θα έχουμε συσκευές να χρησιμοποιήσουμε στη διάταξή μας, εκτός από κάποιες πολύ βασικές, όπως κάποιους μεταγωγούς (switch και hub), έναν εξομοιωτή ηλεκτρονικού υπολογιστή με βασικές λειτουργίες και δύο συσκευές (ένα Nat και ένα Cloud) για τη σύνδεση της διάταξης με τον εξωτερικό κόσμο.



Εικόνα 15: Εργαλειοθήκη Συσκευών

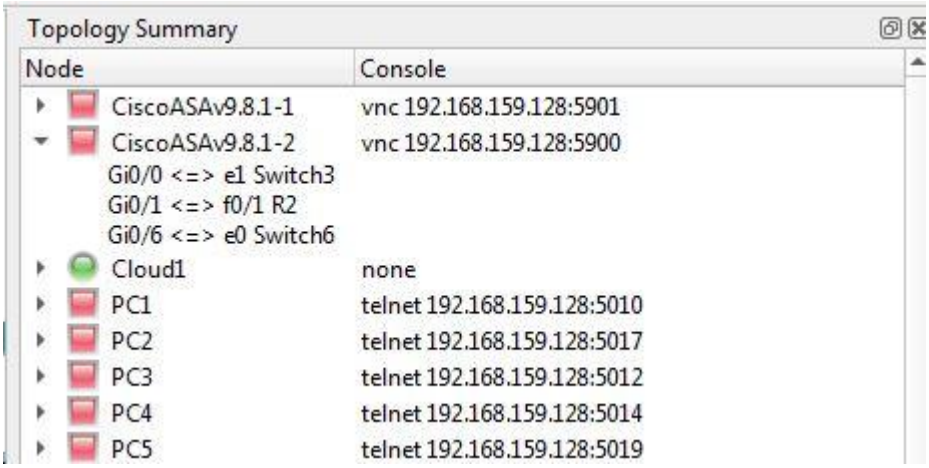
Οι συσκευές επιλέγονται από την εργαλειοθήκη συσκευών και όπως προαναφέρθηκε, την πρώτη φορά που θα εκτελέσουμε την εφαρμογή, στην εργαλειοθήκη αυτή υπάρχουν μόνο πολύ βασικές συσκευές. Οι συσκευές είναι κατηγοριοποιημένες και στην πρώτη θέση θα εισαχθούν οι δρομολογητές, στη δεύτερη οι μεταγωγείς, στην τρίτη οι υπολογιστές και οι συσκευές διασύνδεσης με τον έξω κόσμο και στην τέταρτη οι συσκευές που θα λειτουργούν ως τοίχος προστασίας. Στην επόμενη θέση εμφανίζονται όλες οι διαθέσιμες συσκευές που υπάρχουν στην εφαρμογή και τέλος στην επόμενη τα καλώδια διασύνδεσης των συσκευών αυτών.

Πατώντας σε κάθε κατηγορία η εφαρμογή εμφανίζει μια πλευρική στήλη στην οποία παρουσιάζει τις συσκευές της κατηγορίας. Προκειμένου να εισαχθούν στη διάταξή μας ο χρήστης επιλέγει την επιθυμητή συσκευή, την τραβά και την αποθέτει στην επιφάνεια εργασίας της εφαρμογής.



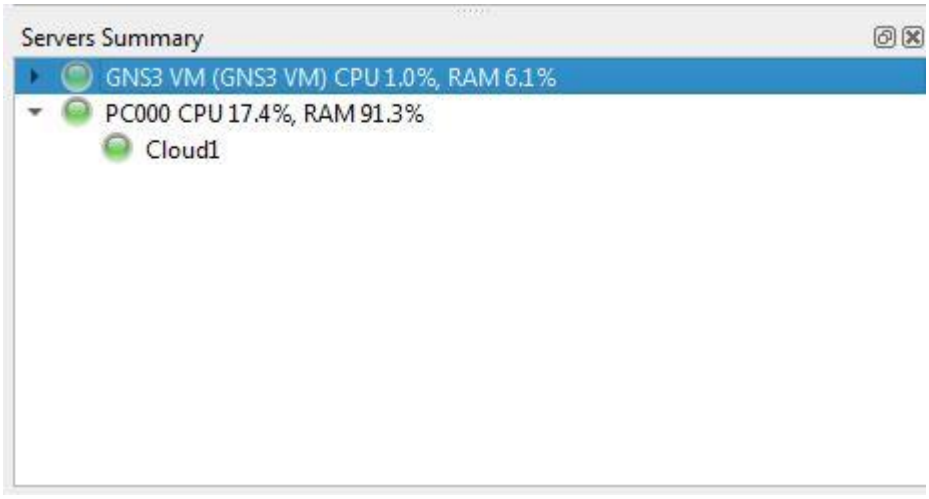
Εικόνα 16: Εισαγωγή συσκευών στο χώρο εργασίας

Μετά την απόθεση της συσκευής η εφαρμογή εμφανίζει ένα μήνυμα και ζητά από το χρήστη να δηλώσει που θα φιλοξενηθεί η συσκευή. Οι διαθέσιμες επιλογές είναι ο τοπικός υπολογιστής και η εικονική μηχανή GNS3 VM. Για τις περισσότερες προτείνεται η δεύτερη. Στη συνέχεια αυτή εμφανίζεται στην καρτέλα Τοπολογία είτε με χρώμα πράσινο αν είναι ενεργοποιημένη είτε με κόκκινο αν είναι ανενεργή. Πατώντας στο βέλος αριστερά της, ο χρήστης θα δει τις ιδιότητές της όπως IP διεύθυνση, τις διάφορες διασυνδέσεις που διαθέτει κλπ. Η διαχείριση της συσκευής πραγματοποιείται από το μενού που εμφανίζεται όταν ο χρήστης κάνει δεξί κλικ πάνω της.



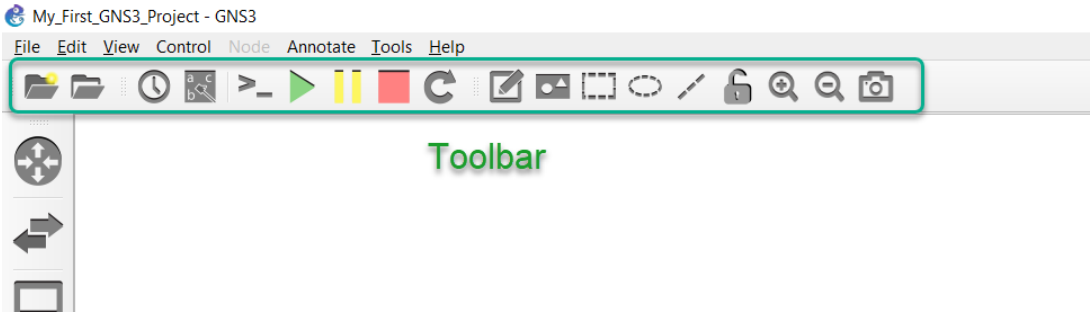
Εικόνα 17: Οι συσκευές της τοπολογίας

Πέρα από την καρτέλα Τοπολογία η κάθε συσκευή εμπεριέχεται και στον εξυπηρετητή που φιλοξενείται στην καρτέλα των εξυπηρετητών. Η καρτέλα αυτή εμφανίζει το σύνολο των εξυπηρετητών που χρησιμοποιεί η εφαρμογή, τοπικούς και απομακρυσμένους, παρουσιάζοντας με πράσινο χρώμα αυτούς που εκτελούνται και με γκρι τους ανενεργούς.



Εικόνα 18: Οι διαθέσιμοι εξυπηρετητές

Από το γραφικό περιβάλλον της εφαρμογής δεν απουσιάζει και η γραμμή με την Εργαλειοθήκη η οποία περιέχει τα βασικά εργαλεία της εφαρμογής. Από το σημείο αυτό ο χρήστης μπορεί να δημιουργήσει νέες διατάξεις, να εκκινήσει ή να σταματήσει τις συσκευές της διάταξης, να γράψει σημειώσεις και σχήματα στην επιφάνεια εργασίας κλπ.



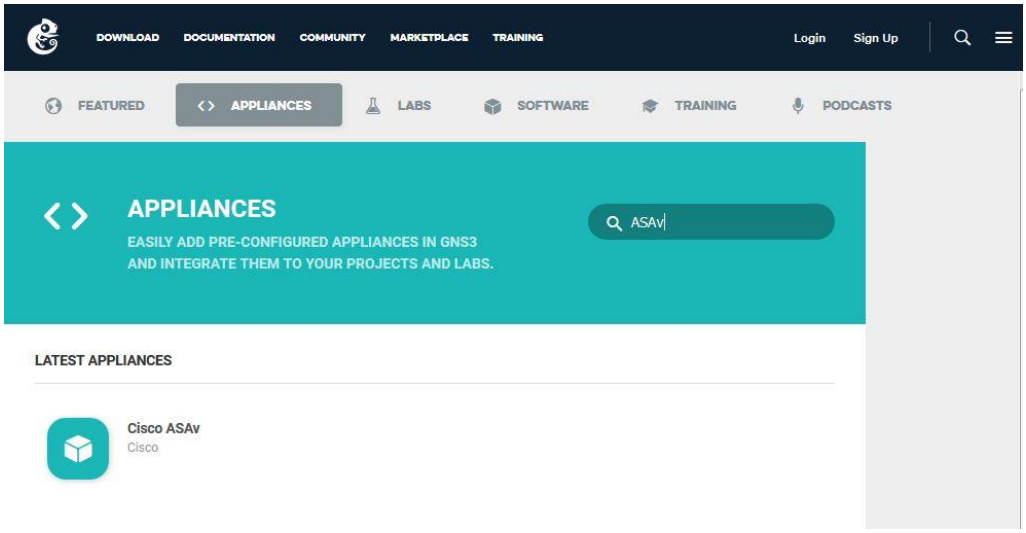
Εικόνα 19: Η εργαλειοθήκη της εφαρμογής

Τέλος στο κάτω μέρος της εφαρμογής υπάρχει το παράθυρο κονσόλας μέσω της οποίας η εφαρμογή εμφανίζει μηνύματα στο χρήστη αλλά και δέχεται εντολές. Με κόκκινο χρώμα εμφανίζει τα προβλήματα τα οποία εμφανίζονται και σαν παράθυρα στην πάνω αριστερή γωνία.

4.1.5 Εισαγωγή συσκευών στο GNS3

4.1.5.1 Απόκτηση των αρχείων εικόνας

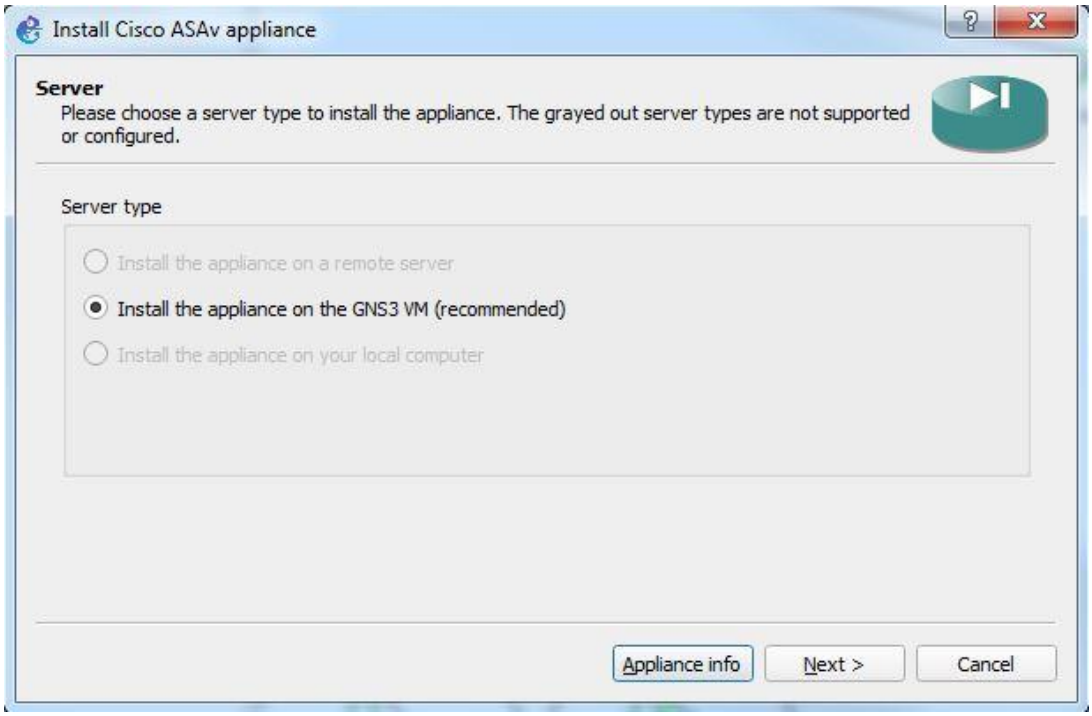
Το πρώτο βήμα για την εισαγωγή ενός αρχείο εικόνας είναι να κατεβάσουμε από τον ιστότοπο την περιγραφή του που η εφαρμογή το ονομάζει Appliance. Η διεύθυνση από την οποία είναι διαθέσιμα είναι η https://gns3.com/marketplace/appliances. Τα αρχεία διατίθενται δωρεάν και αρκεί μια αναζήτηση για να μας φέρει το ζητούμενο αρχείο. Εδώ θα εισάγουμε στην εφαρμογή ένα αρχείο περιγραφής ενός CISCO ASA Firewall.



Εικόνα 20: Λήψη αρχείων περιγραφής

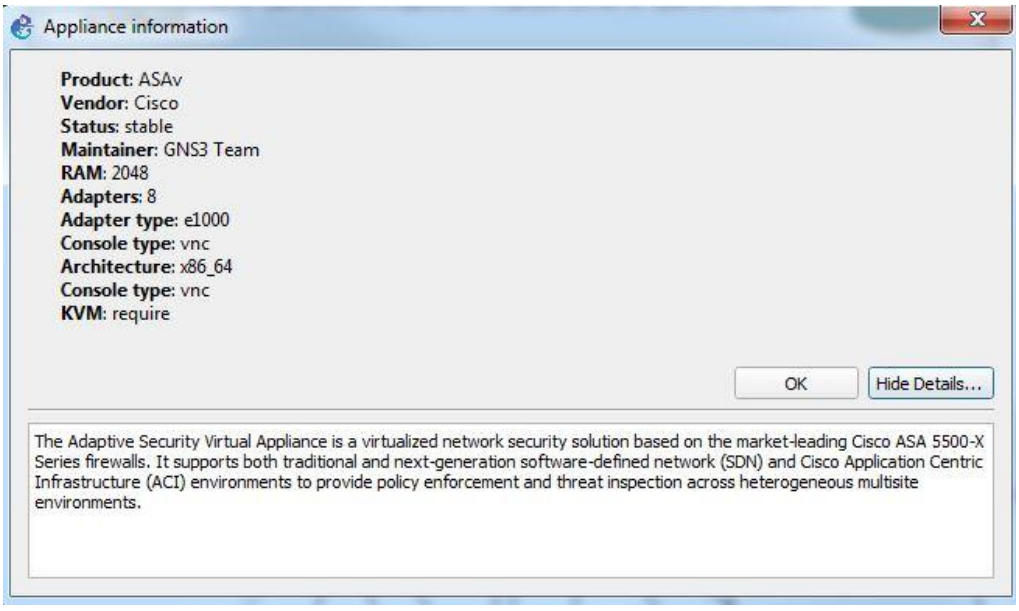
Επιλέγοντας το σύνδεσμο εμφανίζεται μια νέα σελίδα με μια περιγραφή του αρχείου και κουμπί λήψης. Ακολούθως εμφανίζει κριτικές και σχόλια των χρηστών. Μετά τη λήψη του αρχείου ο χρήστης το εισάγει στην εφαρμογή μέσω του μενού Αρχείο / Εισαγωγή Περιγραφή

4.1.5.2 Εισαγωγή των αρχείων εικόνας



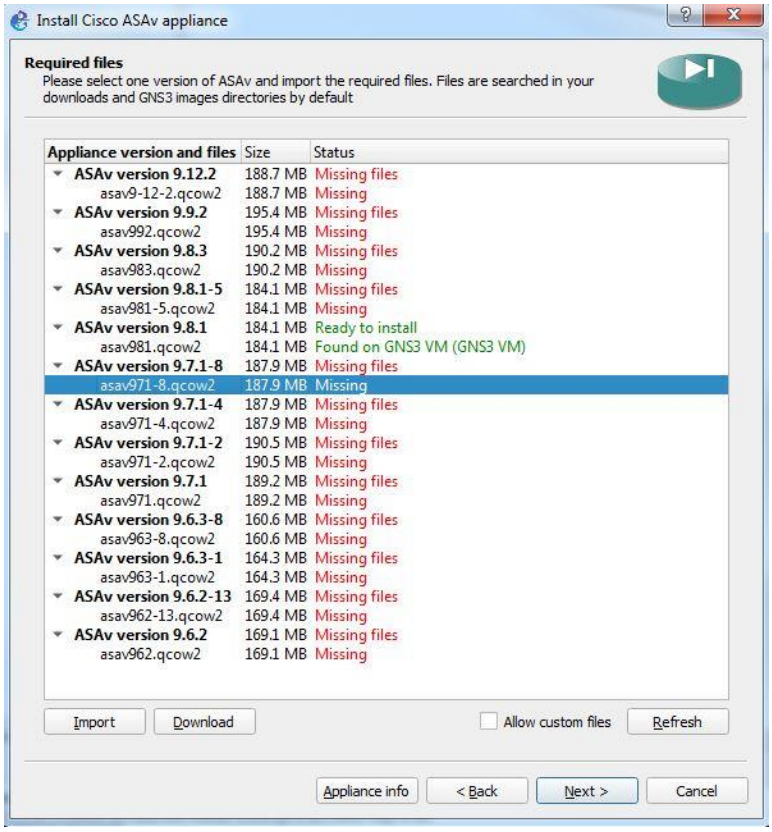
Εικόνα 21: Εισαγωγή αρχείου περιγραφής

Μόλις ο χρήστης επιλέξει το αρχείο για εισαγωγή η εφαρμογή εμφανίζει αυτό το παράθυρο που τον ενημερώνει ότι η συσκευή θα εισαχθεί στο GNSVM. Όλα τα αρχεία που υπάρχουν στον άνω ισότοπο προκειμένου να λειτουργήσουν θα πρέπει να εισαχθούν στην άνω εικονική μηχανή. Το κουμπί Πληροφορίες Περιγραφής εμφανίζει τις ιδιότητες του αρχείου.



Εικόνα 22: Πληροφορίες αρχείου περιγραφής

Το επόμενο βήμα είναι αυτό που θα εισάγει ο χρήστης το πραγματικό αρχείο εικόνας της συσκευής στην εφαρμογή. Η εφαρμογή διαβάζει το αρχείο περιγραφής και δημιουργεί τη συλλογή με τις διάφορες διαθέσιμες συσκευές, τα αρχεία τους και τις τοποθεσίες λήψης τους.



Εικόνα 23: Εισαγωγή αρχείου συσκευής

Από το παράθυρο αυτό θα επιλέξει ο χρήστης το αρχείο της συσκευής που επιθυμεί να εισάγει στην εφαρμογή. Στο παράδειγμα μας έχουμε ήδη εισάγει στην εφαρμογή το αρχείο εικόνας asav981 που εκτελείται μέσα στη σειρά ASA Firewall 5500 και για το λόγο αυτό αναγράφεται ως διαθέσιμο. Για να εισάγουμε κάποιο άλλο επιλέγουμε το αρχείο και πατάμε Λήψη και η εφαρμογή ανοίγει μια καρτέλα στο φυλλομετρητή μας και με τη χρήση των κωδικών μας έχουμε πρόσβαση στο αρχείο εικόνας.

Cisco ASAv 9.7.1-8

IMAGES REQUIRE

File	MD5	Size	
asav971-8.qcow2	b2486c8d0f6fda149ce877208b816818	197.0 MB	Download

Cisco ASAv 9.7.1-4

IMAGES REQUIRE

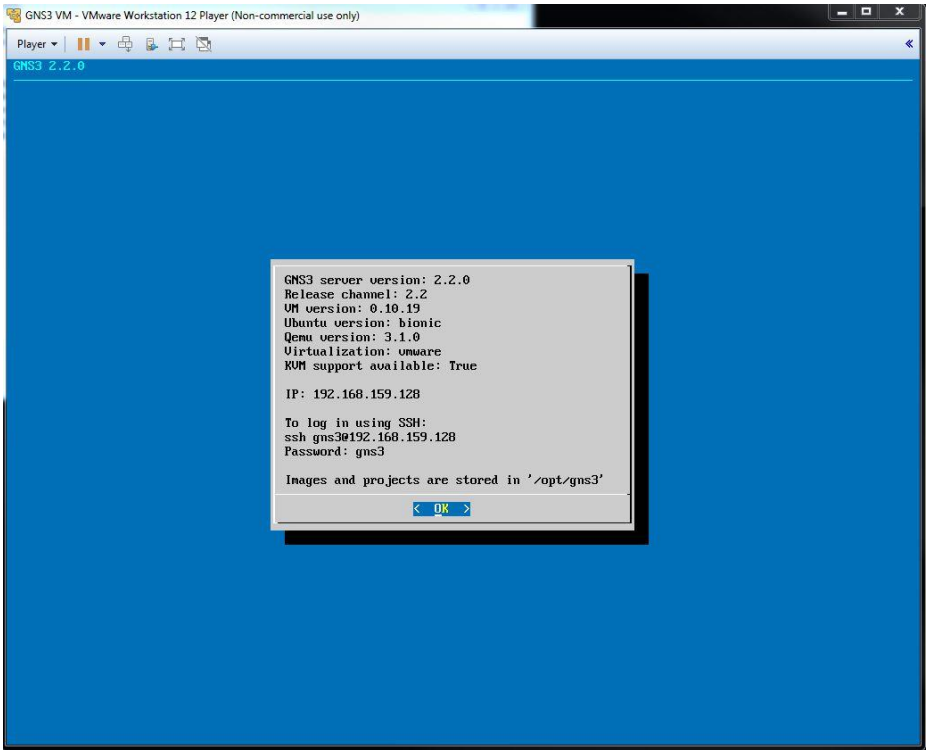
File	MD5	Size	
asav971-4.qcow2	f9a671d1ceaf983f7241f19df15e787f	197.0 MB	Download

Εικόνα 24: Λήψη των αρχείων εικόνας

Εναλλακτικά ο χρήστης μπορεί να επισκεφθεί τον ιστότοπο υποστήριξης της CISCO https://docs.gns3.com και με μια αναζήτηση με τον όρο cisco asa appliances εμφανίζεται η σελίδα με τις λεπτομέρειες εισαγωγής αρχείων καθώς και τα αρχεία.

Όταν η μεταφορά του αρχείου ολοκληρωθεί ο χρήστης επιλέγει το πλήκτρο εισαγωγή. Ακολούθως το αρχείο εισάγεται στην εικονική μηχανή και μετά από ένα χρονικό διάστημα, που εξαρτάται από το μέγεθος του αρχείου και τις δυνατότητες του υπολογιστή, το αρχείο είναι διαθέσιμο για εγκατάσταση. Στην περίπτωση που το αρχείο εικόνας είναι πολύ μεγάλο, όπως για παράδειγμα το αρχείο εικόνας ενός Windows 7 που ξεπερνά τα 11Gb, θα πρέπει να εισαχθεί στο GNS3 VM, μέσω εφαρμογής τύπου WINSCP στη διαδρομή που μας ορίζει, διαφορετικά μέσω της εφαρμογής η μεταφορά αποτυγχάνει.

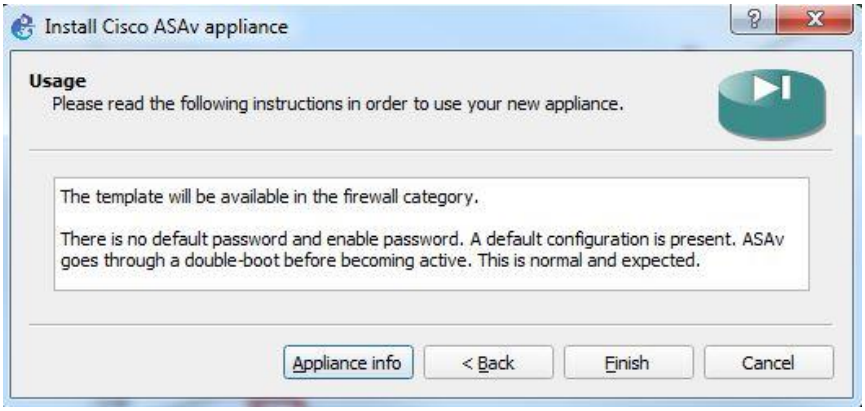
Στο δικό μας παράδειγμα για να συνδεθούμε στο GNS3 VM θα συνδεθούμε μέσω του WINSCP στη διεύθυνση 192.168.159.128 πόρτα 22 μέσω του πρωτοκόλλου SFTP με όνομα χρήστη gns3 και κωδικό ομοίως gns3 και θα μεταφέρουμε το αρχείο εικόνας στη διαδρομή /opt/gns3. Μετά την εισαγωγή του αρχείου αυτό θα εμφανίζεται στην εφαρμογή σαν έτοιμο προς εγκατάσταση. Τα στοιχεία αυτά μας τα δίνει το GNS3 VM.



Εικόνα 25: Στοιχεία του GNS3 VM

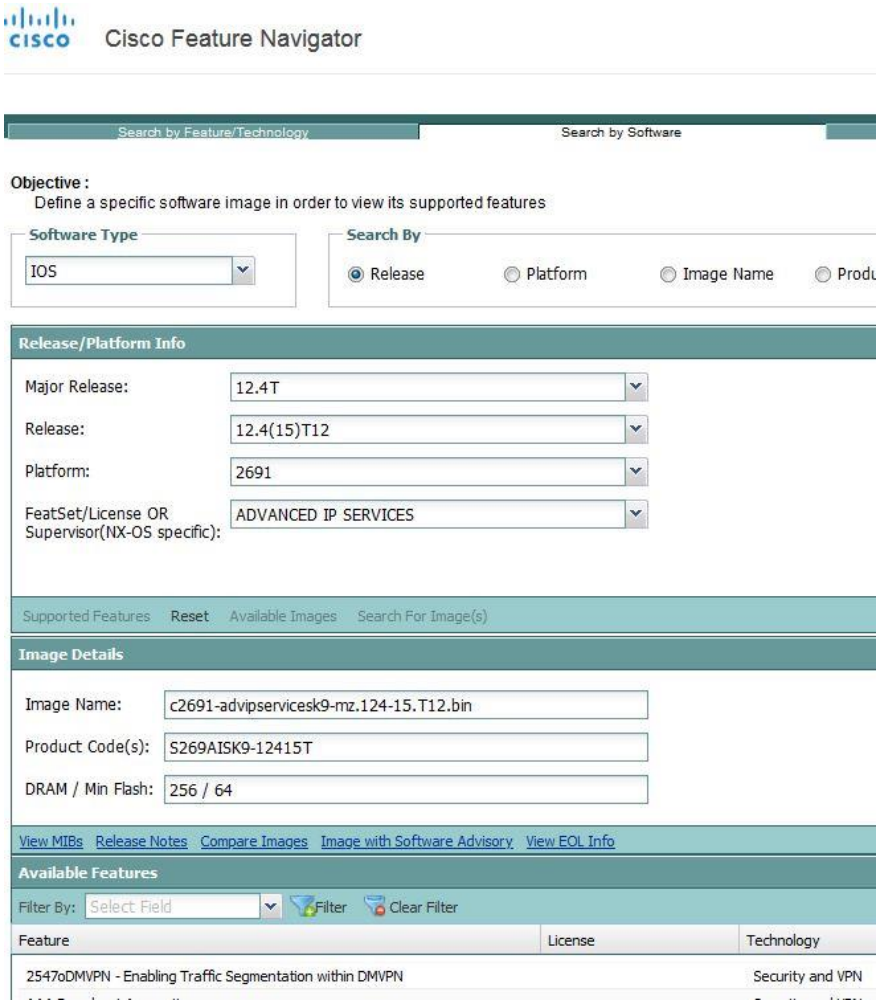
Αφού φορτωθεί το αρχείο εικόνας στην εφαρμογή και γίνει η εγκατάσταση, η εφαρμογή εμφανίζει τις απαραίτητες οδηγίες για τις λειτουργίες της συσκευής. Στο παράδειγμά μας η εφαρμογή μας ενημερώνει ότι η συσκευή διαθέτει μια παραμετροποίηση, για τη μη ύπαρξη κωδικού στη συσκευή μας ώστε να μπορέσουμε να συνδεθούμε και να τη λειτουργήσουμε και τέλος ότι πριν είναι έτοιμη για χρήση θα πρέπει να επανεκκινηθεί.

Τέλος η διαδικασία ολοκληρώνεται επιλέγοντας το πλήκτρο Ολοκλήρωση. Η εφαρμογή εμφανίζει ένα μήνυμα για την επιτυχή ολοκλήρωση της διαδικασίας ενημερώνοντας παράλληλα το χρήστη για το όνομα της συσκευής που μόλις έχει δημιουργηθεί.



Εικόνα 26: Λεπτομέρειες Συσκευής

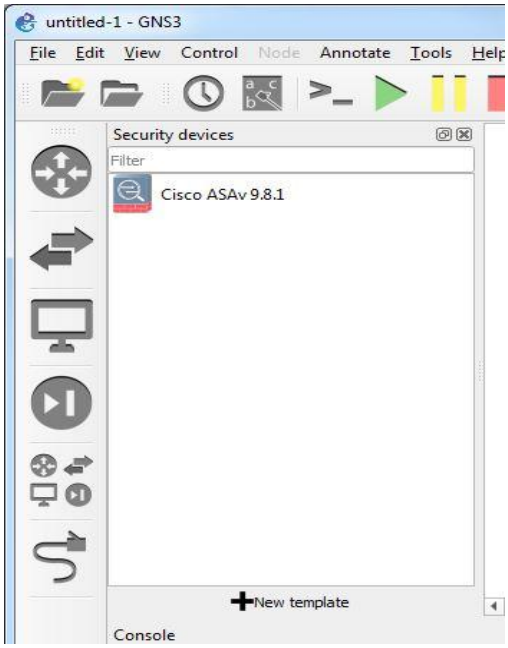
Στο σημείο αυτό αξίζει να αναφερθεί ότι η διαδικασία εισαγωγής δρομολογητή ενδέχεται να συμπεριλαμβάνει ένα επιπλέον βήμα στο οποίο ο χρήστης θα πρέπει να εισάγει κάποιες λεπτομέρειες στην εφαρμογή προκειμένου εκείνη να δημιουργήσει το κατάλληλο περιβάλλον για να λειτουργήσει η συσκευή. Μία από αυτές είναι το μέγεθος της μνήμης που θα πρέπει να διαθέσει στο δρομολογητή. Ο κατασκευαστής παρέχει τη λεπτομέρεια αυτή καθώς και άλλες στη διεύθυνση: https://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/SearchBySoftware.jsp όπου ο χρήστης μπορεί απλά να εισάγει το όνομα του αρχείου εικόνας που θα χρησιμοποιήσει και το σύστημα θα του δώσει τις απαραίτητες πληροφορίες. Ειδικότερα για τη μνήμη θα πρέπει ο χρήστης να δώσει την ελάχιστη δυνατή.



Εικόνα 27: Λεπτομέρειες αρχείου εικόνας

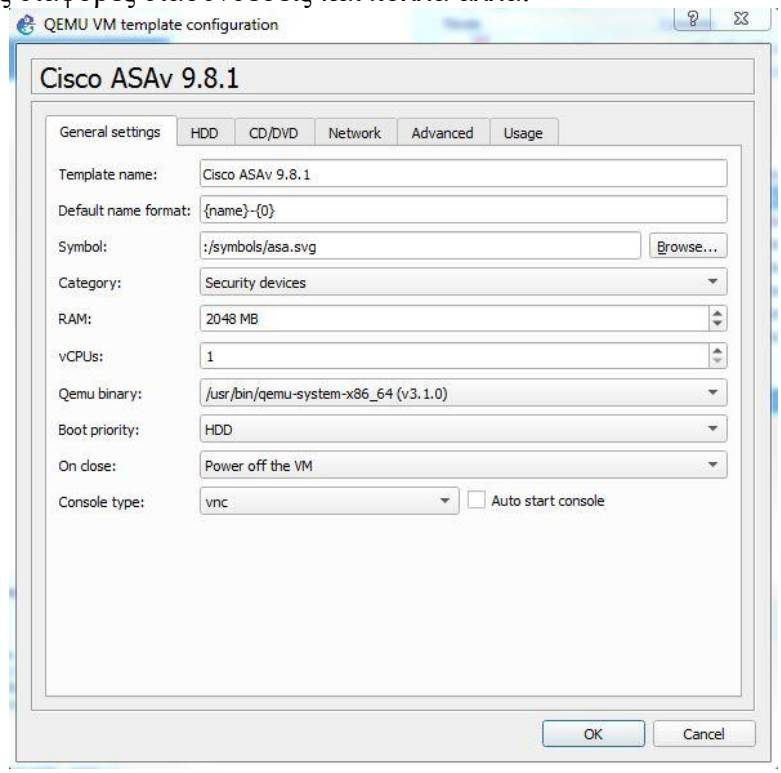
4.1.6 Χρήση συσκευής

Από τη στιγμή που η συσκευή έχει εισαχθεί θα είναι προσβάσιμη από το εικονίδιο της εφαρμογής. Στην περίπτωση του Firewall, όπως στο παράδειγμά μας, η συσκευή βρίσκεται στην ενότητα των συσκευών ασφαλείας.



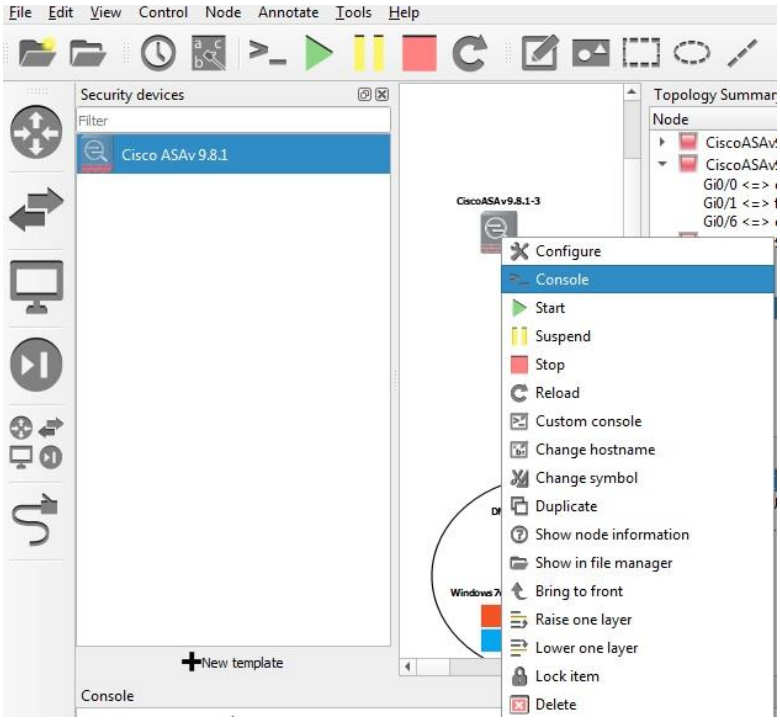
Εικόνα 28: Ο νέος Firewall έτοιμος προς χρήση

Κάνοντας δεξί κλικ πάνω στη συσκευή και επιλέγοντας παραμετροποίηση ο χρήστης μπορεί να παραμετροποιήσει διάφορες τιμές της συσκευής όπως το όνομα της, τη διαθέσιμή μνήμη της, το δίσκο, τις διάφορες διασυνδέσεις και πολλά άλλα.



Εικόνα 29:Παραμετροποίηση Συσκευής

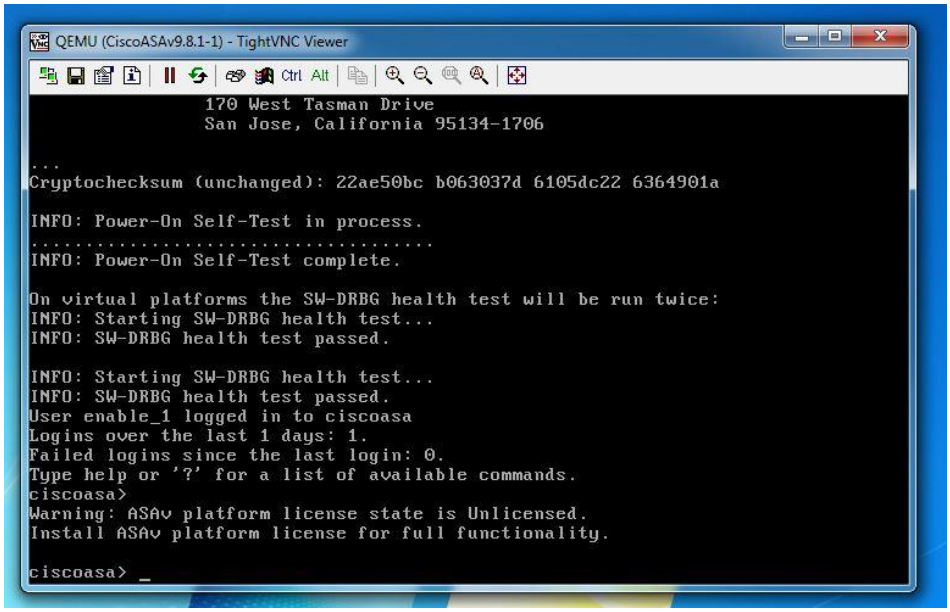
Προκειμένου να εισαχθεί σε μία διάταξη ο χρήστης θα τον επιλέξει, ακολούθως θα τον σύρει και θα τον αποθέσει στην επιφάνεια εργασίας. Η εφαρμογή θα τον εισάγει αυτόματα στον GSN3 VM εξυπηρετητή στην καρτέλα των εξυπηρετητών αλλά και στην καρτέλα της τοπολογίας. Στη συνέχεια ο χρήστης θα πρέπει να τον ενεργοποιήσει επιλέγοντας την εκκίνηση από την εργαλειοθήκη και αφού εκκινηθεί η συσκευή θα μπορεί να συνδεθεί μέσω παραθύρου κονσόλας κάνοντας δεξί κλικ πάνω της και επιλέγοντας Console από το αναδυόμενο μενού.



Εικόνα 30: Διαχείριση συσκευής

Από το μενού αυτό ο χρήστης έχει πρόσβαση σε πληθώρα επιλογών όπως η εκκίνηση της συσκευής, η παύση και ο τερματισμός της, η διαχείριση της, έναρξη παραθύρου κονσόλας και πολλά άλλα.

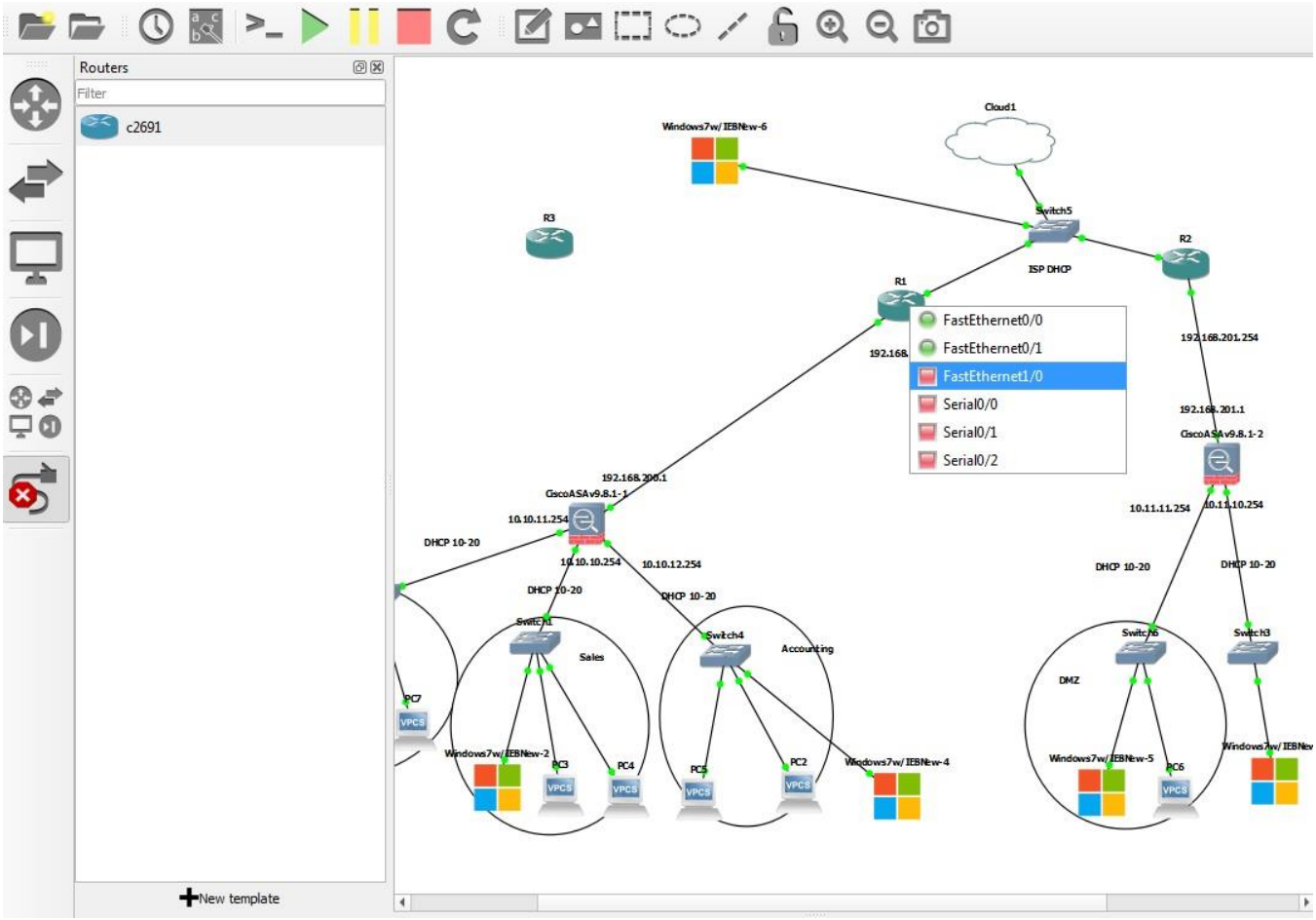
Επιλέγοντας την έναρξη του παραθύρου κονσόλας η εφαρμογή μας ανοίγει ένα παράθυρο κονσόλας μέσω της εφαρμογής VNC, όπως είναι προεπιλεγμένο στις ρυθμίσεις της συσκευής. Με τον τρόπο αυτό ο χρήστης εισάγει εντολές στη συσκευή όπως ακριβώς θα έκανε συνδεδεμένος μέσω καλωδίου σε ένα πραγματικό μηχάνημα.



Εικόνα 31: Παράθυρο κονσόλας στη συσκευή Firewall

4.1.6.1 Σύνδεση των συσκευών

Οι συσκευές, μετά τη μεταφορά και απόθεση στην επιφάνεια εργασίας της εφαρμογής θα πρέπει να συνδεθούν με καλώδιο προκειμένου να μπορέσουν να επικοινωνήσουν. Για να επιτύχει αυτό ο χρήστης επιλέγει από την εργαλειοθήκη των συσκευών το κουμπί Προσθήκη σύνδεσης με το καλώδιο και ο κέρσορας μετατρέπεται σε σταυρό αντί για το γνωστό δείκτη. Κάνοντας κλικ πάνω στη συσκευή που επιθυμεί να συνδέσει τη μία άκρη του καλωδίου, η εφαρμογή το ρωτά σε ποια διασύνδεση να συνδέσει το καλώδιο εμφανίζοντας το σύνολο των διασυνδέσεων που διαθέτει η συσκευή. Οι δεσμευμένες θύρες εμφανίζονται με πράσινο κύκλο ενώ οι ελεύθερες με κόκκινο τετράγωνο. Ο χρήστης θα πρέπει να επιλέξει μια ελεύθερη θύρα διαφορετικά η εφαρμογή τον ενημερώνει ότι η σύνδεση σε δεσμευμένη θύρα δεν είναι εφικτή.

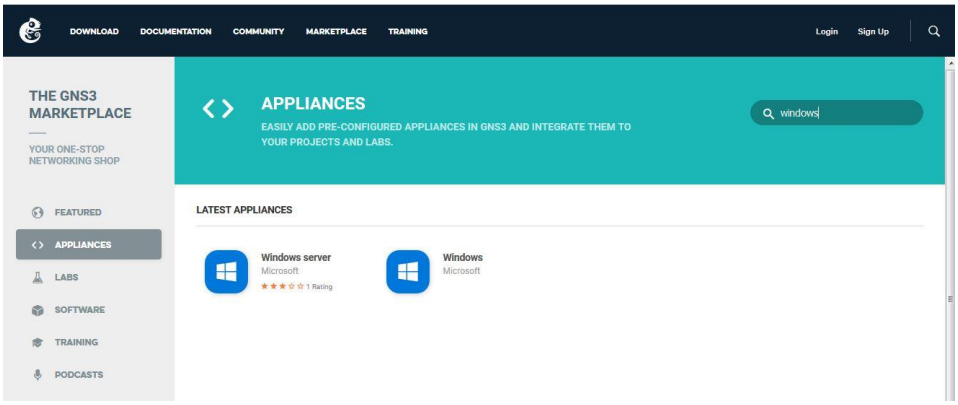


Εικόνα 32: Διασύνδεση συσκευής. Το εργαλείο Add a Link είναι ενεργοποιημένο και η εφαρμογή εμφανίζει τις διαθέσιμες για διασύνδεση θύρες.

4.1.7Windows 7 VM μέσα στο GNS3

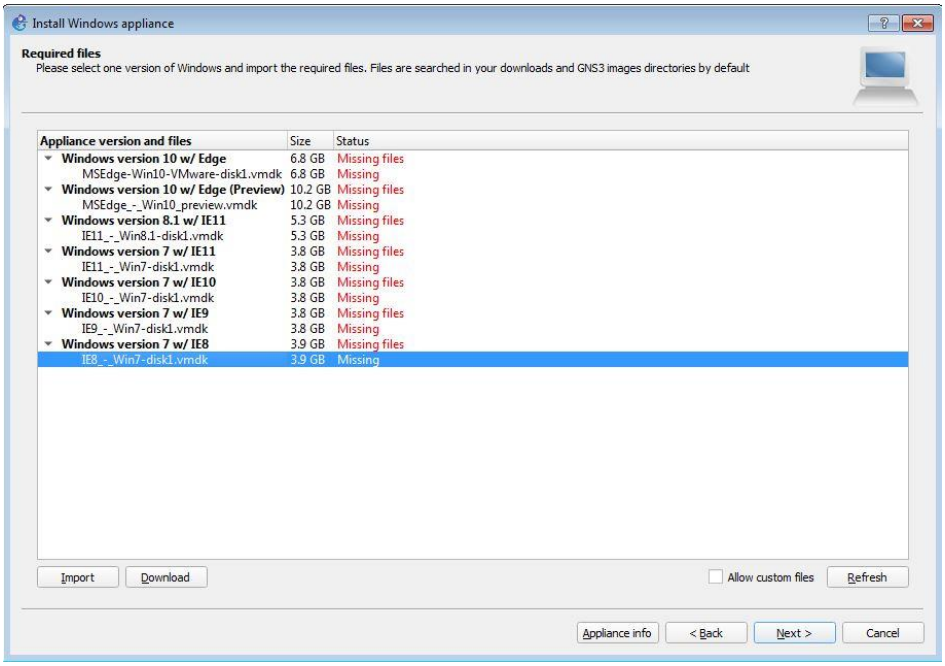
Οι υπολογιστές με λειτουργικό Windows είναι παρόντες σε κάθε υπολογιστικό σύστημα. Για το λόγο αυτό δε θα μπορούσαν να απουσιάζουν από μία διάταξη εντός του GNS3. Η εφαρμογή παρέχει τη δυνατότητα να εκτελέσει και άλλα λειτουργικά όπως Linux, η χρήση όμως των Windows είναι απαραίτητη και για την παραμετροποίηση του ASA Firewall, τμήμα της οποίας πραγματοποιείται μέσω του Internet Explorer και της Java.

Για τη δημιουργία ενός εικονικού υπολογιστή με λειτουργικό σύστημα απαιτείται η εισαγωγή ενός αρχείου περιγραφής και του αρχείου εικόνας του λειτουργικού, όπως περιγράψαμε παραπάνω. Για τα Windows 7, που θα χρησιμοποιήσουμε στο παράδειγμά μας, ο χρήστης θα κατεβάσει το αρχείο περιγραφής από τον ιστότοπο: https://gns3.com/marketplace/appliance αφού αναζητήσει με τη λέξη Windows.



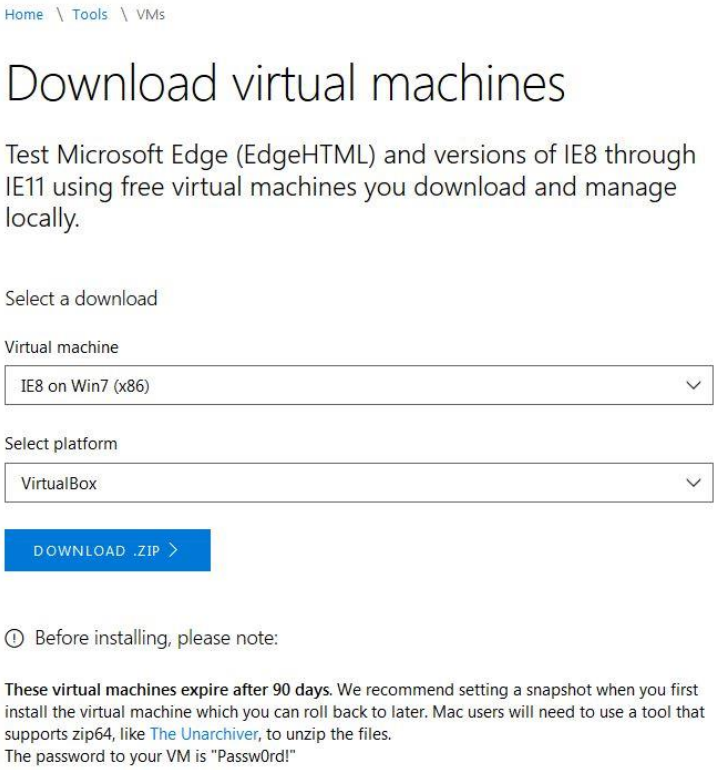
Εικόνα 33:Λήψη αρχείο περιγραφής Windows

Το αρχείο εικόνας θα το προμηθευτεί ο χρήστης από οποιονδήποτε μεταπωλητή του λειτουργικού. Εμείς, για τις ανάγκες της εργασίας, αρκεστήκαμε στις δοκιμαστικές εκδόσεις των λειτουργικών της Microsoft που θα είναι λειτουργικά για 90 μέρες από τη στιγμή της εγκατάστασης. Η διεύθυνση για τη λήψη του αρχείου δίνεται από το κουμπί Download του παραθύρου εισαγωγής του αρχείου περιγραφής.



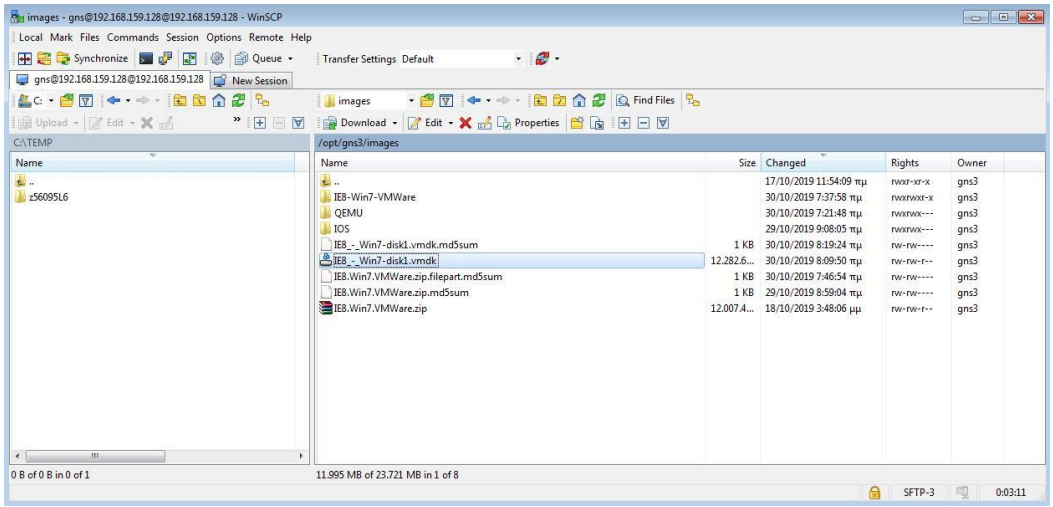
Εικόνα 34: Εισαγωγή αρχείου εικόνας Windows

Επιλέγοντας το λειτουργικό που μας ενδιαφέρει και πατώντας Λήψη η εφαρμογή ανοίγει μια καρτέλα στο φυλλομετρητή μας με τη διεύθυνση της Microsoft από την οποία ο χρήστης θα επιλέξει το λειτουργικό που τον ενδιαφέρει.



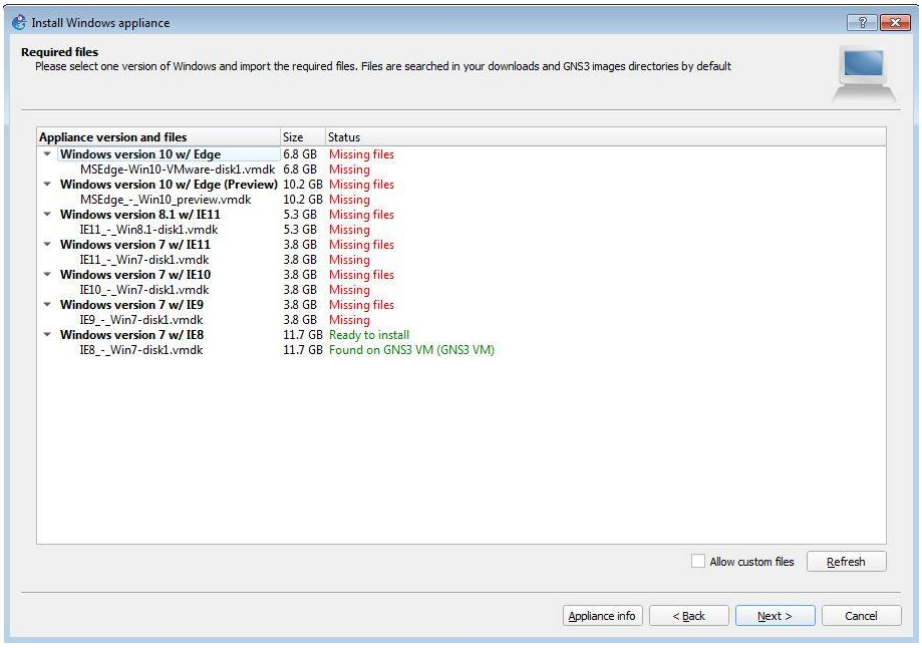
Εικόνα 35: Λήψη αρχείου εικόνας Windows

Το αρχείο αυτό θα πρέπει να εισαχθεί στο GNSVM μέσω εφαρμογής τύπου WINSCP μιας και η μεταφορά μέσω του κουμπιού Εισαγωγή αποτυγχάνει λόγω του μεγάλου μεγέθους του αρχείου. Στο παράδειγμα μας είναι 12Gb, οπότε ο χρήστης κάνει μια SFTP σύνδεση με την IP του μηχανήματος 192.168.159.128 δίνοντας ως όνομα χρήστη το gns3 και κωδικό το ίδιο και μεταφέρει το αποσυμπιεσμένο αρχείο στη διαδρομή /opt/gns3.



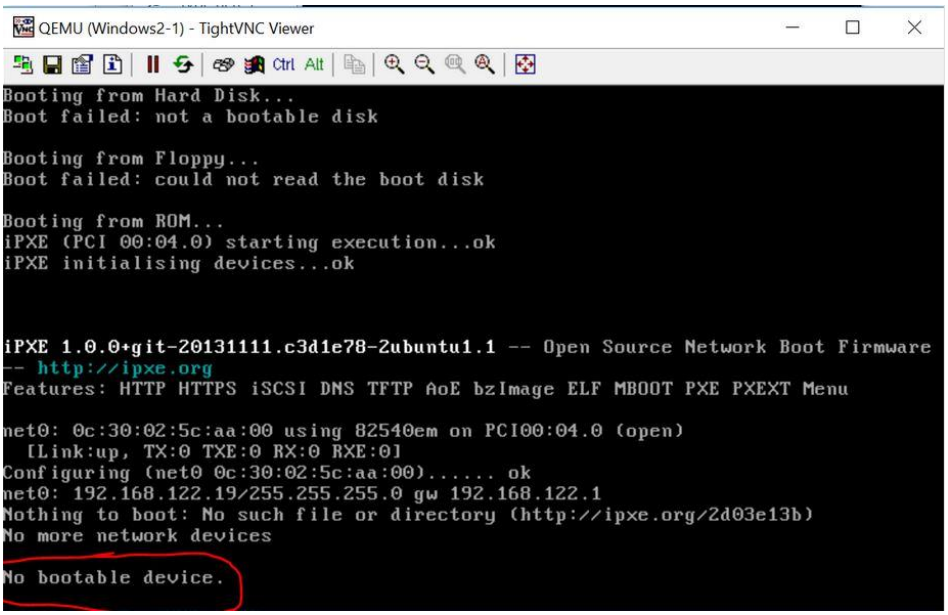
Εικόνα 36: Μεταφορά του αρχείου μέσω WINSCP

Μετά από την επιτυχημένη μεταφορά του αρχείου η εφαρμογή ενημερώνει το χρήστη ότι το λειτουργικό είναι διαθέσιμο και μπορεί να ολοκληρώσει την εγκατάστασή του.



Εικόνα 37: Το VM έτοιμο προς εγκατάσταση

Αν ο χρήστης προσπαθήσει να χρησιμοποιήσει το εικονικό αυτό μηχάνημα θα διαπιστώσει ότι δεν μπορεί να ξεκινήσει.

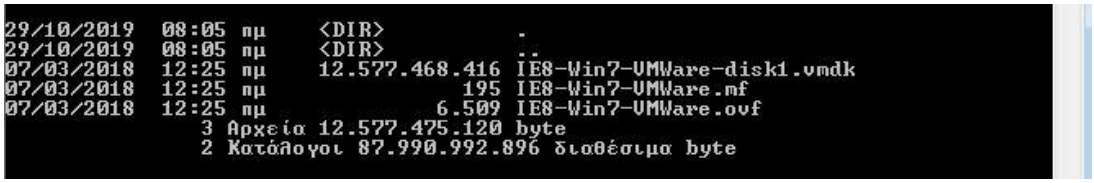


Εικόνα 38: Αδυναμία εκκίνησης μηχανής

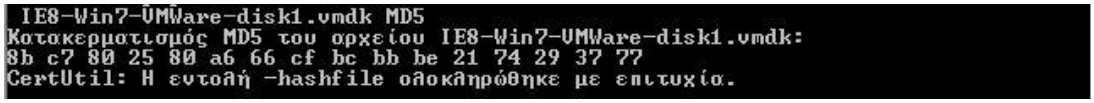
Ο λόγος που συμβαίνει αυτό είναι διότι τα αρχεία εικόνας της Microsoft αλλάζουν συχνά ενώ τα αρχεία περιγραφής τους δεν ενημερώνονται με τον ίδιο ρυθμό. Αποτέλεσμα αυτού είναι ενώ το αρχείο έχει πραγματικό μέγεθος 12Gb, το αρχείο περιγραφής το αναφέρει μόλις 3.9Gb και επίσης είναι και λάθος η τιμή MD5.

Για να διορθωθεί αυτό θα πρέπει ο χρήστης να ενημερώσει το αρχείο περιγραφής που κατέβασε από το ίντερνετ με τις σωστές τιμές. Το πραγματικό μέγεθος του αρχείου σε Windows 7 το βρίσκει κανείς εκτελώντας την εντολή DIR στη γραμμή εντολών στη θέση του αρχείο, ενώ την τιμή MD5 εκτελώντας certutil – hashfile ακολουθούμενο με το όνομα του

αρχείου και MD5. Στο παράδειγμά μας: certutil –hashfile IE8-Win7-VMWare-disk1.vmdk MD5



Εικόνα 39: Το πραγματικό μέγεθος του αρχείου

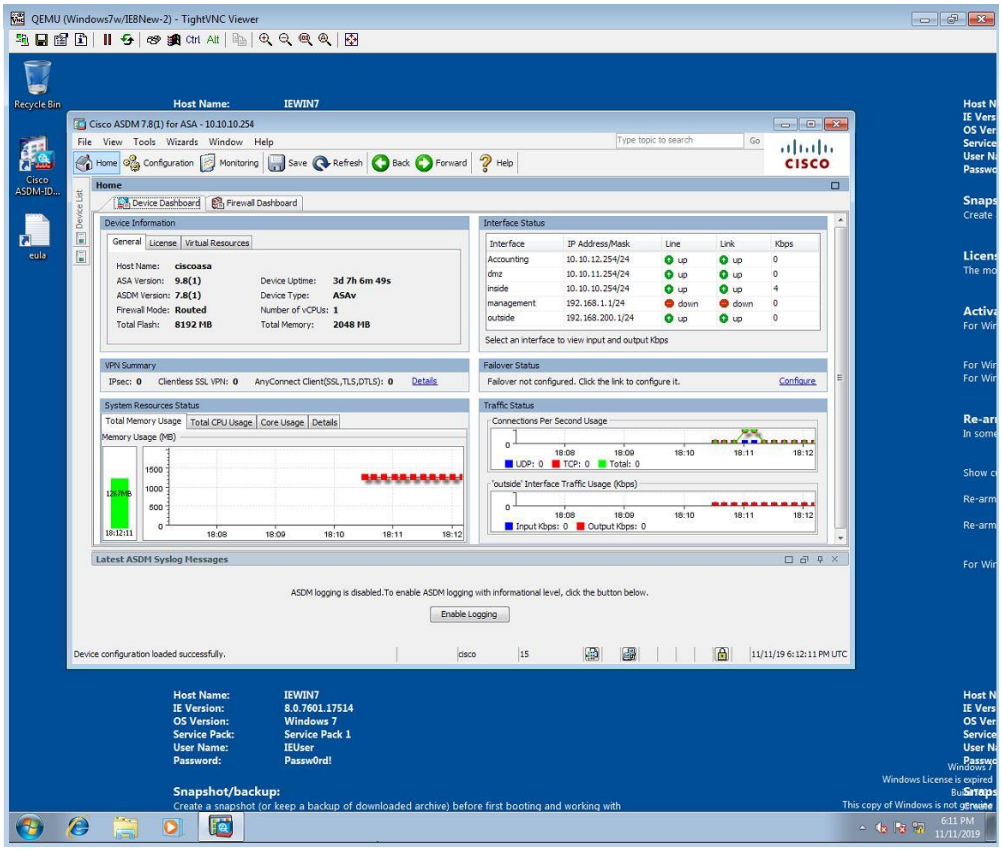


Εικόνα 40: Η τιμή MD5

Το τελευταίο βήμα είναι η ενημέρωση του αρχείου περιγραφής με τις σωστές τιμές. Αυτό θα πρέπει να ανοιχθεί με ένα πρόγραμμα επεξεργασίας κειμένου, όπως το Notepad++ και στο σημείο περιγραφής του δικού μας αρχείου να ενημερωθούν οι τιμές md5sum και filesize. Ακολούθως εισάγει το τροποποιημένο αρχείο περιγραφής στο GNS3 και στη συνέχεια το αρχείο εικόνας όπως περιγράψαμε παραπάνω.

Εικόνα 41: Ενημέρωση του αρχείου περιγραφής με τις σωστές τιμές

Πλέον ο χρήστης έχει εισάγει με επιτυχία ένα πραγματικό μηχάνημα που εκτελεί Windows 7 και μπορεί να αξιοποιήσει όλες τις δυνατότητες που του προσφέρει όπως ακριβώς ένα πραγματικό μηχάνημα.

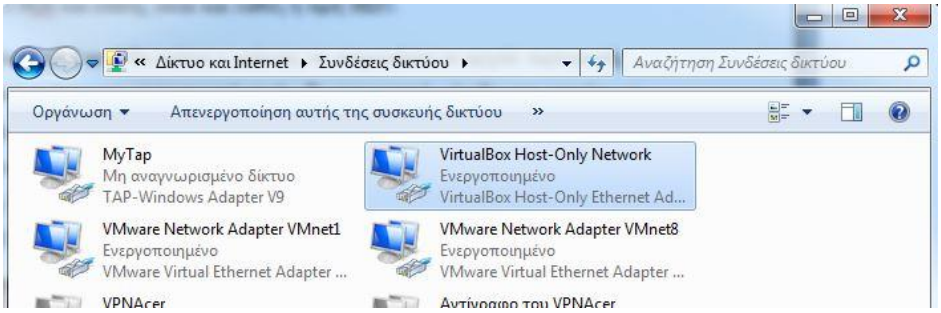


Εικόνα 42: Windows 7 με ASDM εντός του GNS3

4.1.8 Σύνδεση εξωτερικών μηχανών στο GNS3

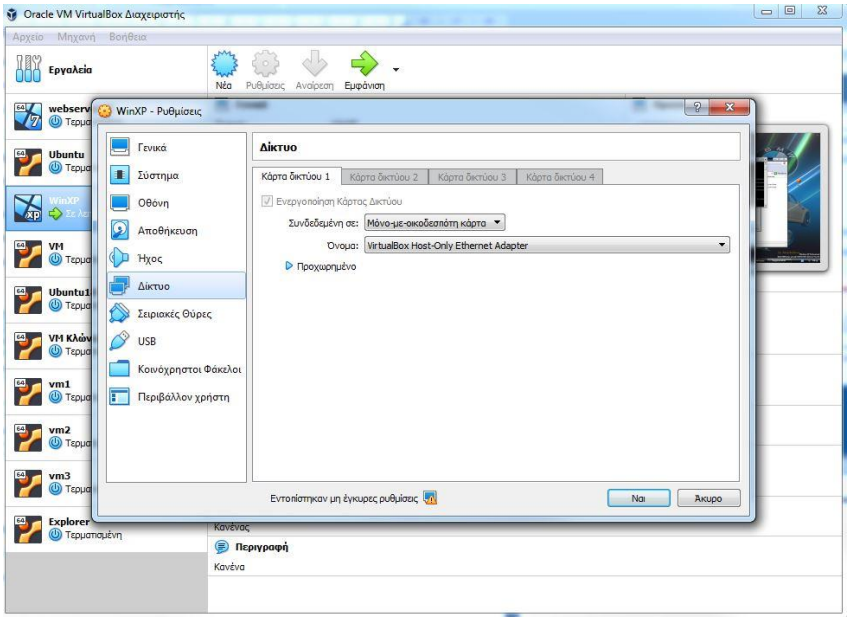
Τα εικονικά μηχανήματα που μας παρέχει το GNS3 και που εκτελούνται μέσα στο περιβάλλον του είναι αρκετά εξυπηρετικά πλην όμως υπόκεινται σε διάφορους περιορισμούς λόγω δικαιωμάτων αδειών χρήσης και γενικά παρουσιάζουν κάποιες δυσκολίες χρήσης. Για το λόγο αυτό συχνά δημιουργείται η ανάγκη να συνδέσουμε ήδη υπάρχοντα μηχανήματα είτε πραγματικά είτε εικονικά στο GNS3. Αυτό επιτυγχάνεται μέσω της συσκευής Cloud.

Στο παράδειγμά μας έχουμε δημιουργήσει ένα εικονικό μηχάνημα μέσω της εφαρμογής της Oracle το οποίο διαθέτει ένα εικονικό interface για να συνδέεται στο δίκτυο. Έτσι ο υπολογιστής μας στα διαθέσιμα interfaces παρουσιάζει και το εικονικό interface.



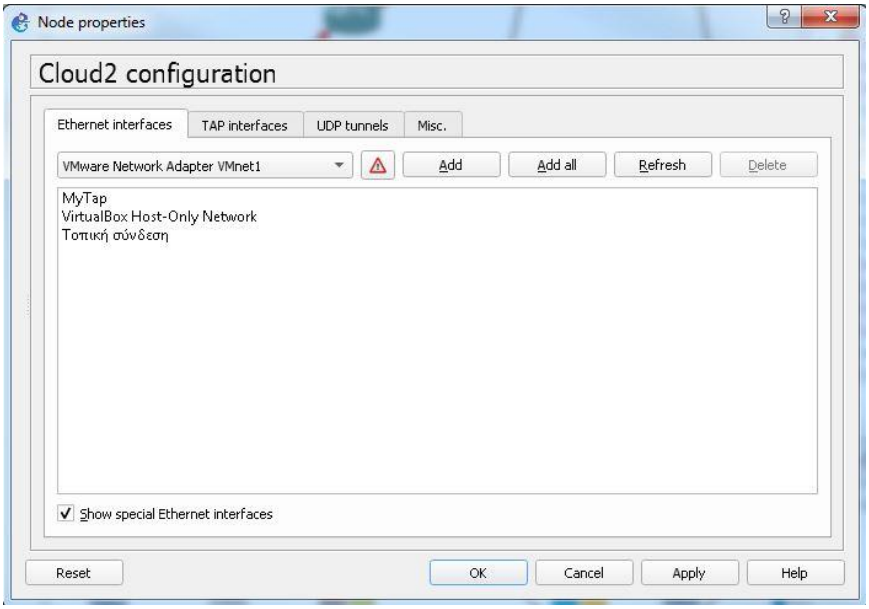
Εικόνα 43: Το εικονικό interface που θα συνδεθεί στο GNS3

Μετά τη δημιουργία του εικονικού αυτού interface, ο υπολογιστής θα πρέπει να επανεκκινηθεί ώστε να γίνει διαθέσιμο στο GNS3. Η εικονική μηχανή που θα το χρησιμοποιήσει θα πρέπει να είναι σε λειτουργία Οικοδεσπότη Μόνο (Host Only Adapter).



Εικόνα 44: Το interface θα πρέπει να είναι Host Only

Ακολούθως από το GNS3 επιλέγουμε το Cloud, κάνουμε δεξί κλικ πάνω του και επιλέγουμε Configure από το αναδυόμενο μενού.



Εικόνα 45: Εισαγωγή του Virtual Box interface στο GNS3

Προκειμένου να εμφανιστούν τα interfaces αυτά πρέπει να επιλέξουμε Show special Ethernet interfaces. Ακολούθως συνδέουμε το interface αυτό του Cloud σε όποιο σημείο της διάταξης μας επιθυμούμε.

Με τον τρόπο αυτό έχουμε το εικονικό μας μηχάνημα συνδεμένο σε όποιο σημείο της διάταξης επιθυμούμε. Το μηχάνημα αυτό δεν είναι υποχρεωτικό να είναι εικονικό. Θα μπορούσε να

είναι και φυσικό ή ακόμα και δίκτυο με την προσθήκη μιας επιπλέον φυσικής κάρτας δικτύου στον υπολογιστή μας.

4.2 Δρομολογητές

Στο παράδειγμά μας θα χρησιμοποιήσουμε ένα δρομολογητή της σειράς 2600 και συγκεκριμένα τον 2691 εφοδιασμένο με μια επιπλέον διασύνδεση Fast Ethernet, το module NM-1FE-TX.

Εικόνα 46: Ο δρομολογητής της διάταξής μας

Εικόνα 47: Το πρόσθετο NM-1FE-TX

Πρόκειται για έναν ιδιαιτέρως διαδεδομένο δρομολογητή που απευθύνεται τόσο σε μικρούς όσο και σε μεγάλους οργανισμούς και προσφέρει μεγάλη ποικιλία δυνατοτήτων. Μεταξύ των δυνατοτήτων διακρίνουμε την υποστήριξη VPN, τη δρομολόγηση με διαχείριση διαθέσιμου εύρους ζώνης, τη δρομολόγηση στο εσωτερικό εικονικό δίκτυο καθώς και τη μεγάλη ποικιλία πρόσθετων συσκευών που δύναται να δεχθεί, μέσω των οποίων μπορεί να αποκτήσει επιπλέον δυνατότητες, όπως το πρόσθετο που εμείς χρησιμοποιήσαμε για να αυξήσουμε τις διασυνδέσεις. Ο δρομολογητής διαθέτει δύο διασυνδέσεις Fast Ethernet και για το λόγο αυτό εμείς προσθέτουμε και το module για να τον εφοδιάσουμε με μία ακόμα. Άλλα διαθέσιμα modules του επιτρέπουν να αποκτήσει ιδιότητες μεταγωγέα (Switch) με 16 πόρτες, σύστημα εντοπισμού απειλών (IDS) καθώς και πολλά άλλα. [15] [16]

Εικόνα 48: Module για Switch 16 θυρών

Εικόνα 49: Module IDS

4.2.1 Παραμετροποίηση δρομολογητή

Στη διάταξή μας ο κάθε δρομολογητής συνδέεται με έναν ISP μέσω του εξωτερικού interface Fast Ethernet 0/0 από τον οποίο παίρνει αυτόματα διεύθυνση IP και εξυπηρετεί ένα εσωτερικό δίκτυο μέσω του εσωτερικού interface Fast Ethernet 0/1 με IP διεύθυνση 192.168.20X.254. Εκτελεί NAT ανάμεσα στο εξωτερικό και εσωτερικό δίκτυο και σαν προεπιλεγμένη πύλη έχει το εξωτερικό interface Fast Ethernet 0/0.

Για να ρυθμίσουμε το δρομολογητή μας επιλέγουμε το δρομολογητή, τον εκκινούμε και αφού ολοκληρωθεί η διαδικασία εκκίνησης κάνουμε δεξί κλικ πάνω του και από το αναδυόμενο μενού επιλέγουμε Console. Ακολούθως πληκτρολογούμε en και κατόπιν conf t για να μπούμε σε λειτουργία παραμετροποίησης.

Για να δώσουμε διεύθυνση IP σε κάποιο interface πληκτρολογούμε το όνομα του interface αρχικά : interface f0/0 και ακολούθως τη διεύθυνση ακολουθούμενη από τη μάσκα: ip address 192.168.200.254 255.255.255.0. Στην περίπτωση που θέλουμε η διεύθυνση να λαμβάνεται από DHCP Server η εντολή γίνεται ip address dhcp. Τέλος, πρέπει να ενεργοποιήσουμε το interface πληκτρολογώντας: no shut.

Η δρομολόγηση των πακέτων στη δική μας διάταξη διακρίνεται σε δύο κατηγορίες, το internet και το εσωτερικό δίκτυο του GNS3. Για να έχουν πρόσβαση οι συσκευές στο internet θα πρέπει να ορίσουμε στους δρομολογητές ότι η στάνταρ έξοδος των πακέτων θα είναι ο ISP και επειδή δε γνωρίζουμε τη διεύθυνση του, αλλά και για λόγους φορητότητας του παραγόμενου αρχείου του GNS3 θα δώσουμε το όνομα του εξωτερικού interface του δρομολογητή μας με την εντολή : ip route 0.0.0.0 0.0.0.0 f0/0.

Για την εσωτερική δρομολόγηση θα χρησιμοποιήσουμε το πρωτόκολλο RIP μιας και έχουμε μικρό αριθμό δρομολογητών χωρίς ιδιαίτερες διακυμάνσεις στο φόρτο εργασίας. Για την παραμετροποίησή του αρχικά το ενεργοποιούμε με την εντολή: router rip, και ακολούθως δηλώνουμε τα δίκτυα που ο δρομολογητής εξυπηρετεί κάθε ένα ξεχωριστά: network 192.168.200.0 για όλο το δίκτυο ήnetwork 10.10.0.1 για τη σύνδεση. Η παραμετροποίηση ολοκληρώνεται με την εντολή end. Η δρομολόγηση των πακέτων απαιτεί χρόνο μέχρι να ενημερώσουν όλοι οι δρομολογητές τους εσωτερικούς τους πίνακες δρομολόγησης και για το λόγο αυτό ενδεχομένως τα πρώτα πακέτα να απορριφθούν.

Τέλος, για την υπηρεσία NAT θα πρέπει να ονομάσουμε τα interfaces σε εσωτερικά και εξωτερικά για να γνωρίζει ο δρομολογητής πώς θα κάνει τη μετάφραση. Έτσι επιλέγουμε το εσωτερικό interface : interface f0/1, το ονομάζουμε : ip nat inside και με τον ίδιο τρόπο ονομάζουμε και το εξωτερικό: ip nat outside. Ακολούθως θα πρέπει να φτιάξουμε μια λίστα πρόσβασης ACL που να επιτρέπει την κίνηση: access-list 1 permit any και τέλος να ενεργοποιήσουμε τη μετάφραση: ip nat inside source list 1 interface f0/0 overload.

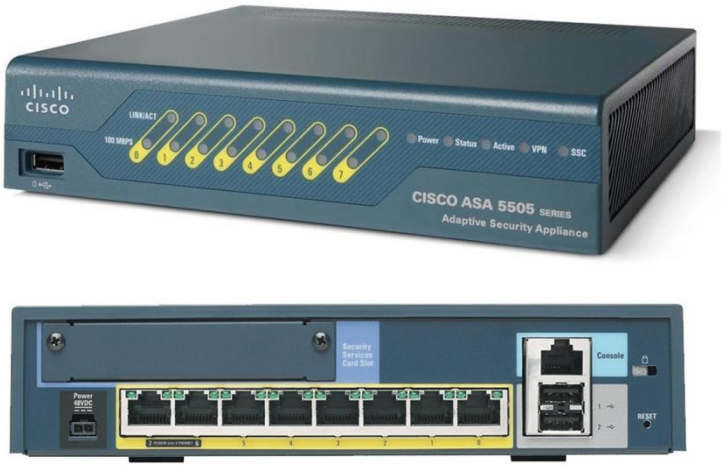
Μετά το τέλος της κάθε παραμετροποίησης οι ρυθμίσεις θα πρέπει να αποθηκευτούν. Αυτό επιτυγχάνεται πληκτρολογώντας την εντολή: wr. Ο δρομολογητής τώρα είναι έτοιμος. Αφού δοκιμαστεί στο ασφαλές περιβάλλον του GNS3 μπορεί να μεταφερθεί το αρχείο με τις ρυθμίσεις του σε έναν πραγματικό δρομολογητή.

4.3 Τοίχος προστασίας Cisco ASA

Το αρχείο που θα χρησιμοποιήσουμε στην εργασία αυτή είναι το ASAV9.8.1-1. Είναι το αρχείο που εκτελείται σε μία από τις πιο διαδεδομένες σειρές συσκευών τοίχους προστασίας που προσφέρει η εταιρία που απευθύνονται σε ιδιαίτερα ευρύ κοινό και προσφέρουν μεγάλη ποικιλία δυνατοτήτων.[14]

Εικόνα 50: Η σειρά 5500 που εκτελεί το αρχείο της διάταξης μας

Από τη σειρά εμείς θα αξιοποιήσουμε τον 5505, το μικρότερο της σειράς μιας και είναι ο πλέον κατάλληλος για τη διάταξή μας. Είναι εφοδιασμένος με 2048Mb Ram και 8 interfaces Fast Ethernet και παρέχει μεγάλη ποικιλία υπηρεσιών όπως VLAN's, DMZ, VPN και πολλά άλλα.



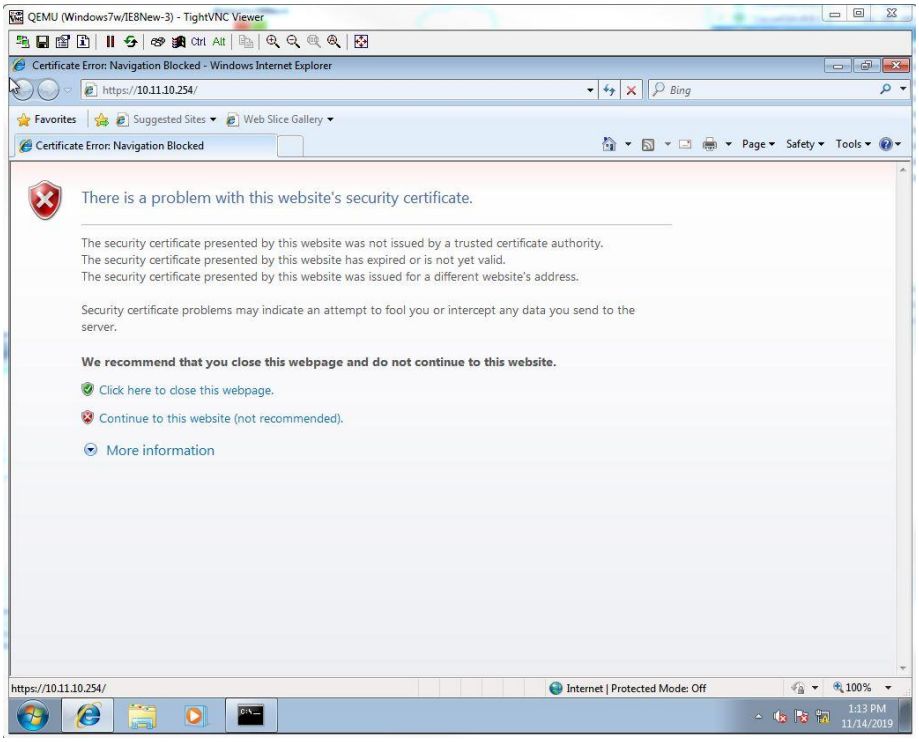
Εικόνα 51: Ο Firewall της διάταξής μας

4.3.1 Παραμετροποίηση τοίχους προστασίας

Η παραμετροποίηση χωρίζεται σε δύο βασικές κατηγορίες όπου η πρώτη γίνεται μέσω κονσόλας και η δεύτερη μέσω της Java εφαρμογής ASDM που εγκαθίσταται τοπικά σε υπολογιστή του διαχειριστή δικτύου και προσφέρει ένα λειτουργικό περιβάλλον για την παραμετροποίηση της συσκευής. Πρώτα θα πρέπει να ολοκληρωθεί η πρώτη που θα δημιουργήσει ο χρήστης και θα δοθεί η διεύθυνση IP της συσκευής ώστε να μπορέσει να συνδεθεί η Client εφαρμογή στη συσκευή.

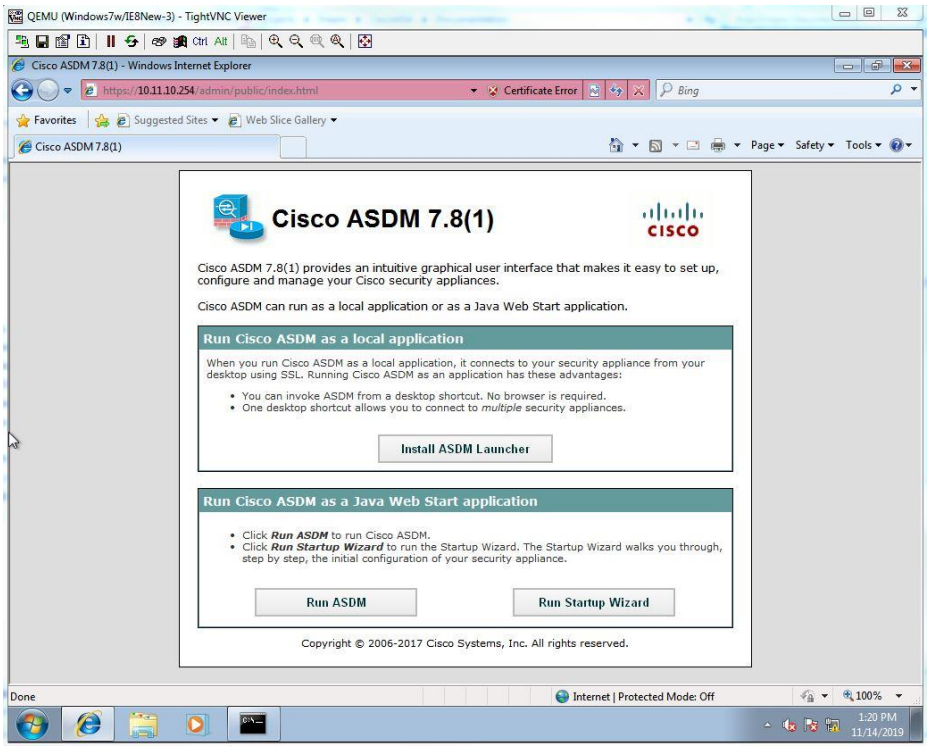
Πρώτο βήμα, μετά την τοποθέτηση της συσκευής στο χώρο εργασίας του GNS3 και κατάλληλη σύνδεσή της με καλώδια, είναι η ενεργοποίηση της. Μόλις η συσκευή γίνει διαθέσιμη κάνοντας δεξί κλικ πάνω της και επιλέγοντας Console ανοίγει το παράθυρο κονσόλας μέσω του οποίου διαβιβάζονται εντολές στη συσκευή. Φέρνουμε τη συσκευή σε κατάσταση παραμετροποίησης πληκτρολογώντας en και ακολούθως conf t και στη συνέχεια δίνουμε διευθύνσεις IP στα interfaces πληκτρολογώντας το όνομα του interface: int g0/0 για το interface Gigabit Ethernet 0/0 και ακολούθως την εντολή ip address ακολουθούμενη με τη διεύθυνση IP και ακολούθως τη μάσκα. Στη συνέχεια ονομάζουμε το interface σαν inside ή outside με την εντολή g0/0 outside για το εξωτερικό Gigabit Ethernet 0/0 ώστε να γνωρίζει ο Firewall πώς θα διαχειριστεί την κίνηση. Στο σημείο αυτό αξίζει να σημειωθεί ο τρόπος με τον οποίο ο Firewall διαχειρίζεται την κίνηση. Τα εσωτερικά interfaces που είναι ‘έμπιστα’ έχουν τιμή 100 ενώ τα εξωτερικά που δεν είναι ‘έμπιστα’ έχουν τιμή 0. Τα ενδιάμεσα, όπως το DMZ έχουν τιμή 50. Οπότε χαρακτηρίζοντας τα interfaces σαν εσωτερικά ο Firewall τα θεωρεί έμπιστα δίδοντας τους την τιμή 100. Επόμενο βήμα είναι η δημιουργία χρήστη διαχειριστή με την εντολή username όνομα χρήστη password κωδικός privilege 15 και τέλος η ενεργοποίηση του webserver στον οποίο συνδέεται η client εφαρμογή. Αυτό γίνεται με την εντολή http server enable και ακολούθως το interface που θα ακούει και τα δικαιώματα http 0 0 inside. Η διαδικασία ολοκληρώνεται με την αποθήκευση των αλλαγών μέσω της wr. Αποτελεί πάγια τακτική της Cisco το αρχείο configuration να ‘ζει’ στη μνήμη της συσκευής και για να περαστεί στο δίσκο της απαιτείται η εντολή write η wr για συντόμευση. Αν δεν αποθηκευτεί στο δίσκο της συσκευής δεν θα υπάρχει μετά από μια επανεκκίνηση.

Αφού ολοκληρωθεί το βασικό configuration της συσκευής ακολουθεί η εγκατάσταση της ASDM εφαρμογής η οποία γίνεται μέσω του φυλλομετρητή Internet Explorer. Μπορούν να χρησιμοποιηθούν και άλλοι φυλλομετρητές αλλά ο Internet Explorer είναι ο πλέον συμβατός. Για να συνδεθούμε με τη συσκευή απαιτείται το πρωτόκολλο HTTPS και κατόπιν η IP διεύθυνση του interface πάνω στο οποίο συνδέεται ο υπολογιστής. Μόλις πληκτρολογήσουμε τη διεύθυνση ο Internet Explorer μας ενημερώνει ότι το πιστοποιητικό δεν είναι ασφαλές. Αυτό συμβαίνει διότι η Cisco υπογράφει η ίδια τα πιστοποιητικά της και δεν απευθύνεται σε κάποια αναγνωρισμένη αρχή πιστοποίησης. Ο χρήστης θα πρέπει να επιλέξει Συνέχεια στον Ιστότοπο.



Εικόνα 52: Ο Internet Explorer ενημερώνει το χρήστη περί μη έμπιστου πιστοποιητικού

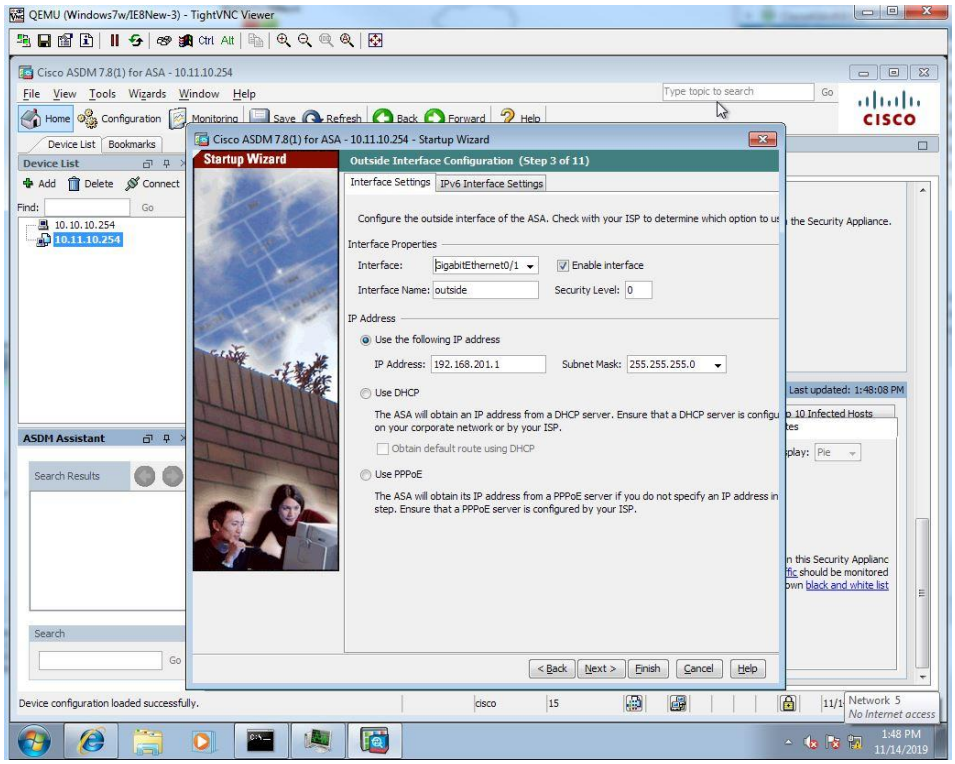
Μόλις ο χρήστης επιλέξει τη συνέχεια η συσκευή εμφανίζει την επόμενη σελίδα.



Αν στον υπολογιστή δεν υπάρχει η Java η εφαρμογή θα ζητήσει από το χρήστη να την εγκαταστήσει και ακολούθως θα πρέπει να επισκεφθεί εκ νέου τον ιστότοπο. Ακολούθως επιλέγει το Install ASDM Launcher που θα εγκαταστήσει την εφαρμογή. Μετά την επιτυχή εγκατάσταση εκτελεί την εφαρμογή κάνοντας διπλό κλικ στη συντόμευσή της στην επιφάνεια εργασίας και η εφαρμογή ξεκινά.

Εικόνα 53: Εκκίνηση της εφαρμογής ASDM

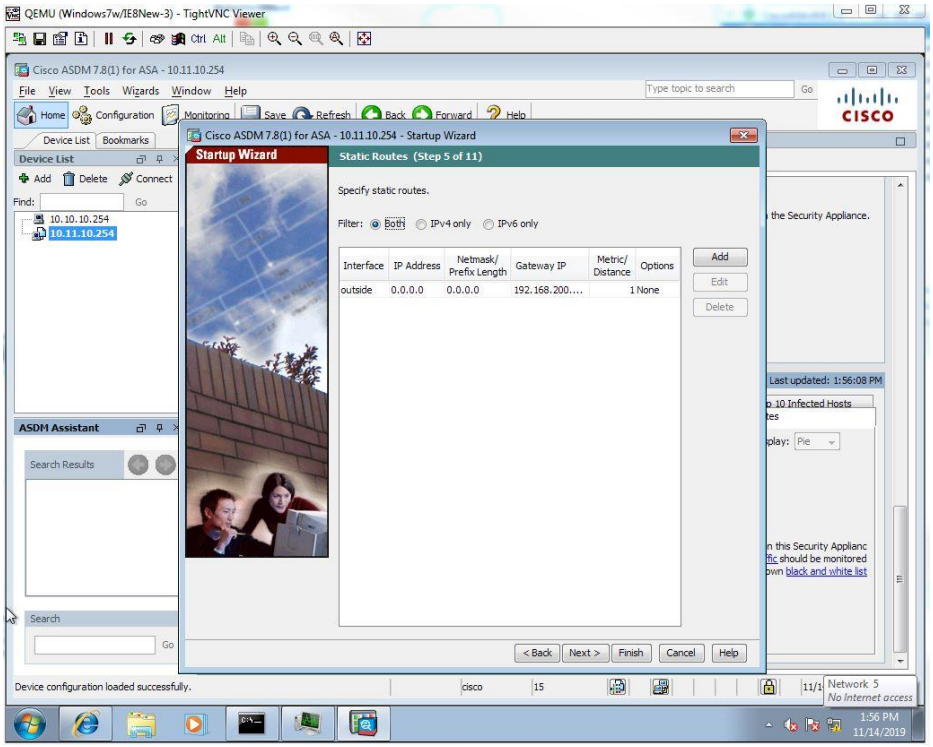
Για την είσοδο ο χρήστης εισάγει τα στοιχεία που έδωσε στην πρώτη φάση της παραμετροποίησης και ακολούθως ξεκινά τον οδηγό παραμετροποίησης ο οποίος θα τον καθοδηγήσει για την πρώτη και βασική παραμετροποίηση της συσκευής. Η πρώτη ρύθμιση αφορά τη φόρτωση της βασικής παραμετροποίησης και στη συνέχεια του ονόματος.



Εικόνα 54: Ρύθμιση των Interfaces

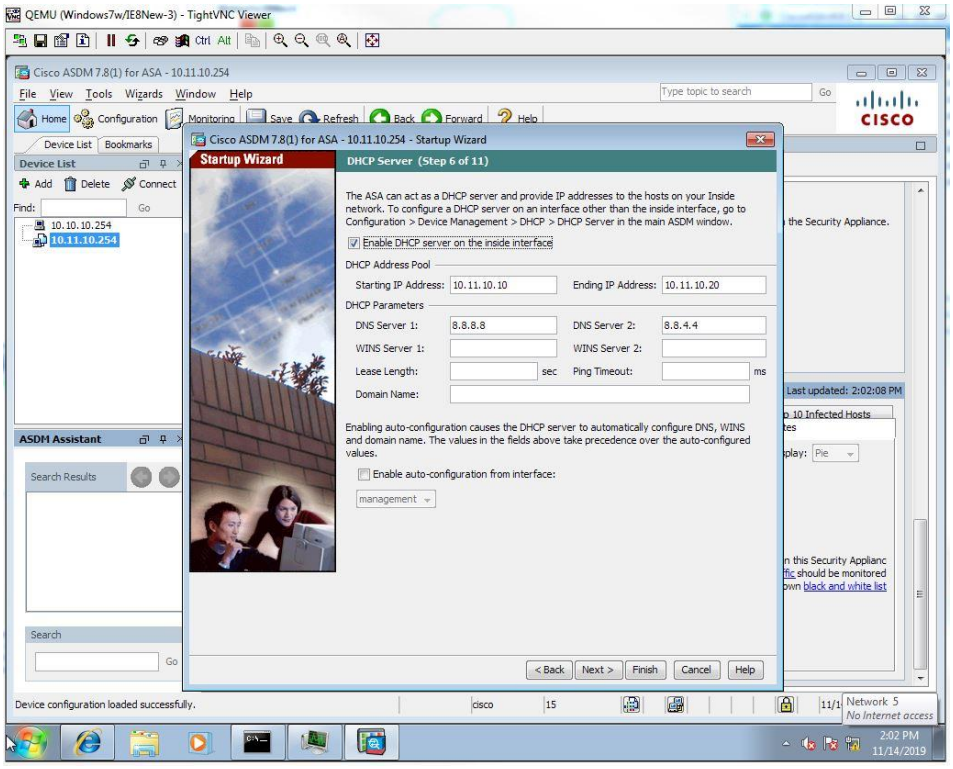
Από το παράθυρο αυτό θα δώσει διευθύνσεις στα interfaces, θα ορίσει το επίπεδο ασφάλειας και θα τα ονομάσει όπως θα έκανε μέσω κονσόλας.

Ακολουθεί η δήλωση των στατικών οδηγιών δρομολόγησης.



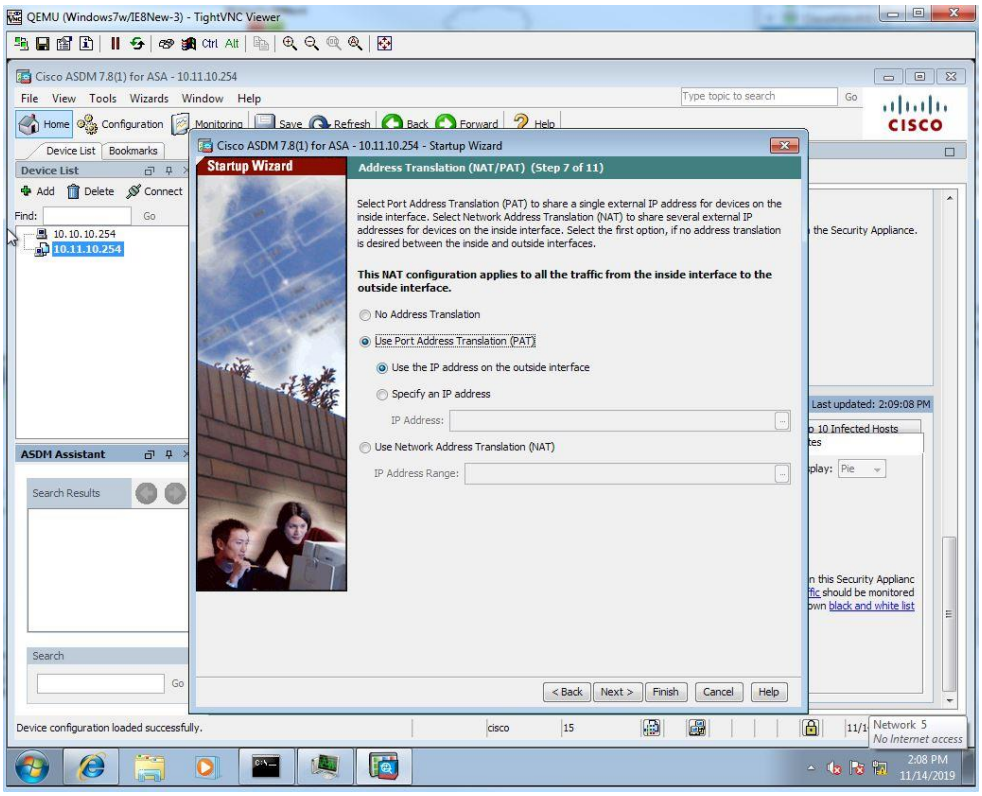
Εικόνα 55: Δήλωση στατικών διαδρομών

Ακολούθως η υπηρεσία DHCP του Firewall. Εμείς θα ενεργοποιήσουμε την υπηρεσία ανά εσωτερικό interface στα VLANS που θα φτιάξουμε. Εδώ ενεργοποιούμε για το inside και του δηλώνουμε να δίνει διευθύνσεις από το 10.11.10.10 έως το 10.11.10.20 με DNS τη Google.

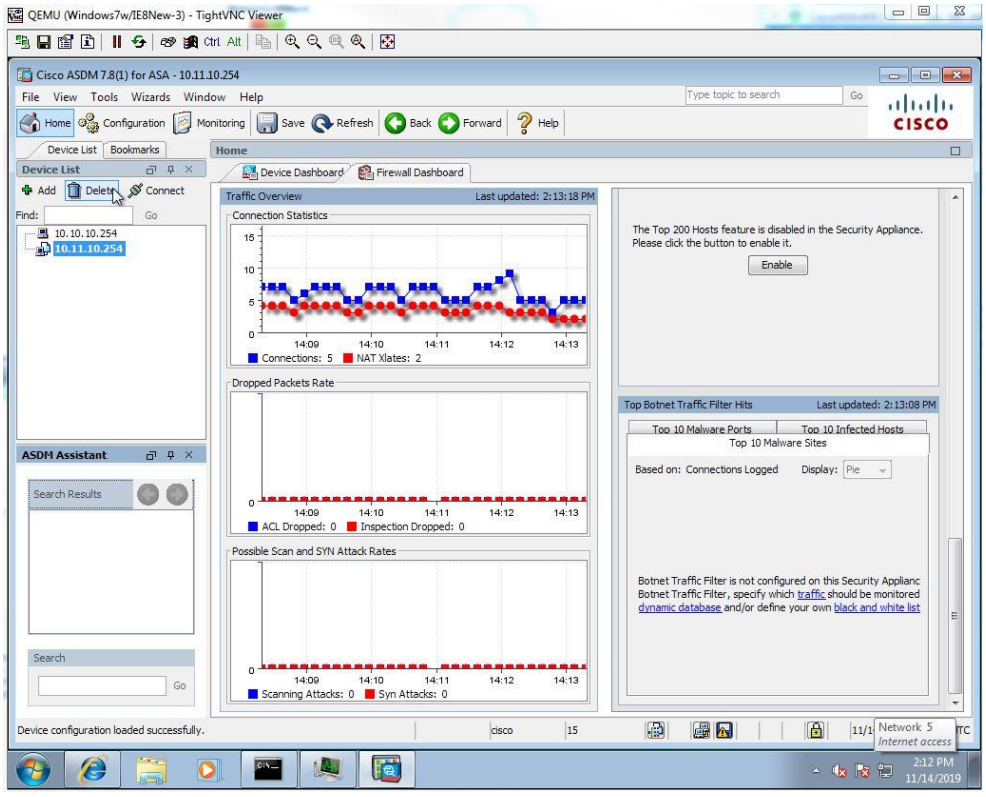


Εικόνα 56: DHCP Server στο Inside interface

Ακολουθεί η ρύθμιση για το Nat όπου για τη μετάφραση θα χρησιμοποιείται η διεύθυνση του εξωτερικού interface. Με το βήμα αυτό ολοκληρώνεται η βασική παραμετροποίηση της συσκευής. Ο υπολογιστής παραλαμβάνει IP διεύθυνση και έχει πρόσβαση στο internet.



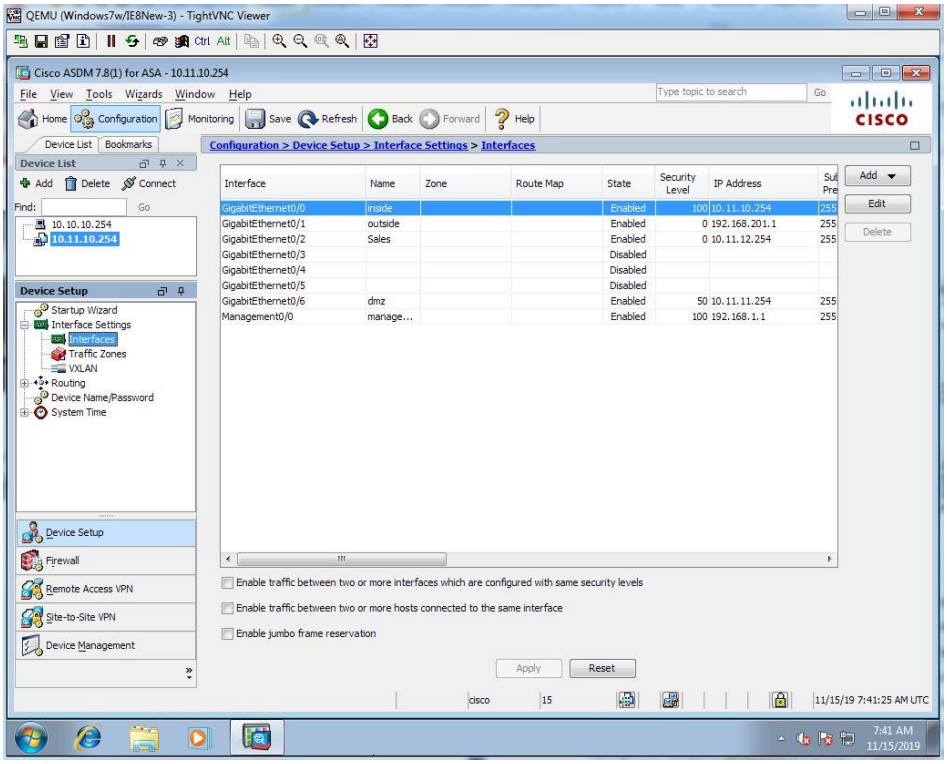
Εικόνα 57: Nat παραμετροποίηση



Εικόνα 58: Ολοκλήρωση του οδηγού. Ο υπολογιστής έχει πλέον πρόσβαση στο Internet

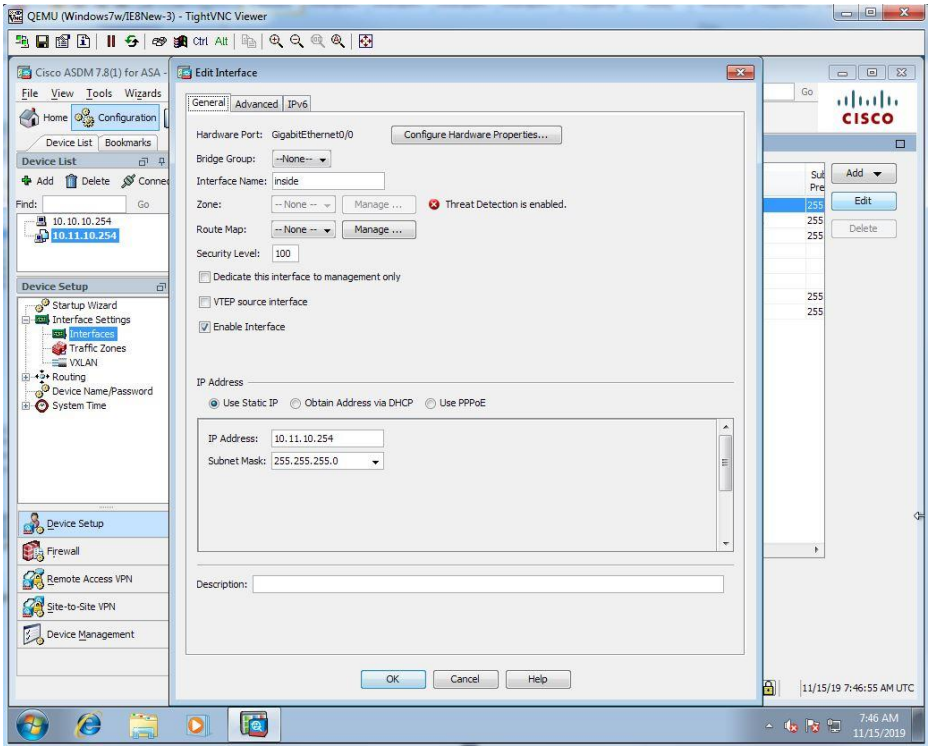
4.3.2 Δημιουργία VLANS

Σε κάθε οργανισμό υπάρχουν διαφορετικά τμήματα τα οποία θα πρέπει να λειτουργούν ανεξάρτητα. Για το λόγο αυτό θα πρέπει να συνδέονται σε διαφορετικά δίκτυα. Ο Firewall της διάταξης μας, μας παρέχει τη δυνατότητα αυτή, αφού μπορούμε να ρυθμίσουμε κάθε Interface, να ανήκει σε δικό του δίκτυο. Με τον τρόπο αυτό μπορούμε να πούμε ότι το interface G0/6 ανήκει στο DMZ ενώ το G0/2 στο τμήμα πωλήσεων. Τα interfaces αυτά παρέχουν IP διευθυνσιοδότηση για το σύνολο των υπολογιστών που εξυπηρετούν και μέσω μεταγωγέα μπορούμε να αυξήσουμε τον αριθμό των θυρών. Η παραμετροποίηση αυτή γίνεται μέσω του Configuration.



Εικόνα 59: Τα διαθέσιμα interfaces με τις παραμέτρους τους

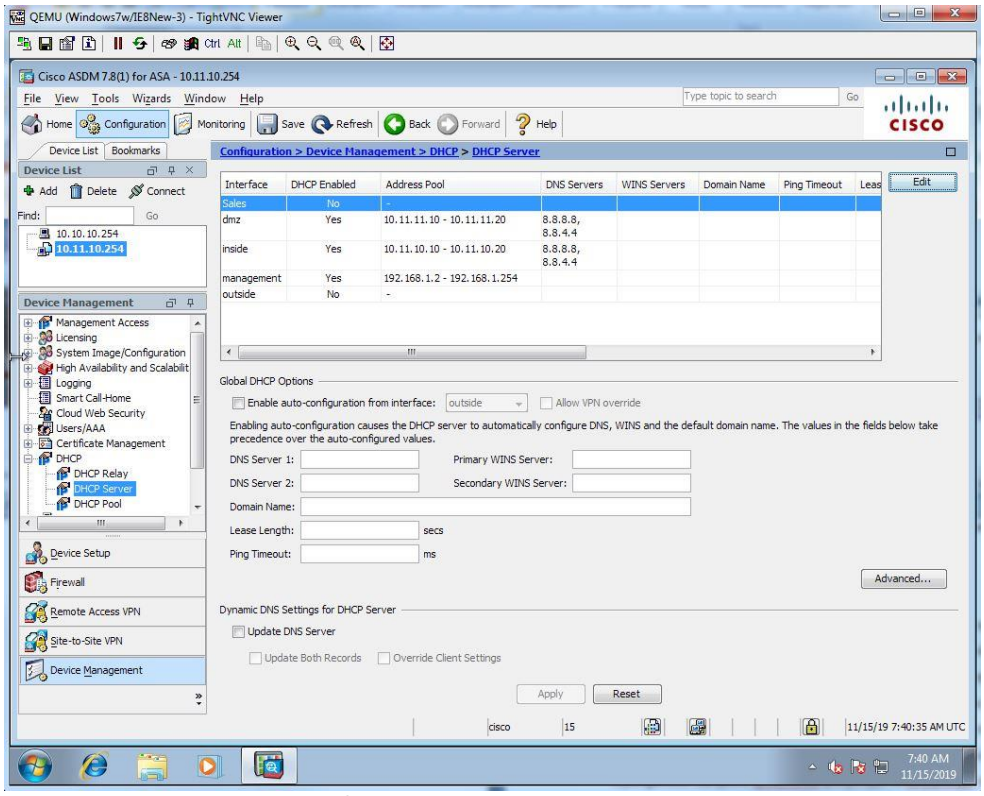
Από το σημείο αυτό μπορούμε να επιλέξουμε τα interfaces και να ορίσουμε τις διάφορες παραμέτρους.



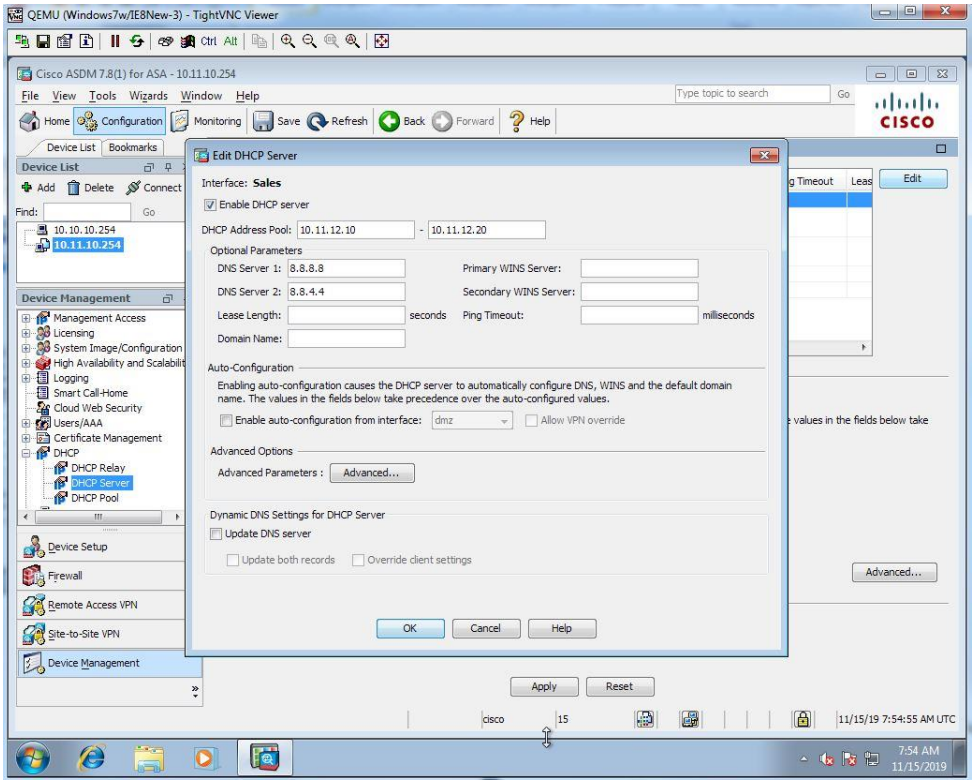
Εικόνα 60: Παραμετροποίηση του επιλεγμένου interface

Από το παράθυρο αυτό θα ονομάσουμε το interface, θα ορίσουμε το επίπεδο εμπιστοσύνης, θα το ενεργοποιήσουμε και θα δώσουμε διεύθυνση IP.

Ακολούθως από την ενότητα Device Management θα ενεργοποιήσουμε DHCP Server ανά interface.



Εικόνα 61: DHCPανάinterface. Το παράθυρο επιλογών ενεργοποιείται επιλέγοντας Edit



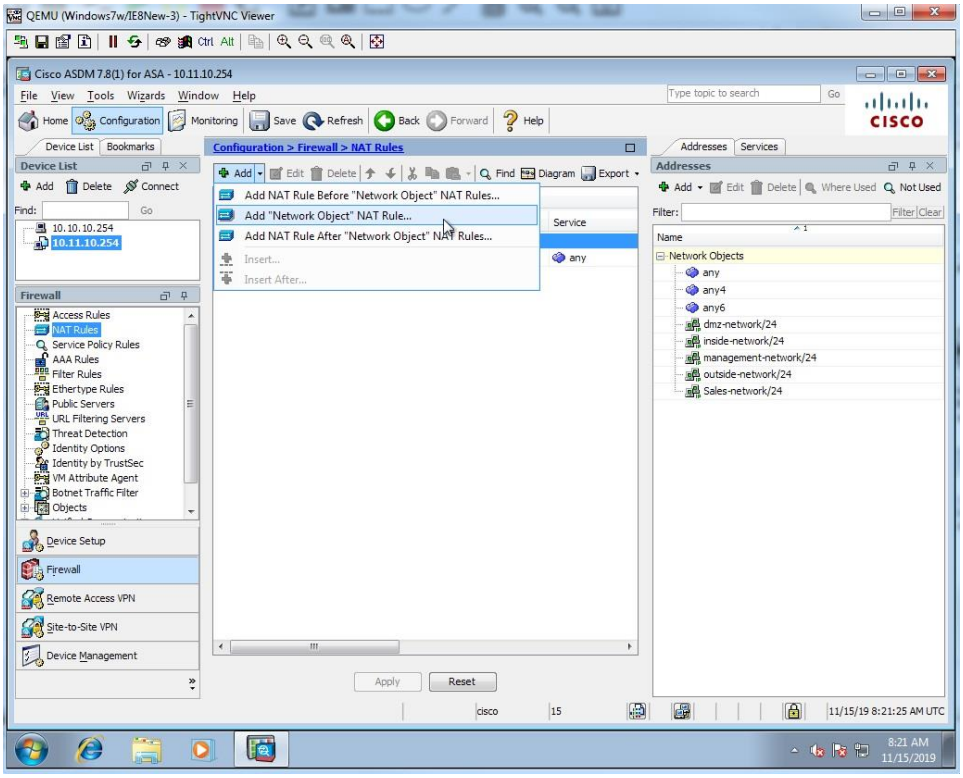
Εικόνα 62: Παραμετροποίηση DHCP

Με την παρούσα παραμετροποίηση το Τμήμα πωλήσεων θα λειτουργεί σε δικό του απομονωμένο υποδίκτυο στο interface Gigabit Ethernet 0/2 και θα μπορεί να δεχτεί 250 υπολογιστές μέσω συσκευών Switch που θα συνδεθούν στο interface αυτό εκ των οποίων οι 10 θα πάρουν αυτόματα διεύθυνση IP από το 10.11.12.10 έως το 20.

4.3.3 Port Forward και ACL

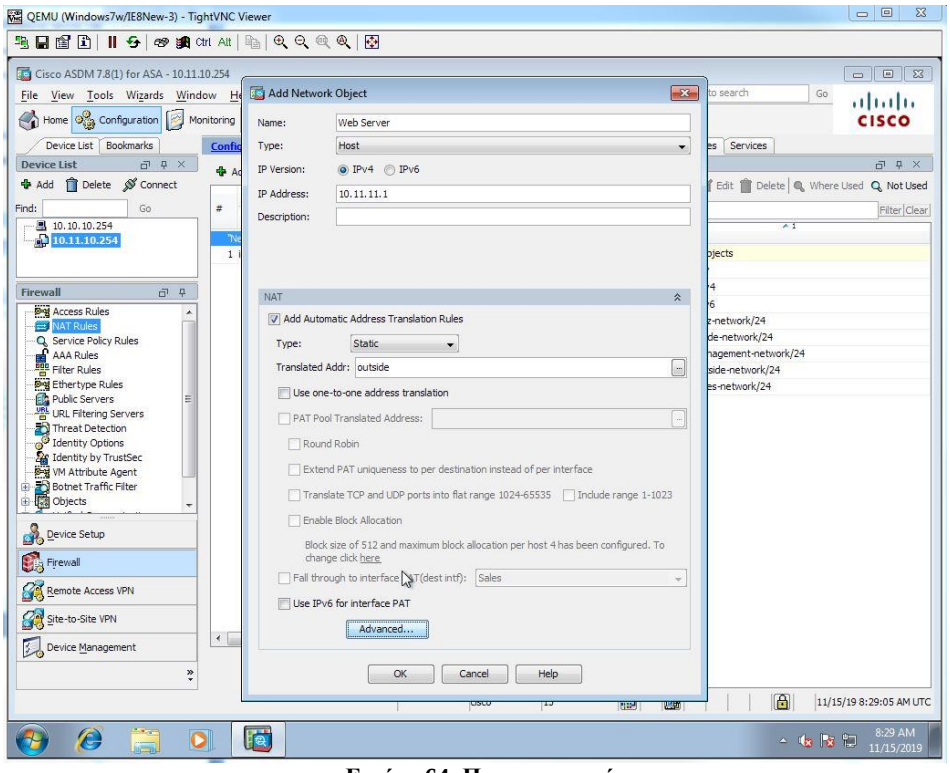
Ο οργανισμός του παραδείγματός μας, διαθέτει ένα Web Server που φιλοξενεί την ιστοσελίδα του. Ο Server αυτός θα πρέπει να είναι προσβάσιμος από οπουδήποτε άλλα για λόγους ασφαλείας δε θα μπορεί να εκκινήσει συνδέσεις από μόνος του. Για το λόγο αυτό, τον τοποθετούμε στο δίκτυο DMZ και παραμετροποιούμε αρχικά το Nat του Firewall ώστε να είναι προσβάσιμος από τον εξωτερικό κόσμο.

Για την παραμετροποίηση του Nat από την καρτέλα Configuration επιλέγουμε Firewall και ακολούθως NAT Rules. Στη συνέχεια Add και Add “Network object’ Nat Rule.

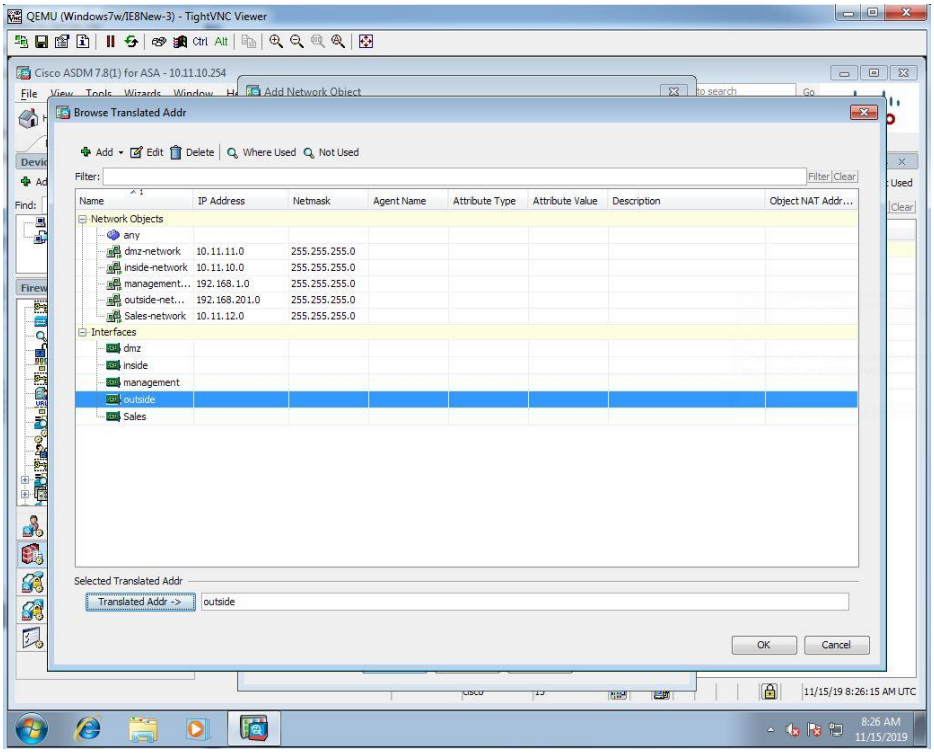


Εικόνα 63: Εισαγωγή κανόνα Nat

Στο παράθυρο αυτό δίνουμε όνομα στον κανόνα Nat για να το ξεχωρίζουμε και ακολούθως τη διεύθυνση του Web Server. Στη συνέχεια, δηλώνουμε ότι η μετάφραση θα γίνεται στο εξωτερικό outside interface από το κουμπί δίπλα στο πεδίο Translate Addr.

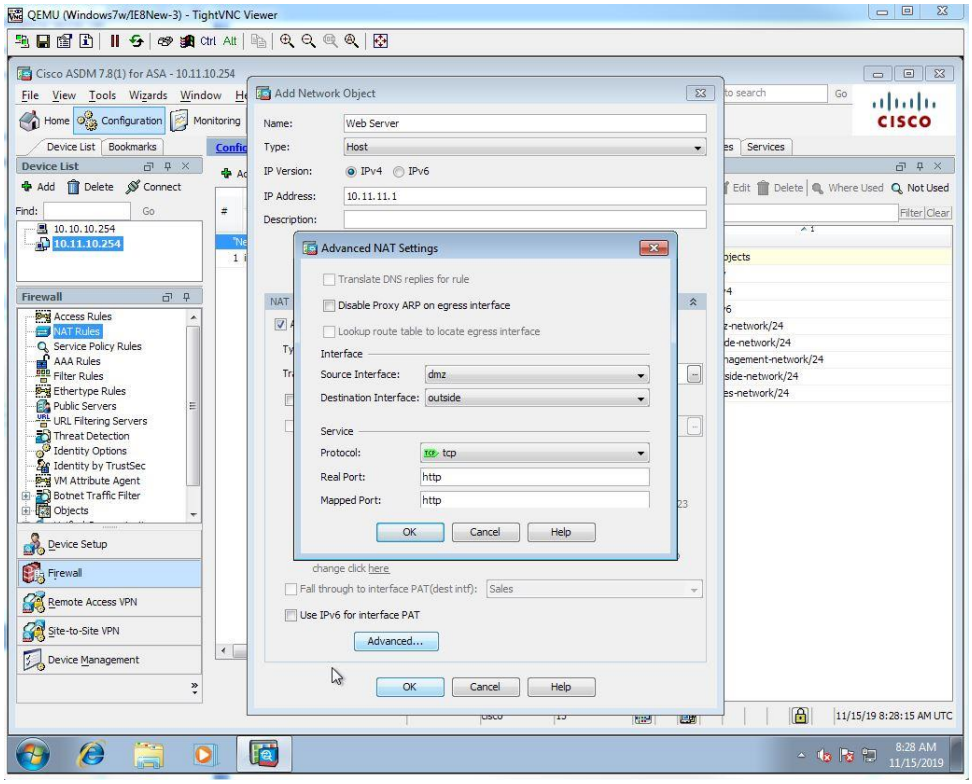


Εικόνα 64: Παραμετροποίηση



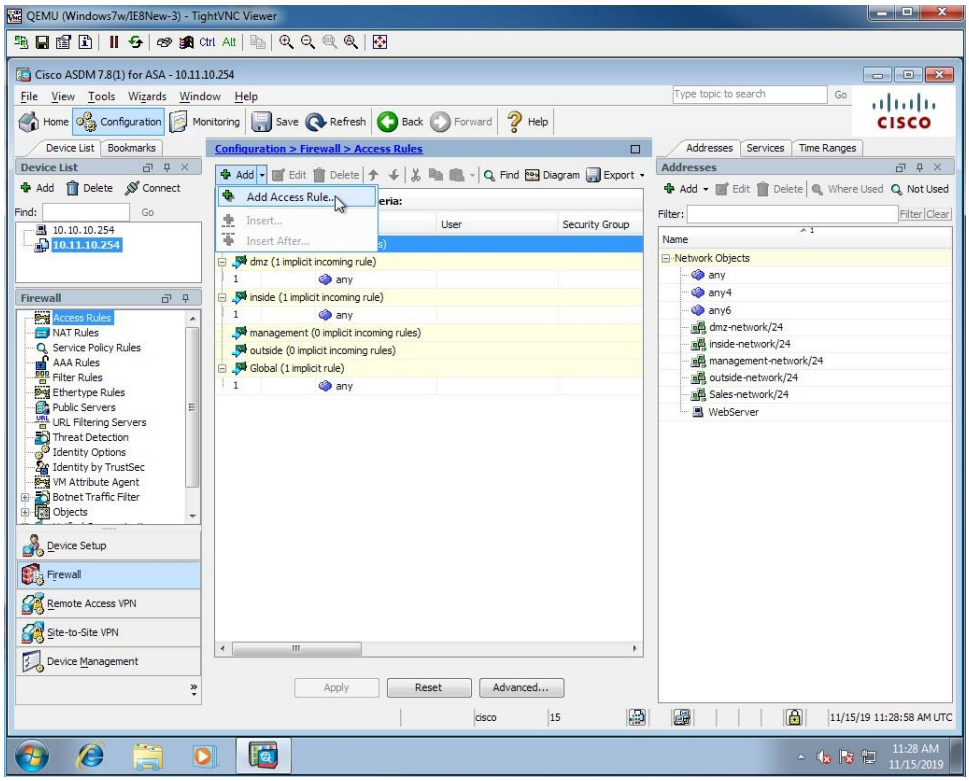
Εικόνα 65: Επιλογή του Interface στο οποίο θα γίνεται η μετάφραση

Ακολουθεί η δήλωση της θύρας στην οποία θα αναφέρεται η κλήση. Δίνεται από το παράθυρο που ανοίγει επιλέγοντας το κουμπί Advanced.

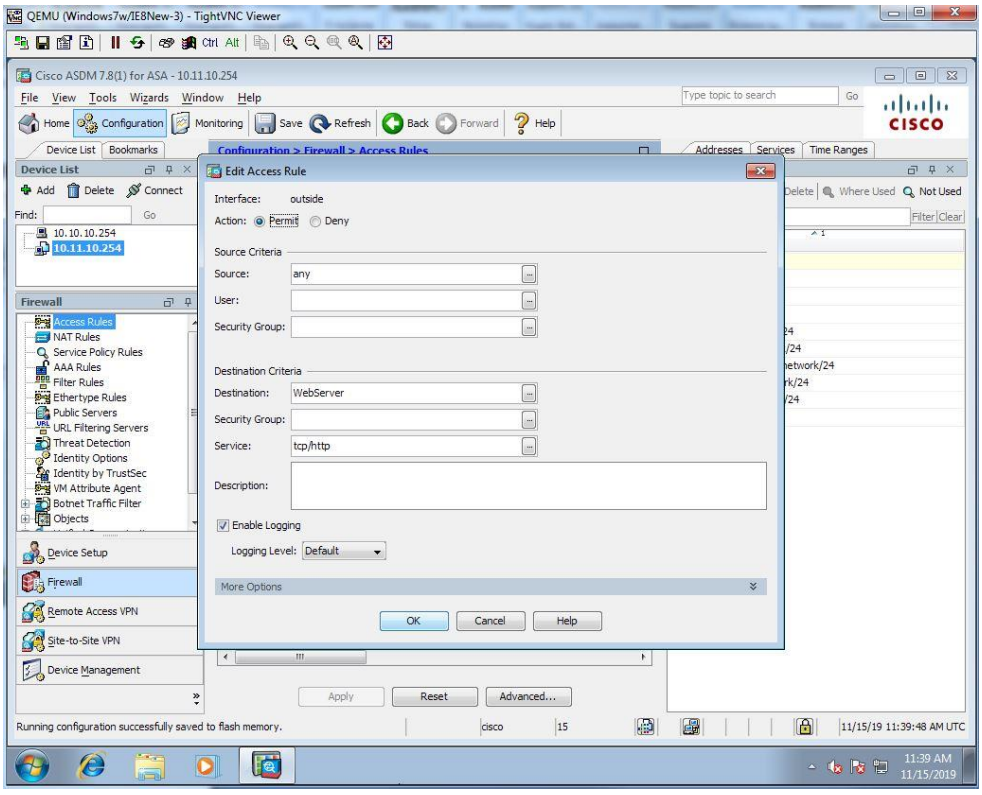


Εικόνα 66: Ρύθμιση πόρτας

Εδώ δίνονται τα interfaces στα οποία θα γίνεται η μετάφραση και η πόρτα. Επόμενο βήμα η παραμετροποίηση της λίστας πρόσβασης ώστε να επιτρέπεται η κίνηση. Επιλέγουμε από την αριστερή καρτέλα Access Rules και από το νέο παράθυρο New Rule.

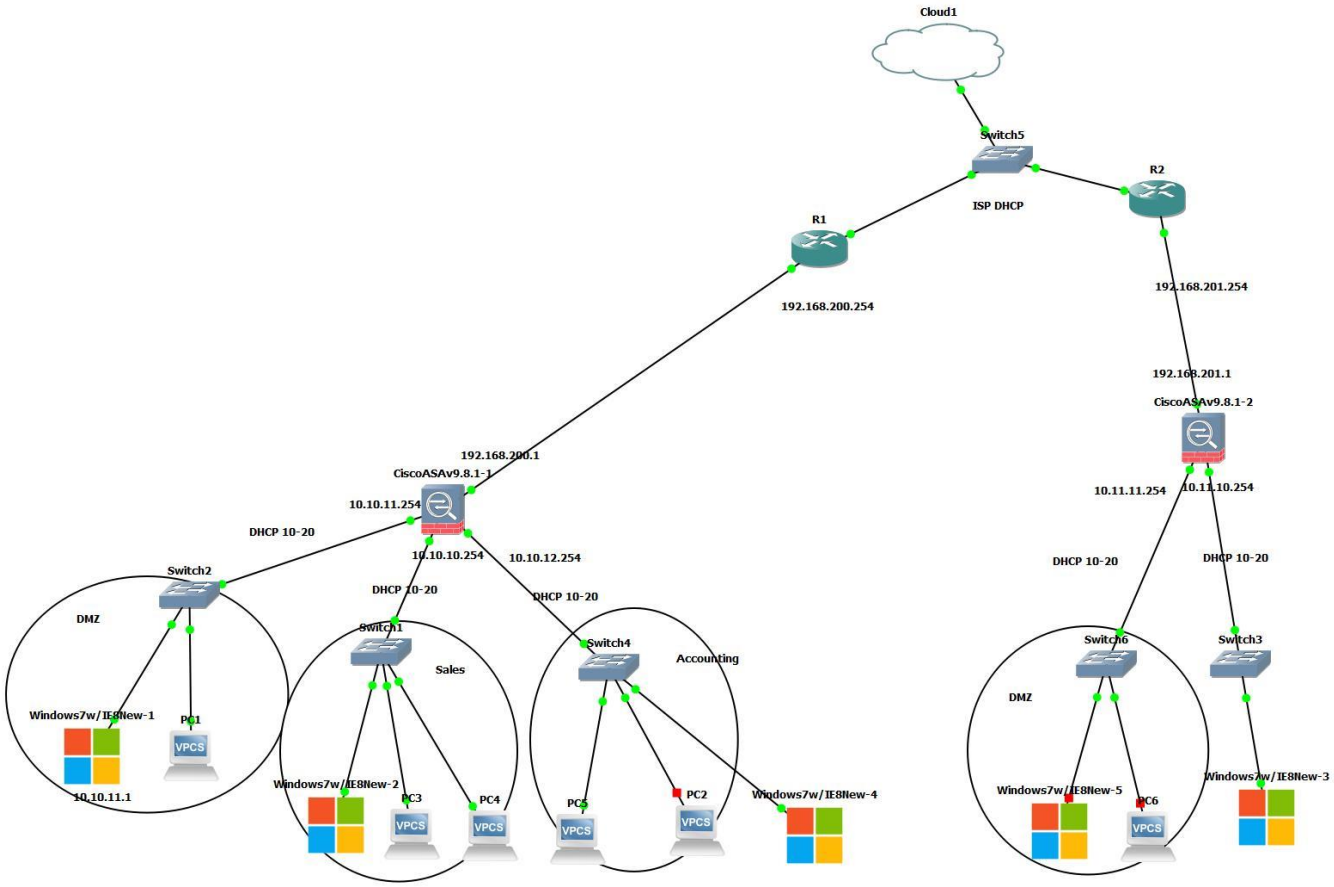


Εικόνα 67: Νέος κανόνας πρόσβασης



Εικόνα 68: Παραμετροποίηση νέου κανόνα

Από το νέο παράθυρο ορίζουμε ότι ο κανόνας θα εφαρμοστεί στο interface outside ώστε να φιλτράρει αυτή την κίνηση, ότι θα επιτρέπει την κίνηση από οπουδήποτε προς το Web Server στην υπηρεσία http. Ο Web Server του οργανισμού είναι τώρα προσβάσιμος από οπουδήποτε.



Εικόνα 69 Τελική απεικόνιση της υλοποίησης

ΚΕΦΑΛΑΙΟ 5 Συμπεράσματα

Συνοψίζοντας, στην παρούσα πτυχιακή χρησιμοποιήθηκαν τα προγράμματα GNS3, VMware και ο εξοπλισμός των συστημάτων Cisco με σκοπό τη δημιουργία ενός σεναρίου ασφάλειας. Δημιουργήθηκαν τέσσερα ανεξάρτητα μεταξύ τους τμήματα (DMZ, Sales, Accounting, Web Server) τα οποία όλα μαζί αποτελούν έναν οργανισμό αλλά θα πρέπει να συνδέονται σε διαφορετικά δίκτυα. Αυτό επιτυγχάνεται μέσω του firewall, ο οποίος με τις ανάλογες παραμετροποιήσεις ρυθμίζει κάθε interface να ανήκει στο δικό του δίκτυο. Στην υλοποίηση του ολικού δικτύου δεν αντιμετωπίστηκαν κάποιες σημαντικές δυσκολίες.

Κλείνοντας, είναι απαραίτητο να επισημανθεί ξανά πως η ασφάλεια των υπολογιστικών συστημάτων και των δικτύων είναι ένα πολύ σοβαρό θέμα που θα πρέπει να αντιμετωπίζεται με την αρμόζουσα ευαισθησία. Καθημερινά αποκαλύπτονται νέες ευπάθειες και κατά συνέπεια νέοι τρόποι παραβίασης των πληροφοριακών συστημάτων. Τα συστήματα ασφάλειας θα πρέπει να είναι σε θέση να αναγνωρίσουν τους κινδύνους αυτούς και να προστατέψουν τα πληροφοριακά συστήματα, χωρίς όμως να δυσανασχετούν τους χρήστες δημιουργώντας τους αισθήματα όπως ότι βρίσκονται υπό παρακολούθηση ή να τους δυσχεραίνουν στην εργασία τους. Είναι αυτονόητο επομένως, ότι υπάρχει αρκετό περιθώριο για περαιτέρω έρευνα τόσο για να αντιμετωπίζονται οι νέοι κίνδυνοι όσο και για να βελτιώνεται η εργασία των χρηστών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Wikipedia, «Δίκτυο Υπολογιστών», [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD [Πρόσβαση 19 8 2020]
2. Wikipedia, «Μητροπολιτικά Δίκτυα», [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/%CE%9C%CE%B7%CF%84%CF%81%CE%BF%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AC_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%B1 [Πρόσβαση 19 8 2020]
3. Abid, H. (2018). «Use of Firewall and IDS to detect & prevent network attacks», *IJTRS,* 289-292.
4. Wikipedia, «Ασφάλεια Δικτύων Υπολογιστών», [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD [Πρόσβαση 19 8 2020]
5. Gokce, K., Dogerlioglu, O. (2019). « "Bring your own device" policies: Perspectives of both employees and organizations»,*KM&EL,*233-246.
6. Wikipedia, «Υπολογιστικό Σύστημα», [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CF%8C_%CF%83%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1
[Πρόσβαση 1 9 2020]
7. Forcepoint, «Cyber Edu: What is an Intrusion Prevention System (IPS)? ». Available: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips
[Πρόσβαση 1 9 2020]
8. Cavusoglu, H., Raghunathan, S., Cavusoglu. H. (2009). «Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems» INFORMS, 198-217.
9. Bace R., Mell P., (2001) «Intrusion Detection Systems», Chapter 2. http://ranger.uta.edu/~dliu/courses/cse6392-ids-spring2007/papers/NIST-IntrusionDetection-2001.pdf
10. Gandhi, M., Srivatsa, S. (2008). «Developing and preventing attacks using network intrusion detection systems». *IJCSS,*49-60.
11. Μαυρίδης Ι. (2015) «Βασικές έννοιες και ζητήματα ασφάλειας», [Ηλεκτρονικό]. Available: https://repository.kallipos.gr/bitstream/11419/1025/1/05_chapter_01.pdf
12. Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, πρόγραμμα συμπληρωματικής εκπαίδευσης (2020), «Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων», Ενότητα 2.
13. Bulajoul, W., James, A., Shaikh, S.(2019). «A new architecture for Network Intrusion Detection and Prevention».*IEEE,*18558-18573.
14. Faizan M., Hedge S., Yaligar N. (2019). «Comparison between Cisco ASA and Fortinet FortiGate». IOSR Journal of Computer Engineering (IOSR-JCE).
15. Cisco 2691, 3725, and 3745 Modular Access Routers FIPS 140-2 Non-Proprietary Security Policy. [Ηλεκτρονικό].
Available:

https://www.cisco.com/en/US/docs/routers/access/3700/hardware/notes/3725fips.html#wp66809 [Πρόσβαση 7 9 2020]
16. Cables and kits. Cisco 1-Port Fast Ethernet Network Module, NM-1FE-TX. [Ηλεκτρονικό]
Available: https://www.cablesandkits.com/equipment/cisco-modules/routing/cisco-nm-cards/nm-1fe-tx/pro-867/ [Πρόσβαση 7 9 2020]

ΠΗΓΕΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Δίκτυο Υπολογιστών [1]
Εικόνα 2: Δίκτυο Κορμού
http://users.sch.gr/npapaz/bibliografia.php?keimeno=%C3%E9%E1%F4%DF+%F7%F1%E7%F3%E9%26%23181%3B%EF%F0%EF%E9%EF%FD%26%23181%3B%E5+%F4%EF+%F4%EF%F0%E9%EA%FC+%E4%DF%EA%F4%F5%EF+%F5%F8%E7%EB%FE%ED+%E5%F0%E9%E4%FC%F3%E5%F9%ED+%F3%E1%ED+%E4%DF%EA%F4%F5%EF+%EA%EF%F1%26%23181%3B%EF%FD%3B&tselida=diktia_II.php&onomaxristi1=&timaxristi1=dsgfdfs&aaa=636
Εικόνα 3: Ασφάλεια δικτύου
https://espaergasia.com/%CE%B5%CE%BA%CF%80%CE%B1%CE%B9%CE%B4%CE%B5%CF%85%CF%83%CE%B7/2019/02/05/%CE%B3%CE%AF%CE%BD%CE%B5-%CF%80%CE%B9%CF%83%CF%84%CE%BF%CF%80%CE%BF%CE%B9%CE%B7%CE%BC%CE%AD%CE%BD%CE%BF%CF%82-%CE%B5%CE%B9%CE%B4%CE%B9%CE%BA%CF%8C%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%CE%B1%CF%83%CF%86/
Εικόνα 4: Τοίχος προστασίας (Firewall)
http://www.logifer.gr/Default.aspx?TabId=128
Εικόνα 5:Δίκτυο Υπολογιστή με χρήση IDS [10]
Εικόνα 6:Dos Attack
https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-
Εικόνα 7:Σχεδιάγραμμα Ευπαθειών [11]
Εικόνα 15: Εργαλειοθήκη Συσκευών
https://docs.gns3.com/1wr2j2jEfX6ihyzpXzC23wQ8ymHzID4K3Hn99-qqshfg/index.html
Εικόνα 16: Εισαγωγή συσκευών στο χώρο εργασίας
https://docs.gns3.com/1wr2j2jEfX6ihyzpXzC23wQ8ymHzID4K3Hn99-qqshfg/index.html
Εικόνα 38: Αδυναμία εκκίνησης μηχανής
https://www.gns3.com/community/discussion/qemu-3