Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Υλοποίηση, απασφαλμάτωση και σύγκριση τεχνολογιών Ιδιωτικών Εικονικών Δικτύων** **Implementation, debugging and comparison of Virtual Private Network (VPN) technologies**
Ονοματεπώνυμο Φοιτητή	**Δημήτριος Βρεττός**
Πατρώνυμο	**Χρήστος**
Αριθμός Μητρώου	**ΜΠΠΛ14008**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Νοέμβριος 2016**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κοτζανικολάου Παναγιώτης Επίκουρος Καθηγητής	Δουληγέρης Χρήστος Καθηγητής	Βέργαδος Δημήτριος Αναπληρωτής καθηγητής

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι να γίνει μια ενδελεχής ανάλυση των υφιστάμενων τεχνολογιών για την υλοποίηση Ιδιωτικών Εικονικών Δικτύων (Virtual Private Networks, VPN). Θα αναφέρουμε τι είναι η τεχνολογία VPN, καθώς και τις βασικές εφαρμογές των VPN. Θα γίνει αναφορά στα βασικά είδη VPN, και τα χαρακτηριστικά του κάθε είδους. Καταλήγοντας στις δυο πιο διαδεδομένες μορφές VPN , δηλαδή του IPsec VPN και του SSL VPN, θα γίνει χρήση του λογισμικού GNS3 για να μπορέσουμε να υλοποιήσουμε αντίστοιχες συνδέσεις. Η υλοποίηση, σε κάθε περίπτωση, θα γίνει και με την εισαγωγή εντολών μέσα από Command Line Interface (CLI), όπως επίσης και με τη χρήση Graphical User Interface (GUI) με τη βοήθεια των προγραμμάτων Cisco Configuration Professional (CCP) και Cisco Adaptive Security Device Manager (Cisco ASDM). Μετά την υλοποίηση θα ακολουθήσει η απασφαλμάτωση (debugging), εξηγώντας τις εντολές που χρειάζεται να εισάγει ο χρήστης για να επιβεβαιώσει την ορθότητα της υλοποίησης αλλά και τι ακριβώς πρέπει να ελέγξει, να εντοπίσει και να διορθώσει σε περίπτωση που παρουσιαστεί κάποιο σφάλμα.

ABSTRACT

The purpose of this master thesis is to make a thorough analysis of existing technologies for the implementation of Virtual Private Networks (VPN). We will mention what is the VPN technology, and the basic implementations of VPN. Also, there will be a reference to the basic types of VPN, and their unique characteristics. Concluding the presentation, we will deal with the two prevalent types of VPN, IPsec VPN and SSL VPN, and with the use ofGNS3 software we will try to create a topology and implement these types of VPN. The implementation, in each case, will be done by inserting commands through Command Line Interface (CLI), as well as using wizards in Graphical User Interface (GUI) with the help of Cisco Configuration Professional (CCP) and Cisco Adaptive Security Device Manager (Cisco ASDM). After the implementation is done, debugging is our main concern. We will explain the commands we need to confirm that the configuration is valid, and if something does not work properly we will try to identify and correct these errors.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Ευρετήριο ξένων λέξεων.

Accounting: Έλεγχος λειτουργιών

Activate CPU throttling: Μείωση χρήσης πόρων από τον επεξεργαστή

Admin Rights: Δικαιώματα χρήσης διαχειριστή

Administrators: Διαχειριστές

Advanced settings: Προηγμένες ρυθμίσεις

Anti-replay protection: Προστασία αντιγραφής δεδομένων

Application: Εφαρμογή

Attack: Επίθεση

Authentication: Αυθεντικοποίηση

Authorization: Εξουσιοδότηση

Auto-configuration: Αυτόματη διαμόρφωση

Bandwidth: Ρυθμός ροής δεδομένων

Browser: Πρόγραμμα περιήγησης

Business policies: Εταιρικές πολιτικές

Certificate authority: Αρχή Πιστοποίησης

Client interface: Διεπαφή χρήστη

Command Line Interface: Γραμμή εντολών

Comparison: Σύγκριση

Cost: Κόστος

Country: Χώρα

Customized settings: Προσαρμοσμένες ρυθμίσεις

Data integrity: Ακεραιότητα δεδομένων

Data-link layer: Επίπεδο ζεύξης δεδομένων

Debugging: Απασφαλμάτωση

Default Licence key: Προεπιλεγμένο κλειδί άδειας

Device: Συσκευή

Digital certificates: Ψηφιακά Πιστοποιητικά

Digital signatures: Ψηφιακές υπογραφές

Discover: Ανακαλύπτω

Download: Λήψη

Dual-stack: Ταυτόχρονη υποστήριξη IPv4/IPv6

Dynamic Host Configuration Protocol (DHCP): Πρωτόκολλο δυναμικής διαμόρφωσης κεντρικού υπολογιστή

Elevated Privileges: Αυξημένα προνόμια διαχείρισης

Encapsulation/Decapsulation: Ενθυλάκωση/Αποθυλάκωση

Encryption/Decryption: Κρυπτογράφηση/Αποκρυπτογράφηση

Enrollment request: Αίτημα υπογραφής

Fingerprint: Αποτύπωμα

Flexibility: Ευελιξία

Frame: Πλαίσιο

Grant-auto: Αυτόματη χορήγηση

Graphical User Interface: Γραφικό περιβάλλον

Hard to configure: Δύσκολο στη διαχείριση

Hardware/software based: βασισμένα σε ηλεκτρονικό μηχάνημα / βασισμένα σε λογισμικό

Hash functions: Συναρτήσεις κατακερματισμού

Hash value: Τιμή κατακερματισμού

Head-Office: Κεντρικά γραφεία

Host/Client: Τελικός χρήστης

Implementation: Υλοποίηση

Infrastructure: Υποδομή

Initiator router: Router που ξεκινά μια διαδικασία

Integrity check: Έλεγχος ακεραιότητας

Interface: Διεπαφή

Internet Providers: Παροχείς Internet

Intrusion Detection System (IDS): Σύστημα ανίχνευσης εισβολής

IP header: Κεφαλίδα IP

Latency-sensitive: Αυξάνεται εύκολα ο χρόνος απόκρισης από τη στιγμή που δίνεται μια εντολή

Launch selected task: Έναρξη επιλεγμένης διαδικασίας

Layer: Επίπεδο

Links: Σύνδεσμοι

Local database: Τοπική βάση δεδομένων

Local Server: Τοπικός εξυπηρετητής

Location: Τοποθεσία

Log files: Αρχεία καταγραφής

Log in: Είσοδος σε εφαρμογή

Low/Medium/High: Χαμηλό/Μέσο/Υψηλό

Malware: Κακόβουλο λογισμικό

Manage: Διαχειρίζομαι

Management: Διαχείριση

Manual: Εγχειρίδιο χρήσης

Message pair exchange: Ανταλλαγή ζεύγους μηνυμάτων

Negotiation: Διαπραγμάτευση

Network adapter: Κάρτα δικτύου

Network: Δίκτυο

New: Νέο

Packet-injection: Έγχυση δεδομένων

Payload: Όγκος δεδομένων

Peer: Κόμβος

Permanent Activation key: Μόνιμο κλειδί ενεργοποίησης

Ping: Έλεγχος ύπαρξης συνδεσιμότητας (σε απομακρυσμένο δίκτυο ή υπολογιστή)

Priority: Προτεραιότητα

Professional: Επαγγελματικός

Project: Σχέδιο

Proprietary protocol: Ιδιόκτητο πρωτόκολλο

Protocol: Πρωτόκολλο

Public/private key: Δημόσιο/Ιδιωτικό κλειδί

Regional Offices: Απομακρυσμένα γραφεία

Remote access: Απομακρυσμένη πρόσβαση

Remote/Roaming users: Απομακρυσμένοι χρήστες

Replay-attacks: Επιθέσεις με στόχο την αντιγραφή των δεδομένων

Replication: Αντιγραφή

Request: Αίτημα

Revocation check: Έλεγχος ανάκλησης πιστοποιητικού

Router: Δρομολογητής

Scalability: Επεκτασιμότητα

Screenshot: Εικόνα

Search: Ψάχνω

Security: Ασφάλεια

Self-signed: Αυτο-υπογεγραμμένο

Sequence number: Ακολουθία

Server: Εξυπηρετητής

Session: Συνεδρία

Source IP/Destination IP:

Spoof: Αλλάζω μορφή

Static routing: Στατική δρομολόγηση

Subnet: Υποδίκτυο

Symmetric/Asymmetric algorithms: Συμμετρικοί/Ασύμμετροι αλγόριθμοι

Topology: Τοπολογία

Unencrypted: Μη κρυπτογραφημένο

Update: Αναβάθμιση

User credentials: Διαπιστευτήρια χρήστη

Username/password: Όνομα χρήστη/κωδικός χρήστη

Virtual Machine: Ψηφιακή συσκευή

Virtual Private Networks (VPN): Εικονικά Ιδιωτικά Δίκτυα

Virus: Ιός

Web sites: Ιστοσελίδες

Wizard: Αυτόματος οδηγός διαχείρισης

0. Στόχος και περιληπτική δομή της εργασίας

0.1. Στόχος της εργασίας

Καθώς η χρήση του internet είναι πλέον μια καθημερινότητα και η συνεχής χρήση "έξυπνων" συσκευών είναι, πλέον, επιβεβλημένη, ένας μέσος χρήστης εκτελεί την πλειονότητα των υποχρεώσεών του από ένα κινητό ή έναν υπολογιστή. Πολλές όμως από αυτές τις "υποχρεώσεις" περιλαμβάνουν από αθώα μέχρι πολύ ευαίσθητα και προσωπικά δεδομένα. Το TCP/IP πάνω στο οποίο στηρίζεται η καθημερινότητα στο internet ποτέ δεν ήταν ασφαλές. Ξεκινώντας από το IPv4, που δεν περιέχει κανένα επίπεδο ασφάλειας και περνώντας στο IPv6 που είναι μεν πιο ασφαλές αλλά θα αργήσει πολύ ακόμη να γίνει η καθημερινότητά μας, καταλαβαίνουμε ότι το πεδίο του Internet αυτή τη στιγμή προσφέρεται για τη δράση κακόβουλων χρηστών. Σε όλο αυτό το πρόβλημα της ασφάλειας, μια πιθανή λύση είναι η τεχνολογία των Virtual Private Networks.

Οι στόχοι της μεταπτυχιακής αυτής διατριβής είναι οι εξής:

- Η θεωρητική ανάλυση και επεξήγηση των VPN.
- Ο διαχωρισμός των VPN ανάλογα με τον τύπο, το είδος και το layer που υλοποιείται.
- Η ειδικότερη μελέτη και επεξήγηση των δυο πιο διαδεδομένων μορφών VPN και η σύγκρισή τους. Θα αναφερθούν τα ιδιαίτερα χαρακτηριστικά τους, ο τρόπος λειτουργίας τους και σε ποιες περιπτώσεις χρησιμοποιείται, κυρίως, το κάθε ένα.
- Η υλοποίηση και ρύθμιση των IPsec VPN και SSL VPN σε εργαστηριακό περιβάλλον με τη βοήθεια των λογισμικών GNS3, CCP και ASDM.
- Debugging των τοπολογιών που δημιουργήσαμε στο προηγούμενο βήμα.

Στις επόμενες γραμμές παρουσιάζουμε μια περίληψη της εργασίας και το τι θα συναντήσουμε σε κάθε κεφάλαιο.

0.2. Περιληπτική δομή της εργασίας

Στο 1^{ο} κεφάλαιο θα παρουσιαστούν οι απειλές που υπάρχουν στο διαδίκτυο καθώς και οι τρόποι επίθεσης και θα γίνει αναφορά στο IPv4 και IPv6. Τέλος, θα γίνει μια σύνδεση των πιο πάνω θεμάτων με την ανάγκη για ασφάλεια που ουσιαστικά οδήγησε στην εμφάνιση της τεχνολογίας του VPN. Θα αναφέρουμε πώς ξεκίνησαν, καθώς και τα μειονεκτήματα και τα πλεονεκτήματα της προηγούμενης τεχνολογίας και πώς καταλήξαμε στα VPN.

Στο 2^{ο} κεφάλαιο θα ασχοληθούμε το θεωρητικό κομμάτι των VPN. Αφού δώσουμε έναν ορισμό, θα αναφερθούμε στα πλεονεκτήματα που προσφέρουν και θα παρουσιάσουμε συνοπτικά τα εργαλεία, τους αλγόριθμους και τα πρωτόκολλα που χρησιμοποιούνται για την υλοποίησή τους. Αμέσως μετά θα τα κατηγοριοποιήσουμε σύμφωνα με είδος, τον τύπο και το επίπεδο δικτύου στο οποίο μπορεί να λειτουργήσει η τεχνολογία αυτή. Στη συνέχεια θα αναφερθούμε στις δυο επικρατούσες μορφές VPN, το IPsec VPN και το SSL VPN. Αρχικά θα γίνει μια γενική περιγραφή, αλλά όσο προχωράμε, θα εμβαθύνουμε ακόμη περισσότερο και θα αναλύσουμε τον τρόπο λειτουργίας τους. Τέλος, αφού μέσα από την περιγραφή θα έχουμε κατανοήσει το πώς λειτουργεί κάθε κατηγορία θα κάνουμε μια σύγκριση μεταξύ τους και θα καταλήξουμε για ποιες περιπτώσεις ενδείκνυται το καθένα και ποιο είναι καλύτερο, αν μπορεί να υποστηριχθεί κάτι τέτοιο.

Περνώντας στο πιο πρακτικό κομμάτι της εργασίας, στο 3^{ο} και 4^{ο} κεφάλαιο θα παρουσιάσουμε τα εργαλεία τα οποία θα χρησιμοποιήσουμε. Θα γίνει μια συνοπτική περιγραφή τους και αμέσως μετά θα παρουσιαστεί ένα σύντομο εγχειρίδιο χρήσης και

παραμετροποίησης του καθενός. Στο GNS3 θα ασχοληθούμε με την εισαγωγή των πιο σημαντικών κομματιών (routers και firewalls) χωρίς τα οποία δε θα μπορούσαμε να προχωρήσουμε. Τα υπόλοιπα δυο εργαλεία δεν χρειάζονται ιδιαίτερη παραμετροποίηση, οπότε το εγχειρίδιο χρήσης θα είναι σαφώς πιο σύντομο από αυτό του GNS3.

Στο 5ο κεφάλαιο, που είναι και το κατ' εξοχήν εργαστηριακό κομμάτι, θα γίνει υλοποίηση (implementation) IPsec VPN και SLL VPN χρησιμοποιώντας GUI αλλά και CLI. Αφού ολοκληρώσουμε την υλοποίηση, θα γίνει η απασφαλμάτωση (debugging), θα αναφερθούν οι εντολές με τις οποίες γίνονται οι έλεγχοι ορθής λειτουργίας και σε περίπτωση ύπαρξης σφάλματος, θα γίνουν οι απαραίτητες ενέργειες για την διόρθωσή του.

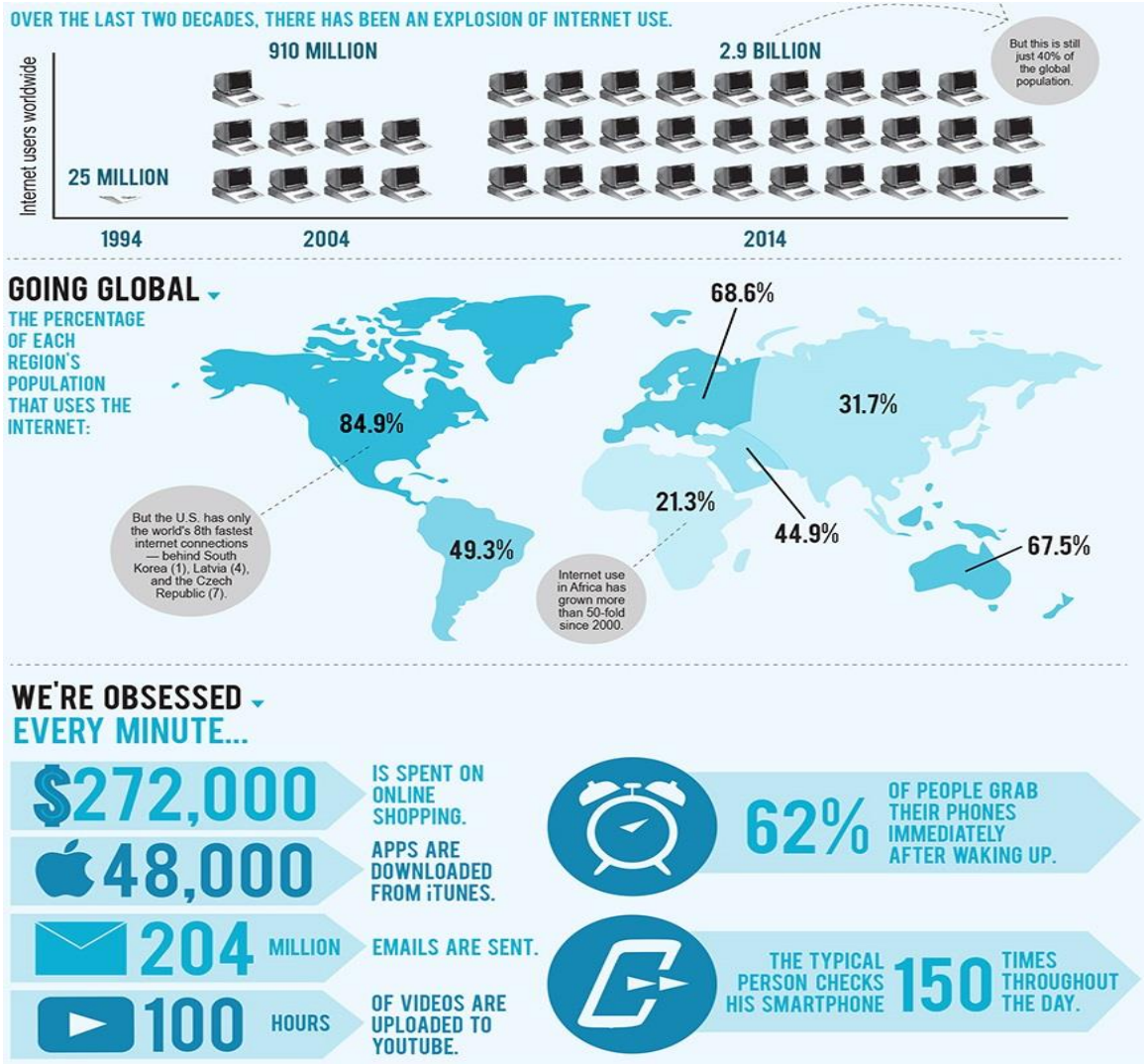
Στο 6ο κεφάλαιο, θα αναφερθούν επιγραμματικά τα κυριότερα σημεία της διπλωματικής εργασίας.

Τέλος, στο Παράρτημα, περιλαμβάνονται τα αρχεία διαμόρφωσης των συσκευών.

1. Εισαγωγή

Η χρήση του Internet έχει παρουσιάσει τεράστια αύξηση τα τελευταία 30 χρόνια. Στις αρχές του 1994 υπήρχαν περίπου 25 εκατομμύρια χρήστες παγκοσμίως. Ο αριθμός αυτός αυξήθηκε κατακόρυφα στις αρχές του 2004 φτάνοντας τα 910 εκατομμύρια, αριθμός πολύ μικρότερος των σχεδόν 3 δισεκατομμυρίων χρηστών του Internet το 2014. Αξιοσημείωτο είναι το γεγονός ότι αυτός ο αριθμός αποτελεί μόλις το 40% του πληθυσμού της Γης. Είναι φανερό, λοιπόν, ότι ο αριθμός χρηστών αυξάνεται και θα συνεχίσει να αυξάνεται με ρυθμούς γεωμετρικής προόδου.

Σε κάθε ήπειρο τα ποσοστά των χρηστών διαφέρουν. Έχουν άμεση σχέση με το βιοτικό και μαθησιακό επίπεδο, την ταχύτητα του Internet και φυσικά η χρήση που κάνει ο καθένας διαφέρει, ανάλογα με τις ανάγκες του. Παρακάτω υπάρχει ένας πίνακας που δείχνει την αύξηση της χρήσης του Internet, το ποσοστό χρήσης σε κάθε Ήπειρο καθώς και τις πιο δημοφιλείς χρήσεις του διαδικτύου.



Εικόνα 1. Αύξηση της χρήσης του Internet, ποσοστό χρήσης σε κάθε Ήπειρο καθώς και οι πιο δημοφιλείς χρήσεις του διαδικτύου Πηγή: Forbes, www.internetlivestats.com, Instagram, Youtube, Billboard, IACP.

Πέρα όμως από την απλή χρήση του Internet για διασκέδαση και μόρφωση, ακόμη και ο μέσος χρήστης χρησιμοποιεί τον υπολογιστή του ή το smartphone του για πιο σημαντικά πράγματα. Από το να δει τα email του μέχρι να πληρώσει λογαριασμούς και να κάνει διαδικτυακές αγορές. Επίσης, η φύση των νέων εταιρών και επιχειρήσεων τους επιβάλει να έχουν πολλές φυσικές παρουσίες σε διαφορετικές γεωγραφικές περιοχές αλλά χωρίς να θέλουν να απωλέσουν τα οφέλη της άμεσης και φυσικής σύνδεσης σε ένα τοπικό ιδιωτικό δίκτυο. Χρειάζονται έναν τρόπο να ανταλλάσσουν πληροφορίες άμεσα και μειώνοντας το ρίσκο όσο το δυνατόν περισσότερο. Γιατί το χρειάζονται αυτό; Γιατί τίποτα, πλέον, στον χώρο της τεχνολογίας δεν είναι ασφαλές.

Όπως η χρήση και οι σκοποί του Internet αλλάξαν, και θα συνεχίσουν να αλλάζουν μέσα στα χρόνια, έτσι έχουν αλλάξει και οι κακόβουλοι χρήστες αλλά και οι απειλές. Υπάρχουν άπειρες απειλές στο Internet, αλλά οι πιο συνηθισμένοι υπαίτιοι πίσω από τις επιθέσεις που δέχονται εταιρίες ή/και μεμονωμένα άτομα είναι οι παρακάτω.

- Τρομοκράτες
- Εγκληματίες
- Hackers
- Δυσαρεστημένοι υπάλληλοι μιας εταιρίας
- Αντίπαλες εταιρίες
- Κρατικές υπηρεσίες
- Γενικά οποιοσδήποτε με έναν υπολογιστή, εξειδικευμένες γνώσεις και θέληση να χρησιμοποιήσει το Internet για κακόβουλες πράξεις

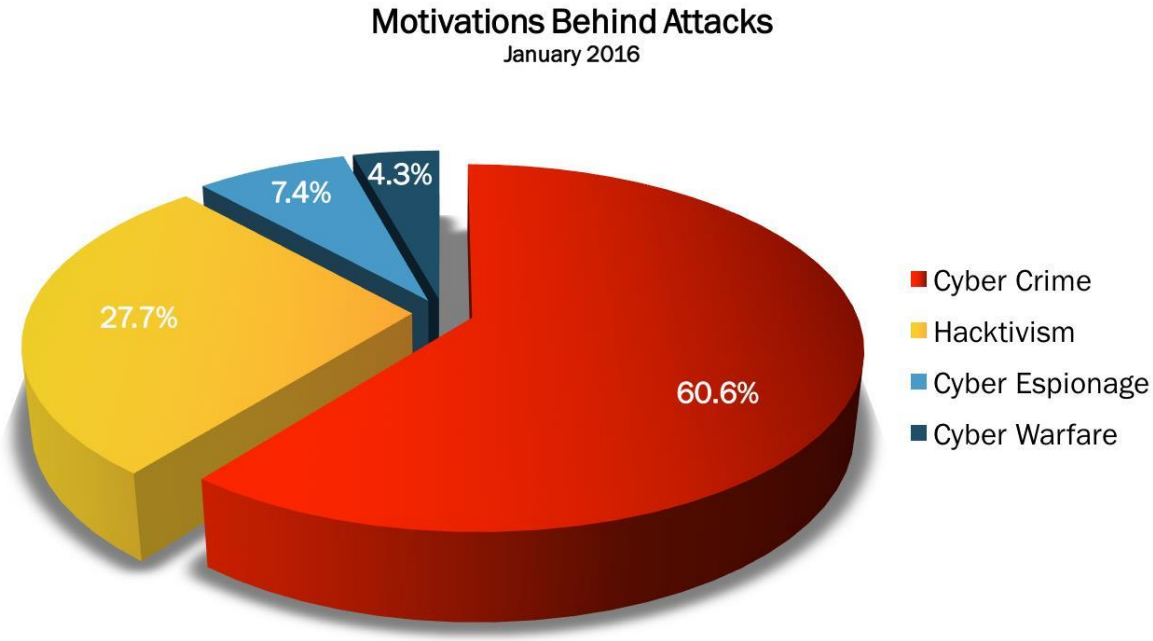
Ο πιο εύκολος τρόπος, αν θα μπορούσε να τον χαρακτηρίσει κανείς εύκολο, για να αντιμετωπίσει κάποιος αυτές τις απειλές, είναι, αφενός, να γνωρίζει και να κατανοεί άριστα το δίκτυό του, να γνωρίζει τις αδυναμίες και τα τρωτά του σημεία, να μπορεί να καταλάβει τί μπορεί να βάλουν στόχο αυτοί οι κακόβουλοι χρήστες και, αφετέρου, να μπορεί να καταλάβει την ψυχολογία αυτών των ατόμων, τα κίνητρά τους και τα ενδιαφέροντά τους και τα μέσα που θα χρησιμοποιήσουν.

Ακόμη και η μελέτη των κινήτρων, όμως, δεν είναι εύκολη υπόθεση. Άλλες φορές τα κίνητρα είναι οικονομικής φύσεως, άλλες φορές αυτοί οι κακόβουλοι χρήστες (από εδώ και πέρα θα τους αναφέρουμε ως επιτιθέμενους) θέλουν απλά να αποκτήσουν φήμη “χτυπώντας” κάποιες γνωστές εταιρίες, άλλες φορές επιθυμούν να αποτρέψουν κάποιες εταιρίες από να πραγματοποιήσουν συγκεκριμένες κινήσεις και, τέλος, απλά κάποιες φορές μεμονωμένα άτομα ή εταιρίες υφίστανται ακούσια χτυπήματα.

Στις απαρχές του Internet, τέλη δεκαετίας του 1990 και αρχές του 2000, οι περισσότερες επιθέσεις και τα viruses/malwares που είχαν σχεδιαστεί είχαν, τα περισσότερα, σαν στόχο την απόκτηση φήμης. Άλλωστε το Internet εκείνη την εποχή ήταν σε υβριδικό στάδιο και η χρήση του αρκετά περιορισμένη και κανείς δεν μπορούσε να προβλέψει πώς θα εξελισσόταν και τι δυνατότητες θα έδινε λίγα χρόνια αργότερα. Τα τελευταία χρόνια όμως όλα αρχίζουν και αλλάζουν και οι περισσότερες επιθέσεις έχουν ως στόχο την υποκλοπή πληροφοριών και το οικονομικό κέρδος. Για παράδειγμα, η απόκτηση πρόσβασης σε ένα PoS δίνει στους επιτιθέμενους πρόσβαση στις πληροφορίες πολλών πιστωτικών/χρεωστικών καρτών, που είτε μπορούν να τις εκμεταλλευτούν χρησιμοποιώντας τες για αγορές είτε να

πουλήσουν τα στοιχεία τους στη μαύρη αγορά. Επίσης, η εταιρική κατασκοπία έχει γνωρίσει μεγάλη "άνθιση".

Στον επόμενο πίνακα φαίνονται τα ποσοστά των επιθέσεων που έχουν γίνει, βάσει κινήτρου, παγκοσμίως τον Ιανουάριο του 2016.



Εικόνα 2. Motivation behind attacks (as from Jan 2016)
Πηγή:http://www.hackmageddon.com/category/security/cyber-attacks-statistics

Παρακάτω θα παρουσιάσουμε τα κυριότερα μέσα επίθεσης που έχουν χρησιμοποιηθεί για κακόβουλο σκοπό αλλά και τρόπους με τους οποίους οι επιτιθέμενοι μελετούν τον στόχο τους.

Επειδή σπάνια κάποιος θα ξεκινήσει μια τυφλή επίθεση, η οποία δε θα έχει μεγάλη πιθανότητα επιτυχίας, οι δυο πιο συνηθισμένοι τρόποι "μελέτης" του στόχου, είναι οι επόμενοι.

- ***Αναγνώριση***: Είναι η διαδικασία κατά την οποία οι επιτιθέμενοι ψάχνουν να βρουν πληροφορίες σχετικά με τον στόχο τους. Αν, για παράδειγμα, πρόκειται για δίκτυο ψάχνουν να δουν ποιες IP απαντούν ή ποια ports στις συσκευές με αυτές τις IP είναι ανοιχτές.
- ***Social Engineering***: Αυτό το κομμάτι στοχεύει τον άνθρωπο, τη μεγαλύτερη αδυναμία που καλείται να αντιμετωπίσει κάθε σύστημα, δίκτυο, εταιρία κ.τ.λ. Αν ο επιτιθέμενος μπορέσει να αποσπάσει πληροφορίες από τον χρήστη, τότε η δουλειά του γίνεται πολύ πιο εύκολη. Χωρίζεται σε phishing και pharming. Το phishing περιλαμβάνει την αποστολή links που φαίνονται ότι έρχονται από έμπιστη πηγή. Όταν ο χρήστης το "πατάει", του ζητάει να δώσει πληροφορίες όπως passwords και usernames, τα οποία έρχονται στην κατοχή του επιτιθέμενου. Το pharming είναι πιο περίπλοκο καθώς η επίθεση είναι πιο προσωπική αφού πρώτα ο επιτιθέμενος έχει μελετήσει τις συνήθειες και γενικά τη ζωή του "στόχου".

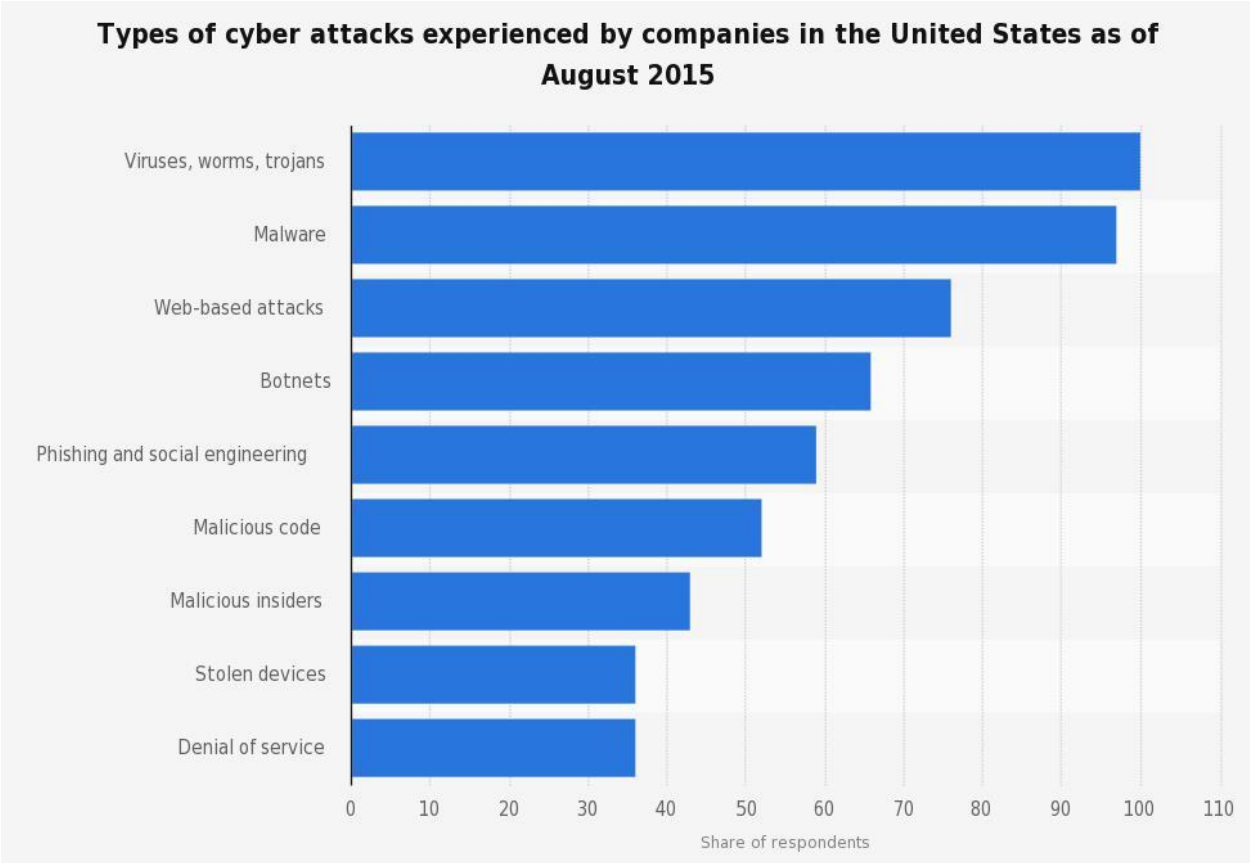
Αφού λοιπόν ο στόχος έχει αναγνωριστεί και έχει μελετηθεί, περνάμε στους τρόπους επίθεσής. Εδώ υπάρχει μεγαλύτερη ποικιλία και οι κυριότεροι τρόποι επίθεσης παρουσιάζονται στην παρακάτω λίστα.

- ***Back doors***: Είναι η εγκατάσταση ενός προγράμματος στο υπό επίθεση σύστημα για να υπάρχει μόνιμη πρόσβαση. Συνήθως αυτά εγκαθίστανται μέσω των malwares.
- ***Εκτέλεση κώδικα***: Όταν ο επιτιθέμενος αποκτήσει πρόσβαση σε μια συσκευή μπορεί να κάνει διάφορα πράγματα. Το πιο σημαντικό όμως είναι η δυνατότητα να εκτελέσει κώδικα. Με την εκτέλεση αυτή μπορεί να αποκτήσει πρόσβαση σε σημαντικές πληροφορίες από την συσκευή (πλήγμα στην εμπιστευτικότητα), μπορεί να αλλάξει το configuration κατά το δοκούν (πλήγμα στην ακεραιότητα των δεδομένων) ή ακόμη και να καταφέρει τη διακοπή της λειτουργίας της (πλήγμα στη διαθεσιμότητα).
- ***DoS/DDoS***: Εδώ γίνεται αναφορά σε Denial of Service/Distributed Denial of Service. Η διαφορά τους έγκειται στο πόσες διαφορετικές "μηχανές" χρησιμοποιούνται στην επίθεση. Πέραν τούτου, ο στόχος είναι ο ίδιος, να θέσουν το δίκτυο ή την συσκευή εκτός λειτουργίας στέλνοντας περισσότερα δεδομένα και δημιουργώντας περισσότερη κίνηση από αυτή που μπορεί να αντέξει. Τα τελευταία χρόνια, έδαφος γνωρίζει άλλος ένας παρόμοιος τρόπος επίθεσής το RDDoS, που σημαίνει Reflected Distributed Denial of Service, δηλαδή όταν η αρχική πηγή δεδομένων έχει "μεταμφιεστεί" και παρουσιάζεται σαν την πραγματική (έχει γίνει spoofed από τον επιτιθέμενο)οπότε και γίνεται, πλέον, μέρος του υπό επίθεση συστήματος[1].
- ***Botnets:*** Εδώ ουσιαστικά αναφερόμαστε σε μια ομάδα μολυσμένων συσκευών που ελέγχονται από ένα τρίτο άτομο, απομακρυσμένα. Αυτές οι συσκευές μπορούν, για παράδειγμα, να λάβουν διαταγή να στέλνουν συνεχή requests σε μια συγκεκριμένη συσκευή, βγάζοντάς την εκτός λειτουργίας.
- ***Brute-force attacks:*** Είναι η διαδικασία κατά την οποία ένα σύστημα κάνει αυτοματοποιημένα έναν μεγάλο αριθμό προσπαθειών (χιλιάδες προσπάθειες ή και περισσότερο) με σκοπό να βρει τον σωστό συνδυασμό username/password. Πρόκειται για τη λεγόμενη password guessing διαδικασία η οποία μπορεί να πραγματοποιηθεί από malware ή από man-in-the-middle attacks χρησιμοποιώντας packet-sniffers και keyloggers. Συνήθως αντιμετωπίζεται περιορίζοντας τις συνεχόμενες ανεπιτυχείς προσπάθειες εισόδου και με ταυτόχρονη επαναφορά του κωδικού. Packet-sniffer είναι ένα λογισμικό με δυνατότητα παρακολούθησης της ροής πακέτων ενός δικτύου. Όταν γίνει αντιληπτό κάποιο πακέτο το οποίο ικανοποιεί συγκεκριμένα κριτήρια, καταγράφεται σε ένα αρχείο[2]. Keyloggers είναι προγράμματα που εγκαθίστανται στο registry ενός υπολογιστή και καταγράφουν όσα ο χρήστης πληκτρολογεί[3].
- ***Viruses/malware/Trojans:*** Είναι είδη κακόβουλου λογισμικού, τα οποία έχουν ως στόχο να καταστρέψουν χρήσιμα αρχεία ενός συστήματος (viruses), να υποκλέψουν σημαντικά αρχεία και πληροφορίες μεταμφιεζόμενα σε χρήσιμο μέρος της συσκευής (Trojans), είτε να υποκλέψουν προσωπικά δεδομένα και

[1] The Practice of Network Security: Deployment Strategies for Production Environments
[2] Packet-sniffer: A comparative study
[3] An introduction to keyloggers: Rats and Malware

κωδικούς στέλνοντάς τους στον επιτιθέμενο και να φορτώσουν το σύστημα με αχρείαστη δραστηριότητα επηρεάζοντας το bandwidth (malwares).

Πιο κάτω βλέπουμε έναν πίνακα που φαίνονται τα ποσοστά του κάθε τύπου επίθεσης ανά κατηγορία, σε 58 αμερικάνικες εταιρίες, χώρα στην οποία γίνονται και οι περισσότερες επιθέσεις. Η έρευνα έγινε στο τέλος του 2015 και αφορά περίοδο από 08/2015 έως 12/2015.



Εικόνα 3. Types of cyber-attacks experienced in US (as of August 2015)
Πηγή:http://www.statista.com/statistics/293256/cyber-crime-attacks-experienced-by-us-companies/

Υπάρχει όμως κάτι άλλο, πέρα όμως από τους κινδύνους που υπάρχουν στο διαδίκτυο, που οδήγησε στην ανάγκη για VPN; Για να απαντηθεί αυτό το ερώτημα το μόνο που έχουμε να κάνουμε είναι να δούμε λεπτομερώς την ιστορία και τα χαρακτηριστικά του IP protocol. Το Internet λειτουργεί με IP διευθύνσεις. Οι IP διευθύνσεις είναι τα νούμερα αυτά που επιτρέπουν σε όλες τις συσκευές που έχουν πρόσβαση στο Internet να επικοινωνούν μεταξύ τους[4]. Αν και εμείς συνηθίζουμε να μιλάμε με διευθύνσεις της μορφής www.unipi.gr, οι συνδεδεμένες στο Internet συσκευές μεταφράζουν αυτές τις διευθύνσεις σε αριθμητικές διευθύνσεις για να στέλνουν τα δεδομένα στη σωστή κατεύθυνση. Οι δυο μορφές των IP διευθύνσεων είναι η IPv4 (version 4) και η IPv6 (version 6). Οι διαφορές τους είναι πολλές και ξεκινούν από τον τρόπο που αναπαρίστανται μέχρι και στο θέμα ασφάλειας. Οι IPv4 έχουν κυριαρχήσει τα τελευταία 30 χρόνια, ενώ αντίθετα οι IPv6 διευθύνσεις αποτελούν μια νέα πρόταση που έχει έρθει στην επιφάνεια εδώ και λίγα χρόνια. Ενώ έχουν πολλά πλεονεκτήματα έναντι των IPv4, δεν έχουν

[4] Beginner's guide to Internet Protocol addresses

καταφέρει να κερδίσουν τον κόσμο του διαδικτύου. Μάλιστα έχει ονομαστεί και σαν Second Internet επειδή αλλάζει κατά πολύ την μέχρι τώρα οπτική που είχαμε μέχρι τώρα για τα δίκτυα[5].

Πριν ξεκινήσουμε να δούμε τι είναι αυτό που τις διαφοροποιεί στο θέμα της ασφάλειας, που είναι και το βασικό θέμα αυτής της διπλωματικής εργασίας, ας δούμε κάποιες γενικές διαφορές.

1. Οι διευθύνσεις IPv4 είναι της μορφής xxxx.xxxx.xxxx.xxxx ενώ οι IPv6 είναι της μορφής xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.
2. Μπορούν να υπάρξουν 2^{32} διαθέσιμες IPv4 ενώ το πλήθος των IPv6 ανέρχεται στα 2^{128}
3. Χρειάζεται DHCP (Dynamic Host Configuration Protocol) ή στατικό configuration για να αποδοθούν IP διευθύνσεις στους hosts ενώ στο IPv6 μπορούν να χρησιμοποιείται stateless auto-configuration[6]. Από το DHCP χρησιμοποιούνται μόνο κάποιες λειτουργείες, περισσότερο για να μάθουν άλλες πληροφορίες, όπως πληροφορίες σχετικές με του DNS (Domain Name Servers) servers.
4. Ακριβώς επειδή οι IPv4 διευθύνσεις κυριαρχούν εδώ και χρόνια, υπάρχουν ελάχιστες συσκευές που υποστηρίζουν και IPv4 μαζί με IPv6 και ακόμη λιγότερες που υποστηρίζουν μόνο IPv6. Παρόλα αυτά ή μεταφορά από IPv4 σε IPv6 είναι κάτι αναπόφευκτο, κυρίως λόγω του πεπερασμένου αριθμού IPv4 διευθύνσεων και, αργά ή γρήγορα, αυτή η μεταφορά θα ολοκληρωθεί.
5. Το IPv4 χρησιμοποιεί NAT (Network Address Translation) για να μπορέσει ουσιαστικά να επεκτείνει το εύρος των χρησιμοποιούμενων διευθύνσεων, ενώ το IPv6, λόγω του τεραστίου εύρους των διευθύνσεων δεν το χρειάζεται. Όπως θα δούμε παρακάτω το NAT εμποδίζει τη σωστή λειτουργία του IPsec, οπότε, εκ των πραγμάτων αποτελεί μεγάλο μειονέκτημα του IPv4.

Η μεγαλύτερη όμως διαφορά, που άπτεται του θέματός μας, είναι ότι το IPv4 δημιουργήθηκε χωρίς η ιδέα της ασφάλειας να απασχολεί. Αυτό είχε σαν αποτέλεσμα να στηρίζεται στους τελικούς χρήστες (end-hosts) για να προσφέρουν τα απαραίτητα επίπεδα ασφάλειας κατά την επικοινωνία τους (κυρίως με τη χρήση του IPsec)[7]. Αυτό σημαίνει ότι χωρίς τα απαραίτητα πρωτόκολλα ασφαλείας, το IPv4 είναι εντελώς ανοιχτό σε επιθέσεις και δεν προσφέρει κανένα επίπεδο ασφάλειας στους χρήστες. Από την άλλη, το IPv6 έχει δημιουργηθεί με ενσωματωμένο το IPsec χωρίς όμως αυτό να σημαίνει ότι είναι προϋπόθεση η υλοποίησή του για να λειτουργήσει το IPv6. Όπως αναφέραμε και πιο πάνω, η παντελής απουσία του NAT κάνει πολύ πιο εύκολη τη λειτουργία του IPsec. Επίσης, είναι πολύ σημαντικό να αναφέρουμε ότι το IPv6 έχει μια λειτουργία η οποία προσφέρει ανωνυμία όταν αυτό είναι απαιτητό[8].

Σε αυτό το σημείο, ο οποιοσδήποτε, θα μπορούσε με ευκολία να πει ότι αντί να καταφύγουμε στην υλοποίηση των VPN θα μπορούσαμε να κάνουμε άμεσα τη μετάβαση σε IPv6. Αυτό όμως δεν είναι τόσο εύκολο, κατ' αρχάς, επειδή σημαντικό ρόλο παίζει η

[5] The Second Internet. Reinventing Computer Networking with IPv6
[6] IPv6 Essentials
[7] IPv6-to-IPv4 Transition and Security Issues
[8] Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks

συμβατότητα των μηχανημάτων. Αυτή τη στιγμή, η πλειοψηφία των μηχανημάτων που για να λειτουργήσουν χρειάζονται μια IP, είναι συμβατά μόνο με IPv4. Οπότε, η πλήρης μετάβαση σε IPv6 είναι ένας στόχος ο οποίος θα καθυστερήσει αρκετά να επιτευχθεί. Μια ενδιάμεση λύση, η οποία αρχίζει σιγά σιγά να χρησιμοποιείται, είναι η ταυτόχρονη χρησιμοποίηση IPv4 και IPv6. Σε αυτό βοηθούν αρκετά και τα πρωτόκολλα δρομολόγησης, όπως το BGP, EIGRP και OSPF. Η κατάσταση κατά την οποία IPv4 και IPv6 συνυπάρχουν, ονομάζεται dual-stack[9].

Είναι όμως πραγματικά έτσι; Είναι το dual-stack ή η πλήρης μεταφορά σε IPv6 η λύση; Ας πάρουμε πρώτα την περίπτωση του dual-stack. Το μεγάλο μειονέκτημα είναι ότι η υποστήριξη IPv4 και IPv6 πάνω στα ίδια links, διπλασιάζει και το πιθανό πεδίο επίθεσης[10]. Ο διπλασιασμός όμως του πιθανού πεδίου επίθεσης, παρά τους κινδύνους που εγκυμονεί, σε ένα καλό και σωστά σχεδιασμένο σύστημα ανίχνευσης “εισβολής” (Intrusion Detection System) υπάρχουν διπλάσιες πιθανότητες ανίχνευσης απειλών που έχουν τη βάση τους στη μη σωστή υλοποίηση των πρωτοκόλλων ασφαλείας.

Τέλος, ακόμη και στην περίπτωση που με κάποιον τρόπο γινόταν άμεση μεταφορά στο IPv6, δε θα είχαμε απαλλαχθεί από τις πιθανές απειλές. Υπάρχουν αρκετά προβλήματα ασφαλείας αυτή τη στιγμή. Ένα από αυτά είναι οι πολλοί τρόποι που μπορεί να γραφτεί μια διεύθυνση IPv6[11]. Για παράδειγμα η IP 2001:0DB8:0BAD:0000:0000:0000:0000:0DAD, μπορεί να γραφτεί 2001:0DB8:0BAD::0DAD ή 2001:DB8:BAD:0:0:0:0:0DAD ή 2001:db8:bad::dad. Αυτό από μόνο του κάνει πολύ δύσκολη την αναζήτηση σε αρχεία καταγραφής (log files) που σχετίζονται με την ασφάλεια του συστήματος. Επίσης, δεν έχουν καταρτιστεί πλήρεις λίστες με web sites που είναι πήγες malware. Γενικά, στο IPv6 δεν έχουν γίνει ακόμη πλήρη και εκτενή τεστ, οπότε δεν μπορούμε να είμαστε σίγουροι ότι δεν υπάρχει κάποια ευπάθεια την οποία θα μπορέσουν να χρησιμοποιήσουν οι κακόβουλοι χρήστες.

Παρατηρώντας όλα τα παραπάνω, είναι φανερή σε όλους, η όλο και περισσότερο αυξανόμενη ανάγκη για ασφάλεια. Είτε πρόκειται για μια απλή online αγορά, είτε πρόκειται για ανταλλαγή ευαίσθητων και πολύτιμων δεδομένων μεταξύ δυο υπολογιστών πολυεθνικών εταιριών. Πέρα από τις βασικούς τρόπους αντιμετώπισης των απειλών, το VPN έρχεται να προστεθεί σαν ένα επιπλέον όπλο στη φαρέτρα της διαδικτυακής ασφάλειας παρέχοντας προστασία, η κρυπτογράφηση στις συνδέσεις μεταξύ δυο συσκευών.

Πάμε να δούμε όμως, επιγραμματικά, ποια είναι η πορεία των VPN μέσα στο χρόνο. Μια πρώιμη μορφή των ιδιωτικών δικτύων παρουσιάζεται στις αρχές του 1960 και ονομάζονται μισθωμένες γραμμές. Οι μισθωμένες γραμμές ήταν ουσιαστικά η τηλεπικοινωνιακή σύνδεση δύο ή περισσοτέρων σημείων που όμως η ταχύτητα μεταφοράς δεδομένων ήταν ορισμένη από πριν. Για να γίνει πιο κατανοητό, μισθωμένες γραμμές είναι ένα είδος δικτύου που το χρησιμοποιούσε μια εταιρία, περισσότερο για ενδοεταιρική χρήση, κάτι σαν ένα τοπικό ιδιωτικό δίκτυο. Η μεγάλη διαφορά είναι ότι αυτού του είδους οι γραμμές δεν ανήκουν στο δημόσιο τηλεπικοινωνιακό δίκτυο και οποιαδήποτε point-to-point σύνδεση γινόταν χωρίς τη μεσολάβηση του τηλεπικοινωνιακού παρόχου. Αυτές οι μισθωμένες γραμμές εκτελούσαν

[9] Security Mechanisms for the IPv4 to IPv6 Transition
[10] http://searchtelecom.techtarget.com/answer/What-security-issues-arise-with-IPv6-and-IPv4-in-a-multi-tenant-cloud
[11] http://www.esecurityplanet.com/network-security/

πολλαπλές λειτουργίες, μέσα στις οποίες, οι κυριότερες, ήταν η μεταφορά δεδομένων, η χρήση fax, η τηλεφωνική επικοινωνία καθώς και η σύνδεση με το Internet.

Τα πλεονεκτήματα ήταν:

1. Σταθερή χωρητικότητα
2. Υποστήριξη αναλογικής αλλά και ψηφιακής γραμμής
3. Πανελλαδική και διεθνής γεωγραφική κάλυψη
4. Ποιότητα και αξιοπιστία.

Ειδικά η ποιότητα και η αξιοπιστία ήταν το πλεονέκτημα που οδήγησε τις μισθωμένες γραμμές να έχουν τόσο μεγάλη επιτυχία.

Τα μειονεκτήματα ήταν:

1. Έλλειψη ευελιξίας
2. Σταθερό κόστος μίσθωσης που ήταν ανεξάρτητο από τον όγκο των δεδομένων που μεταφέρονται
3. Υψηλό κόστος μίσθωσης.

Βλέπουμε λοιπόν ότι η ποιότητα και η αξιοπιστία που παρουσιαζόταν σαν τα μεγαλύτερα πλεονεκτήματα, ουσιαστικά οδηγούσαν και στην ύπαρξη του υψηλού κόστους που ήταν από τα βασικά μειονεκτήματα. Η σύγκρισή πλεονεκτημάτων και μειονεκτημάτων, οι συνεχώς μεταβαλλόμενες ανάγκες των εταιριών καθώς και η αλματώδης ανάπτυξη της επιστήμης της πληροφορικής και των δικτύων είναι οι κύριοι λόγοι που το project των μισθωμένων γραμμών σταμάτησε να είναι τόσο δημοφιλές και έγινε η μετάβαση στα Virtual Private Networks με τη σημερινή μορφή.

Στη συνέχεια της παρούσας μεταπτυχιακής διατριβής θα δούμε τί είναι τα VPN, τί μας προσφέρουν, σε ποιές κατηγορίες χωρίζονται αλλά και πώς μπορούμε να τα εγκαταστήσουμε για να εκμεταλλευτούμε τις δυνατότητες που προσφέρουν.

2. Ιδιωτικά Εικονικά Δίκτυα (Virtual Private Networks - VPN)

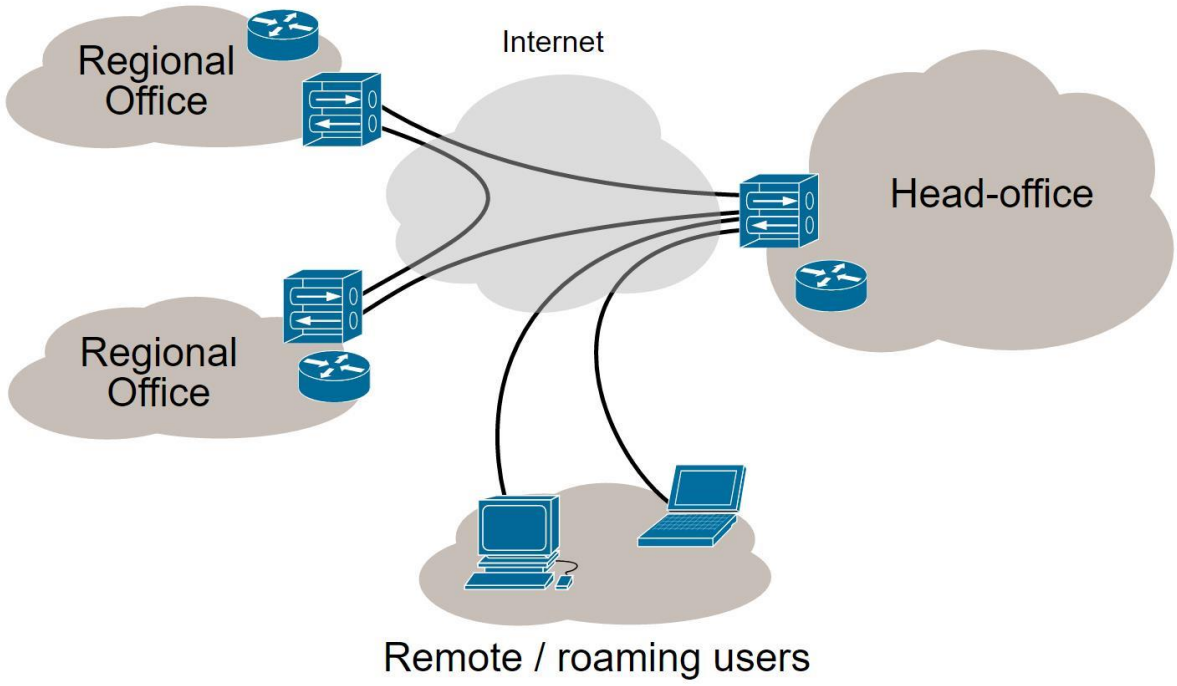
2.1. Τί είναι το VPN;

Για να καταλάβουμε καλύτερα τι είναι ένα VPN είναι πιο εύκολο να το χωρίσουμε στις τρεις λέξεις που το αποτελούν. VPN σημαίνει Virtual Private Network. Ας πάρουμε τις λέξεις μια-μια για να μπορέσουμε να καταλήξουμε σε έναν ορισμό.

- Virtual: Όπως προκύπτει από τη ακριβή μετάφραση, virtual σημαίνει εικονικός. Σε μια προσπάθεια ευρύτερης κατανόησης του όρου, το virtual αναφέρεται στη λογική και όχι τόσο στην φυσική σύνδεση μεταξύ δυο συσκευών. Τόσο επειδή συνδέονται δυο συσκευές απομακρυσμένα σα να ήταν στο ίδιο τοπικό δίκτυο, αλλά και επειδή αυτή η σύνδεση δεν είναι μόνιμη, ενεργοποιείται ad hoc, δηλαδή κάθε φορά που αυτές οι δυο συσκευές θέλουν να επικοινωνήσουν.
- Private: Και σε αυτό το σημείο το private είναι ακριβώς αυτό που δηλώνει η σημασία της λέξης. Μια σύνδεση ιδιωτική στην οποία συμμετέχουν μόνο οι εκάστοτε δυο συσκευές που θέλουν να επικοινωνήσουν. Δεν είναι όμως μόνο η ιδιωτικότητα που μας ενδιαφέρει. Αν ήταν μόνο αυτό, δε θα διέφερε σε τίποτα από μια σύνδεση με καλώδιο. Θέλουμε και την ασφάλεια που μπορεί να μας προσφέρει αυτή η ιδιωτικότητα. Ασφάλεια και προστασία από οποιαδήποτε εξωτερική παρέμβαση, αφού στην πλειονότητα, οι πληροφορίες που μεταφέρονται μέσα από ένα VPN είναι σημαντικές και απόρρητες.
- Network: Είναι η πιο απλή και η πιο εύκολα κατανοήσιμη λέξη. Δίκτυο είναι μια φυσική σύνδεση κατά την οποία επικοινωνούν συσκευές μεταξύ τους. Για να θεωρήσουμε κάτι σαν δίκτυο, θα πρέπει να επικοινωνούν τουλάχιστον δυο συσκευές, χωρίς κάποιον περιορισμό για ανώτατο αριθμό. Αυτές τις συσκευές μπορεί να τις χειρίζεται άνθρωπος (end user) είτε κάποιες από αυτές μπορεί αν είναι αυτοματοποιημένες και να μην εμπλέκεται ο ανθρώπινος παράγοντας στο χειρισμό του.

Βλέποντας την πιο πάνω ανάλυση των επιμέρους στοιχείων, θα προσπαθήσουμε να δώσουμε έναν ορισμό στο VPN. Κατά καιρούς έχουν εμφανιστεί διαφορετικοί ορισμοί. Για παράδειγμα, ένας ορισμός αναφέρει ότι *"VPN είναι μια επέκταση ενός ιδιωτικού εταιρικού δικτύου πάνω σε ένα δημόσιο δίκτυο όπως το Internet"* [12]. Ένας άλλος ορισμός αναφέρει ότι *"το VPN είναι μια σύνδεση που δίνει τη δυνατότητα στους χρήστες να στέλνουν και να λαμβάνουν δεδομένα μέσω κοινών ή δημοσίων δικτύων, σα να ήταν συνδεδεμένα σε ιδιωτικό δίκτυο"* [13]. Ένας τρίτος, λίγο πιο πολύπλοκος, αναφέρει ότι " *ένα VPN είναι ένα "κλειστό" (Private) group κόμβων που θέλουν να συνδεθούν σε ένα δίκτυο (Network) και είναι πρόθυμοι να χρησιμοποιήσουν εικονικές συνδέσεις, ή ψεύδο-καλώδια (Virtual) αντί για φυσικές συνδέσεις*"[14]. Βλέπουμε ότι οι ορισμοί δεν απέχουν και πολύ μεταξύ τους. Αν θα προσπαθούσαμε να ορίσουμε κ εμείς το VPN βάσει των γνώσεων που έχουμε, θα μπορούσαμε να το ορίσουμε σαν μια σύνδεση δικτύου που μας επιτρέπει να δημιουργήσουμε μια ασφαλή σύνδεση ανάμεσα σε δυο απομακρυσμένα ιδιωτικά δίκτυα, πάνω στο δημόσιο Internet.
Όλα όσα αναφέρθηκαν πιο πάνω θα μπορούσαν να αναπαρασταθούν στην πιο κάτω εικόνα.

[12]A technical guide to IPsec Virtual Private Networks
[13]https://en.wikipedia.org/wiki/Virtual_private_network
[14]Recent Advances in Networking



Εικόνα 4. Αναπαράσταση VPN
Πηγή:https://upload.wikimedia.org/wikipedia/commons/thumb/0/00/Virtual_Private_Network_overview.svg/2000px-Virtual_Private_Network_overview.svg.png

2.2. Πλεονεκτήματα VPN

Τα κύρια πλεονεκτήματα του VPN παρουσιάζονται παρακάτω. Δε νοείται σωστά σχεδιασμένο VPN που να μην έχει τα παρακάτω χαρακτηριστικά.

- **Κόστος (Cost):** Ένα χαρακτηριστικό που κάνει τη χρήση του VPN προτιμητέα σε σχέση με άλλες τεχνολογίες είναι φυσικά το κόστος. Η άλλη προφανής λύση θα ήταν η επικοινωνία μεταξύ των δυο συσκευών μέσω ενός dedicated link. Το κόστος όμως του να αγοράσει κανείς μια σύνδεση αποκλειστικά την επικοινωνία δυο συσκευών είναι απαγορευτικό, ειδικά από τη στιγμή που για να συνδεθεί ασφαλώς με κάθε άλλο επιθυμητό host, θα έπρεπε να αγοραστεί ξεχωριστό dedicated link. Τί πιο φτηνό λοιπόν και εύκολο από το να χρησιμοποιηθεί το ίδιο το Internet και μέσω κάποιου ISP (Internet Service Provider) να επιτευχθεί αυτή η σύνδεση;
- **Επεκτασιμότητα (Scalability):** Στηριζόμενοι ακριβώς στο προηγούμενο επιχείρημα, ότι δηλαδή ο πιο φτηνός τρόπος επικοινωνίας είναι μέσω ενός ISP, προκύπτει και το επόμενο πλεονέκτημα του VPN. Επειδή όλες οι συσκευές, πλέον, είναι συνδεδεμένες στο Internet, η δυνατότητα επεκτασιμότητας είναι άλλο ένα μεγάλο πλεονέκτημα που συναντούμε στο VPN σε σχέση με τις ασφαλείς συνδέσεις μέσω του public Internet. Άρα η γεωγραφική και η αριθμητική επέκταση δεν αποτελούν πρόβλημα, αφού το μέσο παραμένει το ίδιο.

- **Ευελιξία (Flexibility):** Και πάλι το μέσο, δηλαδή το Internet, είναι αυτό που παρέχει το πλεονέκτημα της ευελιξίας. Δε χρειάζονται ειδικές συσκευές ή συμβατός εξοπλισμός για να επικοινωνήσουν οι εκάστοτε δύο συσκευές. Ο ISP κάνει όλη τη δουλειά.
- **Διαχείριση (Management):** Όλες οι πολιτικές ασφαλείας, το IP addressing, οι πολιτικές πρόσβασης και οτιδήποτε άλλο χρειάζεται για να επιτευχθεί μια σωστή και ασφαλής πρόσβαση μέσω VPN, βρίσκονται και διαχειρίζονται από το ίδιο σημείο.
- **Ασφάλεια (Security)**: Το πιο σημαντικό κομμάτι είναι η ασφάλεια. Αυτό που κάνει το VPN ιδιαίτερο είναι το γεγονός ότι δεν είναι εύκολο για κάποιον να παρακολουθήσει και να καταγράψει τα δεδομένα μιας επικοινωνία μεταξύ των συσκευών που χρησιμοποιούν VPN. Οι τέσσερεις έννοιες που κυριαρχούν στο VPN είναι η εμπιστευτικότητα (confidentiality), η ακεραιότητα των δεδομένων (data integrity), η αυθεντικοποίηση (authentication) και η προστασία αντιγραφής δεδομένων (anti-replay protection).

2.3. Εργαλεία, αλγόριθμοι και πρωτόκολλα που χρησιμοποιούνται για την επίτευξη των πλεονεκτημάτων του VPN

Η εμπιστευτικότητα επιτυγχάνεται με την κρυπτογράφηση, οπότε ακόμη και αν υποθέσουμε ότι κάποιος καταφέρνει να υποκλέψει δεδομένα, χωρίς τα απαραίτητα κλειδιά δε θα μπορούσε, με ευκολία τουλάχιστον, να καταλάβει το περιεχόμενο των δεδομένων. Οι αλγόριθμοι που χρησιμοποιούνται για την κρυπτογράφηση είναι γνωστοί και εδώ μεγάλο ρόλο παίζουν τα κλειδιά. Αν ο αποστολέας και ο παραλήπτης έχουν τα απαραίτητα κλειδιά μπορούν ευκολά να αποκρυπτογραφήσουν τα δεδομένα. Σχετικά με την ακεραιότητα των δεδομένων χρησιμοποιούνται πολλαπλοί έλεγχοι ακεραιότητας έτσι ώστε να είναι σίγουρο ότι το ένα άκρο του VPN λαμβάνει την αρχική πληροφορία ακριβώς όπως την στέλνει το άλλο άκρο, χωρίς να έχει αλλαχθεί ή χαθεί τίποτα. Περνώντας στο anti-replay protection, είναι σημαντικό, πέρα από το να διασφαλίσουμε ότι δε θα πειραχτούν τα δεδομένα που στέλνονται από τον έναν υπολογιστή στον άλλον μέσω του VPN, να είμαστε σίγουροι ότι κάποιος τρίτος δε θα αντιγράψει τα δεδομένα και δε θα τα στείλει σε μια συσκευή δημιουργώντας ακόμη μια VPN σύνδεση. Υπάρχουν λοιπόν ενσωματωμένοι μηχανισμοί ελέγχου που ελέγχουν κάθε πακέτο που στέλνεται. Αν ο έλεγχος αυτός παρατηρήσει ένα πανομοιότυπα πακέτο με κάποιο άλλο που έχει σταλεί νωρίτερα, τότε αυτό το πακέτο θεωρείται ως μη έγκυρο. Όλα τα παραπάνω είναι πολύ σημαντικά και διασφαλίζουν σε μεγάλο βαθμό την ασφάλεια μεταφοράς δεδομένων. Τι γίνεται όμως αν η μια άκρη του VPN δε μπορεί να εξακριβώσει ότι ο χρήστης στην άλλη άκρη είναι αυτός που δηλώνει ότι είναι και τελικά καταλήξει να συνδεθεί με τον υπολογιστή του επιτιθέμενου; Σε αυτή την περίπτωση δεν έχει σημασία κανένα μέτρο προστασίας που χρησιμοποιούμε. Εδώ λοιπόν μπαίνει η έννοια του authentication.

2.3.1. Αλγόριθμοι

Συμμετρικοί/Ασύμμετροι (Symmetric/Asymmetric) αλγόριθμοι: Αυτοί οι αλγόριθμοι χρησιμοποιούνται για να γίνει κρυπτογράφηση των δεδομένων. Στους συμμετρικούς αλγόριθμους χρησιμοποιείται το ίδιο κλειδί για να κρυπτογραφηθεί και να αποκρυπτογραφηθεί η πληροφορία που ανταλλάσσεται ανάμεσα στα δυο άκρα του VPN. Άρα

για να μπορέσουν να επικοινωνήσουν αποτελεσματικά οι δυο hosts, θα πρέπει και οι δυο να έχουν το ίδιο κλειδί. Φυσικά, για λόγους ασφαλείας αυτό το κλειδί κρυπτογραφείται χρησιμοποιώντας έναν symmetric encryption αλγόριθμο. Οι πιο γνωστοί symmetric αλγόριθμοι είναι οι DES, 3DES, AES, RC2, RC6, Blowfish και Serpent. Αυτού του είδους οι αλγόριθμοι χρησιμοποιούνται ευρέως από τα VPN γιατί δεν επιβαρύνουν το σύστημα και χρησιμοποιούν μικρή ισχύ από τη CPU. Σε κάθε αλγόριθμο σημασία παίζουν τα bit κρυπτογράφησης. Όσο περισσότερα τα bit, τόσο πιο ασφαλής είναι η κρυπτογράφηση. Συνήθως τα bit που χρησιμοποιούνται είναι 128 και είναι το ασφαλές ελάχιστο για την κρυπτογράφηση. Μια κρυπτογράφηση όμως με 256 bit είναι σαφώς ασφαλέστερη από μια με 128 bit. Οι ασύμμετροι αλγόριθμοι είναι μια άλλη κατηγορία που διαφέρει σε αρκετά σημεία με τους συμμετρικούς. Εδώ χρησιμοποιούμε ένα ζεύγος κλειδιών. Ένα public και ένα private κλειδί. Μιλάμε για διαφορετικά κλειδιά γιατί εδώ χρησιμοποιούμε το ένα για να γίνει η κρυπτογράφηση και το δεύτερο για να γίνει η αποκρυπτογράφηση. Για να καταλάβουμε καλύτερα τη λειτουργία του ζεύγους κλειδιών, θα δώσουμε ένα παράδειγμα. Ας υποθέσουμε ότι έχουμε ένα μεγάλο χρηματοκιβώτιο το οποίο έχει μια μεγάλη κλειδαριά που έχει 2 εσοχές κλειδιών. Μια μεγάλη και μια μικρή. Αν κλειδώσουμε το χρηματοκιβώτιο με το μεγάλο κλειδί, τότε ο μόνος τρόπος να το ξεκλειδώσουμε είναι να χρησιμοποιήσουμε το μικρό κλειδί. Αντίστοιχα, αν κλειδώσουμε με το μικρό κλειδί, θα χρειαστούμε το μεγάλο για να ξεκλειδώσουμε. Αυτό το παράδειγμα δόθηκε για να γίνει καλύτερα αντιληπτή η λειτουργία του ζεύγους κλειδιών καθώς και η αναγκαιότητα και η αλληλοσυμπλήρωσή τους. Τα ονόματά τους, private και public τα πήραν ακριβώς για αυτό που σημαίνουν. Το public key είναι το κλειδί το οποίο μπορεί να διατεθεί σε οποιονδήποτε και το γνωρίζει κάθε ένας που θέλει να το χρησιμοποιήσει. Το private key όμως είναι ένα κλειδί το οποίο το γνωρίζει μόνο αυτός που το δημιουργεί. Οι πιο γνωστοί ασύμμετροι αλγόριθμοι είναι οι ECC, DSA, YAC, RSA, Diffie-Hellman. Οι αλγόριθμοι αυτοί δε χρησιμοποιούνται τόσο στην κρυπτογράφηση αλλά στην αυθεντικοποίηση του χρήστη καθώς ναι μεν είναι πιο ασφαλείς, αλλά χρειάζονται μεγάλη ισχύ CPU. Και σε αυτή την περίπτωση όσο περισσότερα είναι τα bit κρυπτογράφησης, τόσο μεγαλύτερη ασφάλεια έχουμε. Το ασφαλές ελάχιστο είναι τα 2048 bit και μπορούμε να φτάσουμε μέχρι και 4096 bit.

Συναρτήσεις Κατακερματισμού (Hash function): Οι αλγόριθμοι αυτοί χρησιμοποιούνται για την προστασία της ακεραιότητας των δεδομένων (data integrity). Ακόμη και αν καταφέρουμε να κρυπτογραφήσουμε επαρκώς τα δεδομένα που στέλνονται από τον έναν χρήστη στον άλλον, θα πρέπει να βρούμε έναν τρόπο να είμαστε σίγουροι ότι τα δεδομένα που έφυγαν από τον αποστολέα, θα φτάσουν χωρίς καμία αλλαγή στον παραλήπτη. Η διαδικασία λειτουργεί ως εξής. Χρησιμοποιώντας μια συνάρτηση hash, τα δεδομένα δίνονται σαν είσοδος στη συνάρτηση και ως έξοδος λαμβάνεται μια τιμή κατακερματισμού (hash value). Όπως είναι λογικό, τα ίδια ακριβώς δεδομένα παράγουν ίδια hash value. Εδώ θα πρέπει να τονίσουμε το εξής. Ενώ πρακτικά είναι σχεδόν απίθανο, θεωρητικά είναι πιθανό, διαφορετικά δεδομένα να παράγουν το ίδιο hash value. Όταν λοιπόν το ένα άκρο του VPN στέλνει δεδομένα προσαρτά αυτό το hash value στο πακέτο που στέλνει. Ο παραλήπτης, ο οποίος γνωρίζει τον αλγόριθμο που έχει χρησιμοποιηθεί, χρησιμοποιεί και αυτός τον ίδιο αλγόριθμο στο πακέτο. Αν το hash value είναι το ίδιο, βάσει των προαναφερθέντων, σημαίνει ότι το πακέτο δεν έχει υποστεί καμία αλλοίωση και θεωρείται έγκυρο. Οι τρείς πιο γνωστοί hash αλγόριθμοι είναι οι MD5 (128 bit), SHA1(160 bit) και SHA2 (224-512 bit). Και σε αυτή την περίπτωση, όσα περισσότερα τα bit, τόσο μεγαλύτερη η ασφάλεια.

Η χρήση των συναρτήσεων κατακερματισμού, επαρκεί μόνο για την προστασία παθητικών επιθέσεων. Ο μηχανισμός HMAC (Hashed Message Authentication Code) παρέχει προστασία και από ενεργητικές επιθέσεις. Εδώ έχουμε μια διαφορετική λειτουργία, αφού συνδυάζεται το hashing με την ύπαρξη ενός μυστικού κλειδιού. Έτσι, ο μόνος που μπορεί να επιβεβαιώσει το hash value είναι ο παραλήπτης του πακέτου που γνωρίζει αυτό το μυστικό κλειδί. Ακόμη, λοιπόν και στην περίπτωση που κάποιος καταφέρει να παρέμβει, δεν μπορεί να προσθέσει ή να αλλάξει δεδομένα, αφού δεν ξέρει το μυστικό κλειδί που χρησιμοποιήθηκε στον υπολογισμό.

2.3.2. Εργαλεία

Ψηφιακές Υπογραφές (Digital Signatures): Με τις ψηφιακές υπογραφές, επιτυγχάνουμε, κυρίως, τους στόχους της αυθεντικοποίησης και της ακεραιότητας των δεδομένων. Πέρα από αυτά τα δυο, επιτυγχάνεται και ένας τρίτος στόχος, που δεν είναι βέβαια μέσα στα τέσσερα βασικά χαρακτηριστικά του VPN, η μη αποποίηση ευθύνης (η μη ύπαρξη δυνατότητας να αποποιηθεί κάποιος, κάποια πράξη). Αυτό που, ουσιαστικά, θέλουμε να πετύχουμε είναι να μπορεί να αποδείξει το ένα άκρο του VPN στο άλλο, ότι πραγματικά είναι αυτός που δηλώνει. Εδώ κάνει την εμφάνισή της μια νέα έννοια, η Αρχή Πιστοποίησης (Certificate Authority - CA), δηλαδή μια αρχή έκδοσης πιστοποιητικών. Αυτή η CA θεωρείται έμπιστη και από τα δυο μέρη. Αφού λοιπόν, τα δυο μέλη του VPN έχουν δημιουργήσει ένα ζεύγος public και private κλειδιών, κάνουν μια αίτηση και παραλαμβάνουν από αυτή την Αρχή ένα πιστοποιητικό το οποίο περιλαμβάνει και το public key. Ο αποστολέας παίρνει τα δεδομένα που θέλει να στείλει, δημιουργεί ένα hash (όπως αναφέραμε και σε προηγούμενο κομμάτι της διατριβής), το κρυπτογραφεί με το private key του, το επισυνάπτει στα δεδομένα και το στέλνει στον παραλήπτη. Ο παραλήπτης από τη μεριά του, μόλις λάβει τα δεδομένα, αποκρυπτογραφεί το hash χρησιμοποιώντας το public key του αποστολέα, και μετά τρέχει τον ίδιο αλγόριθμο που χρησιμοποίησε για το hash ο αποστολέας. Αν το hash value επιβεβαιωθεί, ο παραλήπτης γνωρίζει άμεσα δυο πράγματα. Πρώτον ότι τα δεδομένα δεν έχουν αλλαχθεί και είναι ακριβώς τα ίδια που εστάλησαν, αλλά και ότι ο μοναδικός που θα μπορούσε να κάνει την κρυπτογράφηση είναι ο αποστολέας, χρησιμοποιώντας το private key του. Έτσι λοιπόν επιτυγχάνεται ο διττός στόχος της αυθεντικοποίησης και της ακεραιότητας των δεδομένων.

Εδώ όμως προκύπτει ένα εύλογο ερώτημα. Πώς ξέρει ο παραλήπτης το public key του αποστολέα; Όπως εύλογα θα μπορούσε να υποθέσει κάποιος, η όλη διαδικασία προϋποθέτει την ανταλλαγή πιστοποιητικών ανάμεσα στα δυο άκρα. Και εκεί όμως υπάρχει κάποια κρυπτογράφηση για να είμαστε σίγουροι ότι κάποιος δε θα υποκλέψει το πιστοποιητικό με το public key ώστε στη συνέχεια να υποκλέψει και να μπορέσει να διαβάσει τα κρυπτογραφημένα δεδομένα.

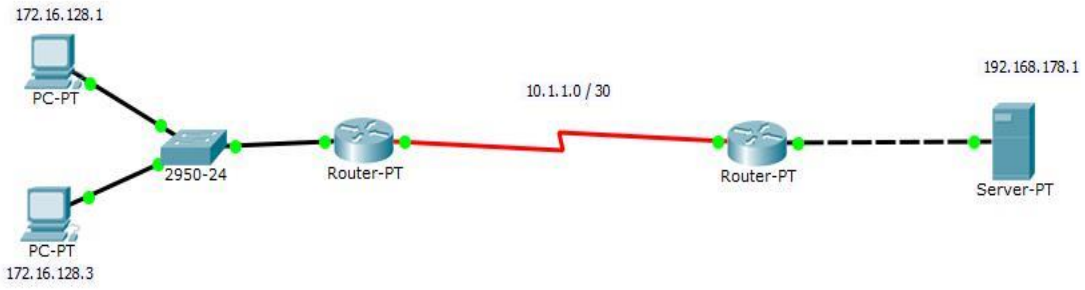
Firewalls: Το όνομά του στα ελληνικά μεταφράζεται σαν “πύρινο τείχος”. Αυτό από μόνο του υπονοεί ένα επίπεδο προστασίας για την οντότητα, μπροστά από την οποία είναι τοποθετημένο. Γενικά όμως με τον όρο firewall ορίζουμε ένα δικτυακό πρόγραμμα προστασίας, είτε hardware-based είτε software-based, το οποίο ελέγχει την εξερχόμενη και την εισερχόμενη κίνηση ενός δικτύου βασισμένο σε κάποιους κανόνες[15]. Συνήθως τοποθετείται ανάμεσα σε ένα έμπιστο και σε ένα μη-έμπιστο δίκτυο. Αν το firewall δε ρυθμιστεί σωστά τότε ο σκοπός του

[15]http://searchsecurity.techtarget.com/definition/firewall

αυτόματα αναιρείται. Η σωστή, όμως, ρύθμιση προϋποθέτει και άριστη γνώση του συστήματός μας, έτσι ώστε να γνωρίζουμε επακριβώς τι θέλουμε να επιτρέψουμε και τι όχι, αλλά και να γνωρίζουμε πώς να παραμετροποιούμε σωστά ένα firewall ώστε να ανταποκρίνεται σε ad hoc ανάγκες. Με να firewall ορίζουμε τις επιτρεπόμενες ανοιχτές θύρες, το είδος των εισερχόμενων, κυρίως, πακέτων, τα επιτρεπόμενα πρωτόκολλα κ.α. Μπορούμε ακόμη και να ρυθμίσουμε το χρονικό περιθώριο χρήσης μιας VPN session.

ACL (Access control lists): Οι access-lists βοηθούν να συγκεκριμενοποιήσουμε τον τύπο πακέτων, πρωτοκόλλων και IPs που θα έχουν τη δυνατότητα να εισέρχονται ή να εξέρχονται από μια interface ενός router ή ενός firewall. Οι access-lists χωρίζονται σε δυο κατηγορίες, τις basic και τις advanced. Όπως λέει και το όνομά τους, οι basic υλοποιούν έναν γενικό κανόνα ενώ οι advanced συγκεκριμενοποιούν αυτόν τον κανόνα. Σημαντικό είναι να γνωρίζουμε ότι με τον ορισμό μιας access-list πρέπει να μην αμελήσουμε να την ορίσουμε στη σωστή interface και με το σωστό προσανατολισμό (in/out) και να θυμόμαστε ότι στο τέλος, αν και δεν αναφέρεται, υπονοείται πάντα η εντολή *deny all*. Αν δεν λάβουμε αυτή την παράμετρο υπόψιν μας, οι ACLs δε θα ανταποκρίνονται σε αυτά που ζητάμε. Παρακάτω θα δώσουμε κάποια παραδείγματα με ACL για να δείξουμε πώς ακριβώς λειτουργούν.

Έχουμε την εξής τοπολογία. Υπάρχουν δυο υπολογιστές στο εσωτερικό δίκτυο που συνδέονται στο router που επικοινωνεί με ένα άλλο, απομακρυσμένο router, πίσω από το οποίο υπάρχει ένας Server. Στις παρακάτω εικόνες θα δείξουμε πώς μπορούμε να ρυθμίσουμε κατά το δοκούν ποιος υπολογιστής θα μπορεί να επικοινωνεί με τον Server, αλλά και τί είδους επικοινωνίας θα είναι αυτή. Όλα αυτά θα επιτευχθούν με την εισαγωγή κάποιων εντολών, άλλες απλές και άλλες πιο σύνθετες, στο router στο οποίο είναι συνδεδεμένοι οι υπολογιστές μας. Υποθέτουμε ότι το router πριν τον Server δεν έχει κάποιες ACLs.



Εικόνα 5. Τοπολογία για επεξήγηση Access Control Lists (ACL)

Αρχικά, όταν δεν έχουμε βάλει καμία ACL, ο host *172.16.128.1* όπως και ο 172.16.128.3 μπορούν να κάνουν ping, traceroute και να έχουν http πρόσβαση στον Server με IP *192.168.178.1*. Για του λόγου το αληθές παραθέτουμε τα αντίστοιχα screenshots.

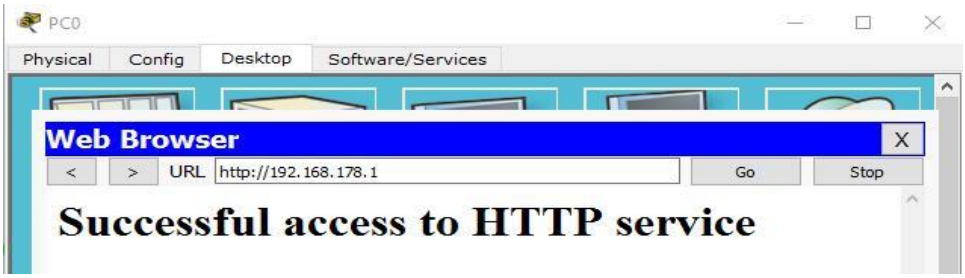
Από 172.16.128.1

```
PC>ping 192.168.178.1

Pinging 192.168.178.1 with 32 bytes of data:

Reply from 192.168.178.1: bytes=32 time=11ms TTL=126
Reply from 192.168.178.1: bytes=32 time=3ms TTL=126
Reply from 192.168.178.1: bytes=32 time=1ms TTL=126
Reply from 192.168.178.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.178.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 4ms
```

Εικόνα 6. Επιτυχημένο ping από 192.16.128.1

```
PC>tracert 192.168.178.1

Tracing route to 192.168.178.1 over a maximum of 30 hops:

  1    0 ms      0 ms      1 ms      172.16.128.2
  2    5 ms      1 ms      1 ms      10.1.1.2
  3    0 ms      1 ms      0 ms      192.168.178.1

Trace complete.
```

Εικόνα 7. Επιτυχημένο traceroute από 192.16.128.1



Εικόνα 8. Επιτυχημένη κλήση http από 192.16.128.1

Από 172.16.128.3

```
PC>ping 192.168.178.1

Pinging 192.168.178.1 with 32 bytes of data:

Reply from 192.168.178.1: bytes=32 time=2ms TTL=126
Reply from 192.168.178.1: bytes=32 time=1ms TTL=126
Reply from 192.168.178.1: bytes=32 time=1ms TTL=126
Reply from 192.168.178.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.178.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>tracert 192.168.178.1

Tracing route to 192.168.178.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      172.16.128.2
  2    1 ms      1 ms      8 ms      10.1.1.2
  3    1 ms      1 ms      0 ms      192.168.178.1

Trace complete.
```

Εικόνα 9. Επιτυχημένο ping και traceroute από 192.16.128.3

Εικόνα 10. Επιτυχημένη κλήση http από 192.16.128.3

Θα δούμε λοιπόν πως θα αλλάξουν τα αποτελέσματα αν τοποθετήσουμε κάποιες access-lists.

Παράδειγμα basic ACL

Access-list 1 permit 172.16.128.1 (επιτρέπει να περάσουν από ένα router πακέτα τα οποία προέρχονται ΜΟΝΟ από τη διεύθυνση 172.16.128.1. Όλα τα υπόλοιπα δεν επιτρέπεται να περάσουν γιατί εννοείται το deny all).

Πλέον το 172.16.128.1 μπορεί να κάνει ping.

```
PC>ping 192.168.178.1

Pinging 192.168.178.1 with 32 bytes of data:

Reply from 192.168.178.1: bytes=32 time=11ms TTL=126
Reply from 192.168.178.1: bytes=32 time=3ms TTL=126
Reply from 192.168.178.1: bytes=32 time=1ms TTL=126
Reply from 192.168.178.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.178.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 4ms
```

Εικόνα 11. Επιτυχημένο ping από 192.16.128.1

Το 172.16.128.3,όχι.

```
Pinging 192.168.178.1 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 192.168.178.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Εικόνα 12. Ανεπιτυχές ping από 192.16.128.3

Παράδειγμα advanced ACL

access-list 102 permit tcp any any eq www (επιτρέπει να περάσουν πακέτα από οποιονδήποτε host προς οποιονδήποτε host μόνο αν πρόκειται για TCP πακέτα και συγκεκριμένα HTTP. Πάλι το deny all εννοείται στο τέλος).

Όπως βλέπουμε το ping δε μπορεί να ολοκληρωθεί

```
Pinging 192.168.178.1 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 192.168.178.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Εικόνα 13. Ανεπιτυχές ping από 192.16.128.1

Η κλήση HTTP, μπορεί να ολοκληρωθεί.

Εικόνα 14. Επιτυχημένη κλήση http από 192.16.128.1

AAA Servers: Οι AAA Servers είναι Servers που προσφέρουν μια επιπρόσθετη ασφάλεια και πραγματοποιούν ελέγχους όταν κάποιος προσπαθεί να συνδεθεί σε ένα VPN. Έχουν πάρει το όνομά τους, το AAA, από τους 3 ελέγχους που πραγματοποιεί. Authentication (ποιός είναι δηλαδή ο χρήστης), Authorization (τί είδους πρόσβαση έχει) και, τέλος, Accounting (τί λειτουργίες μπορεί να πραγματοποιεί).

2.3.3. Πρωτόκολλα

IPsec: Το IPsec (Internet Protocol Security) είναι ένα σύνολο πρωτοκόλλων και αλγόριθμων που προσφέρουν ασφάλεια στις επικοινωνίες μέσω Internet, στο layer 3, δηλαδή στο network Layer[16]. Χρησιμοποιεί όλα τα προαναφερθέντα, αλλά μπορεί να εγγυηθεί και την τέταρτη κυρίαρχη έννοια στο VPN, την προστασία αντιγραφής δεδομένων, δηλαδή προστασία από την συνεχή αποστολή ίδιων πακέτων από κακόβουλο χρήστη. Το IPsec χρησιμοποιεί μια λειτουργία που ονομάζεται *anti-replay sliding window* και χρησιμοποιείται στις *replay attacks*[17]. Η λειτουργία του στηρίζεται στο γεγονός ότι κάθε πακέτο που στέλνεται σε κάθε session έχει ένα sequence number. Αυτό το sliding window κάνει κάποιους ελέγχους μόλις λάβει ένα πακέτο. Παρατηρούμε λοιπόν τρεις περιπτώσεις[18]. Αν το sequence number είναι μικρότερο από όλα τα sequence numbers στο window, ο anti-replay μηχανισμός δε μπορεί να επιβεβαιώσει αν το έχει λάβει νωρίτερα. Για να είναι ασφαλής, απορρίπτει το πακέτο θεωρώντας ότι το έχει ήδη λάβει. Αν το sequence number είναι μεγαλύτερο από όλα στο window, τότε πακέτο γίνεται δεκτό μιας και θεωρείται ότι δεν το έχει λάβει ακόμη και ταυτόχρονα το window μεταφέρεται τόσες θέσεις προς τα δεξιά έτσι ώστε αυτό το sequence number να είναι, πλέον, το ανώτατο άκρο. Τελευταία περίπτωση είναι αυτή κατά την οποία το sequence number είναι μέσα στα όρια του window. Αν λοιπόν το πακέτο με αυτό το sequence number δεν έχει παραληφθεί πιο πριν, γίνεται δεκτό.

[16]https://tools.ietf.org/html/rfc6071
[17]international conference on computer communications and networks, 2003 (ICCN 2003)
[18]Anti-Replay Window Protocols for Secure IP

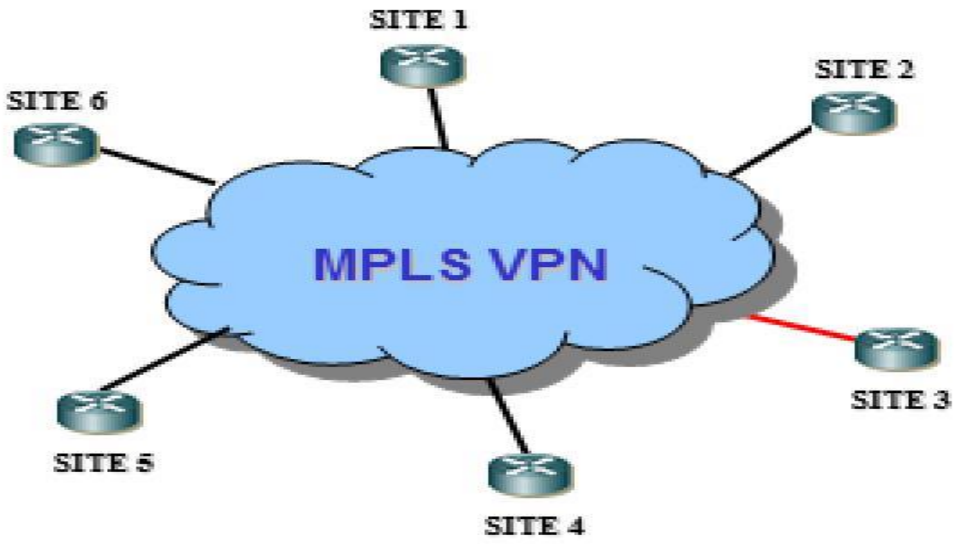
Αν έχει παραληφθεί, απορρίπτεται. Εδώ φυσικά είναι πολύ σημαντικό να πούμε ότι μετά το anti-replay sliding window τα πακέτα περνούν από integrity check. Αν αυτός ο έλεγχος δεν είναι επιτυχής, τότε τα πακέτα απορρίπτονται.

2.4. Είδη VPN

Υπάρχουν πολλές τεχνολογίες VPN όμως οι τρεις πιο σημαντικές είναι το MPLS VPN, το IPsec VPN και το SSL VPN[19]. Παρακάτω θα πούμε λίγα λόγια για τις τρεις αυτές τεχνολογίες.

2.4.1. MPLS VPN

Το MPLS σημαίνει Multi-protocol Label Switching. Τα VPN με αυτή την τεχνολογία ονομάζονται πλήρως MPLS Layer 3 VPN ή αλλιώς MPLSL3VPN. Τέτοιου είδους VPN παρέχονται από τους Internet providers και έχουν κυρίως ζήτηση από τις εταιρίες που έχουν πολλά γραφεία σε διαφορετικές γεωγραφικές περιοχές. Αυτές οι εταιρίες λοιπόν επιθυμούν τα διάφορα γραφεία τους (sites) να έχουν "λογική" σύνδεση μεταξύ τους χρησιμοποιώντας το δίκτυο του Internet service provider για τη μεταφορά των δεδομένων. Αυτός ο τύπος VPN γλιτώνει από το εταιρικό δίκτυο μεγάλο bandwidth έτσι ώστε να μπορέσει να το χρησιμοποιήσει στις εταιρικές εφαρμογές που όσο περνάει ο καιρός γίνονται όλο και περισσότερο bandwidth-hungry και latency-sensitive. Παρά το γεγονός ότι θα περίμενε κανείς αυτή η τεχνολογία να είναι και η πιο δημοφιλής, αντί αυτού δεν προτιμάται πολύ. Ο λόγος είναι ότι εξ 'αρχής δεν υπάρχει καθόλου κρυπτογράφηση. Για να επιτευχθεί αυτό χρησιμοποιούνται άλλοι και εξωτερικοί μηχανισμοί προστασίας και κρυπτογράφησης όπως το IPsec. Στην επόμενη εικόνα φαίνεται ακριβώς αυτό που αναφέραμε πιο πάνω.



Εικόνα 15 MPLS VPN Πηγή: http://www.implsvpn.net/uploads/image/140729040445.jpg

[19] www.quora.com

2.4.2. IPsec VPN

Το IPsec κάνει ακριβώς αυτό που αναφέρει το όνομά του (IP και sec εκ του security). Το IPsec χρησιμοποιείται για να προστατεύει τα IP πακέτα. Το IPsec είναι ένα σύνολο protocols και αλγορίθμων που προστατεύουν τα IP πακέτα στο layer 3 του OSI model. Προσφέρει τα πλεονεκτήματα της εμπιστευτικότητας μέσω της κρυπτογράφησης , data integrity μέσω του κατακερματισμού αυτών (hashing) και μέσω HMAC , και authentication μέσω της χρήσης pre-shared keys (παρόμοια με τα passwords). Επίσης , το IPsec προσφέρει προστασία anti-replay.Σαν λειτουργία υπάρχει εδώ και πολλά χρόνια και στις ημέρες μας χρησιμοποιείται περισσότερο σε remote-access VPN αλλά και σε site-to-site VPN. Περισσότερα θα αναφέρουμε σε επόμενο κομμάτι αυτού του κεφαλαίου που θα γίνει σύγκριση μεταξύ IPsec VPN και SSL VPN.

2.4.3. SSL VPN

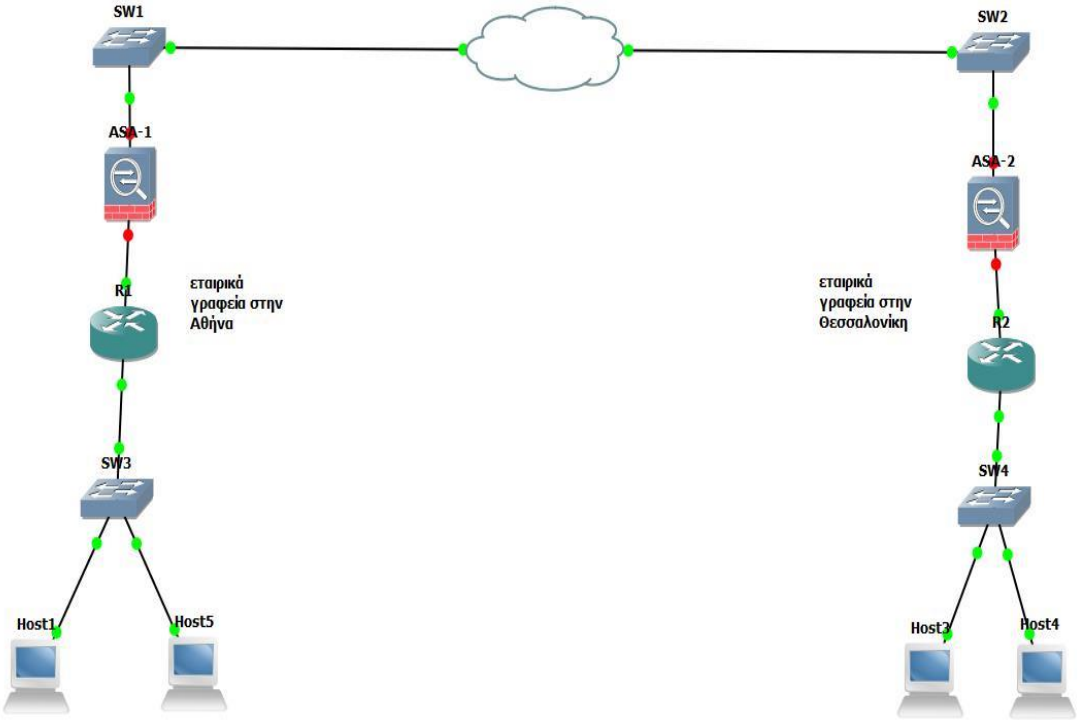
Το SSL έχει πάρει το όνομά του από το Secure Socket Layer. Το SSL παρέχει ασφάλεια σε TCP sessions μέσω των κρυπτογραφημένων SSL tunnels του μοντέλου OSI. Βρίσκει μεγάλη εφαρμογή σε remote-access VPNs αλλά και σε περιπτώσεις που είναι επιθυμητή η ασφαλής σύνδεση σε έναν Web Server μέσω HTTPS (secure HTTP).

2.5. Τύποι VPN

Οι δυο κύριοι τύποι VPN είναι τα site-to-site VPN και τα remote-access VPN.

2.5.1. Site-to-site VPN

Αυτός ο τύπος VPN χρησιμοποιείται κυρίως από εταιρίες που έχουν δύο ή περισσότερα γραφεία σε διαφορετικές περιοχές και σκοπός τους είναι να τα συνδέσουν με τέτοιο τρόπο ώστε να υπάρχει ασφαλής επικοινωνία μεταξύ τους. Τα site-to-site VPNs κατά κύριο λόγο χρησιμοποιούν την τεχνολογία IPsec. Μία εικόνα από site-to-site VPN είναι η παρακάτω.



Εικόνα 16. Τοπολογία Site-to-site VPN

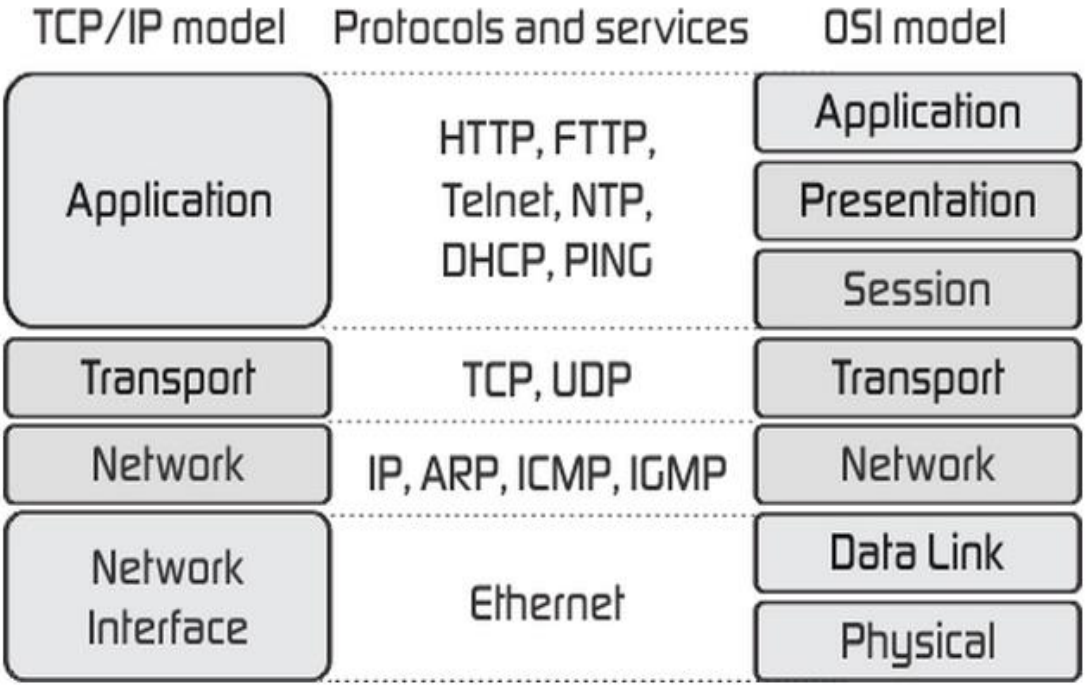
2.5.2. Remote-access VPN

Πλέον, πολλοί χρήστες, ακόμη και όταν βρίσκονται εκτός χώρου εργασίας μπορεί να θέλουν να συνδεθούν μέσω VPN με το εταιρικό δίκτυο. Αυτό ακριβώς είναι και το remote-access VPN, δηλαδή η απομακρυσμένη ασφαλής σύνδεση. Σε αυτό το είδος VPN μπορεί να χρησιμοποιείται είναι το IPsec είτε το SSL. Αυτό ακριβώς που περιγράψαμε παρουσιάζεται στην επόμενη εικόνα.

Εικόνα 17. Τοπολογία remote-access VPN

2.6. Σύγκριση VPN Layer 2 με VPN Layer 3 και VPN Layer 7

Όπως είδαμε πιο πάνω υπάρχουν διάφορες τεχνολογίες και τύποι VPN. Παρόλα αυτά το VPN δεν υφίσταται μόνο σε ένα επίπεδο, αλλά μπορούμε να το διαχωρίσουμε σε VPN που υλοποιείται στο επίπεδο 2 (εφεξής layer), σε VPN που υλοποιείται στο layer 3 και σε αυτό που υλοποιείται στο layer 7. Μιλώντας για layers θα πρέπει να πούμε ότι αναφερόμαστε στα 7 layers του OSI model. Το TCP/IP model είναι λίγο διαφορετικό μας και ενοποιεί μερικά από τα layers του OSI model.



Εικόνα 18.TCP/IP and OSI model. Πηγή: http://www.whatisnetworking.net/wp-content/uploads/2015/02/TCP-IP-model-vs-OSI-model.png

Όπως βλέπουμε και στην εικόνα 18, μιλώντας για layer 2, layer 3 και layer 7 αναφερόμαστε στο data link layer, στο network layer και στο application layer. Αν θα θέλαμε να ορίσουμε τα layers στο έτερο μοντέλο, το TCP/IP model, τότε θα μιλούσαμε και VPN Layer 1, VPN Layer 2 και VPN layer 4 . Γενικά, όπως θα δούμε και πιο κάτω, δεν τίθεται ζήτημα για το ποιο είναι καλύτερο και ποιο προτείνεται να χρησιμοποιείται. Το κάθε ένα προσφέρει τα δικά του χαρακτηριστικά και ανάλογα με τα χαρακτηριστικά και τις ανάγκες του καθενός, χρησιμοποιείται η αντίστοιχη τεχνολογία. Πάμε όμως να πούμε λίγα λόγια για το τί ακριβώς σημαίνει να υλοποιείται το VPN στο data link layer, τί στο network layer και τί στο application layer.

2.6.1. VPN Layer 2

Όπως αναφέραμε και πιο πάνω το layer 2 είναι το data link layer. Αφού προσομοιώνεται αυτό το επίπεδο, χρήστες που βρίσκονται σε διαφορετικές τοποθεσίες εμφανίζονται σα να είναι μέσα στο ίδιο LAN, άρα και στο ίδιο subnet. Είναι δηλαδή σα να έχουν συνδεθεί αυτές οι απομακρυσμένες τοποθεσίες με ένα καλώδιο. Εδώ, το replication των broadcast/multicast frames, η διαδικασία εκμάθησης των MAC addresses και γενικά όλες τις βασικές λειτουργίες ενός Ethernet δικτύου, πρέπει να καταφέρει να τα διαχειριστεί το VPN. Αυτό επιτυγχάνεται κυρίως με τη διαδικασία του tunneling. Σε γενικές γραμμές τα VPN σε αυτό το επίπεδο, είναι πολύ απλά στην υλοποίησή τους και δεν δημιουργούν κανένα πρόβλημα λειτουργίας στις εφαρμογές που χρησιμοποιούμε. Αυτή όμως τη απλότητα είναι που το αφήνει εκτεθειμένο σε κινδύνους και πολλές φορές παρουσιάζει προβλήματα ασφαλείας. Επίσης, θα πρέπει να αναφερθεί ότι ο ISP (Internet Service Provider) δε χρειάζεται να γνωρίζει την τοπολογία, ούτε τα policies, ούτε να έχει πρόσβαση σε routing information. Όλα αυτά τα διαχειρίζεται και τα ορίζει μόνος του ο κάτοχος του δικτύου. Το να προστεθεί μια νέα τοποθεσία στο ήδη υπάρχον

δίκτυο, είναι πολύ εύκολο και δε χρειάζεται να γίνουν network/routing configurations. Επειδή, όπως είπαμε πιο πάνω, όλα λειτουργούν σα να βρίσκονται στο ίδιο LAN, κάθε πιθανό νέο site που προστίθεται επικοινωνεί άμεσα και χωρίς πρόβλημα με τα ήδη υπάρχοντα (και το αντίστροφο). Τέλος, το VPN Layer 2 δε μπορεί να υποστηρίξει παραπάνω από 20 συνδέσεις.

2.6.2. VPN Layer 3

Το layer 3 είναι το network layer, οπότε εδώ το VPN λειτουργεί λίγο διαφορετικά. Αφού προσομοιώνεται το network layer, μας δίνεται η δυνατότητα να κάνουμε route το εσωτερικό μας δίκτυο "μέσα" από το Internet. Αυτό σημαίνει ότι σε αντίθεση με το layer 2 τα δύο άκρα του VPN βρίσκονται σε διαφορετικό subnet και τα IP πακέτα μας δρομολογούνται μέσω του VPN που έχουμε υλοποιήσει. Γενικά το VPN στο layer 3 είναι σαφώς πιο επεκτάσιμο από αυτό στο layer 2, αλλά επειδή είναι πιο πολύπλοκο αν δεν υλοποιηθεί σωστά μπορεί να δημιουργήσει δυσλειτουργίες στις εφαρμογές που θέλουμε να χρησιμοποιήσουμε. Σε αντίθεση με το layer 2, εδώ θα πρέπει να παρέχονται στον ISP οι πληροφορίες για το network topology, καθώς ο ISP είναι αυτός που ορίζει τα policies. Τα routing protocols που υποστηρίζονται για την επικοινωνία με τον ISP είναι μόνο τα BGP (Border Gateway Protocol), OSPF (Open Shortest Path First)και EIGRP (Enhanced Interior Gateway Routing Protocol). Το τελευταίο είναι Cisco proprietary protocol και υλοποιείται μόνο με προϊόντα της Cisco. Τέλος, σε αντίθεση με το VPN Layer 2, το VPN Layer 3 δεν έχει κάποιο περιορισμό σε αριθμό συνδέσεων που θα προστεθούν αφού έτσι κ αλλιώς οι "άκρες" είναι σε διαφορετικό subnet.

2.6.3. VPN Layer 7

Τέλος, υπάρχουν και τα VPN που υλοποιούνται στο layer 7 (layer 4 στο TCP/IP model), δηλαδή στο application layer. Αυτού του είδους τα VPN έχουν έρθει στην επιφάνεια τον τελευταίο καιρό και έχουν τραβήξει την προσοχή σε σχέση με τις ήδη υπάρχουσες τεχνολογίες. Όπως φανερώνει και το όνομά τους, δημιουργούνται στο layer 7 και δίνουν τη δυνατότητα ασφαλούς σύνδεσης με απομακρυσμένες εφαρμογές. Επειδή ακριβώς υλοποιούνται σε αυτό το επίπεδο, το οποίο είναι πιο κατανοητό, δίνει την δυνατότητα στους admins να διαμορφώσουν πιο εύκολα security policies. Αυτού του είδους τα VPN λειτουργούν σαν ενδιάμεσοι όταν ένας απομακρυσμένος χρήστης κάνει ένα αίτημα σε μια εφαρμογή που είναι server-based. Με το που γίνεται αυτό το αίτημα, το VPN συλλέγει τις πληροφορίες, ορίζει security policy και γενικά παίζει το ρόλο του φύλακα ανάμεσα στο Internet και στο private network. Τα αιτήματα, δηλαδή, δεν στέλνονται απευθείας στον Server, αλλά αφού τα διαχειριστεί το VPN και τα μετατρέψει στα κατάλληλα και ασφαλή back-end protocols, τότε προωθούνται στον application Server. Σε αυτές τις περιπτώσεις τα VPN βασίζονται στο SSL (κρυπτογράφηση μεταξύ web-browsers και Servers που τρέχουν το SSL) και στο SSH (μηχανισμός για τις κρυπτογραφημένες και ασφαλείς login sessions). Βάσει αυτών των χαρακτηριστικών, είναι δεδομένο ότι αυτού του είδους τα VPN αποκτούν όλο και περισσότερους υποστηρικτές. Όπως είναι όμως φυσικό, καμία τεχνολογία δε μπορεί να έχει μόνο θετικά. Το μεγάλο μειονέκτημα του VPN layer 7 είναι ότι για να δημιουργηθεί το VPN ο χρήστης πρέπει κάθε φορά να εκκινεί την εφαρμογή, σε αντίθεση με τα VPN Layer 2 και 3 που προσφέρουν αδιάληπτη VPN σύνδεση. Ένα ακόμη μειονέκτημα παρατηρείται στο γεγονός ότι ένα application σπάνια μένει σταθερό. Συνεχώς γίνονται

προσπάθειες βελτίωσής του και συχνά προστίθενται νέες υπηρεσίες. Αυτές οι νέες προσθήκες και οι αναβαθμίσεις δεν υποστηρίζονται άμεσα και εξ ’αρχής από το VPN σε αυτό το επίπεδο, αλλά χρειάζεται να υπάρξει κάποια μελέτη για την ομαλή προσθήκη τους χωρίς να χαθεί κάτι από τα προηγούμενα.

2.7. Σύγκριση IPsec VPN με SSL VPN

Όπως αναφέραμε και σε προηγούμενο σημείο, οι δυο επικρατέστεροι τύποι VPN είναι το IPsec VPN και το SSL VPN. Σε αυτό το κομμάτι της διπλωματικής θα γίνει μια σύγκριση μεταξύ τους. Θα πρέπει να τονιστεί ότι δε θα γίνει αναφορά και σύγκριση του πρωτοκόλλου IPsec και του SSL, αλλά των δεδομένων υλοποιήσεων VPN.
Θα ξεκινήσουμε τη σύγκριση αναφέροντας τα βασικά χαρακτηριστικά τους. Ξεκινώντας από το IPsec VPN, πρέπει να πούμε ότι χρησιμοποιείται κυρίως για άτομα που θέλουν να συνδεθούν με το εταιρικό δίκτυο, απομακρυσμένα, μέσω ενός μη ασφαλούς δικτύου (για παράδειγμα του οικιακού δικτύου) είτε στις περιπτώσεις που θέλουν να συνδεθούν τα απομακρυσμένα γραφεία της ίδιας εταιρίας. Η χρήση του IPsec VPN γίνεται αποκλειστικά και μόνο μέσα από σταθερή γραμμή. Από την άλλη το SSL VPN χρησιμοποιείται και από σταθερή γραμμή αλλά και μέσω δικτύου κινητής τηλεφωνίας (smartphones/tablets). Ο τύπος αυτός του VPN έχει πιο ευρεία χρήση καθώς μπορεί να χρησιμοποιείται από χρήστες κινητών τηλεφώνων, από πελάτες που θέλουν να κάνουν με ασφαλή τρόπο τις αγορές τους και γενικά έχει ένα ύφος πιο “casual” σε σχέση με το “business” ύφος που αποπνέει το IPsec VPN.
Βάσει των παραπάνω, θα μπορούσε κάποιος να πει ότι είναι προτιμότερη η χρήση του SSL VPN. Είναι όμως έτσι; Το μόνο που μας ενδιαφέρει είναι μια ελαφριά και εύκολη σύνδεση με μια εφαρμογή; Κοιτώντας το ψυχρά, και οι δυο τύπο VPN προσφέρουν ασφαλή απομακρυσμένη σύνδεση. Ο τρόπος που το επιτυγχάνουν αυτό, το κόστος της υλοποίησης και η ασφάλεια που προσφέρουν, όμως, είναι και αυτά που τους διαφοροποιεί και αυτό ακριβώς είναι που κάθε χρήστης κοιτάει ώστε να επιλέξει ποιο θα χρησιμοποιήσει. Οι διαφορές αυτές είναι:

- Το IPsec VPN δίνει πρόσβαση στους hosts σε ολόκληρα private networks, ενώ το SSL VPN δίνει πρόσβαση στους hosts σε συγκεκριμένες υπηρεσίες ή εφαρμογές εντός αυτών των private networks.
- Το IPsec VPN υποστηρίζει όλες τις IP based εφαρμογές και τα όλα τα πακέτα είναι ίδια. Αντίθετα στο SSL VPN αυτό δε γίνεται να συμβαίνει γιατί κάθε εφαρμογή έχει διαφορετικό τρόπο να παρουσιάζει το client interface μέσω του browser.
- Η κύρια διαφορά αυτών των δυο τύπων VPN είναι ότι το IPsec VPN είναι σαφώς πιο “βαρύ” και προϋποθέτει την εγκατάσταση και ύπαρξη κάποιου client software ενώ το SSL VPN είναι συνήθως clientless και χρησιμοποιούν τους browsers, που, στην πλειοψηφία τους, υποστηρίζουν το SSL protocol.
- Αυτό όμως μπορεί να θεωρηθεί και πλεονέκτημα και μειονέκτημα στον τομέα του κόστους (και χρηματικού και εργασιακού). Ακριβώς επειδή το SSL VPN είναι περισσότερο browser-based, όσο πιο πολύπλοκη και ιδιαίτερη είναι μια εφαρμογή τόσο μεγαλύτερη προσπάθεια χρειάζεται για να μπορέσουμε να την παραμετροποιήσουμε έτσι ώστε το SSL VPN να λειτουργεί σωστά και χωρίς

προβλήματα. Πέραν αυτού, μια εφαρμογή συνήθως αλλάζει μέσα στο χρόνο οπότε χρειάζεται συνεχής έλεγχος. Έτσι, από τη μια έχουμε την ευκολία του browser, αλλα και το wildcard ότι μπορεί να χρειαστεί να δημιουργήσουμε/αγοράσουμε πολλά Java/Active-X plugins για την ορθή λειτουργία και από την άλλη έχουμε το μεγαλύτερο κόστος υλοποίησης(αρκετά χρονοβόρο καθώς χρειάζεται πρόσβαση σε κάθε host για την παραμετροποίηση) του IPsec VPN, αλλά την ευκολία διαχείρισής του στη συνέχεια.

- Επίσης, όποιον τύπο VPN και να επιλέξουμε, θα χρειαστεί η ύπαρξη και η παραμετροποίηση VPN gateways, δηλαδή ένας τύπος δικτυακής συσκευής που συνδέει δυο ή περισσότερες συσκευές ή δίκτυα μαζί σε μια VPN infrastructure[20]. Στην περίπτωση του IPsec VPN ο host γίνεται μέρος του δικτύου στο οποίο θα συνδεθεί οπότε υπάρχουν κάποια θέματα που πρέπει να διευθετηθούν για την ομαλή λειτουργία. Από τη στιγμή που ένα VPN tunnel έχει δυο IPs (μια στη μεριά του ISP και μια στη μεριά του εσωτερικού δικτύου που συνδέεται ο host), θα πρέπει οι administrators να καταφέρουν να μοιράσουν σωστά αυτές τις IPs και να δημιουργήσουν “ανοίγματα” στα firewalls. Αυτή ακριβώς η διαδικασία προκαλεί αλλαγές και στα network routes. Επιπλέον χρόνος, λοιπόν, χρειάζεται για να ελέγξουμε πως και από πού θα δρομολογείται η ροή δεδομένων του χρήστη, αν το NAT (Network Address Translation) εμποδίζει τις επιθυμητές ρυθμίσεις κ.α. Από την άλλη το SSL VPN επειδή λειτουργεί διαφορετικά και προσφέρει πρόσβαση στον host σε μια συγκεκριμένη εφαρμογή μέσα σε ένα private network, δε χρειάζεται κάτι από τα προαναφερθέντα.
- Στο κομμάτι της ασφάλειας θα κάνουμε μια σύγκριση βάσει της “συμπεριφοράς” του κάθε τύπου στην ασφάλεια από επίθεση, σχετικά με αυθεντικοποίηση, το access control και σχετικά με το client security.

1. Στην ασφάλεια από επίθεση υπερέχει σαφώς το IPsec VPN καθώς, όπως έχουμε αναφέρει, χρησιμοποιεί το IPsec protocol που είναι συνδυασμός πρωτοκόλλων και αλγορίθμων ασφάλειας. Όχι ότι το SSL VPN δεν είναι ασφαλές, αλλα το IPsec VPN προσφέρει μεγαλύτερη ασφάλεια. Πράγμα που είναι κατανοητό αφού συνήθως χρησιμοποιείται για πρόσβαση σε εταιρικά δίκτυα που τα δεδομένα είναι σαφώς πιο ευαίσθητα. Η μεγαλύτερη ασφάλεια του IPsec VPN έγκειται στο γεγονός ότι τα μήκη κλειδιών που χρησιμοποιεί για block encryption είναι μεγαλύτερα από τα μήκη κλειδιών που χρησιμοποιεί το SLL VPN για το stream encryption, άρα όπως αναφέραμε και σε προηγούμενο σημείο, μεγαλύτερο μήκος κλειδιού σημαίνει μεγαλύτερη ασφάλεια. Παρόλα αυτά, όταν αναφερόμαστε σε απλές επιθέσεις μέσω Internet και τα δυο είναι εξίσου ασφαλή. Τι γίνεται όμως όταν αναφερόμαστε σε λίγο πιο εξελιγμένες και ιδιαίτερες επιθέσεις όπως το DoS/DDoS ή το man-in-the-middle; Ας ξεκινήσουμε με την man-the-middle attack. Και οι δυο τύποι έχουν τη δυνατότητα να ανταπεξέλθουν σε μια τέτοια επίθεσή, με μια μόνο διαφορά. Το IPsec χρησιμοποιεί εμποδίζει την μετατροπή πακέτων. Στις περιπτώσεις όμως που IPsec και NAT χρησιμοποιούνται μαζί, παρουσιάζονται πολλά προβλήματα με αποτέλεσμα να μην υπάρχει ορθή λειτουργία. Έτσι, στην περίπτωση που επιλεχθεί το IPsec VPN θα πρέπει να έχει προβλεφθεί και μια εναλλακτική λύση για να

[20]https://www.techopedia.com/definition/30755/vpn-gateway

αντιμετωπιστεί αυτή η ασυμβατότητα. Είτε λοιπόν θα πρέπει να χρησιμοποιηθεί το IPsec μαζί με το NAT-Traversal, είτε να γίνει μετάβαση σε χρήση μόνο IPv6 διευθύνσεων (αφού τότε το NAT δε θα έχει λόγο ύπαρξης) είτε να χρησιμοποιηθεί ένα project της IETF, το RSIP (Realm Specific IP). Άλλη μια επιλογή είναι να μη χρησιμοποιηθεί καθόλου NAT. Αντίθετα, το SSL VPN επειδή δεν επηρεάζεται από IP και port modifications, ξεπερνάει εύκολα τον σκόπελο του NAT. Επίσης το SSL επισυνάπτει τα sequence numbers μέσα στα κρυπτογραφημένα πακέτα για να αποφεύγει το packet injection. Σχετικά με την DoS/DDoS επίθεση, το IPsec VPN υπερέχει αισθητά. Το γεγονός αυτό οφείλεται στο ότι το IPsec χρησιμοποιεί datagrams ενώ το SSL, TCP sessions. Βέβαια αυτή η υπεροχή μπορεί να δικαιολογηθεί εύκολα, μιας όλες οι IPsec VPN συσκευές και ειδικά αυτές που χρησιμοποιούνται από μεγάλες εταιρίες, έχουν περάσει από άπειρα tests για να αντιμετωπίζουν επιτυχώς αυτή την επίθεση. Από την άλλη, για τα SSL VPN τα αντίστοιχα tests και οι μελέτες, έχουν ξεκινήσει μόλις τα 2-3 τελευταία χρόνια.

2. Στο γεγονός ότι το IPsec VPN χρησιμοποιείται περισσότερο για εταιρική χρήση, δικαιολογεί και την υπεροχή του στο client security. Επειδή δε μπορεί να υπάρξει ασφαλής μεταφορά δεδομένων και επικοινωνία αν το ένα από τα δύο μέρη του VPN tunnel έχει θέμα ασφαλείας, προϋποθέτει σωστή επιλογή, ρύθμιση και συντήρηση anti-virus και firewalls. Το γεγονός και μόνο ότι στις εταιρίες αυτό το αναλαμβάνει ένας administrator και δεν είναι στη διακριτική ευχέρεια ενός απλού χρήστη, προσφέρει ακόμη μεγαλύτερη ασφάλεια. Αυτή η διαδικασία όμως και η ταυτόχρονη προσαρμογή με την business policy, μόνο εύκολη δεν είναι.

3. Τέλος, στο κομμάτι του authentication και access control δεν υπάρχει κάποιος τύπος που να υπερέχει. Η διαφορά είναι στον τρόπο που επιλέγει κάθε τύπος να το υλοποιήσει. Το IPsec VPN χρησιμοποιεί IKE (Internet Key Exchange), ψηφιακές υπογραφές και pre-shared keys για αμφίδρομη αυθεντικοποίηση. Το SSL VPN χρησιμοποιεί πάντα ψηφιακές υπογραφές, ανεξάρτητα της μεθόδου που χρησιμοποιείται για την αυθεντικοποίηση του SSL client. Σε αυτό το κομμάτι χρησιμοποιούνται συνήθως passwords (one-time ή μόνιμα) ή/και tokens. Στο κομμάτι του access control στο SSL VPN δίνεται πρόσβαση ανά άτομο σε κάθε εφαρμογή ενώ στο IPsec VPN δίνεται ομοιόμορφη πρόσβαση σε ομάδες ατόμων στους εταιρικούς Servers και subnets.

Κοιτώντας τον πιο κάτω πίνακα, θα δούμε ότι σχεδόν για κάθε υπηρεσία μπορούμε να χρησιμοποιήσουμε είτε τον έναν είτε τον άλλον τύπο VPN.

Applications and content:	IPSec VPN	SSL VPN
Voice Over IP	X	
Entire subnets with no application access control required	X	
Networks, including intranets and extranets, that require access control		X
Web applications	X	X
Client/server applications	X	X
Intranet content	X	X
Email	X	X
File Servers	X	X
Server socket dependent applications	X	X

Εικόνα19. Περιπτώσεις χρήσης IPsec και SSL VPN. Πηγή:http://sanog.org/ (A non-profit forum for Data Network Operators in South Asia)

Επίσης, κοιτώντας την επόμενη εικόνα θα δούμε μια λίστα με μερικούς από τους μεγαλύτερους vendors. Είναι φανερό, ότι εκτός από το γεγονός ότι τα ποσοστά είναι σχεδόν μοιρασμένα, υπάρχουν αρκετοί που έχουν και τα δυο.

VPN VENDORS*

COMPANY	SSL	IPSec
ArrayNetworks www.arraynetworks.net	✓	
Aspelle www.aspelle.com	✓	
Aventail www.aventail.com	✓	
BorderWare Technologies www.borderware.com		✓
Check Point Software Technologies www.checkpoint.com	✓	✓
Cisco Systems www.cisco.com		✓
Citrix www.citrix.com	✓	
CyberGuard www.cyberguard.com		✓
Enterasys Networks www.enterasys.com		✓
eSoft www.esoft.com		✓
Fortinet www.fortinet.com		✓
InfoExpress www.infoexpress.com		✓
Microsoft www.microsoft.com		✓
Neoteris www.neoteris.com	✓	
Netilla Networks www.netilla.com	✓	
NetScreen Technologies www.netscreen.com		✓
NetSilica www.netsilica.com	✓	
Nokia www.nokia.com	✓	✓
Nortel Networks www.nortel.com	✓	✓
Novell www.novell.com		✓
Permeo Technologies www.permeo.com	✓	
Rainbow Technologies www.rainbow.com	✓	✓
SafeWeb www.safeweb.com	✓	
SonicWALL www.sonicwall.com		✓
Stonesoft www.stonesoft.com		✓
uRoam www.uroam.com	✓	
V-One www.vone.com		✓
WatchGuard Technologies www.watchguard.com		✓
Whale Communications www.whalecommunications.com	✓	

Εικόνα20. VPN Vendors Πηγή: Information Security magazine. August 2013

Παρατηρώντας όλα τα παραπάνω βλέπουμε ότι τελικά το IPsec και το SSL VPN δεν είναι τελείως διαφορετικά μεταξύ τους. Εξυπηρετούν τον ίδιο σκοπό με διαφορετικά μέσα. Είναι, λοιπόν, σωστό να κληθούμε να επιλέξουμε ανάμεσά τους;

Είναι φανερό ότι από τη μεριά των χρηστών το SSL VPN θα παραμένει πάντα μια καλύτερη λύση και το IPsec VPN θα έχει μεγαλύτερη απήχηση σε εταιρίες με μεγαλύτερες ανάγκες από web applications. Παραμένοντας στην εταιρική μεριά, με το πέρασμα του χρόνου

και την αλλαγή που θα υποστούν αρκετές εταιρίες είναι πολύ πιθανό να βγουν από το δίλλημα SSL VPN ή IPsec VPN και να τα χρησιμοποιήσουν και τα δυο μαζί. Άλλωστε σε αντίστοιχο debate έχουν ειπωθεί οι εξής δύο φράσεις. *"Δεν μπορούμε να πούμε ότι το ένα είναι σωστό και το άλλο λάθος"*[21] *και "Στους Power users αρέσει η ιδέα ενός full PC-to-gateway IPsec VPN. Άλλοι χρήστες όμως, αν όχι οι περισσότεροι, συχνά χρησιμοποιούν τα οικιακά τους PC και θέλουν απλή πρόσβαση σε υπηρεσίες που είναι εύκολα προσβάσιμες μέσω ενός web browser, όπως το email. Το SSL VPN προσφέρει ασφαλή πρόσβαση χωρίς τα εμπόδια ενός hard-to-configure client. Άρα πρέπει να βρεθεί τρόπος να εξυπηρετούνται και οι δυο κατηγορίες."* [22]

[21] Doug Torre, Information Technology Executive at The Andrew W. Mellon Foundation, New York CTO Club

[22]Fred Avolio, president and founder of Avolio Consulting

3. Συνοπτική παρουσίαση εργαλείων

Στις παρακάτω γραμμές θα παρουσιάσουμε τα τρία εργαλεία που θα μας βοηθήσουν να ολοκληρώσουμε το πρακτικό κομμάτι της εργασίας. Αυτά είναι το GNS3, το ASDM (Adaptive Security Device Manager) και το CCP (Cisco Configuration Professional).

3.1. GNS3

Το GNS3, είναι το κύριο εργαλείο που θα χρησιμοποιήσουμε. Πρόκειται για ένα virtual περιβάλλον στο οποίο θα στήσουμε το δίκτυό μας. Είναι ένα εργαλείο, με το οποίο γίνεται προσομοίωση δικτύων, με τη μορφή που θα είχαν στην πραγματικότητα, χωρίς την ανάγκη για ύπαρξη πραγματικού hardware. Το μόνο που χρειάζεται είναι κάποια “images” από τα routers και firewalls που θα χρησιμοποιήσουμε. Ακριβώς επειδή πρόκειται για πραγματικό λογισμικό, έχουμε πλήρη λειτουργικότητα και πρόσβαση σε κάθε είδους εντολή. Είναι και ο λόγος που το GNS3 προτιμήθηκε από το σαφώς πιο “ελαφρύ” packet-tracer. Ταυτόχρονα όμως, ακριβώς για αυτό τον λόγο το λογισμικό μας είναι πολύ απαιτητικό και χρειάζεται αρκετή μνήμη και ένας καλός επεξεργαστής. Πάνω στο GNS3 θα γίνει στο μεγαλύτεροι μέρος της εργασίας καθώς η υλοποίηση των VPN που θα γίνουν με CLI, δε χρειάζονται την ύπαρξη κανενός άλλου προγράμματος. Επειδή το λογισμικό εγκαθίσταται “γυμνό”, στη συνέχεια, θα παρουσιαστεί ένα εγχειρίδιο χρήσης για να δείξουμε πώς ακριβώς εισάγουμε όλα αυτά που θα χρειαστούμε για τα επόμενα βήματα της εργασίας.

3.2. CCP (Cisco Configuration Professional)

Το δεύτερο εργαλείο που θα χρησιμοποιήσουμε είναι το CCP (Cisco Configuration Professional). Το εργαλείο αυτό θα μας βοηθήσει να υλοποιήσουμε IPsec VPN συνδέσεις χωρίς να χρησιμοποιήσουμε το CLI (Command Line Interface). Αντίθετα, όλες οι ρυθμίσεις και οι επιλογές θα γίνουν μέσα από GUI (Graphical User Interface). Το CCP εκτός από IPsec VPN configuration wizard υποστηρίζει ακόμη wizards για την υλοποίηση LAN/WAN Interfaces, QoS, IPS, και NAT. Ένα αντίστοιχο εργαλείο με το CCP είναι και το SDM (Security Device Manager). Δεν αλλάζει κάτι ουσιαστικό στη λειτουργία, απλά είναι λίγο διαφορετικό το interface.

3.3. ASDM (Adaptive Security Device Manager)

Παρόμοιο εργαλείο είναι και το ASDM (Adaptive Security Device Manager) μόνο που αυτή τη φορά παρέχονται wizards για το configuration του ASA firewall. Προσφέρει δηλαδή firewall wizard όπου με την χρήση ελάχιστων κουμπιών μπορούμε να ρυθμίσουμε κατά το δοκούν firewall policy settings κάθε επιπέδου (low, medium, high).

4. Εγχειρίδια χρήσης

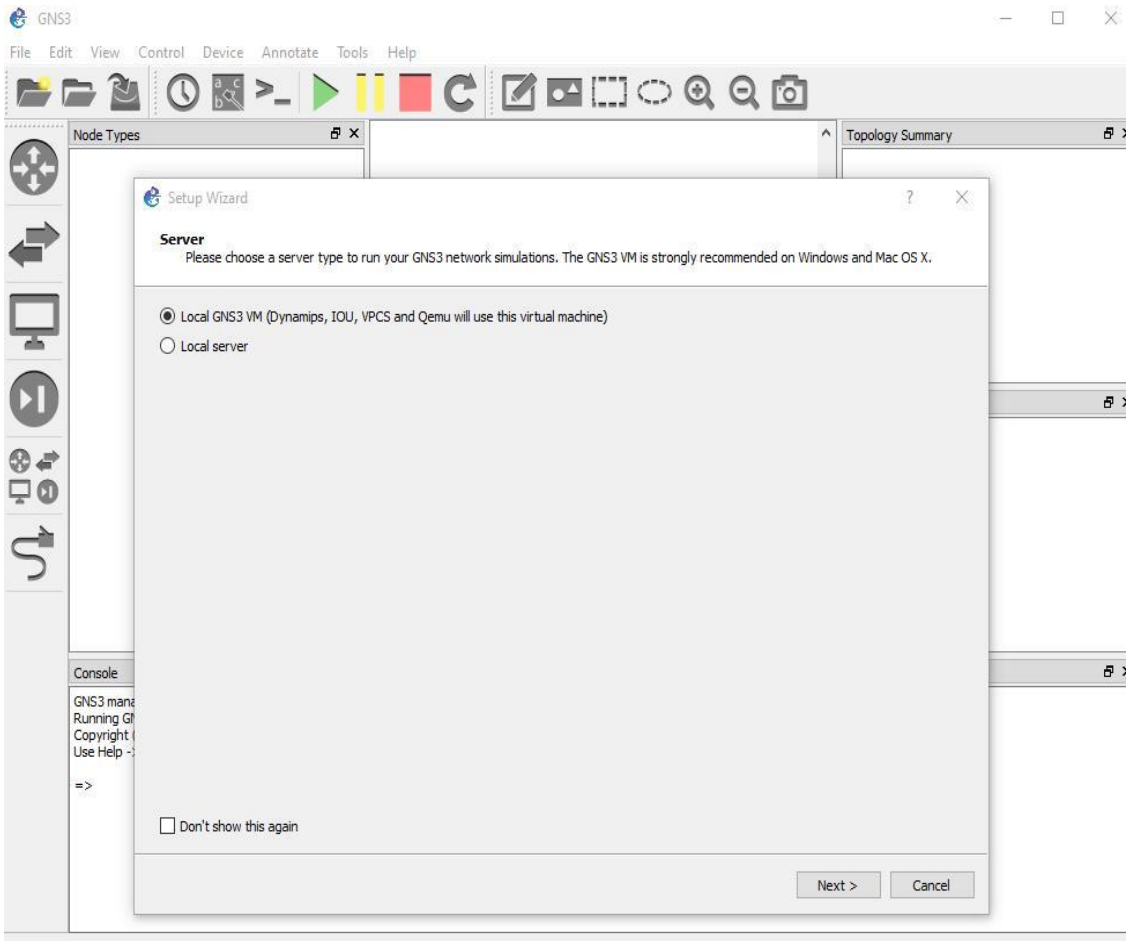
Στις επόμενες γραμμές θα παρουσιάσουμε ένα εγχειρίδιο χρήσης (manual) του βασικού μας εργαστηριακού εργαλείου, του GNS3 και τις βασικές λειτουργίες των δευτερευόντων εργαλείων, του CCP και του ASDM, μιας και δε χρειάζονται κάποια ιδιαίτερη παραμετροποίηση.

4.1. Βασική παραμετροποίηση GNS3

Το εγχειρίδιο χρήσης του GNS3 περιέχει δυο μεγάλα και σημαντικά κεφάλαια. Την εισαγωγή των routers και την εισαγωγή τοy firewall. Χωρία αυτά τα δυο στοιχεία, δε μπορούμε να προχωρήσουμε στην υλοποίηση του εργαστηριακού κομματιού της παρούσας διπλωματικής εργασίας.

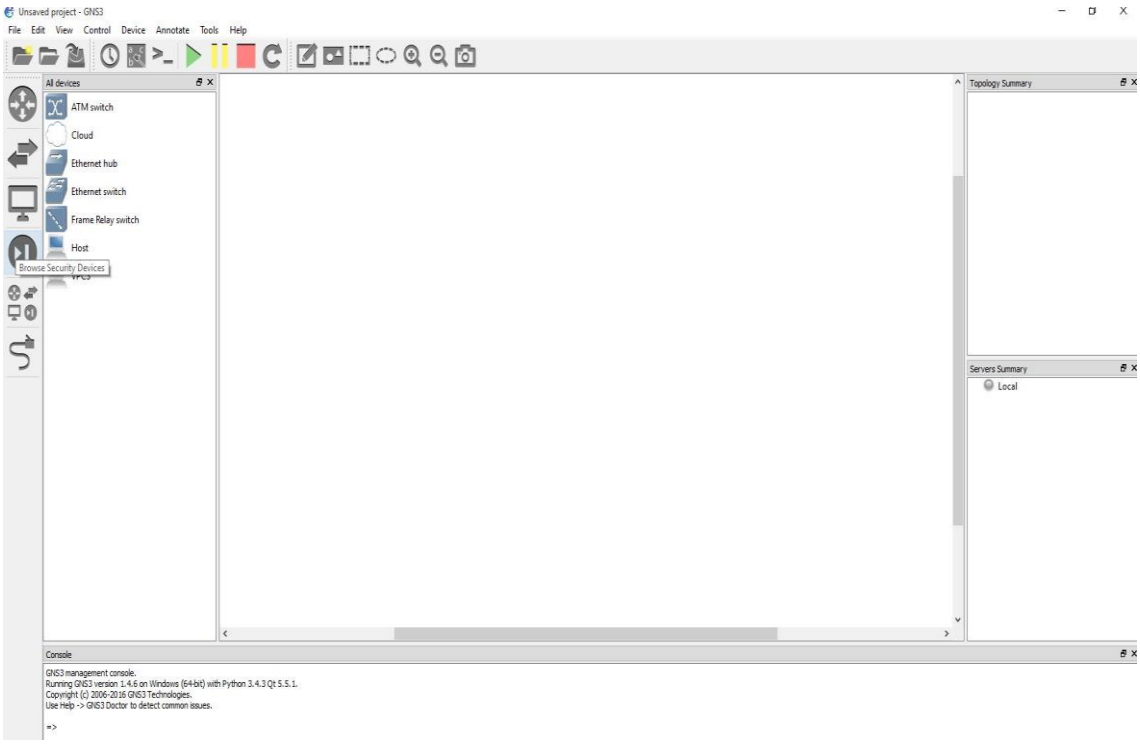
4.1.1. Εισαγωγή router

Μόλις ολοκληρωθεί η εγκατάσταση το σύστημα μας δίνει τη δυνατότητα να επιλέξουμε αν θα λειτουργήσουμε με Local Server ή αν θέλουμε να εγκαταστήσουμε κάποια Virtual Machine (VM) και να έχουμε ξεχωριστό Server. Προς το παρόν, επιλέγουμε Local Server και πατάμε *Next*.



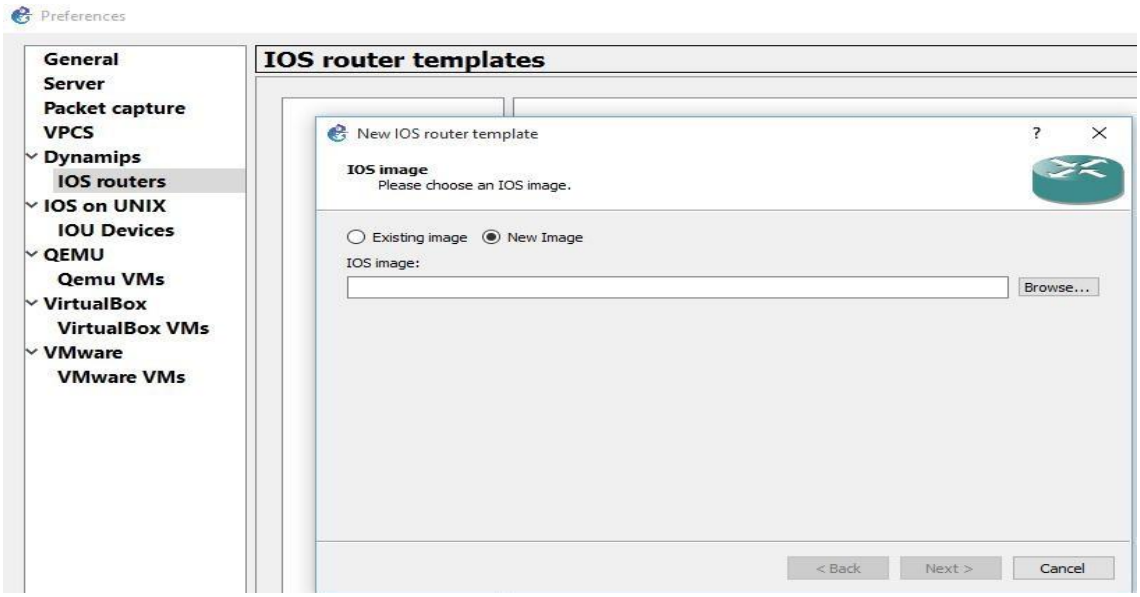
Εικόνα 21. Παραμετροποίηση GNS3 για εισαγωγή router (βήμα 1)

Αφού μπούμε στην κεντρική οθόνη του προγράμματος, βλέπουμε ότι εξ ‘αρχής έχει ενσωματωμένα hubs, switches, frame relay switches, cloud, hosts και VPCs. Δεν υπάρχουν routers και ASA firewalls. Αυτά, λοιπόν θα πρέπει να τα προσθέσουμε εμείς.



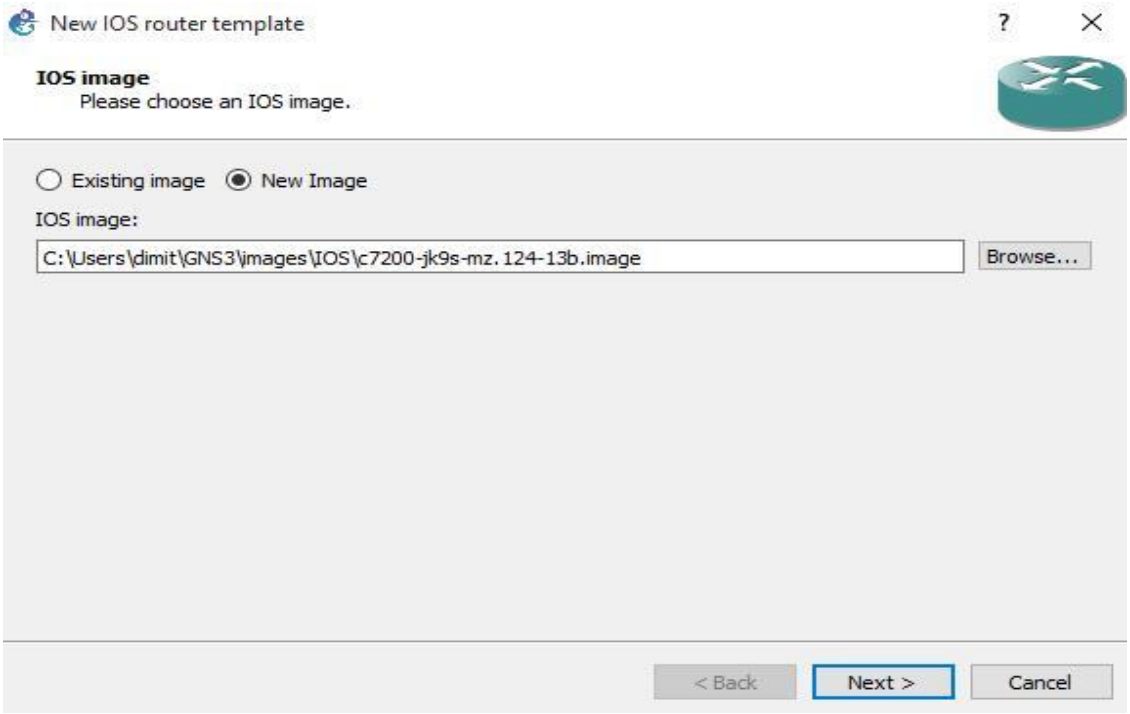
Εικόνα 22. Παραμετροποίηση GNS3 για εισαγωγή router (βήμα 2)

Πάμε να δούμε πώς ακριβώς γίνεται η εισαγωγή και η παραμετροποίηση ενός router. Αφού μπούμε στις επιλογές, πάμε στο *IOS Routers* και επιλέγουμε *new*. Αμέσως μετά μας δίνει τη δυνατότητα να επιλέξουμε μια εικόνα που ήδη έχουμε εισάγει, παλαιότερα στο σύστημα, είτε μια νεα. Επιλέγουμε *New Image* και πατάμε *Next*.



Εικόνα 23. Παραμετροποίηση GNS3 για εισαγωγή router (βήμα 3)

Επιλέγουμε λοιπόν να εισάγουμε στο σύστημα το image του router c7200 που είναι σχετικά καινούριο.

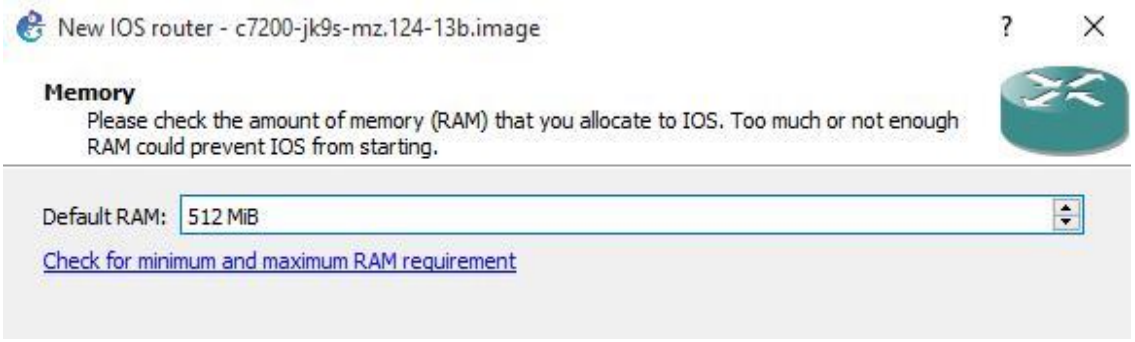


Εικόνα 24. Παραμετροποίηση GNS3 για εισαγωγή router (βήμα 4)

Αφού εισάγουμε την "εικόνα", το GNS3 μας αφήνει να παραμετροποιήσουμε το router κατά το δοκούν. Για αρχή μας ζητάει να επιλέξουμε το είδος των interfaces που θα έχει το router. Εμείς επιλέγουμε τις PA-FE-TX που είναι οι FastEthernet interfaces, τις PA-4T+, που είναι οι Serial interfaces και τις PA-GE που είναι οι GigabitEthernet Interfaces.

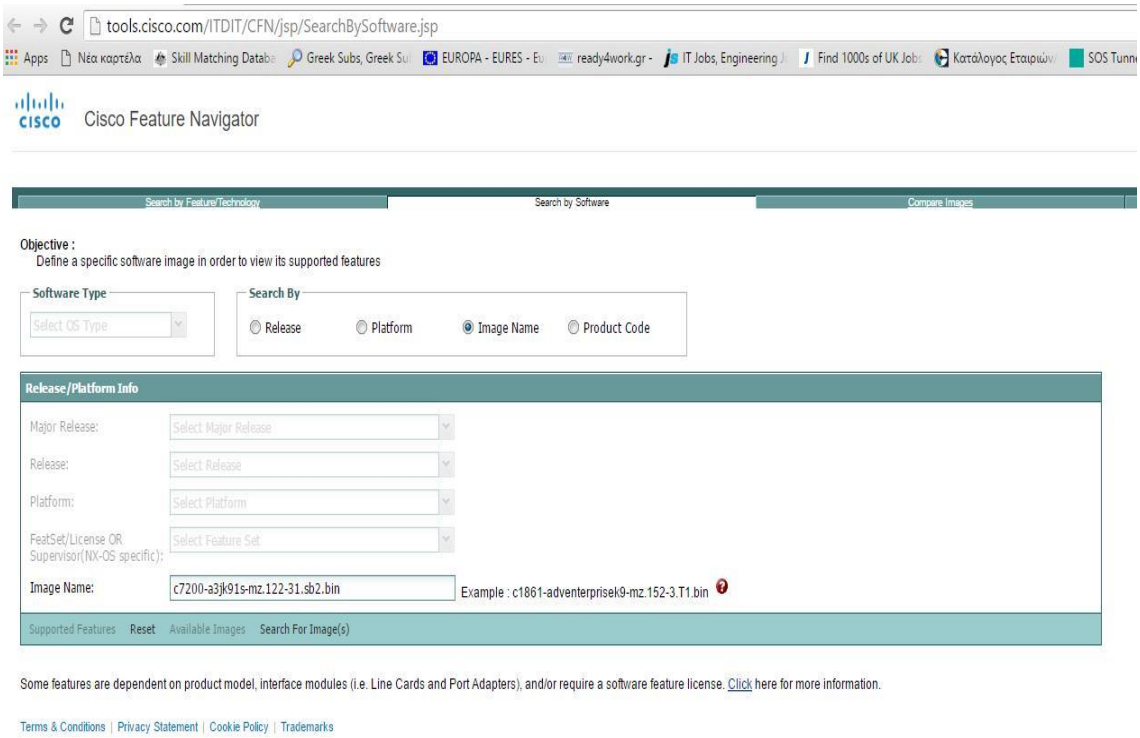
Εικόνα 25. Παραμετροποίηση GNS3 για εισαγωγή router (βήμα 5)

Αμέσως μετά, ζητάει να ορίσουμε την RAM που θα λειτουργεί το router. Εμείς επιλέγουμε 512MB.



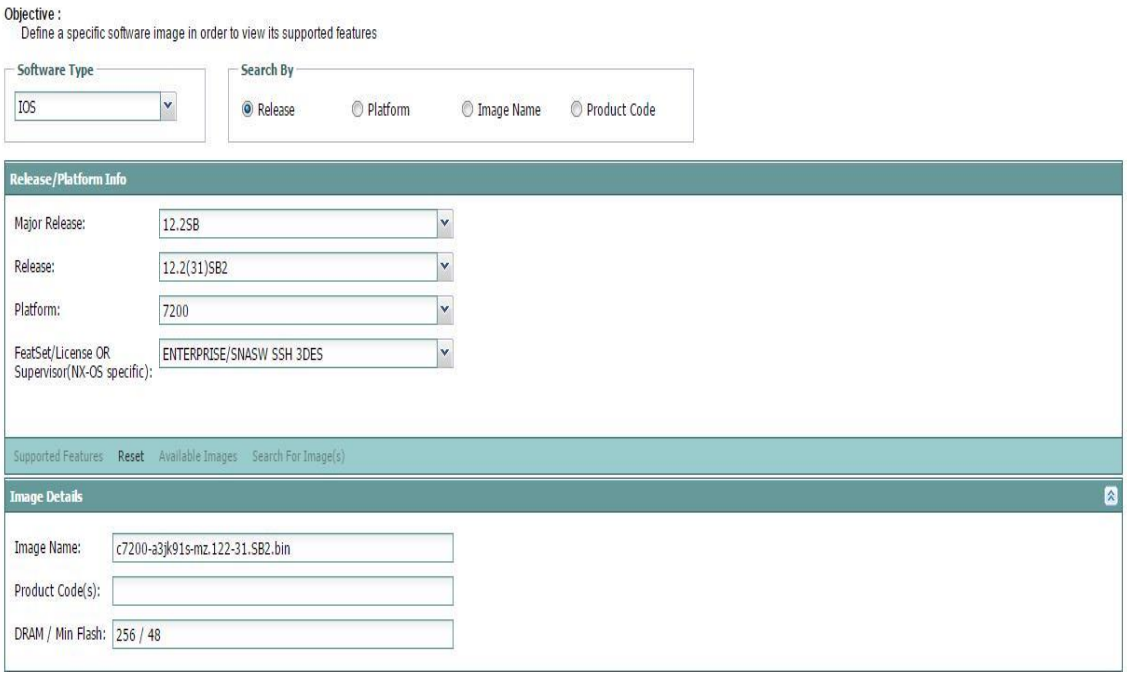
Εικόνα 26. Παραμετροποίηση GNS3 για εισαγωγή router (βήμα 6)

Είναι όμως αρκετό το συγκεκριμένο μέγεθός μνήμης που έχουμε εκχωρήσει στο router; Μια αρκετά μικρή μνήμη μπορεί να προκαλέσει προβλήματα και να μην αφήνει το router να λειτουργήσει σωστά ή ακόμη και να ξεκινήσει. Θα πρέπει λοιπόν να το ελέγξουμε. Για να γίνει αυτό, πηγαίνουμε στην ιστοσελίδα *http://tools.cisco.com/ITDIT/CFN/jsp/SearchBySoftware.jsp*. Εκεί μας ζητάει να βάλουμε το όνομα του image που χρησιμοποιήσαμε, δηλαδή το *c7200-a3jk91s-mz.122-31.sb2.bin*.



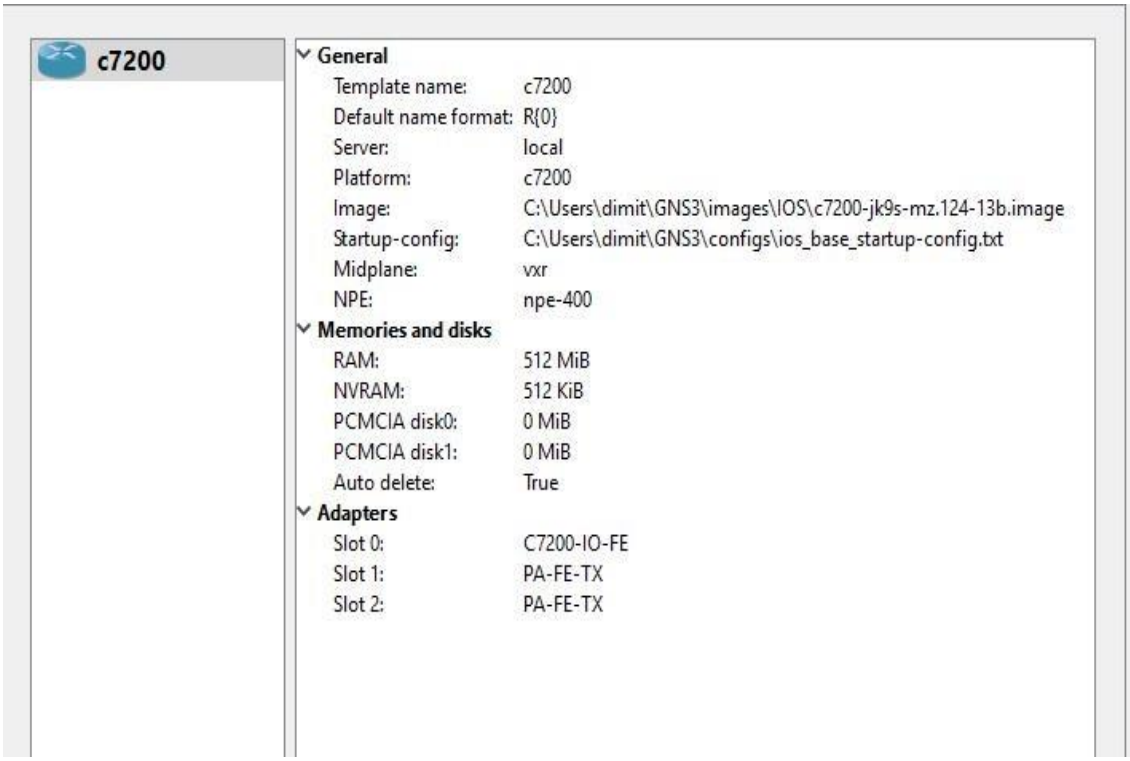
Εικόνα 27. Έλεγχος απαιτήσεων του image router c7200

Πατάμε search for image και εκεί μας εμφανίζει τα χαρακτηριστικά. Εδώ βλέπουμε το release, το όνομα και τη ελάχιστη default RAM που χρειάζεται το router. Όπως βλέπουμε χρειάζεται τουλάχιστον 256MB, οπότε τα 512 που επιλέξαμε εμείς είναι αρκετά για την εύρυθμη λειτουργία.



Εικόνα 28. Έλεγχος απαιτήσεων του image router c7200

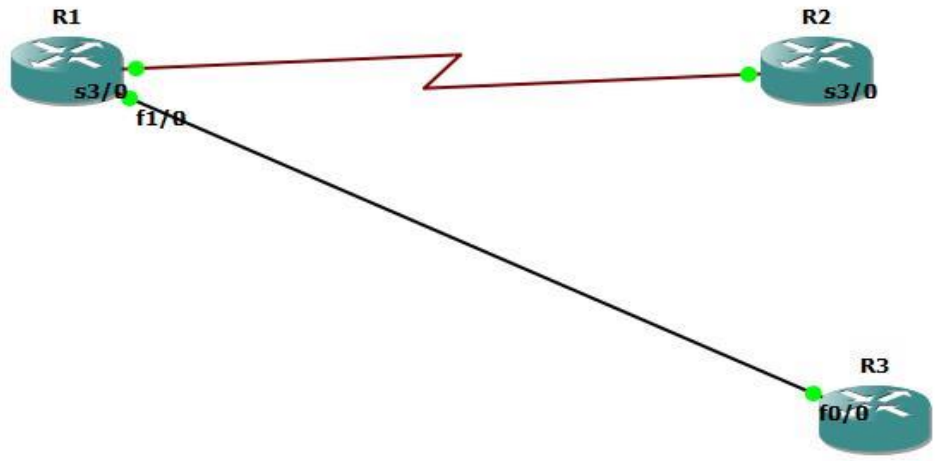
Αμέσως μετά εμφανίζεται μια σύνοψη των επιλογών που κάναμε και μετα πατάμε *apply* και *ok*. Πλέον, το εν λόγω router είναι διαθέσιμο για χρήση.



Εικόνα 29. Παραμετροποίηση GNS3 για εισαγωγή router (βήμα 7)

Στο παρακάτω σχήμα έχουμε επιλέξει να συνδέσουμε το router 1 με το router 3 μέσω των FastEthernet interfaces που εισάγαμε σε προηγούμενο βήμα και το router 1 με το router 2

μέσω Serial interfaces. Αυτό το κάναμε για να δείξουμε ότι το πρόγραμμα είναι πλήρως λειτουργικό.



Εικόνα 30. Σύνδεση routers με Serial και Fast-Ethernet cables

Επιλέγοντας το router 3, μπορούμε να μπούμε στο CLI και να δώσουμε εντολές. Στις παρακάτω εικόνες φαίνεται το configuration που κάναμε στο router 3, δίνοντας μια IP στην interfacefa0/0, κρατώντας την interface μόνιμα ανοιχτή και σώζοντας τις ρυθμίσεις στη μνήμη. Η δεύτερη εικόνα επιβεβαιώνει το σωστό configuration.

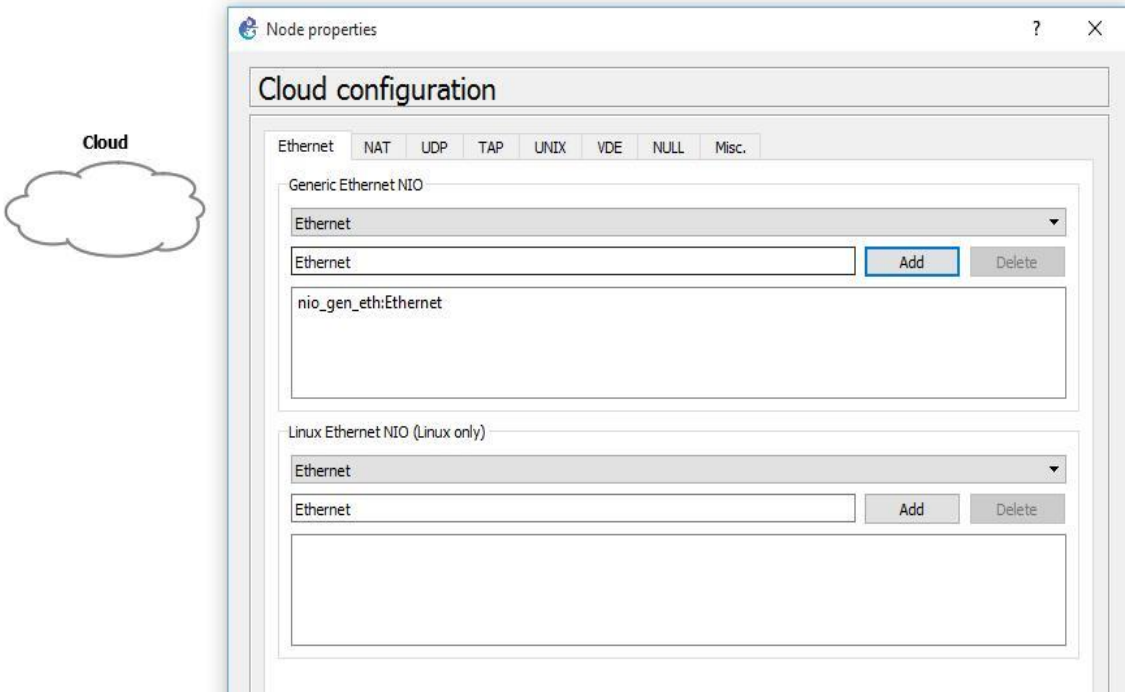
```
R3#enable
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int fa0/0
R3(config-if)#ip add
R3(config-if)#ip address 192.168.1.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#no shutdown
R3(config-if)#
*May 23 10:09:20.499: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R3(config-if)#
*May 23 10:09:20.499: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down
*May 23 10:09:21.499: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-if)#do wr
Building configuration...
[OK]
R3(config-if)#
```

```
R3#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.1     YES manual up                    up
FastEthernet1/0            unassigned      YES unset  administratively down down
FastEthernet2/0            unassigned      YES unset  administratively down down
R3#
```

Εικόνα 31. Εντολές για configuration router και output εντολής show ip interface brief

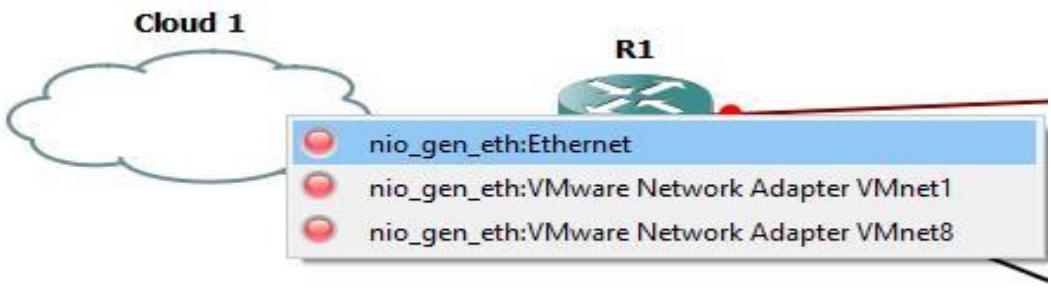
Με τον ίδιο τρόπο προσθέσαμε IPs και subnet masks και στις υπόλοιπες interfaces των routers.

Επειδή όμως ένα κομμάτι της εργασίας αφορά την υλοποίηση IPsec VPN και SSL VPN μέσω GUI, θα πρέπει να βρούμε έναν τρόπο αυτά τα routers να μπορούμε να τα διαχειριστούμε από την εφαρμογή Cisco Configuration Professional. Άρα θα πρέπει από εντελώς virtual να καταφέρουμε να τα συνδέσουμε με το πραγματικό δίκτυό μας. Αυτή ακριβώς τη διαδικασία θα περιγράψουμε ευθύς αμέσως. Προσθέτουμε ένα Cloud και μέσα από το configuration, στον κατάλογο Ethernet, κάνουμε add το *nio_gen_eth:Ethernet*, που αντιστοιχεί στην κάρτα δικτύου μας.



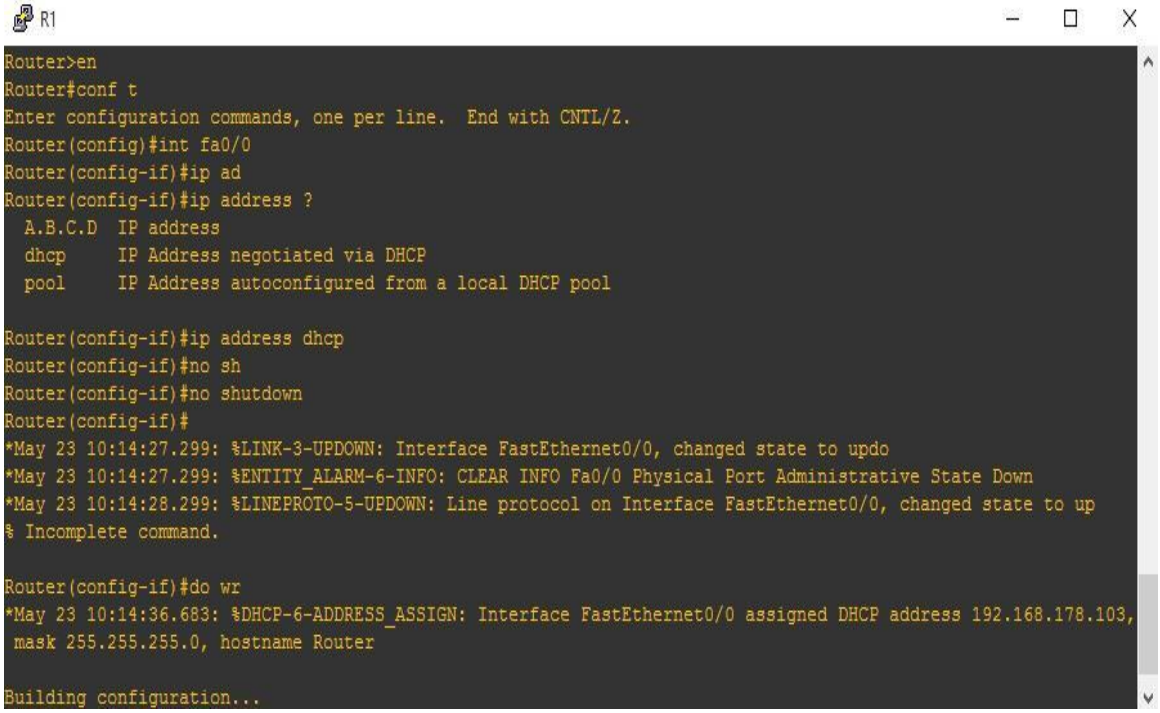
Εικόνα 32. Σύνδεση κάρτας δικτύου με το GNS3 (βήμα 1)

Προσπαθώντας λοιπόν να συνδέσουμε το cloud με το router 1 σαν συνδεσμολογία επιλέγουμε την physical κάρτα δικτύου.



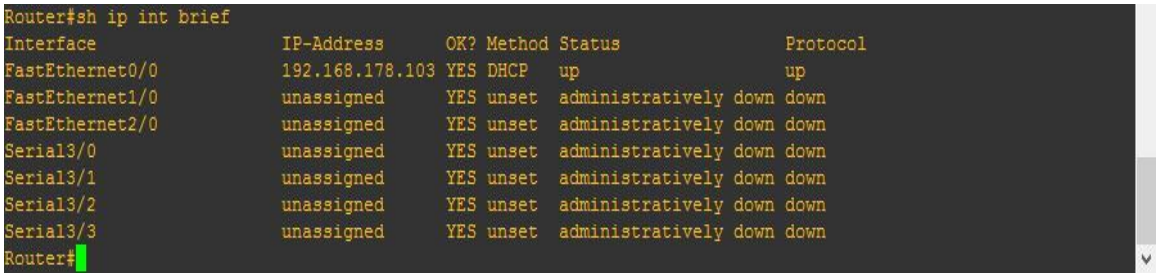
Εικόνα 33. Σύνδεση κάρτας δικτύου με το GNS3 (βήμα 2)

Αμέσως μετά θα χρησιμοποιήσουμε το δικό μας router σαν DHCP Server για να δώσουμε αυτόματα IP στην interfacefa0/0 του router 1 έτσι ώστε να συνδέεται άμεσα με το δικό μας δίκτυο και να το αναγνωρίζει το λογισμικό που θέλουμε.



Εικόνα 34. Εισαγωγή IP μέσω DHCP

Εδώ βλέπουμε την επιβεβαίωση ότι την IP δεν την ορίσαμε εμείς χειροκίνητα, όπως στα προηγούμενα routers αλλά δόθηκε μέσω DHCP.



Εικόνα 35. Επιβεβαίωση ότι η IP προέρχεται από DCHP

Αυτό που θέλουμε τώρα να επιβεβαιώσουμε είναι ότι το router 1 μπορεί να επικοινωνήσει με τον δικό μας υπολογιστή, το physical router μας, αλλά και με τα virtual router 2 και router 3 και ότι το configuration που κάναμε ήταν σωστό. Αρχικά ανοίγουμε το cmd του υπολογιστή μας και με την εντολή *ipconfig* βλέπουμε την δικιά μας IP(192.168.178.29) και την IP του physical router (192.168.178.1)

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\dimit>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fritz.box
   Link-local IPv6 Address . . . . . : fe80::acf5:74a1:4b1d:9202%9
   IPv4 Address. . . . . . . . . . . : 192.168.178.29
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.178.1
```

Εικόνα 36. Εύρεση IP και gateway της πραγματικής κάρτας δικτύου

Θα προσπαθήσουμε λοιπόν να κάνουμε ping από το router 1, την IP του υπολογιστή μας , την IP του physical router μας και τις interfaces se3/0 και fa0/0 του router 2 και router 3, αντίστοιχα. Όπως βλέπουμε πιο κάτω όλα τα ping είναι επιτυχημένα.

R1

```
Router#ping 172.168.178.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.168.178.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/101/116 ms
Router#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/100/256 ms
Router#ping 192.168.178.29

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.178.29, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/36 ms
Router#ping 192.168.178.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.178.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/39/68 ms
```

Εικόνα 37. Επιβεβαίωση σωστής συνδεσμολογίας (βάσει τοπολογίας εικόνας 30)

4.1.2. Εισαγωγή firewall

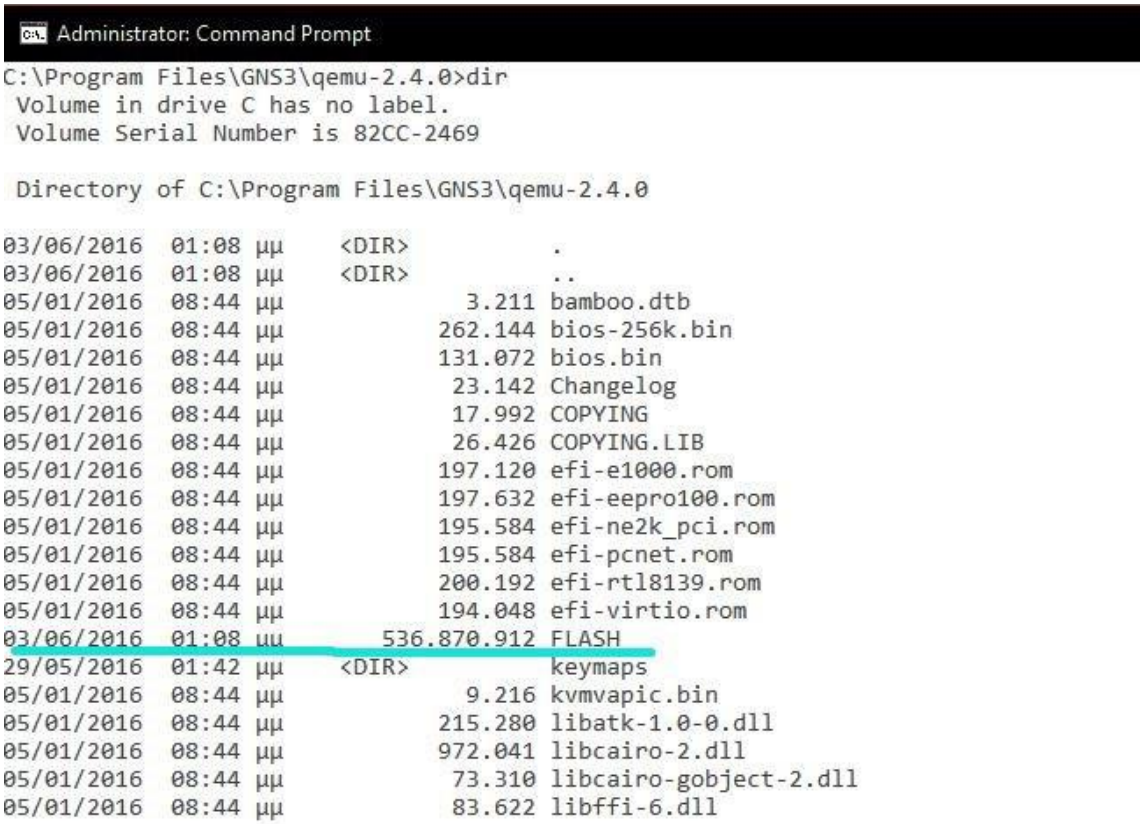
Πάμε τώρα να δημιουργήσουμε σωστά το firewall ASA που θα χρειαστούμε σε επόμενο κομμάτι της εργασίας. Θα χρειαστούμε τα εξής:

- Το GNS3
- Την τεχνολογία Qemu που είναι ενσωματωμένη στο GNS3 και μας βοηθάει στο να εισάγουμε σωστά το firewall ASA. (ASA device version 5520 και ASA software version 8.4(2)).
- Θα χρειαστούμε, επίσης, 2 αρχεία, τα asa842-initrd & asa842-vmlinuz που κατεβάσαμε από το Internet.
- Ένα flash image για την ενεργοποίηση του ASA.

Ξεκινώντας, θα δημιουργήσουμε το flash image. Το path στο οποίο έχει γίνει εγκατάσταση το Qemu είναι το *C:\Program Files\GNS3\qemu-2.4.0* και εκεί θα δημιουργήσουμε το flash image. Ανοίγουμε λοιπόν ένα cmd με elevated privileges (admin rights) και μεταφερόμαστε στον φάκελο αυτό. Αφού μεταφερθούμε, δίνουμε την εντολή *qemu-img create FLASH 512M* για τη δημιουργία της εικόνας.

Εικόνα 38. Δημιουργία image για εισαγωγή firewall στο GNS3

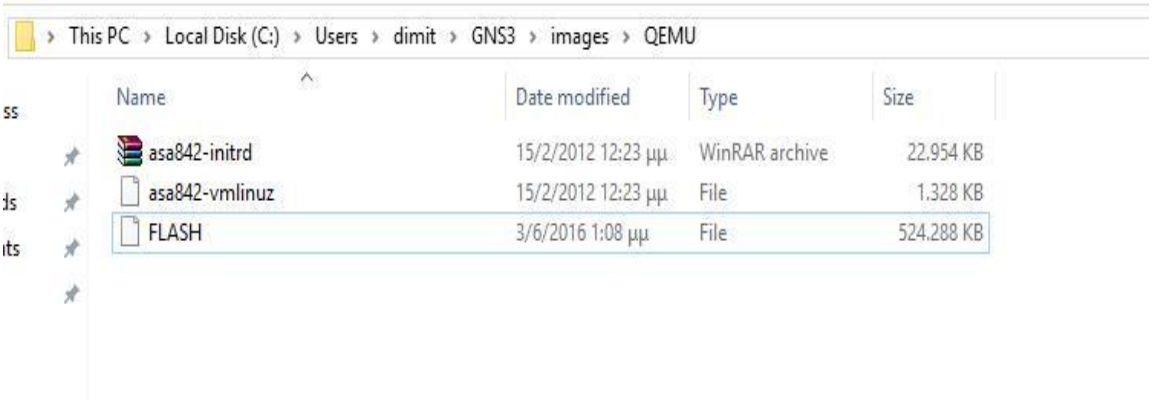
Για να επιβεβαιώσουμε ότι το image file δημιουργήθηκε σωστά πατάμε την εντολή *dir* για να δούμε τα περιεχόμενα του φακέλου. Στην επόμενη εικόνα φαίνεται ότι το αρχείο δημιουργήθηκε σωστά.



Εικόνα 39. Επιβεβαίωση σωστής δημιουργίας image

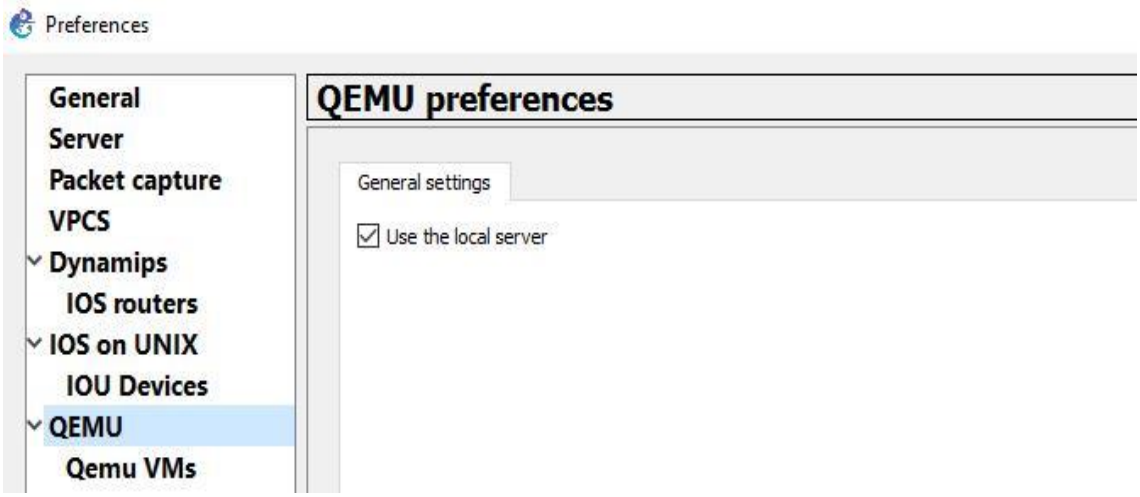
Επόμενη κίνηση είναι να αντιγράψουμε το flash image που μόλις δημιουργήσαμε στον φάκελο που αποθηκεύονται εξ ‘αρχής τα images για το Qemu. Το path αυτό είναι το

C:\Users\dimit\GNS3\images\QEMU και στο σημείο αυτό μεταφέρουμε και τα αρχεία asa842-initrd & asa842-vmlinuz που έχουμε ήδη κατεβάσει.



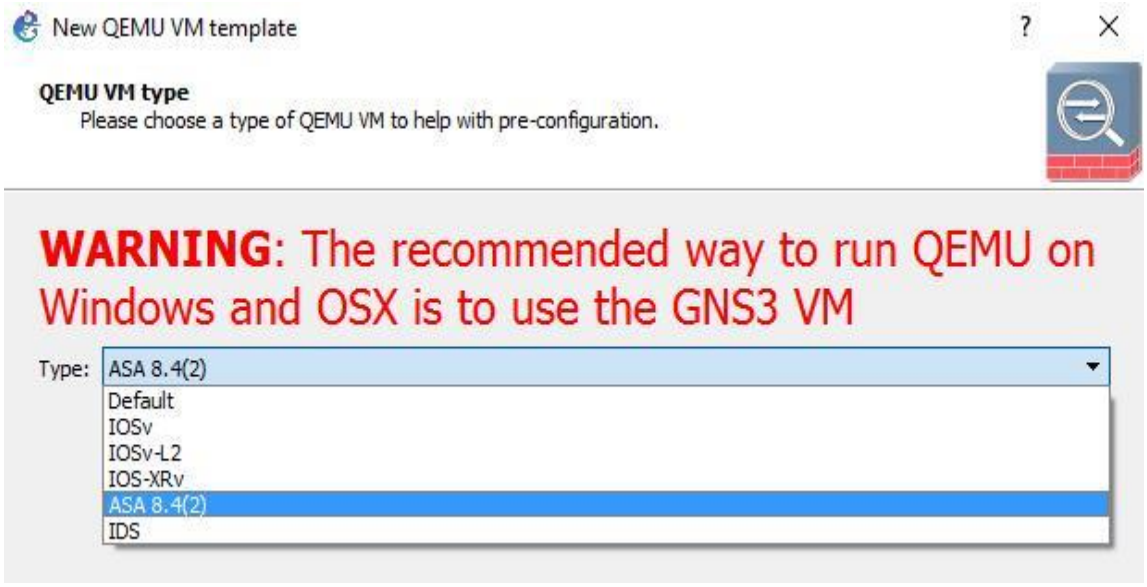
Εικόνα 40. Τοποθέτηση image και .initrd, .vmlinuz αρχείων στο σωστό directory

Ανοίγουμε τώρα το GNS3, πάμε *edit → preferences* και επιλέγουμε Qemu, επιλέγουμε το *Use the local server.*



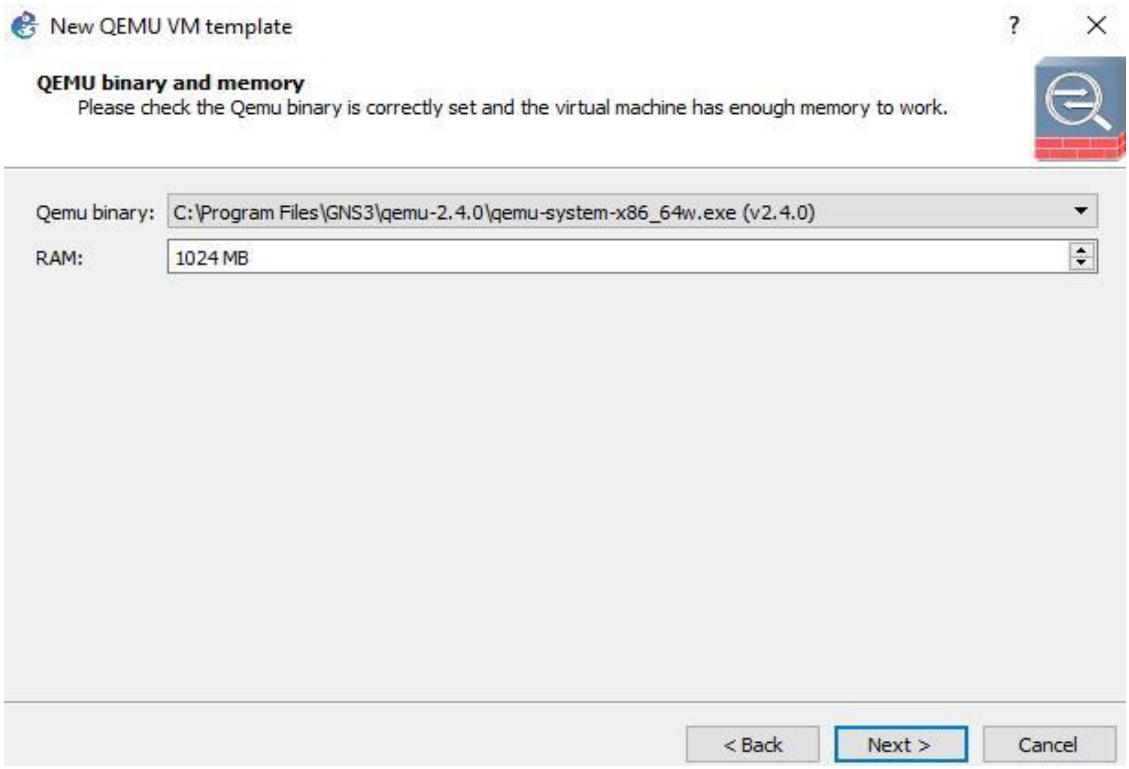
Εικόνα 41. Παραμετροποίηση GNS3 για εισαγωγή firewall (βήμα 1)

Αμέσως μετά, πάμε ακριβώς από κάτω στο Qemu VMs και πατάμε New για να εισάγουμε επιτυχώς στο σύστημα το ASA firewall. Εδώ θα πρέπει να σημειώσουμε ότι ο σωστός τρόπος για την εισαγωγή και χρήση του Qemu είναι μέσω Virtual Machine του GNS3. Επειδή όμως αυτό θα κατανάλωνε πολλούς πόρους από το σύστημά μας με αποτέλεσμα να μη μπορεί να υποστηρίξει τις λειτουργίες που επιθυμούμε να υλοποιήσουμε σε επόμενο κομμάτι της διατριβής, θα το υλοποιήσουμε λίγο διαφορετικά, δημιουργώντας μια “ελαφριά” έκδοση. Η αντίστοιχη ειδοποίηση φαίνεται και στη παρακάτω εικόνα. Αγνοούμε την ειδοποίηση και από το drop down menu επιλέγουμε ASA 8.4(2) και πατάμε *Next*.



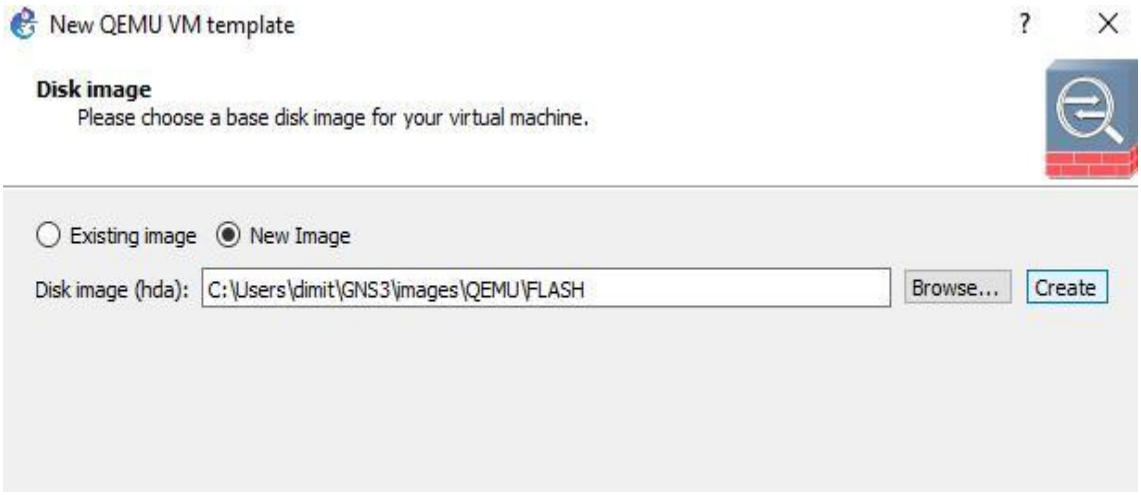
Εικόνα 42. Παραμετροποίηση GNS3 για εισαγωγή firewall (βήμα 2)

Στην αμέσως επόμενη οθόνη επιλέγουμε ένα όνομα (επιλέγουμε απλά ASA) και πατάμε *Next*. Από το drop down menu στην επιλογή Qemu binary επιλέγουμε *C:\Program Files\GNS3\qemu-2.4.0 qemu-system-x86_64w*. Θα μπορούσαμε να κάνουμε οποιαδήποτε άλλη επιλογή, αλλά η συγκεκριμένη είναι η πιο σταθερή όταν δεν χρησιμοποιούμε VM. Στην επιλογή RAM επιλέγουμε 1024MB για να εξασφαλίσουμε απρόσκοπτη λειτουργία. Έχουμε τη δυνατότητα να μειώσουμε τη RAM, αλλά σε καμία περίπτωση δεν πρέπει να έχουμε λιγότερο από 512MB. Αμέσως μετά πατάμε *Next.*



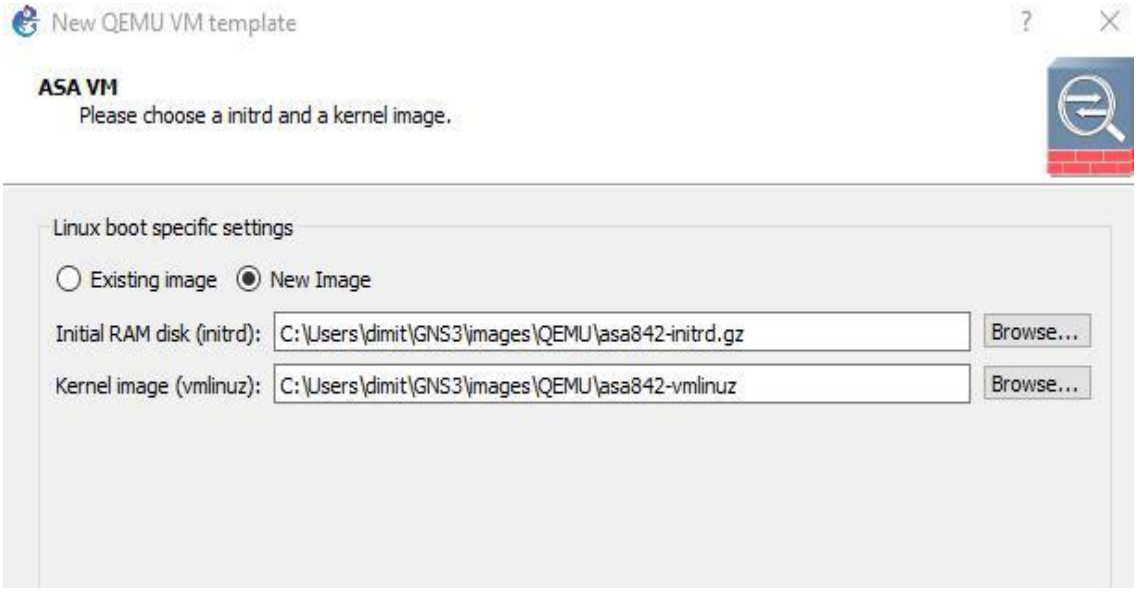
Εικόνα 43. Παραμετροποίηση GNS3 για εισαγωγή firewall (βήμα 3)

Στην αμέσως επόμενη εικόνα ζητάει να εισάγουμε μια disk image (hda). Θα χρησιμοποιήσουμε το image που δημιουργήσαμε στο πρώτο κομμάτι της εγκατάστασης, οπότε θα πατήσουμε *new image* και στο path θα βάλουμε *C:\Users\dimit\GNS3\images\QEMU\FLASH.* Αν δεν την είχαμε δημιουργήσει στην αρχή, το GNS3 δίνει επιλογή να τη δημιουργήσουμε εκείνη τη στιγμή. Πατάμε *Next.*



Εικόνα 44. Παραμετροποίηση GNS3 για εισαγωγή firewall (βήμα 4)

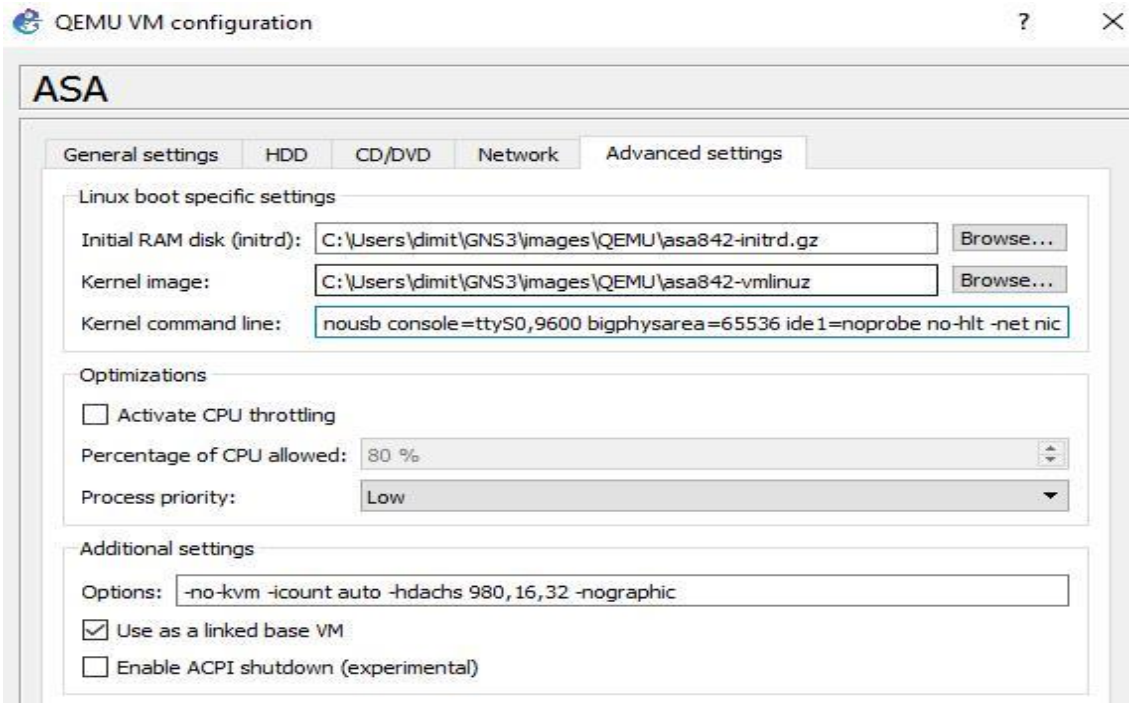
Αμέσως μετά, μας ζητείται να εισάγουμε initial RAM disk (initrd) και Kernel image (vmlinuz). Εδώ λοιπόν θα χρησιμοποιήσουμε τα 2 αρχεία που τοποθετήσαμε στον ίδιο φάκελο με το FLASH image. Πατάμε *Finish* και ολοκληρώνουμε τη διαδικασία.



Εικόνα 45. Παραμετροποίηση GNS3 για εισαγωγή firewall (βήμα 5)

Το τελευταίο βήμα που μένει είναι να παραμετροποιήσουμε το image που δημιουργήσαμε. Πατάμε *apply* και πριν πατήσουμε *OK*, επιλέγουμε *edit*. Πάμε στο *Advanced settings* και απενεργοποιούμε το *Activate CPU throttling*. Αν στο μέλλον δούμε ότι επιβαρύνει

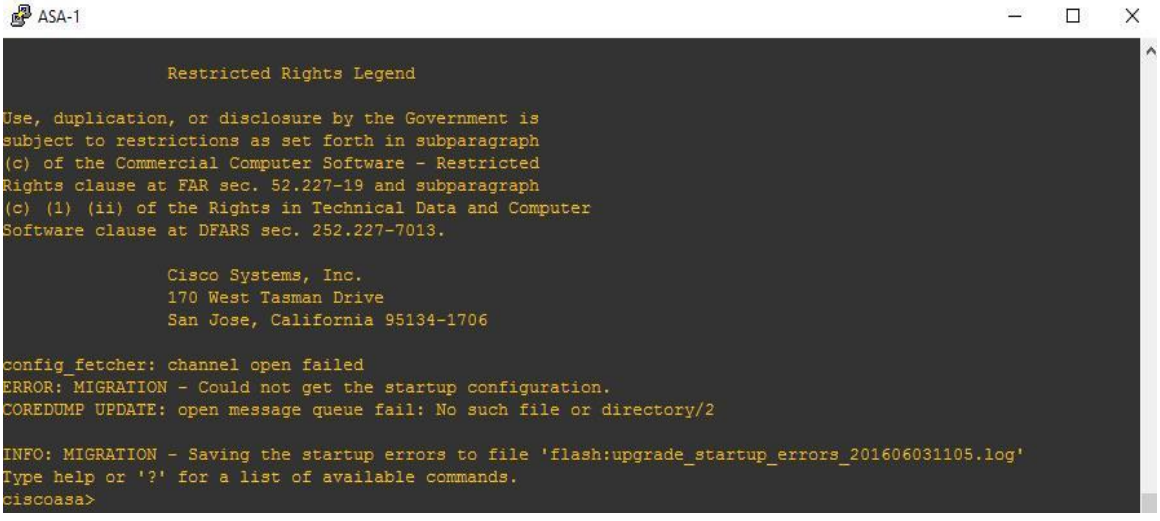
πολύ τον υπολογιστή, μπορούμε ξανά από τα settings να το ενεργοποιήσουμε ξανά και να ορίσουμε μέγιστο όριο χρήσης της CPU.



Εικόνα 46. Παραμετροποίηση GNS3 για εισαγωγή firewall (βήμα 6)

Πατάμε *OK* και *apply* μέχρι να επιστρέψουμε στην αρχική οθόνη και τώρα πάμε να δούμε αν όλα λειτουργούν σωστά. Πατάμε στο *Browse security devices* και βλέπουμε ότι πλέον υπάρχει ένα ASA firewall.

Το επιλέγουμε, πατάμε start, ανοίγουμε console και περιμένουμε να κάνει εκκίνηση. Όταν εμφανίσει το *prompt* με όνομα *ciscoasa,* σημαίνει ότι, μέχρι στιγμής, όλα λειτουργούν σωστά.



Εικόνα 47. Επιβεβαίωση σωστής λειτουργίας firewall

Πληκτρολογούμε *en* για να μπούμε σε *enable mode*. Ζητάει password, αλλά το μόνο που χρειάζεται είναι πατήσουμε *Enter*. Μετά πληκτρολογούμε την εντολή *show version* για να μας δείξει τις πληροφορίες και να επιβεβαιώσουμε ότι δεν υπάρχει κάποιο πρόβλημα.

```
ciscoasa> en
Password:
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 8.4(2)

Compiled on Wed 15-Jun-11 18:17 by builders
System image file is "Unknown, monitor mode tftp booted image"
Config file at boot was "startup-config"

ciscoasa up 55 secs

Hardware:   ASA 5520, 1024 MB RAM, CPU Pentium II 1000 MHz
Internal ATA Compact Flash, 256MB
BIOS Flash unknown @ 0x0, 0KB


 0: Ext: GigabitEthernet0    : address is 0000.ab54.3800, irq 0
 1: Ext: GigabitEthernet1    : address is 0000.ab54.3801, irq 0
 2: Ext: GigabitEthernet2    : address is 0000.ab54.3802, irq 0
 3: Ext: GigabitEthernet3    : address is 0000.ab54.3803, irq 0
```

Εικόνα 48. Επιβεβαίωση version του firewall

```
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 100            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Disabled       perpetual
VPN-DES                           : Disabled       perpetual
VPN-3DES-AES                      : Disabled       perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 5000           perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 5000           perpetual
Total VPN Peers                   : 0              perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Serial Number: 123456789AB
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
Configuration register is 0x0
Configuration has not been modified since last system restart.
ciscoasa#
```

Εικόνα 49. Έλεγχος αν το firewall έχει valid licence

Όπως βλέπουμε, το firewall λειτουργεί χωρίς κανένα πρόβλημα. Στις τελευταίες γραμμές όμως βλέπουμε ότι λειτουργεί με *Default License Key* αφού το *Permanent Activation Key* δεν έχει οριστεί ακόμη, κάτι που δε μας δίνει πρόσβαση στις πλήρεις λειτουργίες. Αυτό που θα πρέπει να κάνουμε είναι να εισάγουμε ένα νέο valid Licence Key. Μπαίνουμε λοιπόν σε *configuration mode* και βάζουμε την εντολή *activation-key 0xb23bcf4a 0x1c713b4f 0x7d53bcbc 0xc4f8d09c 0x0e24c6b6.* Αυτή η διαδικασία θα διαρκέσει περίπου 30 λεπτά και στο τέλος θα χρειαστεί να κάνουμε επανεκκίνηση το firewall κάνοντας save το νέο configuration.

```
ciscoasa# config t
ciscoasa(config)#

*************************** NOTICE ***************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: a
You will be reminded again in 7 days.

If you would like to enable this feature, issue the command
"call-home reporting anonymous".

Please remember to save your configuration.
ciscoasa(config)# activation-key ?

exec mode commands/options:
  <0x0-0xffffffff>  Enter four-or-five-tuple activation-key
  noconfirm         Do not prompt for confirmation
ciscoasa(config)# activation-key 0xb23bcf4a 0x1c713b4f 0x7d53bcbc 0xc4f8d09c 0$
Validating activation key. This may take a few minutes...
Failed to retrieve permanent activation key.
Failover is different.
   running permanent activation key: Restricted(R)
   new permanent activation key: Unrestricted(UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with update flash activation key? [confirm]
The flash permanent activation key was updated with the requested key,
and will become active after the next reload.
ciscoasa(config)#
```

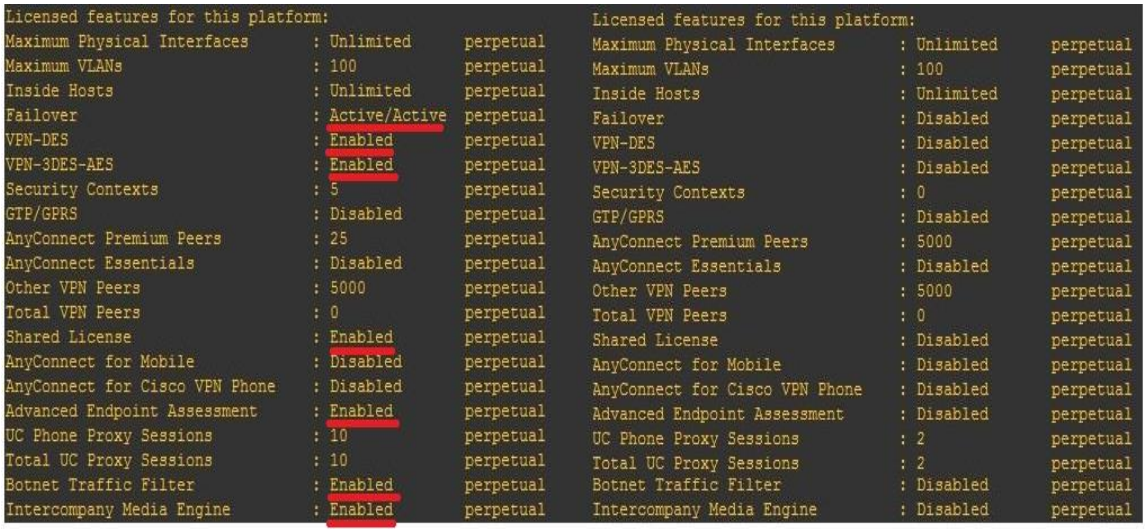
Εικόνα 50. Ενεργοποίηση valid licence στο firewall

Όταν η διαδικασία ολοκληρωθεί θα πληκτρολογήσουμε πάλι *show version*. Τώρα βλέπουμε ότι έχουμε ένα firewall ενεργοποιημένο με ένα valid Licence Key.

```
Serial Number: 123456789AB
Running Permanent Activation Key: 0xb23bcf4a 0x1c713b4f 0x7d53bcbc 0xc4f8d09c 0x0e24c6b6
Configuration register is 0x0
Configuration has not been modified since last system restart.
ciscoasa#
```

Εικόνα 51. Επιβεβαίωση σωστής ενεργοποίησης με valid licence

Τέλος, με αυτή την ενεργοποίηση, αν συγκρίνουμε τις υπηρεσίες που ήταν ενεργοποιημένες πριν και μετά την καταχώρηση του κλειδιού θα δούμε μερικές αξιοσημείωτες διαφορές. Στα δεξιά φαίνεται η εικόνα πριν την ενεργοποίηση και στα αριστερά φαίνονται η εικόνα μετά την ενεργοποίηση.



Licensed features for this platform:			Licensed features for this platform:		
Maximum Physical Interfaces	: Unlimited	perpetual	Maximum Physical Interfaces	: Unlimited	perpetual
Maximum VLANs	: 100	perpetual	Maximum VLANs	: 100	perpetual
Inside Hosts	: Unlimited	perpetual	Inside Hosts	: Unlimited	perpetual
Failover	: Active/Active	perpetual	Failover	: Disabled	perpetual
VPN-DES	: Enabled	perpetual	VPN-DES	: Disabled	perpetual
VPN-3DES-AES	: Enabled	perpetual	VPN-3DES-AES	: Disabled	perpetual
Security Contexts	: 5	perpetual	Security Contexts	: 0	perpetual
GTP/GPRS	: Disabled	perpetual	GTP/GPRS	: Disabled	perpetual
AnyConnect Premium Peers	: 25	perpetual	AnyConnect Premium Peers	: 5000	perpetual
AnyConnect Essentials	: Disabled	perpetual	AnyConnect Essentials	: Disabled	perpetual
Other VPN Peers	: 5000	perpetual	Other VPN Peers	: 5000	perpetual
Total VPN Peers	: 0	perpetual	Total VPN Peers	: 0	perpetual
Shared License	: Enabled	perpetual	Shared License	: Disabled	perpetual
AnyConnect for Mobile	: Disabled	perpetual	AnyConnect for Mobile	: Disabled	perpetual
AnyConnect for Cisco VPN Phone	: Disabled	perpetual	AnyConnect for Cisco VPN Phone	: Disabled	perpetual
Advanced Endpoint Assessment	: Enabled	perpetual	Advanced Endpoint Assessment	: Disabled	perpetual
UC Phone Proxy Sessions	: 10	perpetual	UC Phone Proxy Sessions	: 2	perpetual
Total UC Proxy Sessions	: 10	perpetual	Total UC Proxy Sessions	: 2	perpetual
Botnet Traffic Filter	: Enabled	perpetual	Botnet Traffic Filter	: Disabled	perpetual
Intercompany Media Engine	: Enabled	perpetual	Intercompany Media Engine	: Disabled	perpetual

Εικόνα 52. Διαφορές δυνατοτήτων firewall με valid και χωρίς valid licence

4.2. Βασική παραμετροποίηση CCP

Για να λειτουργήσει το Cisco Configuration Professional, αφού το εγκαταστήσουμε, θα πρέπει να κάνουμε κάποιες ρυθμίσεις στο GNS3, το λογισμικό στο οποίο βρίσκονται τα router μας. Το πρώτο που πρέπει να γίνει είναι να συνδέσουμε ένα router με την κάρτα δικτύου μας και να του δώσουμε αυτόματα μια IP (το πώς γίνεται αυτό, το έχουμε αναφέρει στο manual του GNS3). Αφού ολοκληρωθεί αυτό το στάδιο ανοίγουμε το CLI του router και αφού μπούμε σε configuration mode εισάγουμε με τη σειρά τις παρακάτω εντολές. Αρχικά πρέπει να ρυθμίσουμε το router με ένα username και ένα password. Αυτό γίνεται με την εντολή *username xxxx privilege 15 secret xxxx.* Το *privilege 15* που προσθέσαμε στην εντολή δείχνει το εύρος των δικαιωμάτων που αποκτά το άτομο που κάνει log in στο router χρησιμοποιώντας το συγκεκριμένο username και password. Υπάρχουν 15 επίπεδα δικαιωμάτων (1-15) και όσο μεγαλύτερος ο αριθμός, τόσο περισσότερα τα δικαιώματα. Αν θελήσουμε να κάνουμε έναν παραλληλισμό το privilege 15 είναι αντίστοιχο με τα root privileges στο UNIX είτε με τα admin privileges στα Windows.

```
R1(config)#username jim privilege 15 secret vrettos
R1(config)#
```

Εικόνα 53. Ρύθμιση router για αναγνώρηση από CCP (βήμα 1)

Αμέσως μετά πληκτρολογούμε *ip http server* ή ip *http secure-server.* Το ποια από τις δυο εντολές θα εισάγουμε δεν αλλάζει κάτι στην όλη διαδικασία. Δεν υπάρχει σωστό και λάθος. Απλά αλλάζει το επίπεδο ασφάλειας. Στο συγκεκριμένο παράδειγμα, θα επιλέξουμε το *ip http secure-server*. Στη συνέχεια εισάγουμε με τη σειρά τις εντολές *ip http authentication local* και *line vty 0 4*. Με την πρώτη εντολή θα ενεργοποιήσουμε την συνδεσιμότητα στο router μέσω HTTP. Με τη δεύτερη, ορίζουμε σε ποια logical “connection ports” του router θα έχουμε πρόσβαση με το συγκεκριμένο username και password.

```
R1(config)#ip http secure-server
R1(config)#ip http authentication local
R1(config)#line vty 0 4
```

Εικόνα 54. Ρύθμιση router για αναγνώρηση από CCP (βήμα 2)

Βλέπουμε ότι βγήκαμε από το απλό configuration mode και μπήκαμε σε ένα πιο ειδικό περιβάλλον, αυτό του vty line. Τώρα εισάγουμε την εντολή *login local*. Με αυτή την εντολή απλά ενημερώνουμε το router να κοιτάξει σε μια local database για να επιβεβαιώσει ότι υπάρχει ο χρήστης με το συγκεκριμένο username/password και αν υπάρχει να γνωρίζει τι δικαιώματα θα του παρέχει. Χρησιμοποιείται και είναι προαπαιτούμενο για ssh συνδέσεις. Γνωρίζοντας αυτό, η επόμενη εντολή μας θα είναι *transport input ssh.* Εναλλακτικά μπορούμε να χρησιμοποιήσουμε την εντολή *transport input telnet* αν θέλουμε να έχουμε telnet σύνδεση ή *transport input telnet ssh* αν θέλουμε να έχουμε και τα δυο.

```
R1(config-line)#login local
R1(config-line)#transport input ssh
```

Εικόνα 55. Ρύθμιση router για αναγνώρηση από CCP (βήμα 3)

Μόλις εισάγουμε και την τελευταία εντολή το μόνο που χρειάζεται είναι να εισάγουμε την εντολή *wr* ή *copy running-configuration startup-configuration* για να σώσουμε τις εντολές.

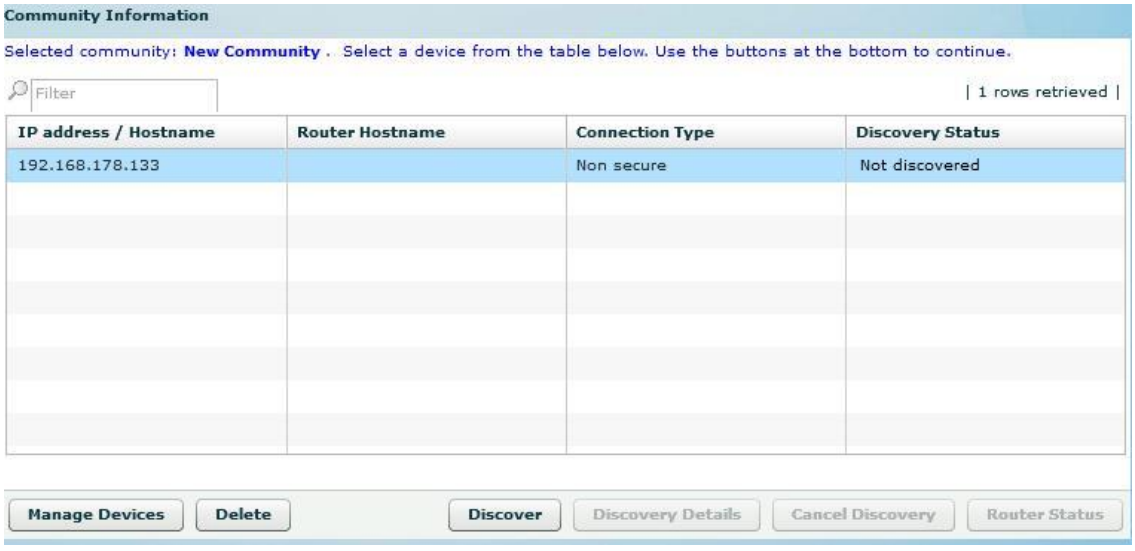
Αμέσως μετά πηγαίνουμε στο CCP . Μόλις το ανοίξουμε, άμεσα ανοίγει μια σελίδα που μας ζητάει να εισάγουμε username/password. Αυτό είναι λογικό μιας και το Cisco Configuration Professional είναι προϊόν της Cisco και για τη λειτουργία του χρειάζεται λογαριασμός. Αφού και για να γίνει download το πρόγραμμα χρειάζεται λογαριασμός, θα χρησιμοποιήσουμε τα στοιχεία που ήδη έχουμε.

Εικόνα 56. Login στο CCP

Αφού ολοκληρωθεί σωστά το log in αυτόματα εμφανίζεται το παράθυρο του community στο οποίο θα πρέπει να εισάγουμε την IP μιας interface του router (στο manual του GNS3 αναφέραμε πώς ακριβώς υλοποιείται αυτό), το username και το password που εισάγαμε σε προηγούμενο βήμα. Επίσης μίας και στο configuration που κάναμε, ζητήσαμε να γίνονται όλα μέσω secure connection θα επιλέξουμε και το Connect Securely. Βλέπουμε από κάτω ότι αυτόματα επιλέγονται *HTTPS: 443* και *SSH: 22.*

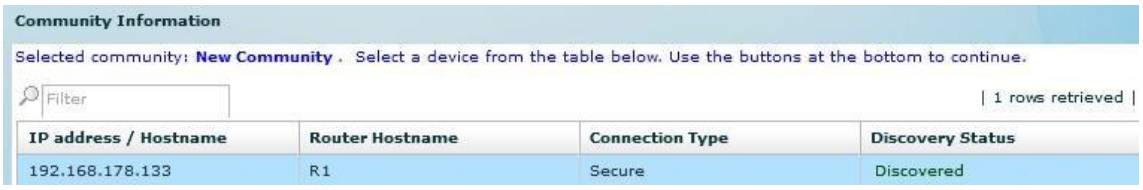
Εικόνα 57. Router discovery (βήμα 1)

Η συσκευή λοιπόν με τα στοιχεία που συμπληρώσαμε έχει προστεθεί στη λίστα αλλά δεν έχει αναγνωριστεί ακόμη από την εφαρμογή. Πατάμε στο κουμπί discover για να ολοκληρωθεί η διαδικασία. Βλέπουμε ότι ακόμη δεν εμφανίζεται ούτε το όνομα του router και ότι το connection type είναι non secure. Αν ολοκληρωθεί σωστά η διαδικασία, αυτά τα πεδία θα πρέπει να αλλάξουν.



Εικόνα 58. Router discovery (βήμα 2)

Αν όλα τα στοιχεία είναι σωστά και ανταποκρίνονται στα στοιχεία που έχουμε εισάγει στο router μας, τότε μετά από λίγο θα μας εμφανίσει μήνυμα ότι η διαδικασία ολοκληρώθηκε επιτυχώς. Διαφορετικά θα εμφανίζει με κόκκινα γράμματα *discovery failed*.



Εικόνα 59. Router discovery (βήμα 3)

Αφού λοιπόν η εφαρμογή αναγνωρίσει επιτυχώς το router μας, στην πάνω αριστερή μεριά του CCP εμφανίζεται η IP που έχουμε καταχωρήσει. Αν έχουμε παραπάνω από ένα router τότε με το drop down menu επιλέγουμε τα υπόλοιπα router. Το κουμπί που θα χρησιμοποιηθεί κατά κόρον από εδώ και πέρα είναι το Configure, από το οποίο εμφανίζονται όλες οι πιθανές ενέργειες (απλές ή advanced) που μπορούμε να ολοκληρώσουμε και μέσω CLI.

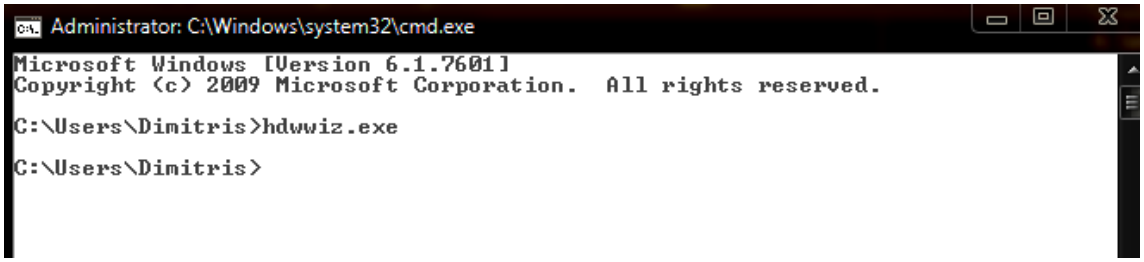
Εικόνα 60. Interface CCP

Στην παραπάνω εικόνα φαίνονται μερικές από τις πιθανές επιλογές που μπορούμε να κάνουμε, αλλά εμάς περισσότερο, για την μεταπτυχιακή εργασία, μας ενδιαφέρει η επιλογή VPN και οι υποκατηγορίες.

4.3. Βασική παραμετροποίηση ASDM

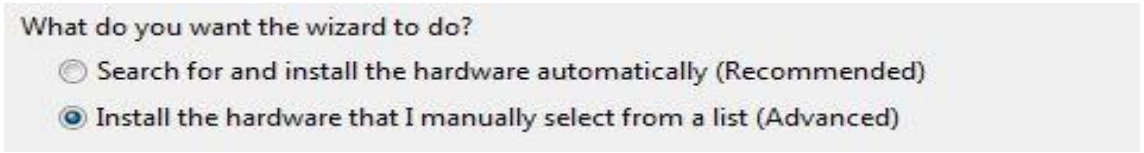
Για να μπορέσουμε να κάνουμε το ASDM να αναγνωρίσει το firewall που εισάγαμε στο σύστημα ακολουθώντας το manual του GNS3 που παρουσιάσαμε πιο πάνω, θα πρέπει να κάνουμε μια λίγο πιο ιδιαίτερη διαδικασία σε σχέση με το CCP. Αρχικά θα πρέπει να ενεργοποιήσουμε το loopback adapter του υπολογιστή μας. Αυτό γίνεται παρακάτω βήματα.

1. Ανοίγουμε ένα cmd και πληκτρολογούμε *hdwwiz.exe*



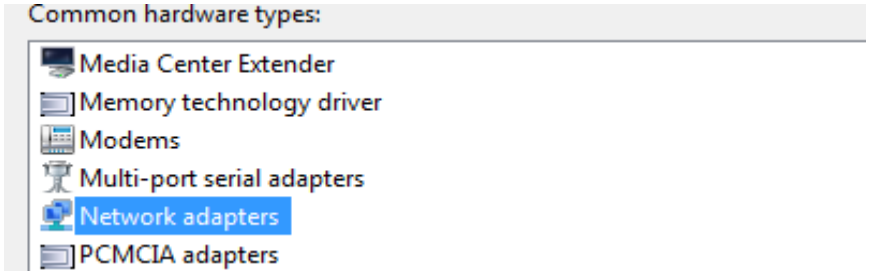
Εικόνα 61. Εισαγωγή loopback adapter (βήμα 1)

2. Αυτή η εντολή ενεργοποιεί τον wizard για να εισάγουμε στο σύστημα οποιοδήποτε hardware θέλουμε. Αφού εμφανιστεί η εισαγωγική σελίδα, πατάμε next και από τις δυο επιλογές, επιλέγουμε το *advanced*.



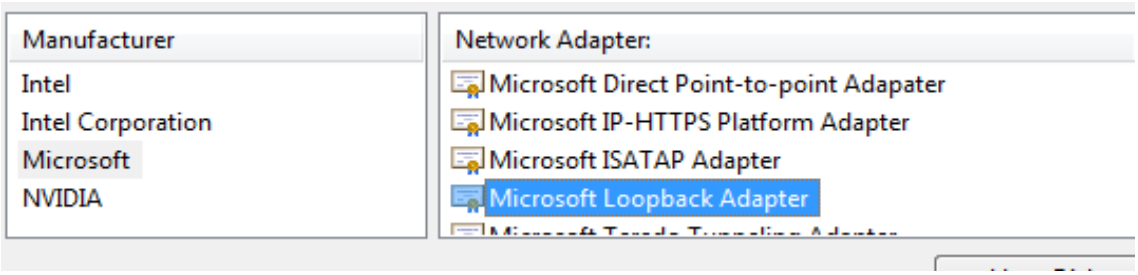
Εικόνα 62. Εισαγωγή loopback adapter (βήμα 2)

3. Από τη λίστα με hardware type επιλέγουμε *network adapters*.



Εικόνα 63. Εισαγωγή loopback adapter (βήμα 3)

4. Στη σελίδα που εμφανίζεται από την κατηγορία manufacturer επιλέγουμε Microsoft και από την κατηγορία *Network adapter* επιλέγουμε *Microsoft Loopback Adapter*.



Εικόνα 64. Εισαγωγή loopback adapter (βήμα 4)

5. Αφού πατήσουμε *Next*, η διαδικασία ολοκληρώνεται επιτυχώς και εμφανίζεται το αντίστοιχο μήνυμα.

Εικόνα 65. Εισαγωγή loopback adapter (βήμα 5)

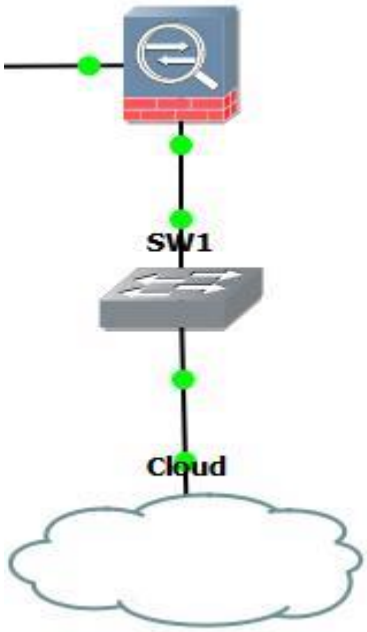
Αμέσως μετά, εισάγουμε ένα cloud στην τοπολογία μας. Με right click επιλέγουμε configure και από το Ethernet Tab μέσω του drop down menu επιλέγουμε την Loopback Adapter.

Εικόνα 66. Παραμετροποίηση GNS3 για εισαγωγή asdm-image στο firewall (βήμα 1)

Τώρα το μόνο που απομένει είναι να συνδέσουμε το cloud με το firewall. Επειδή όμως το cloud δε μπορεί να συνδεθεί απευθείας με καμία interface του firewall, θα πρέπει ενδιάμεσα να εισάγουμε ένα switch. Στο cloud επιλέγουμε να συνδεθούμε μέσω της loopback adapter.

Εικόνα 67. Παραμετροποίηση GNS3 για εισαγωγή asdm-image στο firewall (βήμα 2)

Συνδέουμε λοιπόν το cloud με το switch και το switch με το firewall.



Εικόνα 68. Παραμετροποίηση GNS3 για εισαγωγή asdm-image στο firewall (βήμα 3)

Αφού ολοκληρώσαμε τη συνδεσμολογία θα δώσουμε IP στην interface που συνδέεται με το switch. Θα δώσουμε την IP 192.168.10.1/24.

```
ciscoasa(config)#
ciscoasa#
ciscoasa# conf t
ciscoasa(config)# int gi1
ciscoasa(config-if)# nameif management
INFO: Security level for "management" set to 0 by default.
ciscoasa(config-if)# ip ad
ciscoasa(config-if)# ip address 192.168.10.1 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# no shutdown
```

Εικόνα 69. Παραμετροποίηση firewall για εισαγωγή asdm-image (βήμα 1)

Το επόμενο βήμα είναι να πάμε στο Network and Sharing Center → change adapter settings → επιλέγουμε την loopback adapter → properties → IPv4 και χειροκίνητα βάζουμε την IP 192.168.10.2/24. Σημαντική προϋπόθεση είναι να απενεργοποιήσουμε το firewall του υπολογιστή για να επικοινωνήσει σωστά το firewall μας με την loopback adapter. Παρακάτω φαίνεται μια εικόνα που εμφανίζει το αποτέλεσμα του ping προς την IP 192.168.10.2 πριν και μετά την απενεργοποίηση του firewall.

```
ciscoasa(config-if)# ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
ciscoasa(config-if)# ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

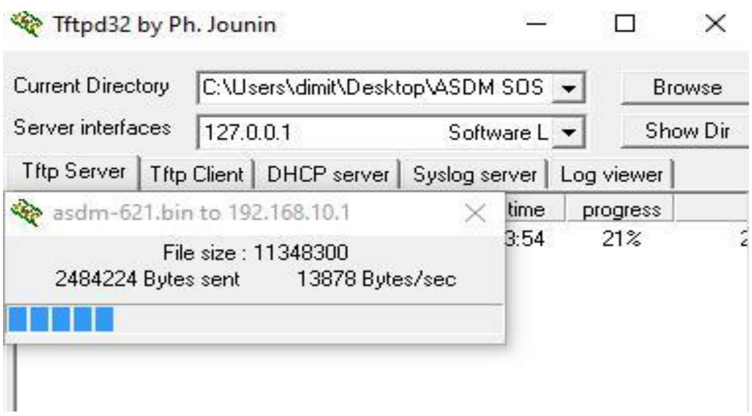
Εικόνα 70. Αποτέλεσμα ping πριν και μετά την απενεργοποίηση του firewall

Αφού έχουμε κάνει download το ASDM, από το site http://tftpd32.jounin.net/tftpd32_download.html εγκαθιστούμε έναν TFTP server και από εκεί εντοπίζουμε το σημείο που αποθηκεύσαμε το αρχείο bin. Ταυτόχρονα από το CLI του firewall, πρέπει να κάνουμε download την asdm image. Εισάγουμε τις παρακάτω εντολές.

```
ciscoasa# copy tftp flash

Address or name of remote host []? 192.168.10.2

Source filename []? asdm-621.bin

Destination filename [asdm-621.bin]?

Accessing tftp://192.168.10.2/asdm-621.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Εικόνα 71. Download asdm-image από TFTP server

Βλέπουμε την αντίστοιχη διαδικασία στον TFTP Server. Περιμένουμε μέχρι να ολοκληρωθεί η διαδικασία.



Εικόνα 72. Επιβεβαίωση σωστού download του asdm-image απο τη μεριά του TFTP server

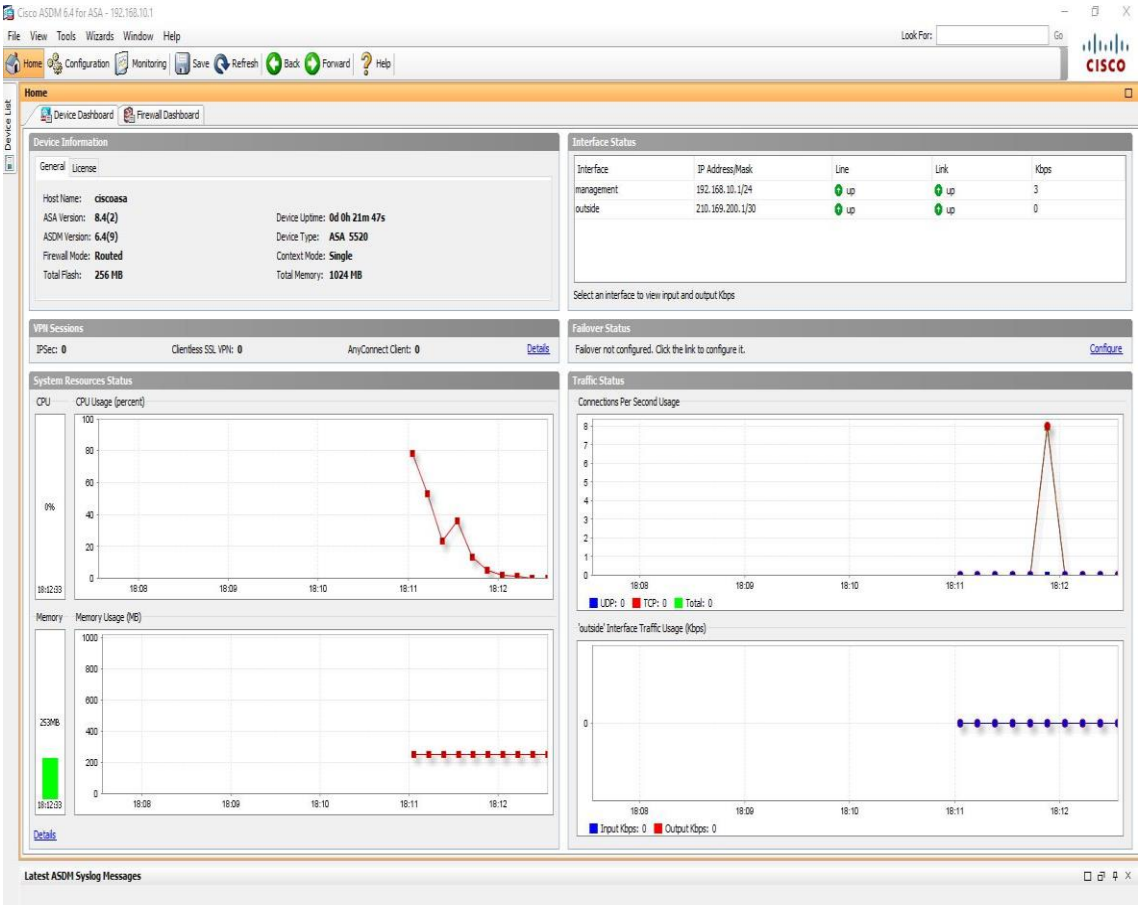
Τώρα, πρέπει να ρυθμίσουμε το firewall να κάνει load το ASDM στην επόμενη επανεκκίνηση, να ενεργοποιήσουμε τον HTTP Server και να θέσουμε username και password.

```
ciscoasa# config t
ciscoasa(config)# asdm image flash:asdm-621.bin
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.10.2 255.255.255.255 management
ciscoasa(config)# username jim password vrettos privilege 15
```

Εικόνα 73. Ενεργοποίηση http server και εισαγωγή username/password για τον administrator

Τέλος, ανοίγουμε το εκτελέσιμο αρχείο του ASDM , εισάγουμε την IP μαζί με το username και password, περιμένουμε να γίνει ένα update και γίνεται είσοδος στο Interface του firewall.

Εικόνα 74. Προσπάθεια εισόδου στο interface του ASDM



Εικόνα 75. Επιτυχημένη είσοδος στο ASDM

5. Υλοποίηση VPN

Από αυτό το σημείο γίνεται η εισαγωγή στο πρακτικό κομμάτι της μεταπτυχιακής διατριβής. Στα επόμενα κεφάλαια θα υλοποιήσουμε IPsec VPN και SSL VPN, θα εξηγήσουμε κάθε ενέργεια που κάνουμε, θα επιβεβαιώσουμε ότι όλα λειτουργούν σωστά και αν βρεθεί κάποιο σφάλμα θα κάνουμε τους απαραίτητους ελέγχους και θα προσπαθήσουμε να βρούμε το σφάλμα και να το διορθώσουμε. Κατά την υλοποίηση θα χρησιμοποιήσουμε κάποιες τεχνικές που περιγράφονται στο εγχειρίδιο χρήσης, οπότε θα γίνεται απλή αναφορά, χωρίς να χρειάζεται κάθε φορά να τις εξηγούμε.

5.1. Υλοποίηση IPsec VPN

Στο κομμάτι αυτό θα δημιουργήσουμε δυο τοπολογίες. Στη μια θα υλοποιήσουμε το IPsec VPN χωρίς την παρουσία κάποιου firewall και στην δεύτερη, η υλοποίηση θα γίνει με τη χρήση του firewall ASA. Και στις δυο τοπολογίες η υλοποίηση θα γίνει και μέσω command line αλλά και μέσω wizards. Το αποτέλεσμα θα είναι το ίδιο, αλλά στόχος είναι να παρουσιάσουμε και τις δυο εναλλακτικές που υφίστανται. Πριν ξεκινήσουμε την υλοποίηση, καλό θα ήταν να πούμε λίγα πράγματα για το πρωτόκολλο IPsec. Το IPsec είναι αυτό που εξασφαλίζει την ασφαλή επικοινωνία στο site-to-site/remote access VPN. Για να το πετύχει αυτό χρησιμοποιεί το IKE (Internet Key Exchange) protocol, το οποίο είναι ένα framework το οποίο προσφέρεται από την ISAKMP (Internet Security Association and Key Management Mechanism).

Το IKE χωρίζεται σε phase 1 και phase 2. Η phase 1 είναι αυτή κατά την οποία τα άκρα του VPN “διαπραγματεύονται” και αυθεντικοποιούν το ένα το άλλο. Κατά την phase 2 “διαπραγματεύονται” θέματα σχετικά με την κρυπτογράφηση των δεδομένων που θα μεταφερθούν μέσα από το tunnel που θα δημιουργήσουμε, καθώς και θέματα αλγορίθμων. Όπως θα περίμενε κανείς, και είναι λογικό, αν το negotiation μεταξύ των δυο peers δεν είναι επιτυχές, δηλαδή δεν συμφωνούν οι αλγόριθμοι, δεν τίθεται θέμα σωστής λειτουργίας της phase 2 , αρά δεν υπάρχει περίπτωση να δημιουργηθεί και το IPsec tunnel.

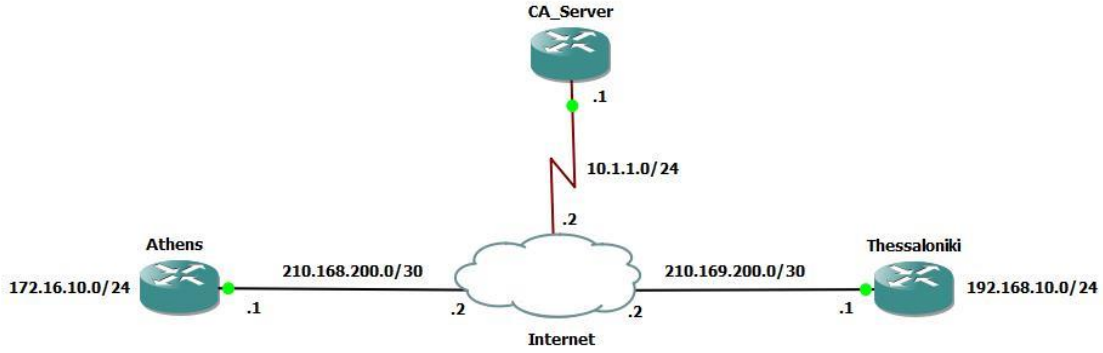
Υπάρχουν δυο version IKE. Το IKEv1 και το IKEv2. Στα παραδείγματα της παρούσας διπλωματικής εργασίας χρησιμοποιούμε μόνο το IKEv1. Επιγραμματικά θα αναφέρουμε τις δυο σημαντικότερες διαφορές τους.

1. IKEv1 (The Internet Key Exchange)[23]
    - Για την ανταλλαγή των μηνυμάτων χρησιμοποιεί είτε main είτε aggressive mode.
    - Στην phase 2 χρησιμοποιεί τουλάχιστον three-message pair exchange.
2. IKEv2 (Internet Key Exchange Protocol)[24]
    - Για την ανταλλαγή των μηνυμάτων δε χρησιμοποιεί main/aggressive mode. Ονομάζεται simple exchange, αλλά εμφανίζονται αρκετά από τα στοιχεία του aggressive mode.
    - Σε αντίθεση με το IKEv1, χρησιμοποιεί two-message pair exchange

[23] https://tools.ietf.org/html/rfc2409
[24] https://tools.ietf.org/html/rfc4306

5.1.1. Υλοποίηση IPsec VPN με IOS Routers

Πριν ξεκινήσουμε την υλοποίηση και για να καταλάβουμε καλύτερα τι είναι αυτό που θέλουμε να δημιουργήσουμε, θα αναφέρουμε ένα case study. Ας υποθέσουμε ότι εργαζόμαστε σαν τεχνικοί δικτύων σε μια εταιρία και ο διευθυντής μας ανέθεσε το εξής project. Η εταιρία μόλις δημιούργησε καινούρια γραφεία στη Θεσσαλονίκη και είναι απαραίτητο να υπάρχει σύνδεση μεταξύ των νέων γραφείων στη Θεσσαλονίκη με τα κεντρικά γραφεία της Αθήνας χωρίς να ξεχνάμε την ανάγκη για εμπιστευτικότητα (confidentiality), ακεραιότητα των δεδομένων (data integrity), αυθεντικοποίηση (authentication) και προστασία αντιγραφής δεδομένων (anti-replay protection). Με λίγα λόγια μας ζητείται να υλοποιήσουμε ένα IPsec VPN. Πριν ξεκινήσουμε να κάνουμε οποιαδήποτε ενέργεια θα πρέπει να καταγράψουμε τα δεδομένα που έχουμε. Σε αυτό θα μας βοηθήσει πολύ η εικόνα της τοπολογίας.



Εικόνα 76. Τοπολογία case study για υλοποίηση IPsec VPN

Όπως βλέπουμε πίσω από τα router Athens και Thessaloniki, στο εσωτερικό, πλέον, δίκτυο, έχουν τοποθετηθεί από loopback addresses που αναπαριστούν τα subnets που υπάρχουν. Θα μπορούσαμε να προσθέσουμε κάποιο VPC που να αναπαριστά κάποιον χρήστη, αλλά οι loopback addresses παίζουν ακριβώς τον ίδιο ρόλο χωρίς να επιβαρύνουν το σύστημά μας. Σε πραγματικές συνθήκες, ανάμεσα στα γραφεία της Θεσσαλονίκης και της Αθήνας, θα υπήρχαν πάρα πολλά router. Χάριν συντομίας όμως, ανάμεσά τους έχουμε τοποθετήσει μόλις ένα router, το οποίο συμβολίζει το Internet και γι' αυτό το αναπαριστούμε με το εικονίδιο του "σύννεφου". Όπως βλέπουμε στην τοπολογία, υπάρχει ένα επιπλέον router με την ονομασία CA_Server. Το router αυτό παίζει πολύ σημαντικό ρόλο στην υλοποίηση του IPsec VPN καθώς παίζει το ρόλο του Certificate Authority. Σχετικά με τα πρωτοκόλλα δρομολόγησης που χρησιμοποιούνται, έχουμε πολλές επιλογές. Η πιο εύκολη, θα ήταν να χρησιμοποιήσουμε static ή default static αλλά αυτό δε θα ανταποκρινόταν στην πραγματικότητα καθώς δεν είναι εφικτό να κάνουμε configure όλα τα ενδιάμεσα routers και αν φυσικά άλλαζε κάτι, η δρομολόγηση πακέτων δε θα λειτουργούσε. Έτσι αποφασίσαμε να χρησιμοποιήσουμε το πρωτόκολλο BGP που απλά χρειάζεται να κάνουμε advertise τα απαραίτητα routes στα γειτονικά routers. Στα δίκτυα που "βλέπει" το router Internet χρησιμοποιήθηκε eBGP (αυτό χρησιμοποιείται και σε κανονικές συνθήκες) και για τα εσωτερικά δίκτυα των routers Athens και Thessaloniki χρησιμοποιήθηκε iBGP. Εναλλακτική θα ήταν το OSPF ή το EIGRP. Δε χρησιμοποιήθηκε NAT καθώς αυτό θα δημιουργούσε αρκετά προβλήματα στην υλοποίηση.

5.1.1.1. Υλοποίηση με CLI (Command Line Interface)

Το πρώτο που θα πρέπει να κάνουμε πριν ξεκινήσουμε την υλοποίηση του IPsec VPN θα πρέπει να επιβεβαιώσουμε ότι η σύνδεση λειτουργεί και ότι οποιοδήποτε router στο εσωτερικό δίκτυο της Αθήνας μπορεί να κάνει ping/traceroute μια IP στο εσωτερικό δίκτυο της Θεσσαλονίκης. Επειδή στη συνέχεια θα υλοποιήσουμε IPsec VPN μας ενδιαφέρει τα πακέτα να φτάνουν επιτυχώς σε οπουδήποτε σημείο στη δεξιά μεριά του router Thessaloniki, καθώς εκεί θεωρείται εσωτερικό δίκτυο. Για του λόγου το αληθές θα προσπαθήσουμε να κάνουμε ping/traceroute από την interface loopback 1 του router Athens στην loopback address του router Thessaloniki. Επίσης θα πρέπει να υπάρχει συνδεσιμότητα μεταξύ των router Athens και Thessaloniki με τον CA_Server. Όπως βλέπουμε στις 2 πιο κάτω φωτογραφίες, όλα λειτουργούν σωστά.

```
Thessaloniki#ping 10.1.1.1 source loopback1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/33/56 ms
```

```
Athens#ping 192.168.10.1 source loopback1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/32/56 ms
Athens#traceroute 192.168.10.1

Type escape sequence to abort.
Tracing the route to 192.168.10.1

  1 210.168.200.2 16 msec 48 msec 12 msec
  2 210.169.200.1 16 msec 56 msec 24 msec
Athens#ping 10.1.1.1 source loopback1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/44/64 ms
```

Εικόνα 77. Επιβεβαίωση σωστής συνδεσιμότητας πριν την υλοποίηση IPsec VPN

Αμέσως μετά, θα πρέπει να ρυθμίσουμε το NTP (Network Time Protocol). Αυτό είναι σημαντικό γιατί και τα δυο router θα πρέπει να έχουν ακριβώς τα ίδια time settings έτσι ώστε όταν σε επόμενο βήμα θα δημιουργήσουμε πιστοποιητικά, να μην υπάρξει απόρριψη λόγω διαφορετικών ρυθμίσεων. Σε πραγματικές συνθήκες το router που έχουμε ονομάσει σαν Internet θα είχε τις σωστές ρυθμίσεις και εμείς το μόνο που θα έπρεπε να κάνουμε είναι να συγχρονίσουμε τα router σε Αθήνα και Θεσσαλονίκη (όλα τα router που βρίσκονται πίσω από αυτά θα συγχρονίζονταν αυτόματα). Στη δικιά μας τοπολογία, αυτό που πρέπει να κάνουμε είναι να ορίσουμε το router CA_Server σαν ntp master και μετά να συγχρονίσουμε τα router Athens, Thessaloniki και Internet.

Για να ολοκληρωθεί αυτή η διαδικασία επιτυχώς θα πρέπει να συνδέσουμε το router CA_Server με την κάρτα δικτύου μας (αναφέρεται στο εγχειρίδιο χρήσης). Πάμε λοιπόν στο router CA_Server και αφού μπούμε σε configuration mode, εισάγουμε την εντολή *ntp master*. Εδώ θα μας ζητηθεί να ορίσουμε ένα *stratum number*. Αυτός ο αριθμός δείχνει το πόσο μακριά ή πόσο κοντά βρισκόμαστε στο Atomic clock source. Το atomic clock είναι ένα ρολόι που χρησιμοποιεί την ηλεκτρονική συχνότητα στην οπτική ή υπεριώδη περιοχή του ηλεκτρομαγνητικού φάσματος των ατόμων σαν πρότυπο συχνότητας για να μπορεί να προσδιορίζει την ώρα[25]. Τέτοιου είδους ρολόγια είναι τα πλέον ακριβή και γι' αυτό θα τα χρησιμοποιήσουμε και εμείς. Μας ζητείται να ορίσουμε έναν αριθμό από το 1-15. Όσο πιο χαμηλός ο αριθμός, τόσο πιο κοντά στο ατομικό ρολόι βρισκόμαστε. Καλό είναι να επιλέγουμε έναν αρκετά χαμηλό αριθμό. Επίσης αν θέλουμε, δεν ορίζουμε αριθμό και το σύστημα επιλέγει έναν μόνο του (συνήθως το stratum 7 ή το stratum 8). Η διαδικασία χρειάζεται περίπου 60 δευτερόλεπτα για να ολοκληρωθεί.

```
CA_Server#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CA_Server(config)#ntp master ?
  <1-15>  Stratum number
  <cr>

CA_Server(config)#ntp master 3
```

Εικόνα 78. Ρύθμιση NTP server

Οι εντολές για να επιβεβαιώσουμε ότι το ρολόι έχει συγχρονιστεί είναι οι *show ntp status* και *show ntp associations*. Αν πληκτρολογήσουμε το show ntp status πριν προλάβει να ολοκληρωθεί ο συγχρονισμός θα δούμε το παρακάτω μήνυμα. Παρατηρούμε ότι έχει stratum number 16 που σημαίνει ότι δεν υπάρχει ακόμη συγχρονισμός (αναφέρεται και στην αρχή του μηνύματος) και η ημερομηνία είναι 01/01/1990.

```
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
```

Εικόνα 79. Εικόνα μη σωστά συγχρονισμένου ntp server

Μόλις ολοκληρωθεί σωστά η διαδικασία, με τις δυο προαναφερθείσες εντολές έχουμε την παρακάτω εικόνα. Βλέπουμε ότι η ημερομηνία και η ώρα έχει ρυθμιστεί σωστά και το stratum number είναι 3, όπως ακριβώς το θέσαμε εμείς. Στην πρώτη εντολή, το show ntp associations, το stratum number είναι 2, γιατί ενδιάμεσα από το atomic clock και το router CA_Server υπάρχει ο server με IP 127.127.7.1 που αυτομάτως αποκτά το ενδιάμεσο stratum number.

[25] https://en.wikipedia.org/wiki/Atomic_clock

```
CA_Server#sh ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
*~127.127.7.1      127.127.7.1      2     0    64   17     0.0    0.00  1875.0
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
CA_Server#sh ntp st
CA_Server#sh ntp status
Clock is synchronized, stratum 3, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is DB4252F7.F5BA822A (21:21:59.959 UTC Tue Jul 26 2016)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
CA_Server#
```

Εικόνα 80. Εικόνα σωστά συγχρονισμένου ntp server

Για να συγχρονίσουμε και τα υπόλοιπα τρία router, θα εισάγουμε σε κάθε ένα την εντολή *ntp peer και την IP της serial 4/0* (την Interface δηλαδή που συνδέεται με το router Internet, την 10.1.1.1). Ελάχιστα δευτερόλεπτα μετά θα δούμε ότι έχουν και αυτά συγχρονιστεί. Έχουν stratum number 4 γιατί συνδέονται με το router CA_Server, στον οποίο θέσαμε stratum number 3, άρα αυξάνεται κατά 1. Φυσικά, μιας και πρόκειται για προσομοίωση, ίσως υπάρχουν κάποιες μικρές αποκλίσεις στο ρολόι όσο απομακρυνόμαστε από τον CA_Server.

```
Athens#show ntp status
Clock is synchronized, stratum 4, reference is 10.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is DB4253A8.CCE3B5DE (21:24:56.800 UTC Tue Jul 26 2016)
clock offset is 5.6905 msec, root delay is 20.11 msec
root dispersion is 13.28 msec, peer dispersion is 7.57 msec
Athens#
```

Εικόνα 81. Εικόνα σωστά συγχρονισμένου ntp peer

Εναλλακτικά, μπορούσαμε είτε να συγχρονίσουμε τα ρολόγια χειροκίνητα με έναν ntp server της επιλογής μας, όπως ο *pool.ntp.org με IP 64.99.80.121*, είτε να ρυθμίσουμε εμείς το ρολόι και την ημερομηνία των routers. Η πρώτη εναλλακτική απορρίφθηκε επειδή χρειάζεται περίπου 15-20 λεπτά ανά router για να ολοκληρωθεί ο συγχρονισμός και η δεύτερη εναλλακτική επειδή θέλαμε να κάτι πιο κοντά στην πραγματικότητα.

Αμέσως μετά πάμε να ρυθμίσουμε την Certificate Authority. Αφού μπούμε σε configuration mode, ενεργοποιούμε τον http Server με την εντολή *ip http server*. Είναι πολύ σημαντικό να μην ξεχάσουμε αυτή την εντολή, διαφορετικά, σε μεταγενέστερο στάδιο, όταν θα χρειαστεί να επικοινωνήσουν τα router Athens και Thessaloniki, με την Αρχή Πιστοποίησης, θα παρουσιαστεί σφάλμα. Αμέσως μετά, εισάγουμε την εντολή *crypto key generate rsa general-keys label test modulus 2048 exportable.* Με αυτή την εντολή δημιουργούμε ένα ζεύγος γενικής χρήσης RSA κλειδιών για κρυπτογράφηση και υπογραφή, με όνομα *test*, μεγέθους *2048 bit*, τα οποία μπορούμε να εξάγουμε, αν χρειαστεί. Σαν όνομα μπορούμε να βάλουμε οτιδήποτε και σαν μέγεθος κλειδιών είχαμε τη δυνατότητα να επιλέξουμε από 360 μέχρι και 2048 bit. Όσο περισσότερα τα bit, τόσο πιο ασφαλή τα κλειδιά και φυσικά τόσο περισσότερη ώρα να δημιουργηθούν. Αμέσως μόλις δημιουργηθεί το ζεύγος κλειδιών, ενεργοποιείται και το SSH.

```
CA_Server#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CA_Server(config)#ip http server
CA_Server(config)#$sa general-keys label test modulus 2048 exportable
The name for the keys will be: test

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...[OK]

CA_Server(config)#
Aug 10 18:57:31.511: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Εικόνα 82. Δημιουργία RSA κλειδιών γενικής χρήσης στον CA_Server

Αμέσως μετά το ζεύγος κλειδιών που δημιουργήσαμε, θα το εξάγουμε και θα το αποθηκεύσουμε στην NVRAM από όπου θα είναι εύκολα προσπελάσιμο, θα κρυπτογραφήσουμε το private key με 3DES (η άλλη επιλογή είναι το DES αλλά επιλέχτηκε το 3DES επειδή παρέχει μεγαλύτερη ασφάλεια) και θα επιλέξουμε και ένα password για την προστασία του private key (όσο πιο δύσκολο το password, τόσο πιο καλά προστατευμένο είναι). Η εντολή που τα κάνει όλα αυτά είναι η *crypto key export rsa test pem url nvram: 3des Am1357!@.* Είναι πολύ σημαντικό να προσέξουμε το όνομα του pem που θα αποθηκεύσουμε στην NVRAM να είναι ίδιο με το όνομα του κλειδιού που πληκτρολογήσαμε στην προηγούμενη εντολή, που στην προκειμένη περίπτωση είναι το test. Αν δώσουμε διαφορετικό όνομα, η εντολή δε θα λειτουργήσει.

```
CA_Server(config)#crypto key export rsa test pem url nvram: 3des Am1357!@
% Key name: test
   Usage: General Purpose Key
Exporting public key...
Destination filename [test.pub]?
Writing file to nvram:test.pub

Exporting private key...
Destination filename [test.prv]?
Writing file to nvram:test.prv
```

Εικόνα 83. Αποθήκευση κλειδιών στην NVRAM και κρυπτογράφησή τους

Το επόμενο βήμα είναι να ονομάσουμε το domain. Στη δική μας περίπτωση θα το ονομάσουμε *thesis.com*. Μετά, θα μπούμε μέσα στον server για να του δώσουμε στοιχεία. Στο *issuer-name* θα βάλουμε *test.thesis.com* (συνδυασμός των ονομάτων που καταχωρήσαμε πιο πάνω), στο *c(country)* θα βάλουμε *Greece* και στο *l(location)* θα βάλουμε *Athens*.

```
CA_Server(config)#ip domain-name thesis.com
CA_Server(config)#crypto pki server ca_server
CA_Server(cs-server)#issuer-name cn=test.thesis.com c=greece l=athens
```

Εικόνα 84. Ονομασία domain και εισαγωγή στοιχειών του CA_Server

Στη συνέχεια θα πρέπει να επιλέξουμε τον τρόπο με τον οποίο θα διαχειρίζονται τα αιτήματα εγγραφής (enrollment requests). Από τις επιλογές που δίνονται, εμείς θα επιλέξουμε το *grant auto*, για να γίνονται αυτόματα δεκτά όλα τα αιτήματα.

```
CA_Server(cs-server)#grant auto
CA_Server(cs-server)#
Aug 10 19:02:01.863: %PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically granted.
```

Εικόνα 85. Ενεργοποίηση επιλογής για αυτόματη αποδοχή όλων των αιτημάτων για έκδοση πιστοποιητικών.

Φτάνουμε στο σημείο που πρέπει να δημιουργηθεί το CA certificate. Για να ξεκινήσει αυτή η διαδικασία δίνουμε την εντολή *no shutdown.* Αμέσως ζητείται ένα passphrase για την προστασία του private key. Το σύστημα εκτελεί όλες τις διαδικασίες και στο τέλος βλέπουμε το μήνυμα *Certificate Server enabled,* που σημαίνει ότι όλα ολοκληρώθηκαν σωστά.

```
CA_Server(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.
```

Εικόνα 86. Ολοκλήρωση ενεργοποίησης Certificate Server

Αφού λοιπόν τελειώσαμε με το configuration του CA_Server, σειρά έχουν τα routers σε Αθήνα και Θεσσαλονίκη. Οι επιλογές που θα κάνουμε στο router της Αθήνας θα πρέπει να είναι ίδιες με αυτές που πρέπει να γίνουν στο router της Θεσσαλονίκης, με εξαίρεση ενός σημείου που θα δούμε σε μεταγενέστερο σημείο. Αν υπάρχει κάποια άλλη αναντιστοιχία, αυτό θα οδηγήσει στην μη λειτουργία του VPN.

Αρχικά ονομάζουμε το domain (το όνομα θα πρέπει να είναι ίδιο με αυτό που επιλέξαμε στο router CA_Server) και ξεκινάμε την παραγωγή κλειδιών RSA. Θα ζητηθεί μέγεθος κλειδιών με εύρος 360-2048 bit. Εμείς θα επιλέξουμε το ένα μεσαίο μέγεθος, τα 1024 bit.

```
Athens#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Athens(config)#ip domain-name thesis.com
Athens(config)#crypto key generate rsa
The name for the keys will be: Athens.thesis.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Athens(config)#
Aug 10 19:05:46.691: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Εικόνα 87. Έκδοση RSA κλειδιών στο router Athens

Αυτό που θα πρέπει να προσέξουμε είναι ότι σαν όνομα επιλέχτηκε αυτόματα το *Athens.thesis.com*, δηλαδή το όνομα του router και το όνομα του domain που ορίσαμε στην αρχή. Εδώ θα πρέπει να τονιστεί, ότι για να ξεκινήσει η παραγωγή κλειδιών, θα πρέπει να

έχουμε αλλάξει το default όνομα του router που είναι *Router*. Διαφορετικά η διαδικασία δε μπορεί να ξεκινήσει.

Στη συνέχεια, θα ονομάσουμε την Certificate Authority (CA) που θέλουμε να χρησιμοποιήσουμε (θα βάλουμε το όνομα που χρησιμοποιήσαμε στον CA_Server και γνωρίζοντας την IP του, θα χρησιμοποιήσουμε αυτά τα στοιχεία για να υπάρξει η σωστή επικοινωνία). Οι εντολές που θα χρησιμοποιηθούν είναι *crypto pki trustpoint ca_server* και *enrollment url* http://10.1.1.1

```
Athens(config)#crypto pki trustpoint ca_server
Athens(ca-trustpoint)#enrollment url http://10.1.1.1
```

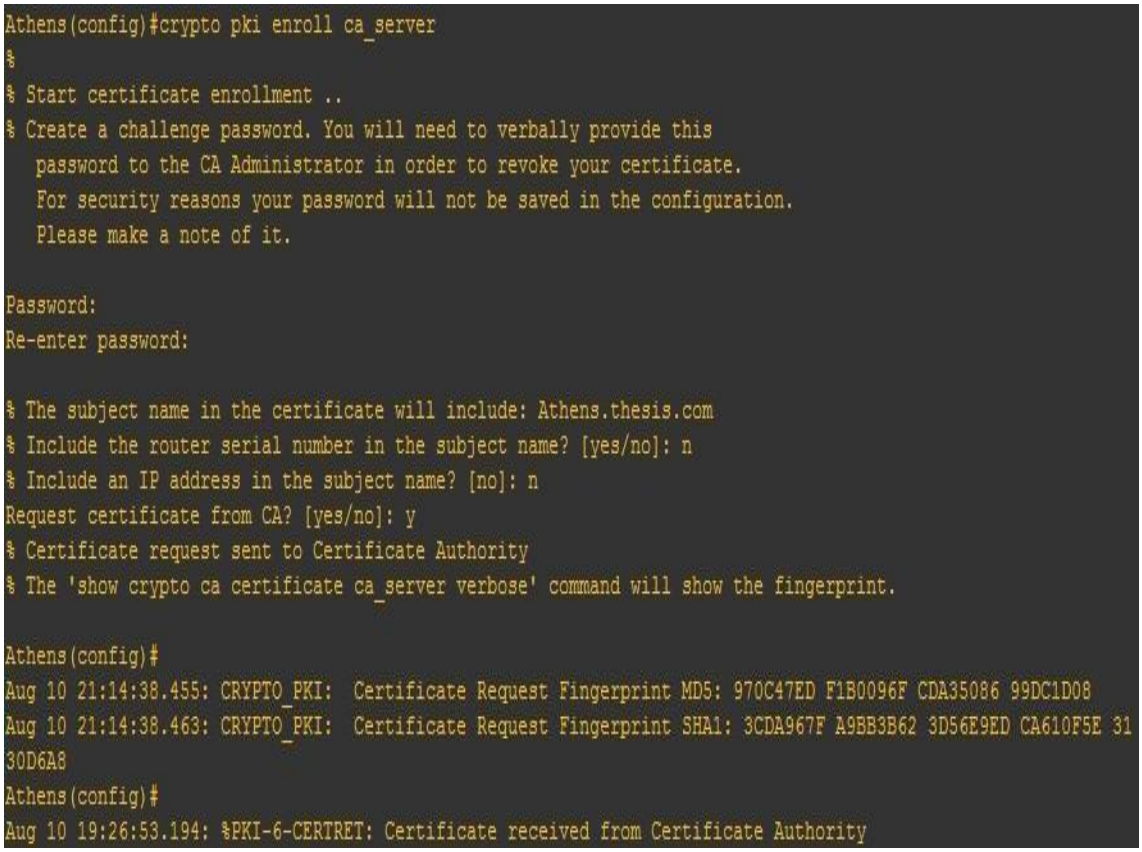
Εικόνα 88. Ορισμός CA_Server που θα χρησιμοποιήσουμε και εισαγωγή IP της interface του

Αμέσως μετά, θα ρυθμίσουμε να γίνεται έλεγχος για ανακληθέντα πιστοποιητικά. Λόγω περιορισμών του λογισμικού αν και θα έπρεπε να δώσουμε την εντολή *revocation-check ocsp* θα δώσουμε την εντολή *revocation-check none*. Στη συνέχεια δίνουμε την εντολή να γίνει δεκτό το certificate του CA_Server. Αρχικά, βλέπουμε και το fingerprint του πιστοποιητικού αυτού σε MD5 και SHA1. Αν τα έχουμε ρυθμίσει όλα σωστά, το ίδιο fingerprint θα πρέπει να εμφανίζει όταν κάνουμε στην αντίστοιχη διαδικασία στο router Thessaloniki. Στο τέλος δηλώνουμε ότι δεχόμαστε το certificate.

```
Athens(ca-trustpoint)#revocation-check none
Athens(config)#crypto pki authenticate ca_server
Certificate has the following attributes:
       Fingerprint MD5: 0F8CDF50 92D75A6A 81BA5D8C 65C1008C
      Fingerprint SHA1: 5F5D858A 36DD2120 F818E0E1 3ED91A80 F763B1AC

% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

Εικόνα 89.Εμφάνιση fingerprint του CA_Server και αποδοχή πιστοποιητικού

Τέλος, αφού δεχτήκαμε το certificate της CA, θα ζητήσουμε ένα certificate υπογεγραμμένο από την CA που δημιουργήσαμε σε προηγούμενο βήμα. Αυτό θα γίνει με την εντολή *crypto pki enroll ca_server.*



Εικόνα 90. Αίτημα από το router Athens για υπογεγραμμένο πιστοποιητικό από τον CA_Server. Επιβεβαίωση επιτυχημένης παραλαβής

Όπως βλέπουμε μας ζητείται ένα password το οποίο χρησιμοποιείται σε περίπτωση που χρειαστεί να γίνει ανάκληση του πιστοποιητικού. Στη συνέχεια μας ζητείται να απαντήσουμε σε δυο ερωτήσεις σχετικά με το τι θέλουμε να αναγράφεται στο πιστοποιητικό. Για λόγους ασφαλείας θα επιλέξουμε να μην αναγράφεται ούτε το serial number του router ούτε η IP του. Απλά δεχόμαστε το certificate που έφτιαξε η CA. Στη συνέχεια φαίνεται το fingerprint του certificate που δημιουργήθηκε και καταλαβαίνουμε ότι όλα είναι σωστά, αφού στο τέλος εμφανίζεται το μήνυμα *Certificate received from Certificate Authority*. Με την εντολή *show crypto ca certificate ca_server* έχουμε εικόνα των περιεχομένων.

```
Athens(config)#do show crypto ca certificate ca_server
Certificate
  Status: Available
  Certificate Serial Number: 04
  Certificate Usage: General Purpose
  Issuer:
    cn=test.thesis.com c\=greece l\=athens
  Subject:
    Name: Athens.thesis.com
    hostname=Athens.thesis.com
  Validity Date:
    start date: 21:14:40 UTC Aug 10 2016
    end   date: 21:14:40 UTC Aug 10 2017
  Associated Trustpoints: ca_server

CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Issuer:
    cn=test.thesis.com c\=greece l\=athens
  Subject:
    cn=test.thesis.com c\=greece l\=athens
  Validity Date:
    start date: 19:03:21 UTC Aug 10 2016
    end   date: 19:03:21 UTC Aug 10 2019
  Associated Trustpoints: ca_server
```

Εικόνα 91. Εικόνα περιεχομένου πιστοποιητικού

Αφού τελειώσαμε με το router Athens, κάνουμε την ίδια διαδικασία και στο router Thessaloniki, έτσι ώστε μετά να προχωρήσουμε στη δημιουργία του IPsec tunnel μεταξύ τους. Για λόγους συντομίας δε θα υπάρξουν screenshots των εντολών στο router Thessaloniki. Άλλωστε στο παράρτημα θα υπάρχει το τελικό configuration. Το μόνο screenshot που θα προσθέσουμε είναι στο σημείο που εμφανίζεται το fingerprint του certificate της CA για να επαληθεύσουμε ότι είναι ίδιο με αυτό που εμφανίστηκε στο router Athens.

```
Thessaloniki(ca-trustpoint)#crypto pki authenticate ca_server
Certificate has the following attributes:
       Fingerprint MD5: 0F8CDF50 92D75A6A 81BA5D8C 65C1008C
      Fingerprint SHA1: 5F5D858A 36DD2120 F818E0E1 3ED91A80 F763B1AC

% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

Εικόνα 92. Επιβεβαίωση ότι και το router Thessaloniki έλαβε το ίδιο fingerprint με αυτό που έλαβε το router Athens

Μετά τη δημιουργία certificates , θα προχωρήσουμε στο configuration της IKEv1 phase 1 policy και IKEv1 phase 2 policy. Εδώ θα πρέπει να τονιστεί ότι δε θα γίνει χρήση pre-shared keys αλλα των digital certificates που δημιουργήσαμε.

Ξεκινάμε λοιπόν να ρυθμίσουμε την isakmp policy. Στα πλαίσια αυτού του policy θα ρυθμίσουμε τον αλγόριθμο κρυπτογράφησης, τον αλγόριθμο hash, τη μέθοδο

αυθεντικοποίησης, το Diffie-Hellman group καθώς και το χρόνο, σε δευτερόλεπτα, που θα παραμένει ενεργό το ISAKMP security association.

```
Athens(config)#crypto isakmp policy 1
Athens(config-isakmp)#encryption aes 256
Athens(config-isakmp)#group 5
Athens(config-isakmp)#authentication rsa-sig
Athens(config-isakmp)#hash sha
Athens(config-isakmp)#lifetime 3600
```

Εικόνα 93. Configuration IKEv1 phase 1 kai phase 2 (βήμα 1)

Το επόμενο βήμα είναι να δημιουργήσουμε ένα map. Αυτό το map δεν είναι τίποτα άλλο πέρα από ένα σύνολο access lists, peers και transform set το οποίο θα ενεργοποιήσουμε στην κατάλληλη interface και θα μας δώσει τη δυνατότητα να ενεργοποιήσουμε το IPsec. Ξεκινάμε λοιπόν με την εντολή *crypto IPsec transform-set MYSET esp-aes esp-sha-hmac*. Στην εν λόγω εντολή το esp-aes έχει σχέση με το κομμάτι του encryption και το esp-sha-hmac με το κομμάτι του authentication.

```
Athens(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
Athens(cfg-crypto-trans)#exit
```

Εικόνα 94. Configuration IKEv1 phase 1 kai phase 2 (βήμα 2)

Στη συνέχεια θα πρέπει να δημιουργήσουμε μια access-list η οποία θα αναφέρει ρητά ποιο δίκτυο θα μπορεί να επικοινωνεί με ποιο. Στη δικιά μας περίπτωση, ορίσαμε ότι μόνο οι IP του δικτύου 172.16.10.0/24 (loopback στο router Athens) να μπορούν να επικοινωνούν με το δίκτυο 192.168.10.0/24 (loopback στο router Thessaloniki). Η εντολή για την access-list θα είναι *access-list 100 permit ip 172.16.10.0 0.0.0.255 192.168.10.0 0.0.0.255*. Ο λόγος που βάζουμε 0.0.0.255 είναι ότι στις access-list χρησιμοποιούμε wildcard mask. Η wildcard mask είναι η διαφορά της subnet mask (255.255.255.0 στην περίπτωσή μας) από το 255.255.255.255. Μετά θα ορίσουμε ένα τύπο if/then στο map έτσι ώστε να ξέρει πότε θα κρυπτογραφεί δεδομένα και πότε όχι. Θα πρέπει να δηλώσουμε ξεκάθαρα ποια access-list θα είναι σε ισχύ καθώς και ποια IP είναι αυτή στην οποία θα καταλήγει το VPN tunnel.

```
Athens(config)#$ 100 permit ip 172.16.10.0 0.0.0.255 192.168.10.0 0.0.0.255
Athens(config)#crypto map MYMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Athens(config-crypto-map)#match address 100
Athens(config-crypto-map)#set peer 210.169.200.1
Athens(config-crypto-map)#set transform-set MYSET
Athens(config-crypto-map)#set pfs ?
  group1  D-H Group1 (768-bit modp)
  group2  D-H Group2 (1024-bit modp)
  group5  D-H Group5 (1536-bit modp)
  <cr>
Athens(config-crypto-map)#set pfs group2
Athens(config-crypto-map)#exit
```

Εικόνα 95. Configuration IKEv1 phase 1 kai phase 2 (βήμα 3)

Τέλος, θα πρέπει να τοποθετήσουμε αυτό το map σε μια interface καθώς αυτό είναι που θα πυροδοτήσει την λειτουργία του IPsec. Αν το πακέτο βρίσκεται μέσα στην ACL που

δημιουργήσαμε, το router θα κρυπτογραφήσει το πακέτο που στέλνουμε. Πολύ σημαντικό είναι στα router που ορίζουμε σαν άκρα του tunnel να υπάρχει σωστά υλοποιημένο routing (το επιβεβαιώσαμε πριν ξεκινήσουμε την υλοποίηση) για να μπορέσει να μεταφερθεί το πακέτο από την αφετηρία, στον επιθυμητό προορισμό.

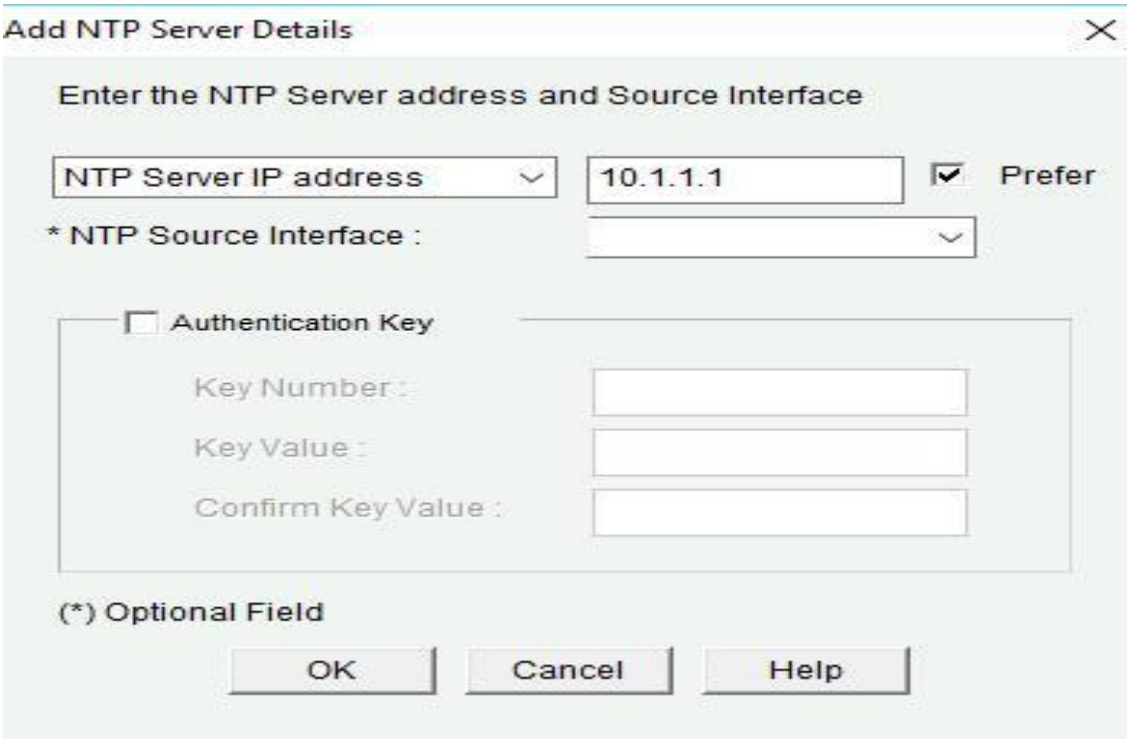
```
Athens(config)#interface gigabitEthernet 1/0
Athens(config-if)#crypto map
Athens(config-if)#crypto map MYMAP
Athens(config-if)#EX
Aug 10 20:37:27.216: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Athens(config-if)#exit
```

Εικόνα 96. Configuration IKEv1 phase 1 kai phase 2 (βήμα 4)

Ίδια διαδικασία γίνεται και στο router Thessaloniki, αλλα προσέχουμε να ορίσουμε σωστά την access-list από την αντίθετη μεριά καθώς και τον peer που θα καταλήγει το tunnel. Αυτό ήταν και το απαραίτητο configuration για την υλοποίηση του IPsec VPN. Στο κεφάλαιο 5.1.1.3 θα δούμε αν το configuration ήταν σωστό και πως διορθώνουμε τα τυχόν λάθη.

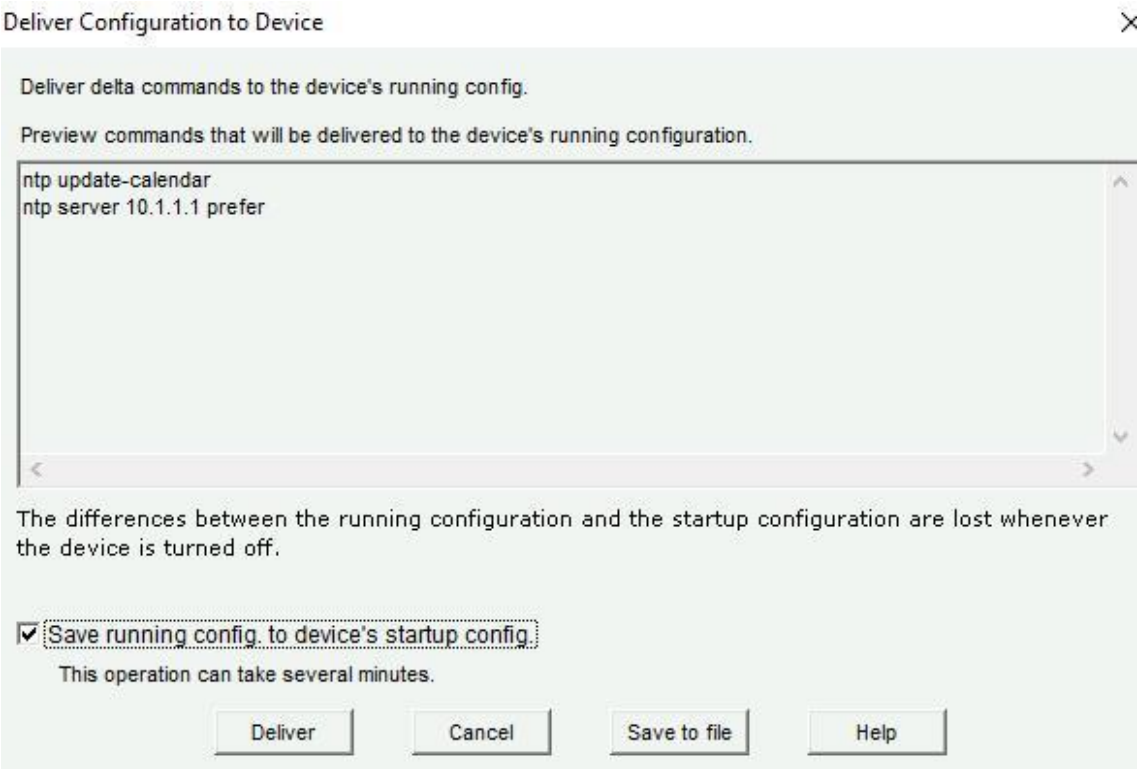
5.1.1.2. Υλοποίηση με GUI (Graphical User Interface)

Πάμε τώρα να δούμε πώς μπορούμε να κάνουμε την ίδια διαδικασία, αλλά με wizards. Αρχικά, ξεκινάμε με το να ρυθμίσουμε την επικοινωνία με τον ntp server. Πηγαίνουμε time → NTP and SMTP και πατάμε add. Εισάγουμε την IP (στην τοπολογία μας είναι η 10.1.1.1) ή το όνομα του NTP server και επιλέγουμε το *prefer*, αν θέλουμε να συγχρονίζεται από τον συγκεκριμένο server.



Εικόνα 97. Ρύθμιση NTP server

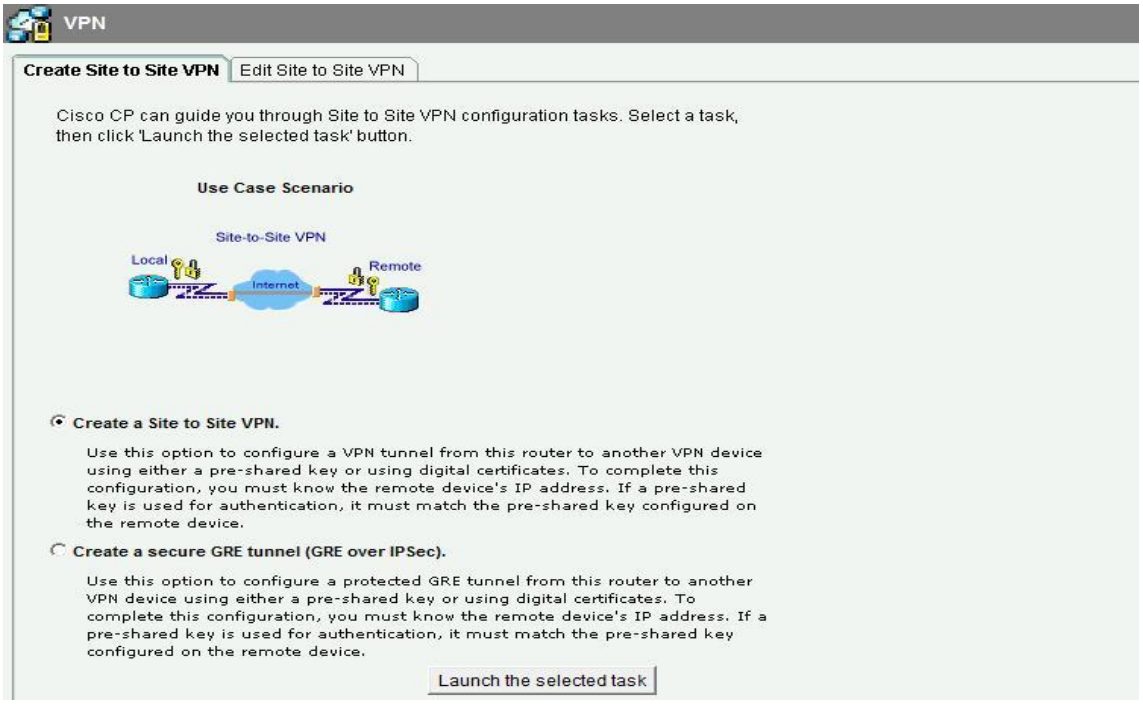
Αμέσως μετά πατάμε OK και εμφανίζεται ένα μήνυμα με τις εντολές που θα εισαχθούν στο router. Επιλέγουμε και να γίνει εγγραφή στην start-up configuration του router και πατάμε *deliver*.



Εικόνα 98. Μεταφορά εντολών στο router

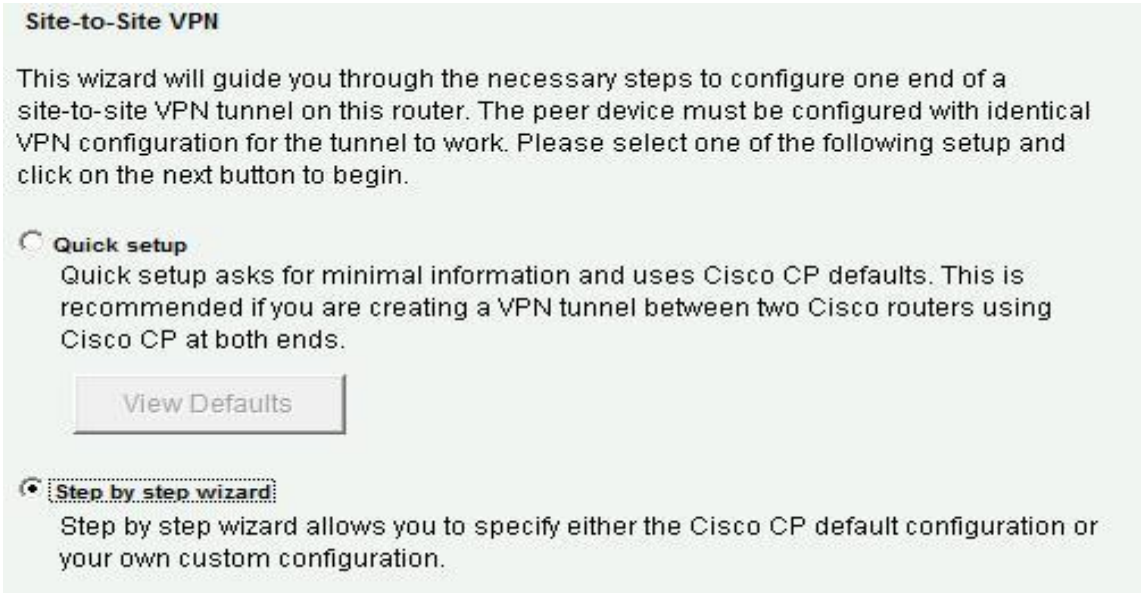
Έχουμε τη δυνατότητα να ορίσουμε με αυτοματοποιημένο τρόπο τις IPs στις interfaces για κάθε ένα από τα router. Κάτι τέτοιο όμως δεν είναι απαραίτητο, καθώς ένας πεπειραμένος network administrator μπορεί εύκολα και σαφώς πιο γρήγορα να ολοκληρώσει αυτές τις διαδικασίες από το CLI.

Από εκεί και πέρα θα χρησιμοποιήσουμε την εφαρμογή για το configuration του IPsec VPN. Φυσικά τα wizards μπορούμε να τα χρησιμοποιήσουμε μονο αφού πριν έχουμε χρησιμοποιήσει το Command Line Interface για να παράγουμε ζεύγη κλειδιών και καταφέρουμε να πάρουμε υπογεγραμμένο το πιστοποιητικό από την CA Authority. Με λίγα λόγια το CCP μας δίνει τη δυνατότητα να ρυθμίσουμε με εύκολο τρόπο, μειώνοντας την πιθανότητα λάθους, το IKEv1 phase 1 και phase 2 (IPsec tunnel). Αφού έχουμε ρυθμίσει τα router με τον τρόπο που δείξαμε στο manual για να τα αναγνωρίσει το CCP , ανοίγουμε το πρόγραμμα και πάμε Configure → security → VPN → site-to-site VPN.



Εικόνα 99. Αρχική σελίδα wizard για υλοποίηση IPsec VPN

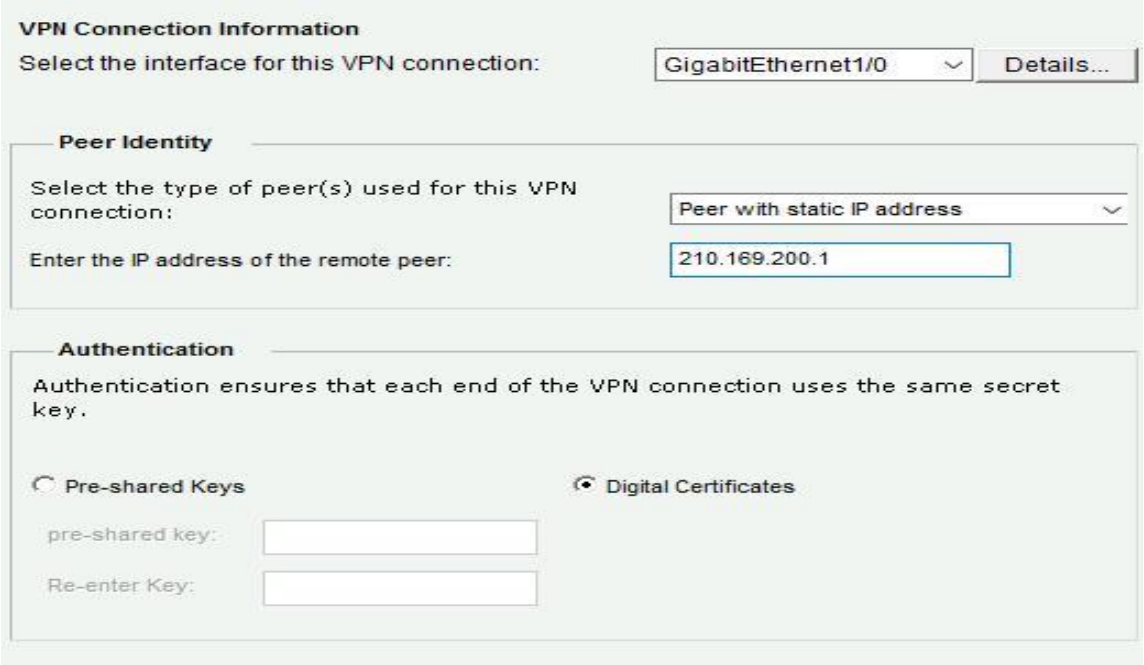
Αφού πατήσουμε το *Launch the selected task* μεταφερόμαστε στην επόμενη σελίδα. Εδώ μας δίνεται η δυνατότητα να υλοποιήσουμε το site-to-site VPN tunnel είτε με default setting, είτε με δικά μας, customized settings. Όπως και στη χειροκίνητη ρύθμιση, θα επιλέξουμε τα δικά μας settings. Οπότε επιλέγουμε *step by step wizard* και θα πατήσουμε *Next*.



Εικόνα 100. Επιλογή customized settings

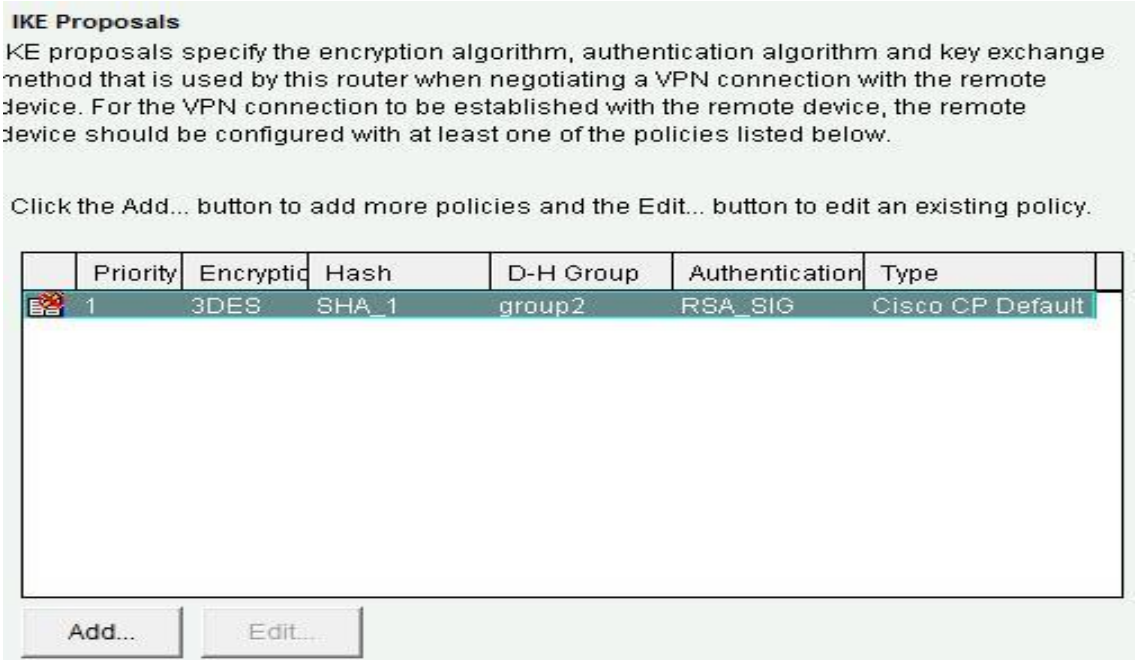
Ακολουθώντας και εδώ την ίδια λογική που είχαμε και στη χειροκίνητη δημιουργία, μας ζητείται να επιλέξουμε το interface από το οποίο θα ξεκινά το tunnel, καθώς και τον απομακρυσμένο peer. Φυσικά θα επιλέξουμε *peer with static IP* μιας και δεν χρησιμοποιούμε

DHCP Server. Όπως τονίσαμε και κατά το CLI configuration, σε αυτό το σημείο χρησιμοποιούμε Digital Certificates και όχι Pre-shared keys.



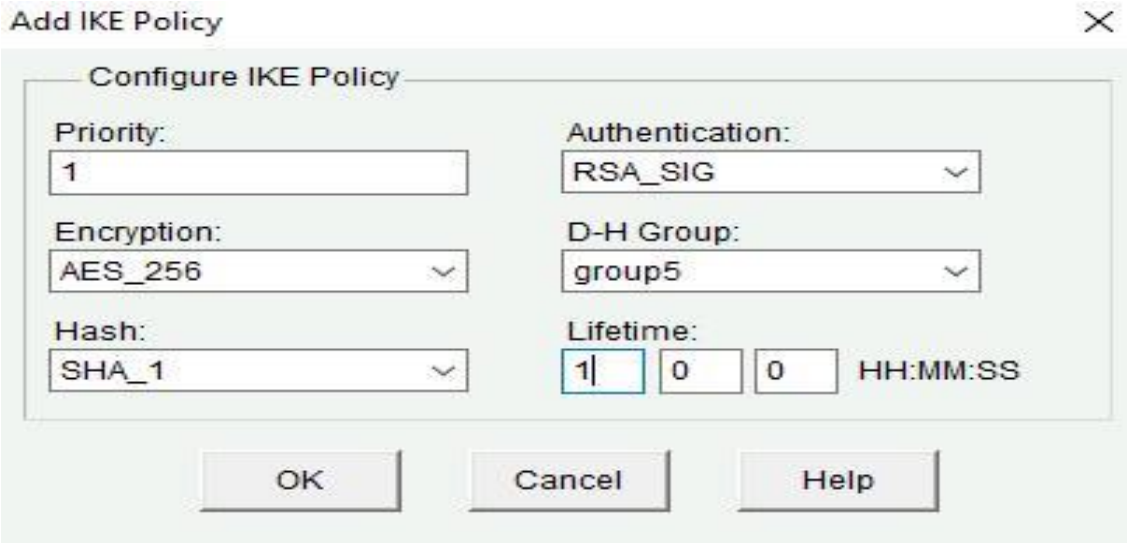
Εικόνα 101. Επιλογή interface που ξεκινάει το VPN, IP που καταλήγει και τρόπου αυθεντικοποίησης (digital certifications)

Στην επόμενη εικόνα θα πρέπει να επιλέξουμε priority policy, encryption algorithm, authentication algorithm, hashing algorithm και Diffie Hellman group.



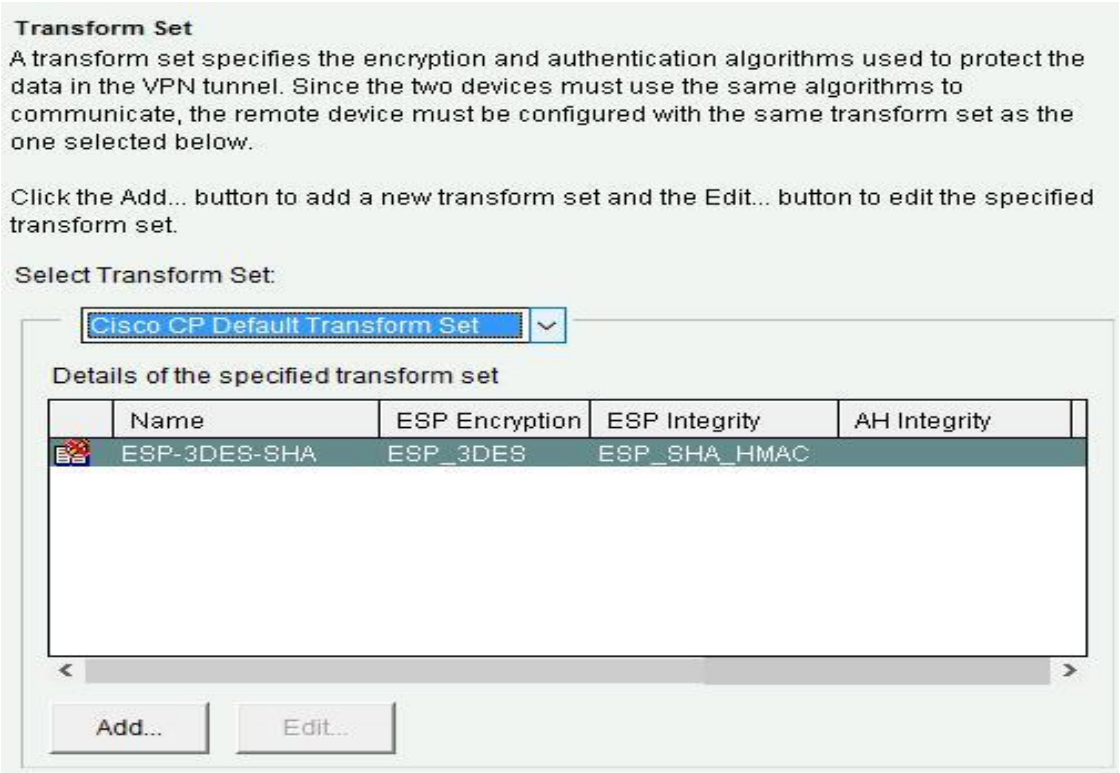
Εικόνα 102. Εικόνα default isakmp policy

Ήδη υπάρχει ένας default συνδυασμός αλλά εμείς θα πατήσουμε Add για να εισάγουμε τα δικά μας. Επειδή τα default settings δε μπορούμε να τα διαγράψουμε, στο policy που θα δημιουργήσουμε εμείς, θα θέσουμε priority 1 και χειροκίνητα θα αλλάξουμε τα default, σε priority 2.



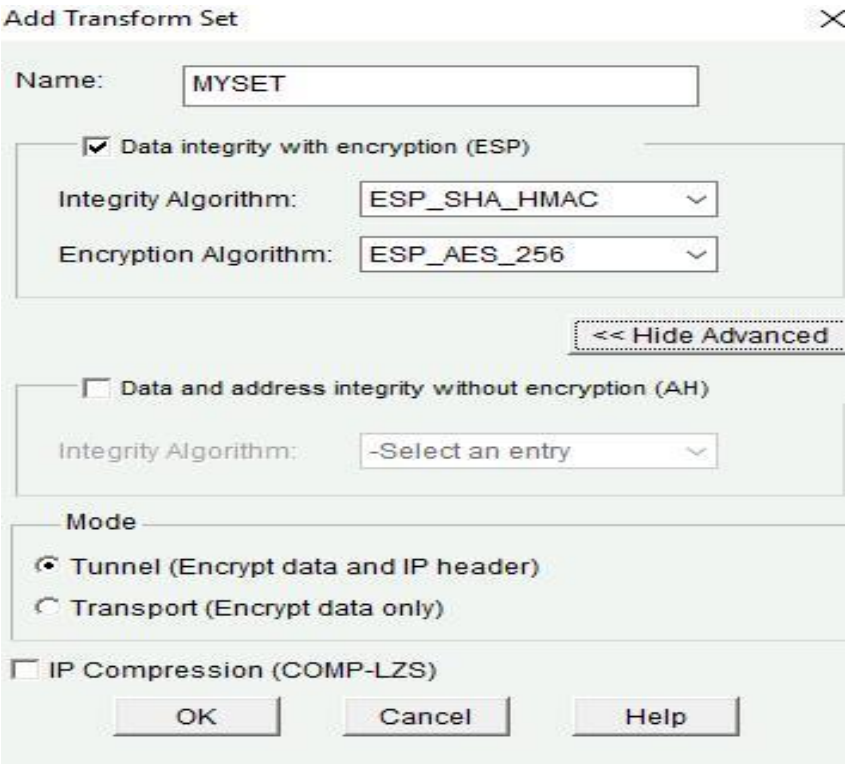
Εικόνα 103. Δημιουργία προσωπικής isakmp policy

Πατώντας Next, δίνεται η δυνατότητα να ρυθμίσουμε το Transform set.



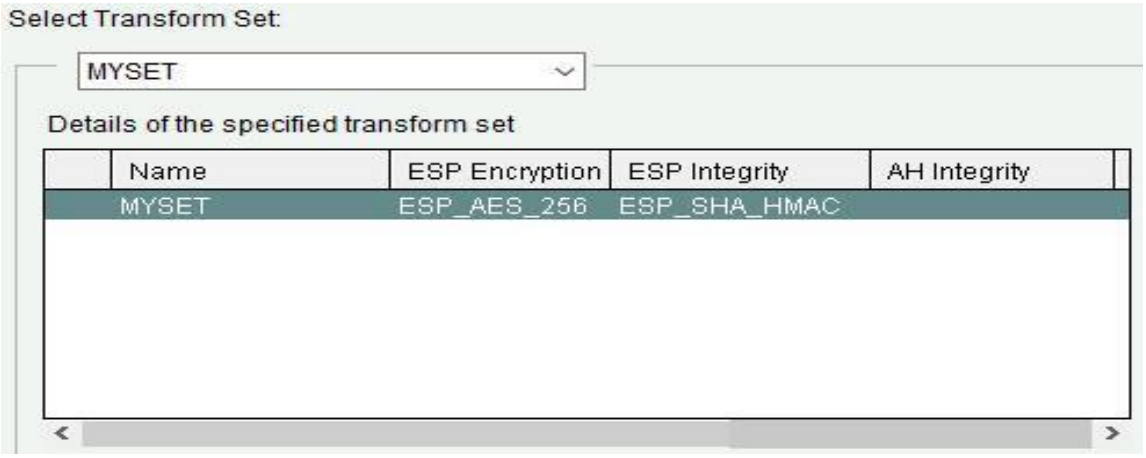
Εικόνα 104. Εικόνα default transform-set

Πάλι υπάρχει κάτι default, αλλά και πάλι θα πατήσουμε Add για να προσθέσουμε τα δικά μας settings.



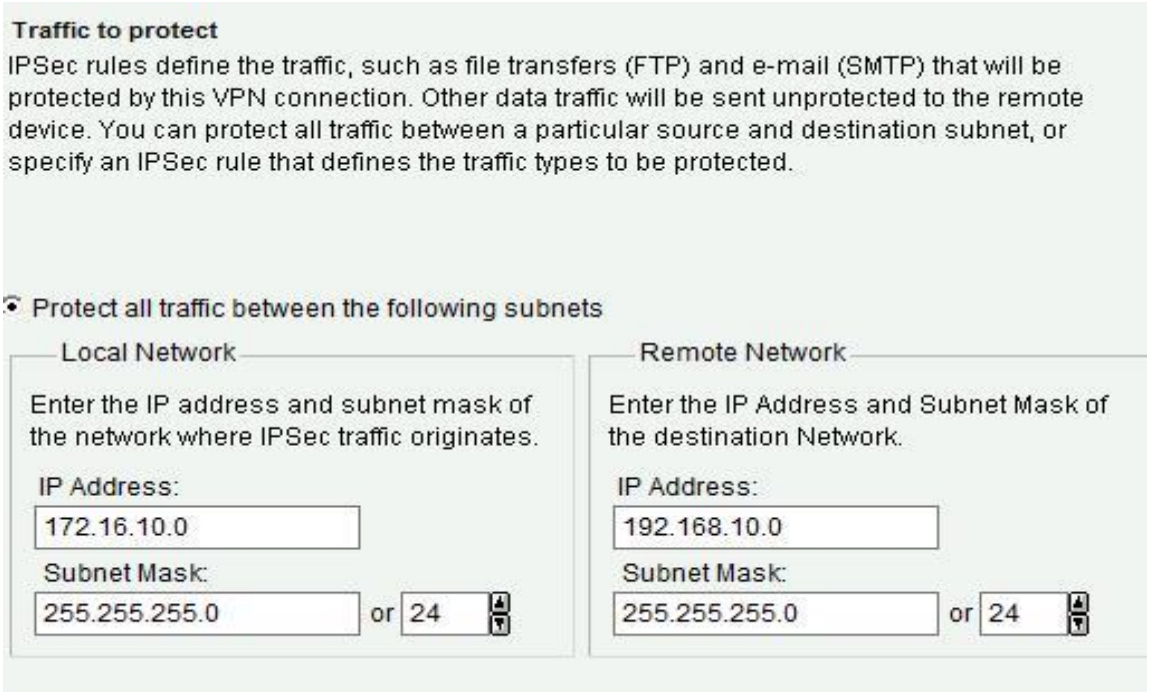
Εικόνα 105. Ρύθμιση προσωπικού transform-set

Αφού ολοκληρώσουμε, πατάμε OK και βλέπουμε ότι σαν default έχουν περάσει οι δικές μας επιλογές.



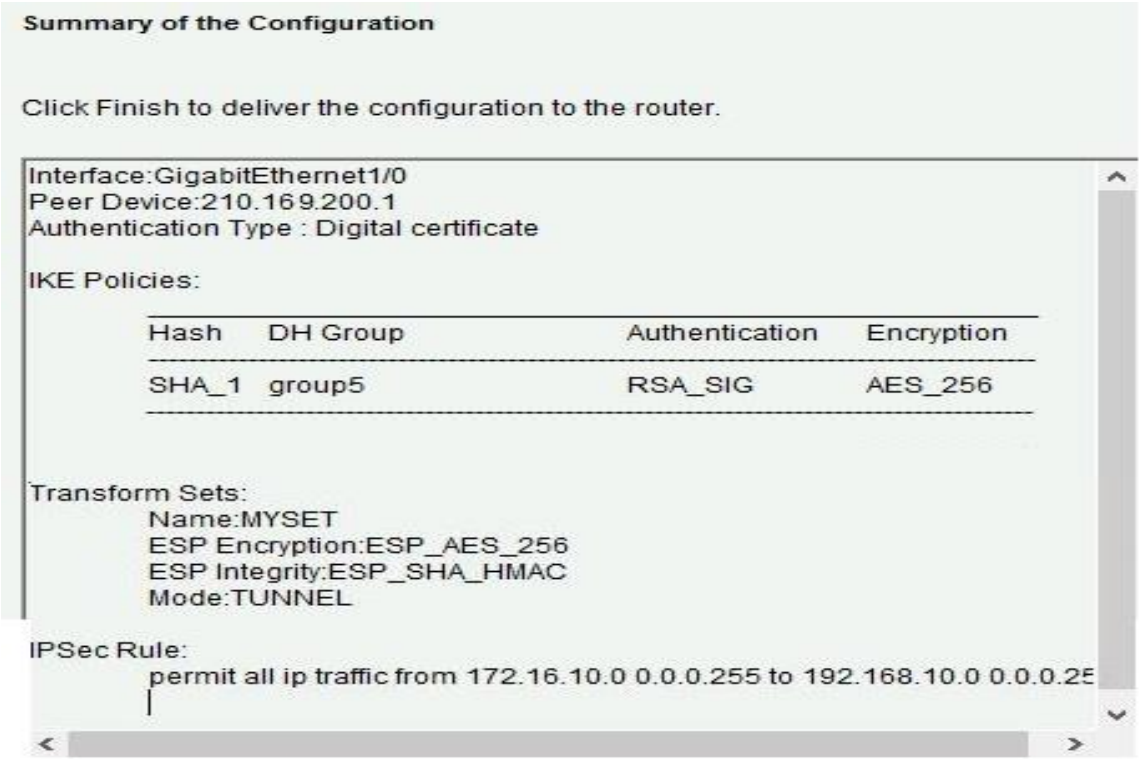
Εικόνα 106. Επιβεβαίωση ορθότητας transform-set

Συνεχίζοντας, έρχεται η στιγμή να ορίσουμε την access-list μας και να ενημερώσουμε το σύστημα ποια subnets επιτρέπεται να επικοινωνούν και ταυτόχρονα να προστατεύονται βάσει των κανόνων που ορίσαμε. Όπως φαίνεται και από την αρχική τοπολογία για το router Athens, το subnet μας είναι 172.16.10.0/24 με προορισμό το 192.168.10.0/24.



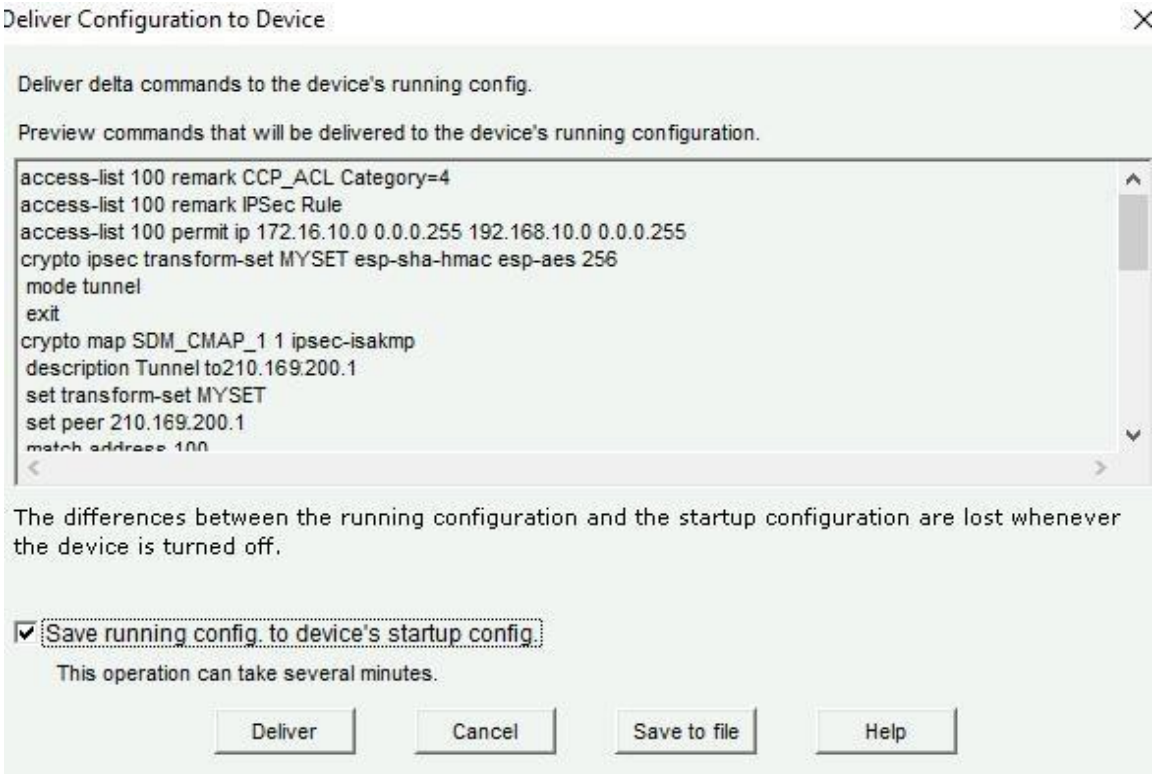
Εικόνα 107. Δημιουργία access-list

Εδώ θα πρέπει να αναφέρουμε κάτι πολύ σημαντικό. Το CCP, προσωρινά, δεν υποστηρίζει wizard για την υλοποίηση του pfs. Άρα αυτό το κομμάτι πρέπει να το κάνουμε χειροκίνητα στα router Athens και Thessaloniki. Αφού ολοκληρωθεί και αυτό, έχουμε φτάσει, αισίως, στο τέλος της διαδικασίας. Πατώντας *Next*, βλέπουμε μια σύνοψη του configuration που κάναμε.



Εικόνα 108. Περίληψη ρυθμίσεων

Πατάμε *Finish,* επιλέγουμε να γίνει save στο start-up configuration και πατάμε *deliver*.



Εικόνα 109. Μεταφορά εντολών στο router

Γίνεται η ίδια διαδικασία και στο άλλο router και το IPsec tunnel, έχει ολοκληρωθεί επιτυχώς. Υπάρχει και μια αυτόματη ρύθμιση για να γίνουν mirror οι ρυθμίσεις στο άλλο router, αλλα συνήθως δεν ολοκληρώνεται σωστά η διαδικασία, οπότε προτιμούμε να χρησιμοποιήσουμε τον ίδιο wizard και στο router Thessaloniki.

Εικόνα 110. Επιβεβαίωση ορθής μεταφοράς ρυθμίσεων

5.1.1.3. Debugging και εντολές ελέγχου ορθής διαμόρφωσης

Ξεκινώντας θα κάνουμε ένα ping για να δούμε αν ολοκληρώσαμε σωστά τη διαδικασία. Αφού θέλουμε να δούμε αν επικοινωνεί η loopback 1 από το router Athens με την loopback 1 στο router Thessaloniki, δε θα κάνουμε απλό ping. Αν εισάγαμε απλά την εντολή *ping 192.168.10.1* στο router Athens, ναι μεν θα ολοκληρωνόταν η διαδικασία, αλλα επειδή εξ 'αρχής επιλέγεται η εξωτερική interface δε θα είχαμε κρυπτογραφημένη κίνηση. Πρέπει λοιπόν να συγκεκριμενοποιήσουμε την πηγή του ping. Θα εισάγουμε λοιπόν την εντολή *ping 192.168.10.1 source loopback 1*.

```
Athens#ping 192.168.10.1 source loopback 1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
.....
Success rate is 0 percent (0/5)
```

Εικόνα 111. Αποτυχημένη προσπάθεια ping που σημαίνει λανθασμένη ρύθμιση IPsec

Βλέπουμε λοιπόν ότι το ping από την IP 172.16.10.1 στην IP 192.168.10.1 δεν ολοκληρώνεται. Θα πρέπει λοιπόν να δούμε για ποιον λόγο γίνεται αυτό. Οι παρακάτω εντολές θα μας δείξουν τι πρέπει να κοιτάξουμε και πώς θα το διορθώσουμε. Αρχικά θα πρέπει να ελέγξουμε τα IKEv1 phase 1 policies. Αν υπάρχει κάποιο σφάλμα σε αυτό το κομμάτι, τότε εκ των πραγμάτων δεν υπάρχει phase 2. Η πρώτη εντολή που θα μας βοηθήσει να ελέγξουμε το τι συμβαίνει είναι η *show crypto isakmp policy*. Εισάγουμε αυτή την εντολή και στα δυο routers και έχουμε την εξής εικόνα για το καθένα.

```
Athens#sh crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Εικόνα 112. Εικόνα isakmp policy (προσωπικής και default) στο router Athens

```
Thessaloniki#sh crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Εικόνα 113. Εικόνα isakmp policy (προσωπικής και default) στο router Thessaloniki

Με την πρώτη λοιπόν ματιά παρατηρούμε το πρώτο σφάλμα. Ενώ στο router Athens ο αλγόριθμος κρυπτογράφησης είναι το AES, στο router Thessaloniki έχει επιλεγεί το 3DES. Για να μπορεί να ολοκληρωθεί σωστά η phase 1 πρέπει οι δυο policies να είναι ίδιες. Μοναδική εξαίρεση είναι το lifetime. Το lifetime που ρυθμίζεται στον router του προορισμού, μπορεί να είναι ίσο ή μεγαλύτερο από το lifetime του initiator router. Πρέπει λοιπόν να αλλάξουμε τον αλγόριθμο. Η διαδικασία που ακολουθείται φαίνεται στην πιο κάτω εικόνα.

```
Thessaloniki(config)#crypto isakmp policy 1
Thessaloniki(config-isakmp)#no encryption 3des
Thessaloniki(config-isakmp)#encryption aes 256
```

Εικόνα 114. Αλλαγή encryption στο router Thessaloniki για να ταιριάζει με αυτή του router Athens

Σε αυτό το σημείο θα μπορούσαμε να ξαναδοκιμάσουμε το ping και να δούμε αν είναι όλα σωστά, αλλά θα προτιμήσουμε να συνεχίσουμε τους ελέγχους. Η επόμενη εντολή είναι η *show crypto map* η οποία μας εμφανίζει όλα τα υπόλοιπα στοιχεία που χρειαζόμαστε.

```
Athens#show crypto map
Crypto Map "MYMAP" 1 ipsec-isakmp
        Peer = 210.169.200.1
        Extended IP access list 100
            access-list 100 permit ip 172.16.10.0 0.0.0.255 192.168.10.0 0.0.0.255
        Current peer: 210.169.200.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): Y
        DH group:  group2
        Transform sets={
                MYSET, esp-aes esp-sha-hmac
        }
        Interfaces using crypto map MYMAP:
                GigabitEthernet1/0
```

Εικόνα 115. Εικόνα crypto map στο router Athens

```
Thessaloniki#sh crypto map
Crypto Map "MYMAP" 1 ipsec-isakmp
        Peer = 172.16.10.1
        Extended IP access list 100
            access-list 100 permit ip 192.168.10.0 0.0.0.255 182.16.10.0 0.0.0.255
        Current peer: 172.16.10.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                MYSET, esp-aes esp-sha-hmac
        }
        Interfaces using crypto map MYMAP:
                GigabitEthernet1/0
```

Εικόνα 116. Εικόνα crypto map στο router Thessaloniki

Αν κοιτάξουμε προσεκτικά αυτά τα δυο screenshots, θα παρατηρήσουμε τρία λάθη, όλα στο router Thessaloniki. Το πρώτο λάθος είναι ότι ενώ το δίκτυο προορισμός μας είναι το 172.16.10.0/24 στην access-list έχουμε ορίσει ότι επιτρέπουμε στους host του δικτύου 192.168.10.0/24 να μπορούν να επικοινωνήσουν μόνο με αυτούς του 182.16.10.0/24. Το δεύτερο λάθος είναι ότι για το router Thessaloniki ο σωστός peer που καταλήγει το IPsec tunnel θα έπρεπε να είναι η interface GI1/0 του router Athens με IP 210.168.200.1 και όχι η 172.16.10.1 που έχουμε ορίσει. Τέλος, το τρίτο σφάλμα είναι ότι ενώ στο router Athens έχουμε ορίσει το pfs, στο router Thessaloniki δεν το έχουμε κάνει. Πάμε λοιπόν να τα διορθώσουμε. Αρχικά, διορθώνουμε την access-list. Δεν αρκεί όμως να εισάγουμε απλά την καινούρια αλλά πρέπει να αφαιρέσουμε και την παλιά.

```
Thessaloniki(config)#no access-list 100 permit ip 192.168.10.0 0.0.0.255 182.16.10.0 0.0.0.255
Thessaloniki(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255 172.16.10.0 0.0.0.255
```

Εικόνα 117. Διόρθωση ACL στο router Thessaloniki

Τα υπόλοιπα δυο λάθη διορθώνονται μαζί καθώς μπορούμε να τα αλλάξουμε όταν εισάγουμε την εντολή *crypto map MYMAP 1 IPsec-isakmp.*

```
Thessaloniki#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Thessaloniki(config)#crypto map MYMAP 1 ipsec-isakmp
Thessaloniki(config-crypto-map)#set pfs group2
Thessaloniki(config-crypto-map)#set peer 210.168.200.1
Thessaloniki(config-crypto-map)#set transform-set MYSET
Thessaloniki(config-crypto-map)#end
```

Εικόνα 118. Διόρθωση IP που καταλήγει το VPN και ενεργοποίηση pfs group

Μετά και από αυτές τις διορθώσεις, δε θα πρέπει να υπάρχει κάποιο σφάλμα και το ping θα πρέπει να ολοκληρώνεται σωστά. Πάμε όμως πρώτα να δούμε τα αποτελέσματα από κάποιες ακόμη εντολές για να είμαστε σίγουροι. Η επόμενη εντολή θα είναι η *show crypto isakmp sa*. Αυτή η εντολή θα μας δείξει αν λειτουργεί σωστά η phase 1. Στο output θέλουμε να δούμε τις σωστές source και destination IP και στο state να φαίνεται QM_IDLE και όχι

MM_NO_STATE. Όπως βλέπουμε, μετά τις διορθώσεις που κάναμε, έχουμε την επιθυμητή εικόνα.

```
Athens#sh crypto isakmp sa
dst             src             state          conn-id slot status
210.169.200.1   210.168.200.1   QM_IDLE              1    0 ACTIVE
```

Εικόνα 119. Output εντολής show crypto isakmp sa

Και αν θέλουμε να δούμε περισσότερες λεπτομέρειες, εισάγουμε την εντολή *show crypto isakmp sa detail.*

```
Athens#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
1     210.168.200.1   210.169.200.1            ACTIVE aes  sha  rsig 5  00:56:21
       Connection-id:Engine-id =  1:1(software)
```

Εικόνα 120. Output εντολής show crypto isakmp sa detail

Για να επιβεβαιώσουμε ότι οι αλγόριθμοι κρυπτογράφησης είναι αυτοί που θέλουμε και δεν έχουμε κάνει κάποιο λάθος εισάγουμε την εντολή *show crypto engine connections active.*

```
Athens#sh crypto engine connections active

  ID Interface           IP-Address      State  Algorithm          Encrypt  Decrypt
   1 GigabitEthernet1/0   210.168.200.1   set    HMAC_SHA+AES_256_C       0        0
2001 GigabitEthernet1/0   210.168.200.1   set    AES+SHA                  0       19
2002 GigabitEthernet1/0   210.168.200.1   set    AES+SHA                 19        0
```

Εικόνα 121. Output εντολής show crypto engine connections active

Φτάνουμε λοιπόν στο σημείο να κάνουμε τελικά το ping. Από τους παραπάνω ελέγχους είμαστε πλέον σίγουροι ότι η εντολή θα ολοκληρωθεί σωστά. Και όντως, όπως βλέπουμε παρακάτω έχουμε επιτυχία με ποσοστό 100%.

```
Athens#ping 192.168.10.1 source loopback 1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/60/92 ms
```

Εικόνα 122. Επιτυχημένο ping μετά τις απαραίτητες διορθώσεις και επιβεβαίωση ότι το IPsec VPN λειτουργεί σωστά.

Τέλος, αν θέλουμε να δούμε και τι βλέπουμε όταν η μεταφορά πακέτων είναι επιτυχής, άρα το IPsec tunnel λειτουργεί σωστά, εισάγουμε την εντολή *show crypto IPsec sa*. Επειδή το

output είναι αρκετά μεγάλο, θα χρωματίσουμε τα σημεία ενδιαφέροντος και θα αναφέρουμε γιατί είναι σημαντικά.

```
Athens#sh crypto ipsec sa

interface: GigabitEthernet1/0
    Crypto map tag: MYMAP, local addr 210.168.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 210.169.200.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 210.168.200.1, remote crypto endpt.: 210.169.200.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1/0
     current outbound spi: 0x78267DE6(2015788518)

     inbound esp sas:
      spi: 0xC064921B(3227816475)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4417564/3326)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x78267DE6(2015788518)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        sa timing: remaining key lifetime (k/sec): (4417564/3316)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
Athens#
```

Εικόνα 123. Output εντολής show crypto IPsec sa

Στα δυο πρώτα κομμάτια που έχουμε κυκλώσει φαίνονται οι σωστές IPs και οι subnet masks και φαίνεται επίσης επιτυχές encapsulation/encryption και decapsulation/decryption. Στα δυο τελευταία κομμάτια που έχουμε κυκλώσει φαίνονται αντίστοιχα τα inbound security association (κίνηση που έρχεται από τον άλλο μέρος του tunnel) και outbound security association (κίνηση που φεύγει με προορισμό το άλλο μέρος του tunnel).

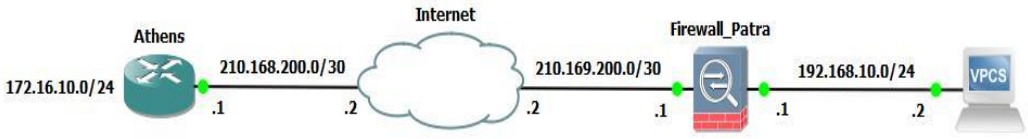
5.1.2. Υλοποίηση IPsec VPN με firewall ASA

Σε αυτό το κεφάλαιο θα προσπαθήσουμε να κάνουμε implementation του IPsec VPN με μια μικρή διαφοροποίηση. Θέλουμε να επικοινωνήσουν τα απομακρυσμένα γραφεία της ίδια εταιρίας, αυτά της Αθήνας με αυτά της Πάτρας, αλλά πριν από τα γραφεία της Πάτρας υπάρχει ένα firewall. Οπότε το VPN μας θα ξεκινάει από το router της Αθήνας και θα τερματίζει στο firewall της Πάτρας. Η ύπαρξη του firewall μας αναγκάζει να κάνουμε και μερικές ακόμη αλλαγές στην τοπολογία μας.

Αρχικά επειδή το firewall που χρησιμοποιούμε είναι version 8.4(2), δεν υποστηρίζει το πρωτόκολλο BGP. Οπότε για την επικοινωνία του router Internet με το firewall και τα εσωτερικά του δίκτυα έχουμε χρησιμοποιήσει static routing. Η επικοινωνία ανάμεσα στα υπόλοιπα routers, όπως και στο προηγούμενο παράδειγμα, γίνεται με BGP.

Η δεύτερη διαφορά παρατηρείται στα εσωτερικά δίκτυα της Πάτρας και της Αθήνας. Ενώ στην Αθήνα έχουμε προσθέσει μια loopback address για να αναπαραστήσουμε το εσωτερικό εταιρικό δίκτυο, από τη μεριά της Πάτρας, αν και εννοείται κάτι αντίστοιχο, δε μπορούμε να κάνουμε το ίδιο. Το firewall εκ των πραγμάτων δεν υποστηρίζει την ύπαρξη loopback addresses, κάτι που θα παραβίαζε τα επίπεδα ασφάλειας που προορίζεται να προσφέρει. Οπότε απλά στην τοπολογία θα συνδέσουμε έναν host, ο οποίος θα αναπαριστά το εσωτερικό δίκτυο. Έτσι και αλλιώς, αυτό που μας ενδιαφέρει είναι να αποδείξουμε ότι μπορούμε να δημιουργήσουμε interesting traffic ανάμεσα στην loopback address του router Athens και στην εσωτερική interface του firewall Patra. Επειδή όμως το firewall έχει εξ ‘αρχής απενεργοποιημένο το ping και επειδή το λογισμικό μας δεν έχει δηλωθεί στην Cisco (προϋποθέτει αγορά hardware), έχει απενεργοποιημένες κάποιες λειτουργίες. Οπότε, θα δημιουργήσουμε ένα tunnel από την loopback address του router Athens που θα καταλήγει στην εξωτερική interface στου firewall. Η λειτουργία είναι ακριβώς η ίδια.

Τέλος, θα πρέπει να αναφέρουμε ότι αφού στο προηγούμενο παράδειγμα δείξαμε το IPsec VPN με digital certificates, αυτή τη φορά θα το υλοποιήσουμε χρησιμοποιώντας pre-shared keys. Τα pre-shared keys είναι τα ίδια σε κάθε άκρο του IPsec. Αυτά τα δυο άκρα (IKE peers), αυθεντικοποιούν το ένα το άλλο στέλνοντας ένα hash πληροφορίας που περιέχει τα pre-shared keys. Αν το peer που θα λάβει αυτό το hash μπορεί από μόνο του να δημιουργήσει αυτό το hash χρησιμοποιώντας το pre-shared κλειδί του, τότε είμαστε σίγουροι ότι και τα δυο άκρα μπορούν να εμπιστευτούν το ένα το άλλο. Αν και τα pre-shared keys είναι εύκολο να γίνουν configure, δεν χρησιμοποιούνται τόσο πολύ γιατί αν ένα peer έχει συνδέσεις με πολλούς έτερους peers από άλλα VPN, θα πρέπει να γίνει ξεχωριστό configuration για κάθε pre-shared key που μοιράζεται. Η τοπολογία έχει την παρακάτω μορφή.



Εικόνα 124. Τοπολογία για υλοποίηση IPsec VPN με τη χρήση firewall ASA

5.1.2.1. Υλοποίηση με CLI (Command Line Interface)

Θα ξεκινήσουμε τη διαδικασία υλοποίησης του IPsec VPN ξεκινώντας από το router Athens. Οι εντολές μοιάζουν λίγο με αυτές που δώσαμε στο προηγούμενο παράδειγμα, αλλά δεν είναι ακριβώς ίδιες.
Ξεκινάμε ορίζοντας την IKEv1 phase 1 policy.

```
Athens#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Athens(config)#crypto isakmp policy 1
Athens(config-isakmp)#authentication pre-share
Athens(config-isakmp)#encryption aes 256
Athens(config-isakmp)#hash sha
Athens(config-isakmp)#group 2
Athens(config-isakmp)#lifetime 3600
Athens(config-isakmp)#exit
```

Εικόνα 125. Ορισμός IKEv1 phsase 1 policy

Στη συνέχεια θα δώσουμε μια εντολή για την δημιουργία ενός pre-shared key (PSK) που θα χρησιμοποιηθεί ως κλειδί για την αυθεντικοποίηση της IKEv1 phase 1 από τον peer 210.169.200.1. Το νούμερο 6 που φαίνεται στην εντολή χρησιμοποιείται για να εμφανίζεται κρυπτογραφημένο το κλειδί στο configuration. Αν είχαμε επιλέξει το 0, το κλειδί θα φαινόταν unencrypted.

```
Athens(config)#crypto isakmp key 6 testkey address 210.169.200.1
```

Εικόνα 126. Δημιουργία pre-shared keys και ορισμός του peer που καταλήγει το VPN (router Athens)

Στο επόμενο βήμα, όπως και στο προηγούμενο παράδειγμα, δημιουργούμε την access-list για να ορίσουμε ποιο δίκτυο θα επικοινωνεί με ποιο. Στη συγκεκριμένη περίπτωση αφού το hardware δε μας δίνει τη δυνατότητα να ενεργοποιήσουμε το ping για την εσωτερική interface, στην access-list μας θα δηλώσουμε μόνο έναν host (την εξωτερική IP του firewall).

```
Athens(config)#access-list 100 permit ip 172.16.10.0 0.0.0.255 host 210.169.200.1
```

Εικόνα 127. Δημιουργία ACL (router Athens)

Στο επόμενο κομμάτι δημιουργούμε το transform-set και επιλέγουμε mode. Εδώ είναι σημαντικό να δικαιολογήσουμε γιατί επιλέγουμε το tunnel mode αντί του transport mode. Καταρχάς το tunnel mode χρησιμοποιείται όταν θέλουμε να επικοινωνήσουν είτε εσωτερικά δίκτυα, είτε ένα εσωτερικό δίκτυο με ένα gateway. Στο tunnel mode, το router θα πάρει τα πακέτα που ταιριάζουν στην access list που δημιουργήσαμε, θα τα κρυπτογραφήσει και μετά θα τα κάνει encapsulate σε ένα καινούριο IPsec πακέτο και θα το στείλει στο firewall. Η άλλη μας επιλογή, το transport mode χρησιμοποιείται κυρίως σε περιπτώσεις που επικοινωνούν δυο endpoints μεταξύ τους (για παράδειγμα ένας υπολογιστής με έναν server χωρίς κάτι ενδιάμεσο

μεταξύ τους). Στο transport mode κρυπτογραφείται μόνο το payload και το ESP trailer, άρα το IP header του αρχικού πακέτου, παραμένει μη κρυπτογραφημένο[26].

```
Athens(config)#crypto ipsec transform-set MYSET esp-sha-hmac esp-aes 256
Athens(cfg-crypto-trans)#mode tunnel
Athens(cfg-crypto-trans)#exit
```

Εικόνα 128. Δημιουργία transform-set (router Athens)

Προχωράμε στη δημιουργία του crypto map τον οποίο θα ορίσουμε στην εξωτερική interface του router Athens και θα περιμένει κίνηση που ταιριάζει στην access list που δημιουργήσαμε. Επίσης ορίζουμε ποια θα είναι η IP στην οποία θα τερματίζει το VPN, άρα η εξωτερική interface του firewall.

```
Athens(config)#crypto map MYMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Athens(config-crypto-map)#match address 100
Athens(config-crypto-map)#set transform-set MYSET
Athens(config-crypto-map)#set peer 210.169.200.1
Athens(config-crypto-map)#exit
```

Εικόνα 129. Δημιουργία crypto map (router Athens)

Τέλος, το μόνο που μας μένει είναι να ορίσουμε την interface στην οποία θα ενεργοποιηθεί το crypto map. Εμφανίζεται και σχετικό μήνυμα για επιτυχή ενεργοποίηση.

```
Athens(config-if)#crypto map MYMAP
Athens(config-if)#
*Sep  6 08:56:24.759: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Athens(config-if)#exit
```

Εικόνα 130. Ορισμός interface που θα ενεργοποιήσουμε τον crypto map (router Athens)

Πάμε τώρα να ρυθμίσουμε και το firewall. Οι εντολές που εισάγουμε εδώ έχουν λίγο διαφορετική μορφή από αυτές που εισάγαμε στο router. Αρχικά δημιουργούμε policy για την IKEv1 phase 1. Προσέχουμε φυσικά να είναι ίδιες με αυτές που θέσαμε και στο router Athens.

```
FirewallPatra(config)# crypto ikev1 policy 1
FirewallPatra(config-ikev1-policy)# authentication pre-share
FirewallPatra(config-ikev1-policy)# encryption aes-256
FirewallPatra(config-ikev1-policy)# hash sha
FirewallPatra(config-ikev1-policy)# group 2
FirewallPatra(config-ikev1-policy)# lifetime 3600
```

Εικόνα 131. Ρύθμιση IKEv1 phase 1 (firewall)

Στη συνέχεια ενεργοποιούμε το ISAKMP στην εξωτερική interface του firewall.

```
FirewallPatra(config)# crypto ikev1 enable outside
```

Εικόνα 132. Ενεργοποίηση isakmp στην εξωτερική interface (firewall)

[26] Demystifying the IPsec Puzzle

Αμέσως μετά, όπως και στο router, φτιάχνουμε μια access-list και ορίζουμε και το transform-set. Προσέχουμε να ορίσουμε σωστά τα δίκτυα που θέλουμε να επικοινωνούν και φροντίζουμε οι επιλογές του transform-set του firewall να ταιριάζουμε με αυτές του router. Άρα οι εντολές θα είναι :

- *Access-list MYLIST extended permit ip host 210.169.200.1 172.16.10.0 255.255.255.0*
- *Crypto IPsec ikev1 transform-set MYSET esp-sha-hmac esp-aes 256*

Τα τρία τελευταία βήματα είναι να δημιουργήσουμε το tunnel group ορίζοντας το pre-share key, τον τύπο και τον απομακρυσμένο peer, να δημιουργήσουμε τον crypto map και φυσικά να την ορίσουμε στην εξωτερική interface του firewall. Το *l2l* που φαίνεται στη δημιουργία του tunnel-group, σημαίνει location to location και ουσιαστικά επιβεβαιώνει ότι δημιουργούμε site-to-site VPN. Παρακάτω φαίνονται τα βήματα αυτά.

```
FirewallPatra(config)# tunnel-group 210.168.200.1 type ipsec-l2l
FirewallPatra(config)# tunnel-group 210.168.200.1 ipsec-attributes
FirewallPatra(config-tunnel-ipsec)# ikev1 pre-shared-key testkey
```

Εικόνα 133. Δημιουργία tunnel group και ορισμός pre-share key (firewall)

```
FirewallPatra(config)# crypto map MYMAP 1 match address MYLIST
FirewallPatra(config)# crypto map MYMAP 1 set peer 210.168.200.1
FirewallPatra(config)# crypto map MYMAP 1 set ikev1 transform-set MYSET
```

Εικόνα 134. Δημιουργία crypto MAP και ορισμός IP που καταλήγει το VPN (firewall)

```
FirewallPatra(config)# crypto map MYMAP interface outside
```

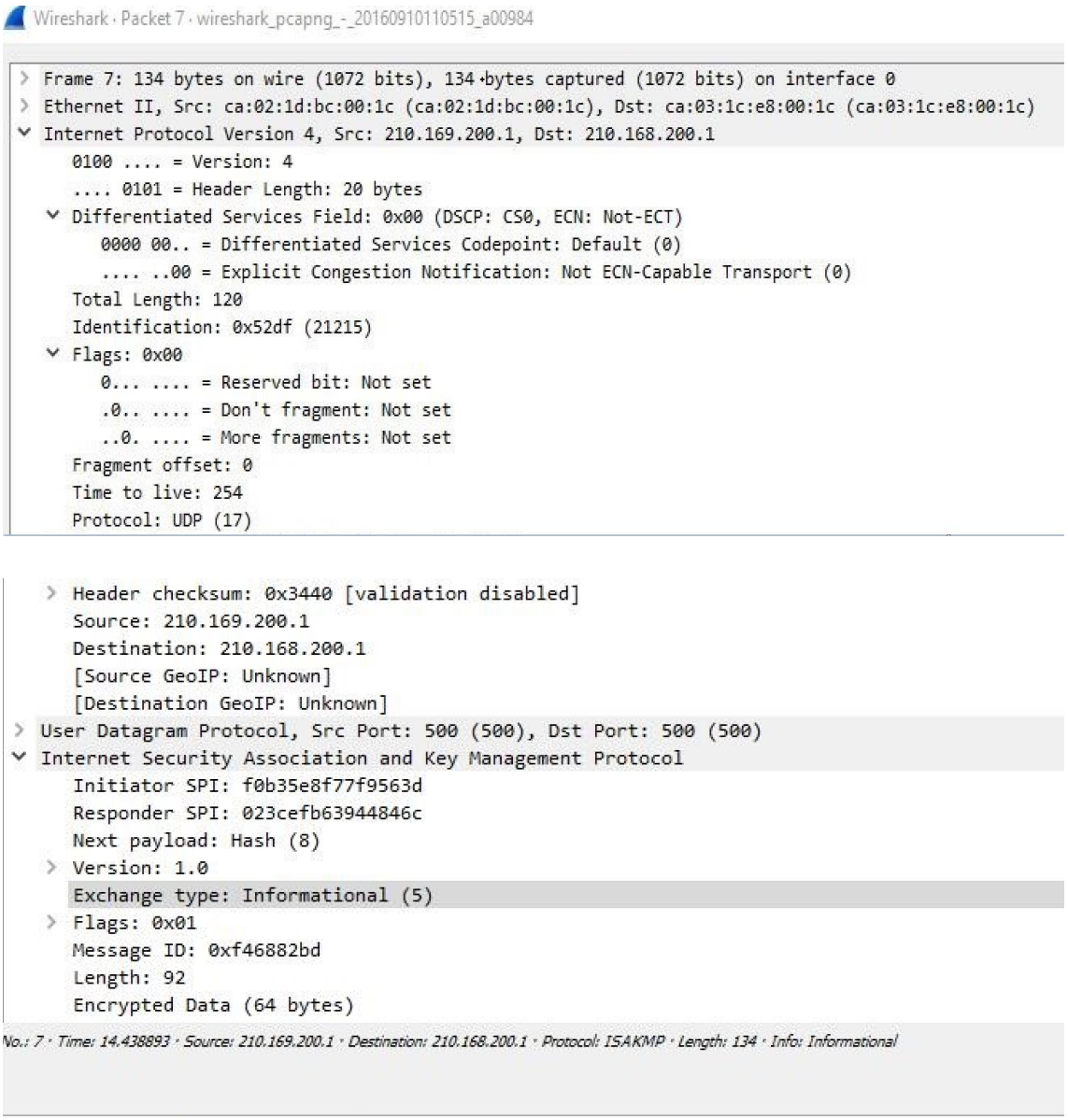
Εικόνα 135. Ενεργοποίηση crypto MAP στην εξωτερική interface (firewall)

Αφού ολοκληρώσαμε το configuration, κάνουμε ping για να δούμε αν όλα ολοκληρώθηκαν σωστά.

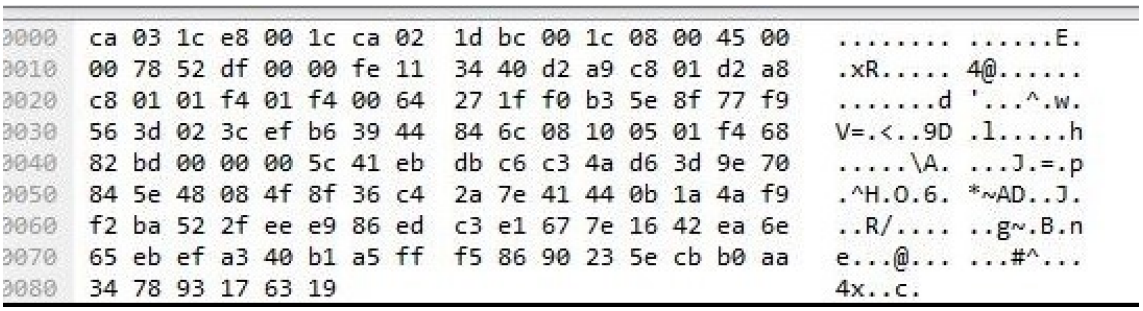
```
Athens#ping 210.169.200.1 source loopback 1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.169.200.1 , timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/60/92 ms
```

Εικόνα 136. Επιτυχημένο ping και επιβεβαίωση ότι το IPsec VPN λειτουργεί σωστά

Αν θέλουμε να επιβεβαιώσουμε ότι το πακέτο πέρασε από τη μια μεριά στην άλλη κρυπτογραφημένο, μπορούμε να πάρουμε και το output από το Wireshark που εμφανίζει την κρυπτογράφηση. Στην πιο κάτω εικόνα μπορούμε να δούμε ξεκάθαρα την κρυπτογράφηση, την source address και την destination address (θα φαίνεται φυσικά η αρχή και το τέλος του IPsec tunnel που δημιουργήσαμε) καθώς και διάφορες άλλες πληροφορίες.



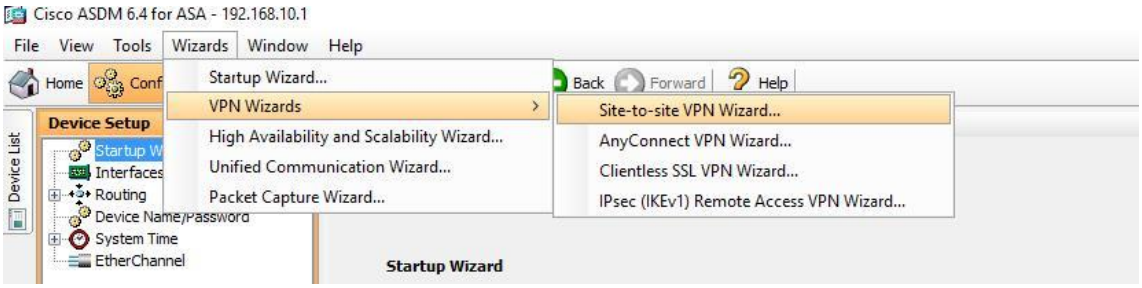
Εικόνα 137. Output από το Wireshark που λήφθηκε μετά το ping που φαίνεται στην εικόνα 136



Εικόνα 138. Επιβεβαίωση κρυπτογράφησης πληροφορίας μέσω του output του Wireshark

5.1.2.2. Υλοποίηση με GUI (Graphical User Interface)

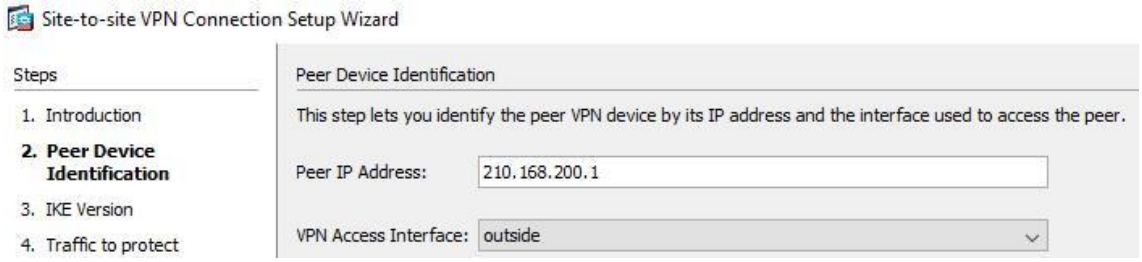
Πριν ξεκινήσουμε το configuration του firewall για την υλοποίηση του VPN, όπως και στο προηγούμενο βήμα θα πρέπει να δημιουργήσουμε pre-shared keys. Μόλις ολοκληρωθεί αυτό το βήμα, για να μπορέσουμε να ξεκινήσουμε το configuration του IPsec VPN επιλέγουμε Wizards → VPN Wizards → Site-to-Site VPN Wizards.



Εικόνα 139. Ρυθμιση του IPsec VPN μέσα από το ASDM (αρχική εικόνα)

Ανοίγοντας τον wizard, βλέπουμε ότι υπάρχουν 6 βήματα για την επιτυχή ρύθμιση.

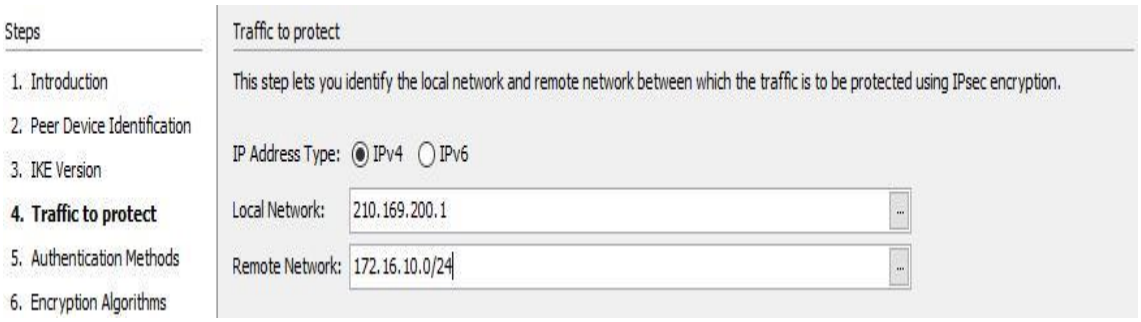
1. Αρχικά μας ζητείται να ρυθμίσουμε ποια είναι η IP στην οποία τερματίζει το VPN καθώς και ποια interface του firewall θα χρησιμοποιήσουμε για να φτάσουμε εκεί. Από την τοπολογία μας βλέπουμε ότι αυτή η IP είναι η 210.168.200.1 δηλαδή η interface GigabitEthernet1/0 του Router Athens. Άρα θα χρησιμοποιήσουμε την outside interface του firewall, αυτή δηλαδή που βρίσκεται στο εξωτερικό δίκτυο.



Εικόνα 140. Ρυθμιση του IPsec VPN μέσα από το ASDM (βήμα 1)

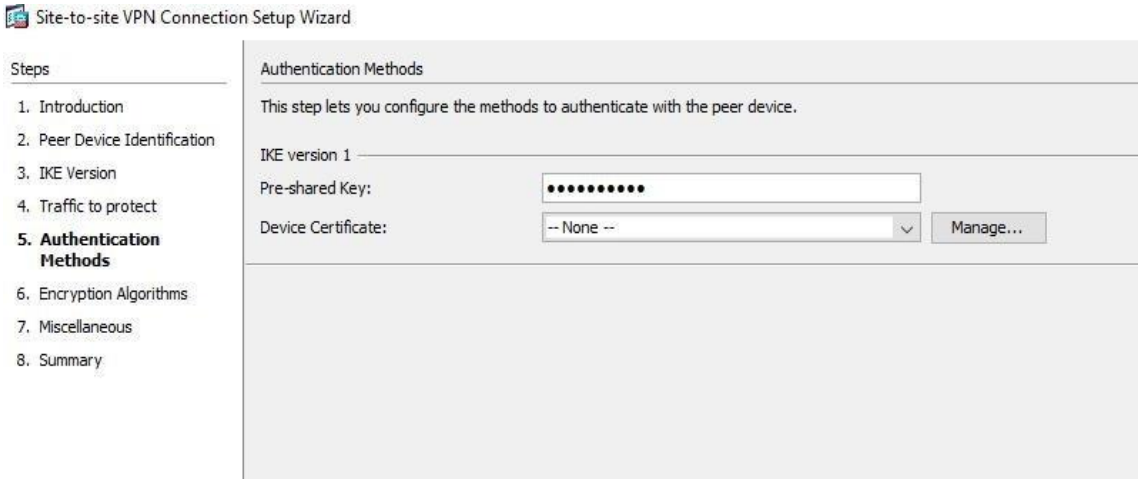
2. Αμέσως μετά έχουμε τη δυνατότητα να επιλέξουμε αν θα κάνουμε configure την IKEv1 ή την IKEv2 ή και τις δυο μαζί. Επιλέγουμε IKEv1 και πατάμε Next.
3. Στη συνέχεια, στο βήμα *traffic to protect*, θα πρέπει να δηλώσουμε ποια είναι τα δίκτυα, τα δεδομένα των οποίων θα μπορούν ελευθέρα να περνούν από το firewall και να περνούν χωρίς πρόβλημα μέσα από το VPN. Είναι κάτι αντίστοιχο με αυτό που κάναμε και κατά το configuration του IPsec VPN με routers. Ορίζοντας τα δυο δίκτυα, ουσιαστικά δημιουργούμε αυτόματα μια access-list. Μας δίνεται η δυνατότητα να επιλέξουμε IPv4 ή IPv6 και ακριβώς από κάτω ορίζουμε τα δίκτυα. Αν έχουμε πολλά δίκτυα πίσω από ένα firewall και δεν τα θυμόμαστε όλα, μπορούμε να πατήσουμε στο κουμπί δίπλα στο local network και αυτόματα θα εμφανιστεί μια λίστα με όλα τα δίκτυα που έχουμε προσθέσει στο firewall. Εναλλακτικά, μπορούμε απλά να τα πληκτρολογήσουμε πριν πατήσουμε Next. Επειδή όπως είπαμε θέλουμε η μεριά του

firewall να ξεκινάει από έναν και μόνο host, στο local network δεν βάζουμε δίκτυο, αλλά host.



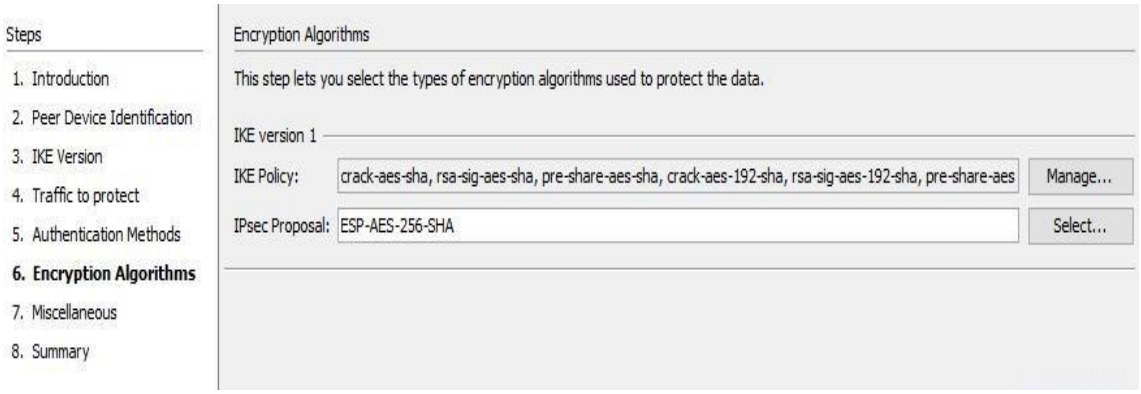
Εικόνα 141. Ρυθμιση του IPsec VPN μέσα από το ASDM (βήμα 2)

4. Στο επόμενο βήμα, ορίζουμε τις authentication methods. Μιας και έχουμε επιλέξει αυτή τη φορά να υλοποιήσουμε το παράδειγμα με pre-shared keys και όχι με digital certificates, το μόνο που έχουμε να κάνουμε είναι να πληκτρολογήσουμε το pre-shared key του local και του remote peer για να μπορέσουμε να προχωρήσουμε.



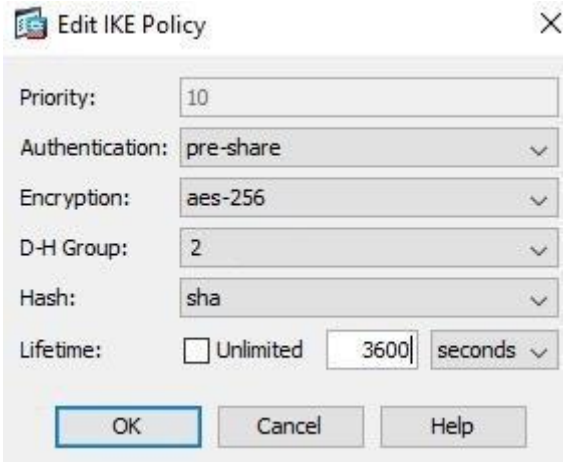
Εικόνα 142. Ρυθμιση του IPsec VPN μέσα από το ASDM (βήμα 3)

5. Προχωρώντας, μας ζητείται να ορίσουμε τους αλγόριθμους κρυπτογράφησης. Εδώ καλούμαστε να πάρουμε την εξής απόφαση. Είτε να μην πειράξουμε κάτι σε αυτό το σημείο και να δεχτούμε όσες default policies υπάρχουν είτε να τις κάνουμε customize και να περάσουμε μόνο αυτά που θέλουμε εμείς. Η πρώτη επιλογή είναι πιο ασφαλής μιας και δεν υπάρχει περίπτωση να κάνουμε κάποιο λάθος, αλλά το μεγάλο μειονέκτημα είναι ότι δυσχεραίνει τον μετέπειτα έλεγχο λόγω του όγκου τον πληροφοριών.



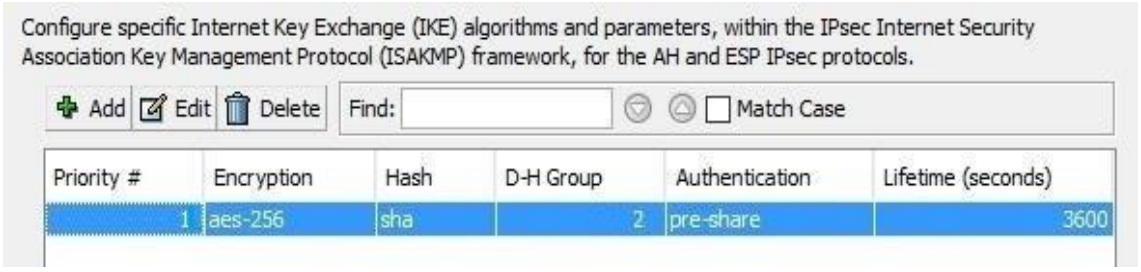
Εικόνα 143.Ρυθμιση του IPsec VPN μέσα από το ASDM (βήμα 4)

Στο δικό μας παράδειγμα θα χρησιμοποιήσουμε customized settings. Επιλέγουμε το manage και εμφανίζεται μια λίστα με policies. Κάνουμε double click στο policy που θέλουμε (συνήθως κρατάμε αυτό με το χαμηλότερο αριθμό) και μας δίνει τη δυνατότητα να επιλέξουμε εμείς ό,τι θέλουμε.



Εικόνα 144. Ρυθμιση του IPsec VPN μέσα από το ASDM (βήμα 5)

Στη συνέχεια με το delete σβήνουμε τα υπόλοιπα policies έτσι ώστε να μείνει μόνο αυτό που θέλουμε και μετά αλλάζουμε το priority σε 1.



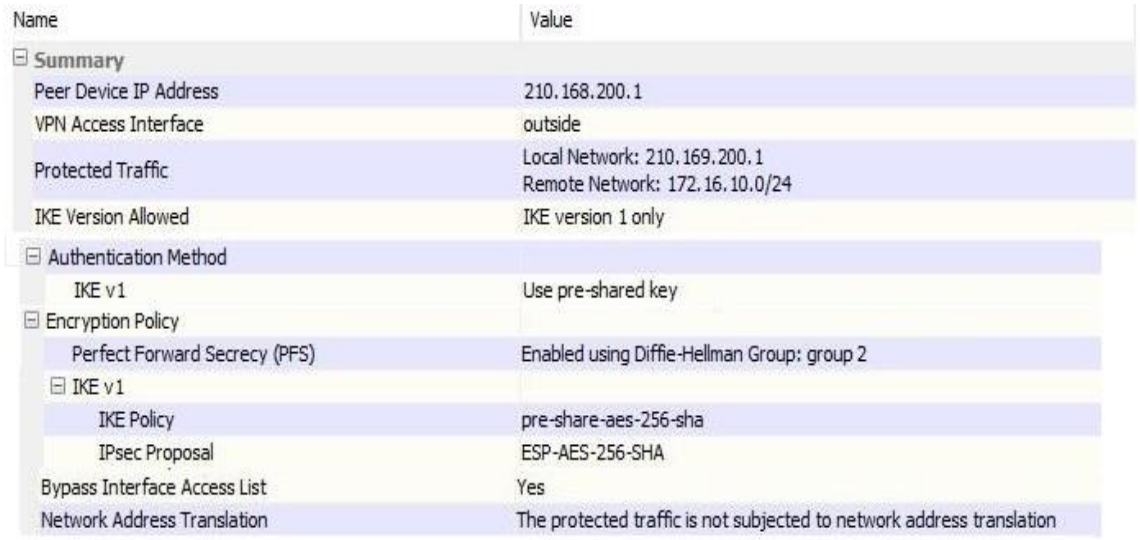
Εικόνα 145. Ρυθμιση του IPsec VPN μέσα από το ASDM (βήμα 6)

Μόλις ολοκληρώσουμε τη διαδικασία και στα δυο πεδία, η εικόνα που έχουμε είναι πιο σαφής σε σχέση με τα default.

Εικόνα 146. Ρυθμιση του IPsec VPN μέσα από το ASDM (βήμα 7)

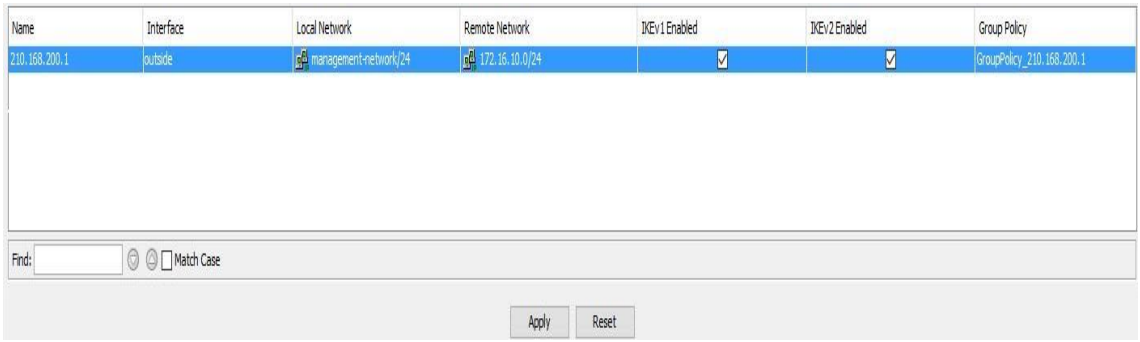
6. Στο πεδίο miscellaneous αφήνουμε τις επιλογές ως έχουν και απλά στο Diffie-Hellman group του pfs επιλέγουμε group2.

Μετά και από αυτή τη ρύθμιση βλέπουμε μια γενική σύνοψη από το configuration πριν ολοκληρώσουμε τη διαδικασία.



Εικόνα 147. Σύνοψη προηγούμενων βημάτων

Τέλος, αν έχουμε περάσει τις σωστές ρυθμίσεις, θα μας εμφανίσει μια οθόνη για να επιλέξουμε ποιο VPN θέλουμε να γίνει apply στο firewall. Αν κατέληγαν πολλά VPN tunnels στο εν λόγω firewall, θα μας εμφάνιζε όλες τις επιλογές. Πατάμε apply και το ASDM μεταφέρει αυτόματα τα settings στο firewall. Δικιά μας ευθύνη είναι απλά να τα κάνουμε save.



Εικόνα 148. Ολοκλήρωση ρύθμισης IPsec VPN

5.1.2.3. Debugging και εντολές ελέγχου ορθής διαμόρφωσης

Αφού ολοκληρώσαμε το configuration, κάνουμε ping για να δούμε αν όλα ολοκληρώθηκαν σωστά.

```
Athens#ping 210.169.200.1 source loopback 1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.169.200.1 , timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/60/92 ms
```

Εικόνα 149. Επιτυχημένο ping και επιβεβαίωση ότι το IPsec VPN λειτουργεί σωστά.

Και σε αυτή την περίπτωση ισχύει η διαδικασία ελέγχου που ακολουθήσαμε στο IPsec implementation με IOS routers. Οπότε με δεδομένο ότι γνωρίζουμε πώς γίνεται ο έλεγχος, θα επικεντρωθούμε στις πιο σημαντικές εντολές που μπορούμε να εισάγουμε στο firewall μετά από την επιτυχή εγκατάσταση του IPsec VPN.
Οι εντολές στις οποίες θα επικεντρωθούμε είναι:

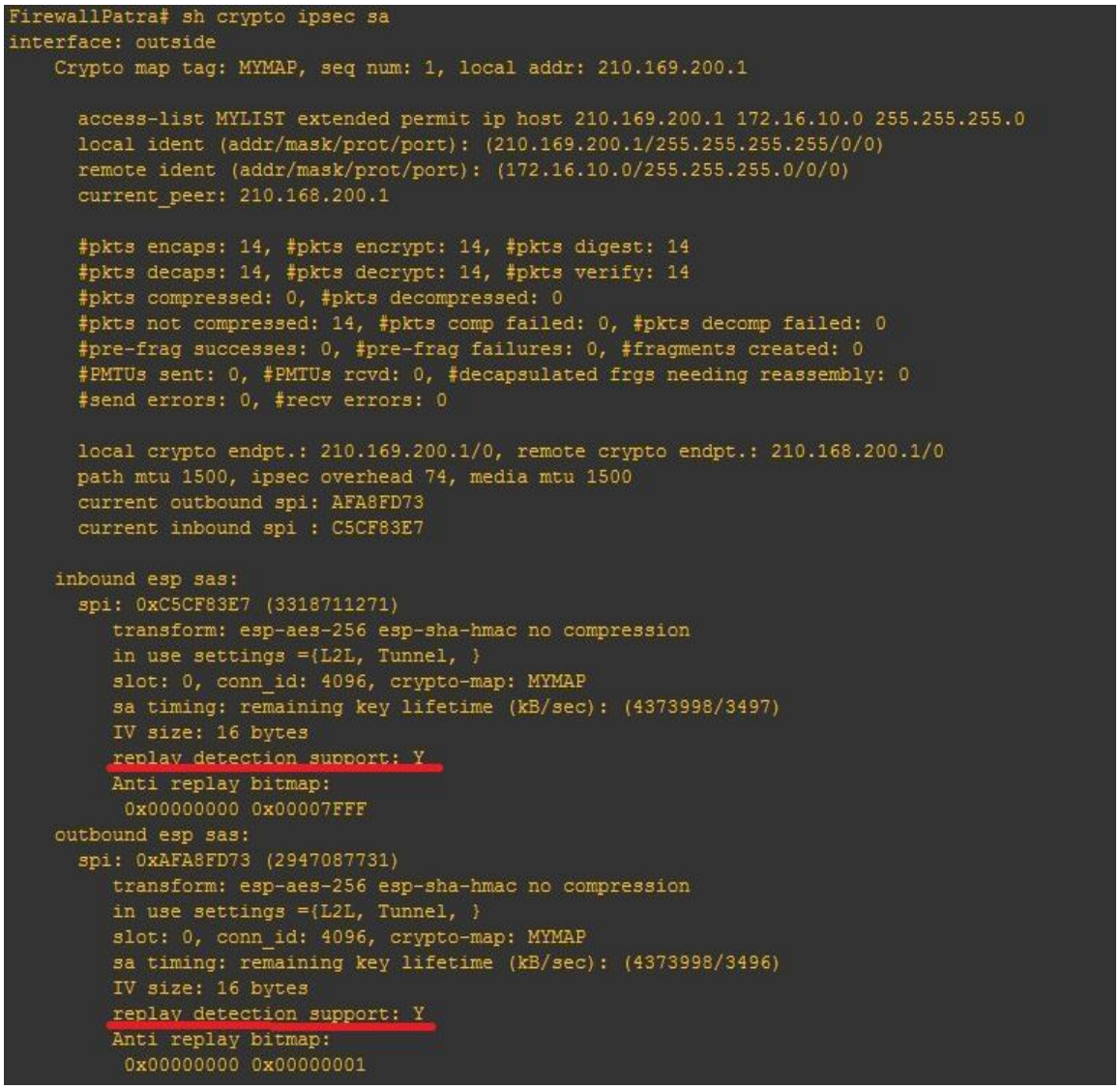
- *Show isakmp sa detail*
- *Show crypto IPsec sa*
- *Show isakmp stats*
- *Show vpn-sessiondb*

Παρακάτω βλέπουμε και τα screenshots με την προαναφερθείσα σειρά. Στην πρώτη εικόνα βλέπουμε ξεκάθαρα όλα όσα κάναμε configure σε προηγούμενα βήματα. Επίσης φαίνεται η κατάσταση (MM_ACTIVE) και ο χρόνος που απομένει μέχρι να λήξει το VPN session (3435 sec από τα αρχικά 3600 sec). Στο role βλέπουμε την κατάσταση initiator καθώς το συγκεκριμένο screenshot είναι μετά από ping από το firewall προς το εσωτερικό δίκτυο του router Athens. Φυσικά, πιο πάνω, υπάρχει screenshot με επιτυχημένο ping και από την αντίθετη μεριά. Τέλος, όπως είναι φυσικό, μιας και έχουμε κάνει configure το firewall μόνο με IKEv1, εμφανίζεται η ειδοποίηση ότι δεν υπάρχουν IKEv2 SAs.

```
FirewallPatra# sh isakmp sa detail

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 210.168.200.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
    Encrypt : aes-256         Hash    : SHA
    Auth    : preshared       Lifetime: 3600
    Lifetime Remaining: 3435

There are no IKEv2 SAs
```

Εικόνα 150. Output εντολής show isakmp sa detail

Στο επόμενο screenshot έχουμε μια πιο γενική εικόνα από το IPsec VPN που δημιουργήσαμε. Σημαντικό είναι να παρατηρήσουμε ότι και στο outbound esp αλλα και στο inbound esp είναι ενεργοποιημένο το *replay detection support*.



Εικόνα 151. Output εντολής show crypto IPsec sa

Στην επόμενη εικόνα βλέπουμε ότι έχουμε ενεργό tunnel, το πλήθος των πακέτων που στάλθηκαν και στο κάτω μέρος της εικόνας επιβεβαιώνουμε ότι δεν έχουμε κανένα πρόβλημα με authentication, authorization και hashing.

```
FirewallPatra# sh isakmp stats

Global IKEv1 Statistics
  Active Tunnels:                1
  Previous Tunnels:              1
  In Octets:                   948
  In Packets:                    7
  In Drop Packets:               1
  In Notifys:                    2
  In P2 Exchanges:               0
  In P2 Exchange Invalids:       0
  In P2 Exchange Rejects:        0
  In P2 Sa Delete Requests:      0
  Out Octets:                  956
  Out Packets:                   6
  Out Drop Packets:              0
  Out Notifys:                   2
  Out P2 Exchanges:              1
  Out P2 Exchange Invalids:      0
  Out P2 Exchange Rejects:       0
  Out P2 Sa Delete Requests:     0
  Initiator Tunnels:             1
  Initiator Fails:               0
  Responder Fails:               0
  System Capacity Fails:         0
  Auth Fails:                    0
  Decrypt Fails:                 0
  Hash Valid Fails:              0
  No Sa Fails:                   0
```

Εικόνα 152. Output εντολής show isakmp stats

Τέλος, βλέπουμε ότι και οι δυο phases, έχουν ολοκληρωθεί σωστά. Στο summary βλέπουμε δυο εγγραφές, την IKEv1 phase 1 και το IPsec που ουσιαστικά πρόκειται για την IKEv1 phase 2.

```
FirewallPatra# sh vpn-sessiondb
--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
Site-to-Site VPN           :      1 :          1 :           1
  IKEv1 IPsec              :      1 :          1 :           1
--------------------------------------------------------------------------
Total Active and Inactive  :      1             Total Cumulative :      1
--------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ----------------------------------------------
IKEv1                      :      1 :          1 :               1
IPsec                      :      1 :          1 :               1
--------------------------------------------------------------------------
Totals                     :      2 :          2
--------------------------------------------------------------------------
```

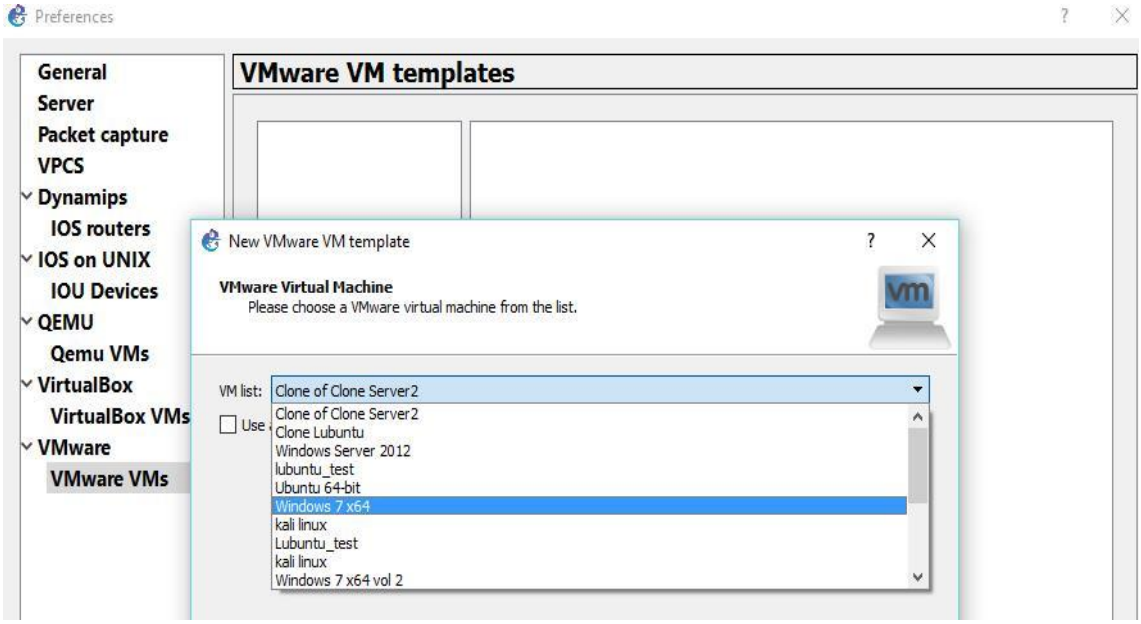
Εικόνα 153. Output εντολής show vpn-sessiondb

5.2. Υλοποίηση SSL VPN

Σε αυτό το κομμάτι, θα προσπαθήσουμε να υλοποιήσουμε το άλλο είδος του VPN, το SSL. Πριν ξεκινήσουμε να αναφέρουμε πως θα υλοποιήσουμε το SSL VPN, καλό θα ήταν να αναφέρουμε λίγα λόγια για το πώς λειτουργεί το SSL. Κατά κύριο λόγο ακολουθούνται τα παρακάτω βήματα.

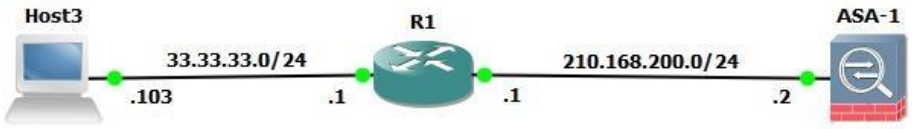
1. Ο client ξεκινά μια σύνδεση με την εφαρμογή (ή server ή οτιδήποτε άλλο) χρησιμοποιώντας την destination IP του τερματικού και την destination TCP port 443. Σαν source IP, θεωρείται η IP του client και σαν source port οποιαδήποτε μη χρησιμοποιούμενη port με αριθμό μεγαλύτερο του 1023.
2. Ακολουθεί η συνηθισμένη διαδικασία για την ολοκλήρωση TCP συνδέσεων, δηλαδή ένα three-way handshake.
3. Από τη στιγμή που ο client αποστείλει το αίτημα για σύνδεση, το άλλο άκρο αποστέλλει το ψηφιακό πιστοποιητικό του, το οποίο περιέχει το δημόσιο κλειδί του.
4. Μόλις ο client το λάβει, πρέπει να πάρει μια απόφαση. Θα δεχτεί σαν έγκυρο το πιστοποιητικό αυτό ή θα το απορρίψει; Και εδώ το PKI μπαίνει στην εξίσωση. Αν το πιστοποιητικό είναι υπογεγραμμένο από μια Αρχή Πιστοποίησης που εμπιστεύεται ο client, οι ημερομηνίες δείχνουν ότι δεν έχει λήξει και αφού ελέγξει την CRL (Certificate Revocation List), αποδέχεται το πιστοποιητικό από όπου και εξάγει το public key.
5. Ο client χρησιμοποιεί το public key που εξήγαγε από το πιστοποιητικό και κρυπτογραφεί το shared secret key που θα χρησιμοποιήσει για την κρυπτογραφημένη επικοινωνία με το τερματικό, στο οποίο και το αποστέλλει.
6. Το τερματικό αποκρυπτογραφεί το symmetric key χρησιμοποιώντας το δικό του private key (αφού η κρυπτογράφηση έχει γίνει με το δικό του public key) οπότε, πλέον και οι δυο συσκευές ξέρουν το shared secret key.
7. Το shared secret key χρησιμοποιείται για την κρυπτογράφηση της SSL σύνδεσης.

Όπως είδαμε στα παραπάνω βήματα, αυτού του είδος το VPN χρησιμοποιείται κυρίως για ασφαλή πρόσβαση σε μια εφαρμογή ή σε έναν server από απομακρυσμένους χρήστες. Άρα η λογική θα είναι διαφορετική. Σε αυτή την περίπτωση δε μας αρκεί να δείξουμε ότι υπάρχει κρυπτογραφημένη συνδεσιμότητα από ένα δίκτυο σε ένα άλλο (περίπτωση ping). Εδώ θέλουμε να δείξουμε ότι υπάρχει πρόσβαση σε μια εφαρμογή. Για να το καταφέρουμε αυτό, θα πρέπει να έχουμε πρόσβαση σε έναν απομακρυσμένο υπολογιστή για να χρησιμοποιήσουμε τον browser του. Αυτό το επιτυγχάνουμε εύκολα αν στο GNS3 από την αντίστοιχη επιλογή στα preferences, εισάγουμε μια Virtual Machine (VM). Φυσικά προϋποθέτει να έχουμε δημιουργήσει από πιο πριν μια VM με το επιθυμητό λογισμικό. Εμείς κάναμε εγκατάσταση Windows 7 x64 (64 bit).



Εικόνα 154. Σύνδεση VMware με GNS3

Από άποψη πρωτοκόλλων, ρυθμίσαμε το firewall με απλά static routes. Στο router δε χρειάζεται να ρυθμίσουμε κάτι, αφού λόγω θέσης γνωρίζει ήδη όλα τα routes που χρειάζεται. Τέλος, από τα δυο είδη SSL VPN, δηλαδή clientless ή με κάποιον client, εμείς θα υλοποιήσουμε το clientless που είναι και το πιο διαδεδομένο. Πρέπει να τονίσουμε ότι το SSL VPN για να λειτουργήσει χρειάζεται digital certificate. Εδώ όμως, δε θα ακολουθήσουμε τα βήματα που είδαμε σε προηγούμενο παράδειγμα, δηλαδή την επικοινωνία με κάποια Certificate Authority και δημιουργία αιτήματος υπογραφής του πιστοποιητικού, αλλά θα δημιουργήσουμε ένα self-signed πιστοποιητικό και θα το χρησιμοποιήσουμε για να ολοκληρώσουμε τη διαδικασία. Λόγω του περιορισμού του λογισμικού δε μπορούμε να κάνουμε αυτόματα τη διαδικασία έκδοσης και υπογραφής του πιστοποιητικού. Αυτή η διαδικασία θα γίνει υποχρεωτικά μέσω CLI. Η τοπολογία μας για το συγκεκριμένο περίπτωση είναι η παρακάτω.



Εικόνα 155. Τοπολογία για υλοποίηση SSL VPN στο GNS3 με χρήση firewall

5.2.1. Υλοποίηση με GUI (Graphical User Interface)

Σε αντίθεση με τα προηγούμενα, θα ξεκινήσουμε με τη διαδικασία υλοποίησης clientless SSL VPN μέσω GUI, που είναι και η πιο διαδεδομένη, και μετά θα ακολουθήσει το CLI.

Όπως είπαμε και πιο πάνω πρέπει να ξεκινήσουμε με την έκδοση και αυτο-υπογραφή του πιστοποιητικού. Τα βήματα που πρέπει να γίνουν είναι τα εξής:

1. Δημιουργούμε ένα ζεύγος κλειδιών γενικής χρήσης και τα ονομάζουμε *sslvpnkey*.

```
ciscoasa> en
Password:
ciscoasa# conf t
ciscoasa(config)# crypto key generate rsa label sslvpnkey
INFO: The name for the keys will be: sslvpnkey
Keypair generation process begin. Please wait...
```

Εικόνα 156. Δημιουργία ζεύγους κλειδιών γενικής χρήσης

2. Δημιουργούμε μια αρχή πιστοποίησης που την ονομάζουμε *TrustPoint0* και δηλώνουμε ότι θα υπογράψει η ίδια το πιστοποιητικό.

```
ciscoasa(config)# crypto ca trustpoint TrustPoint0
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# fqdn sslvpn.test.com
ciscoasa(config-ca-trustpoint)# subject-name CN=sslvpn.test.com
```

Εικόνα 157. Δημιουργία Αρχής Πιστοποίησης και ρύθμιση να αυτό-υπογράψει το πιστοποιητικό που θα εκδώσει

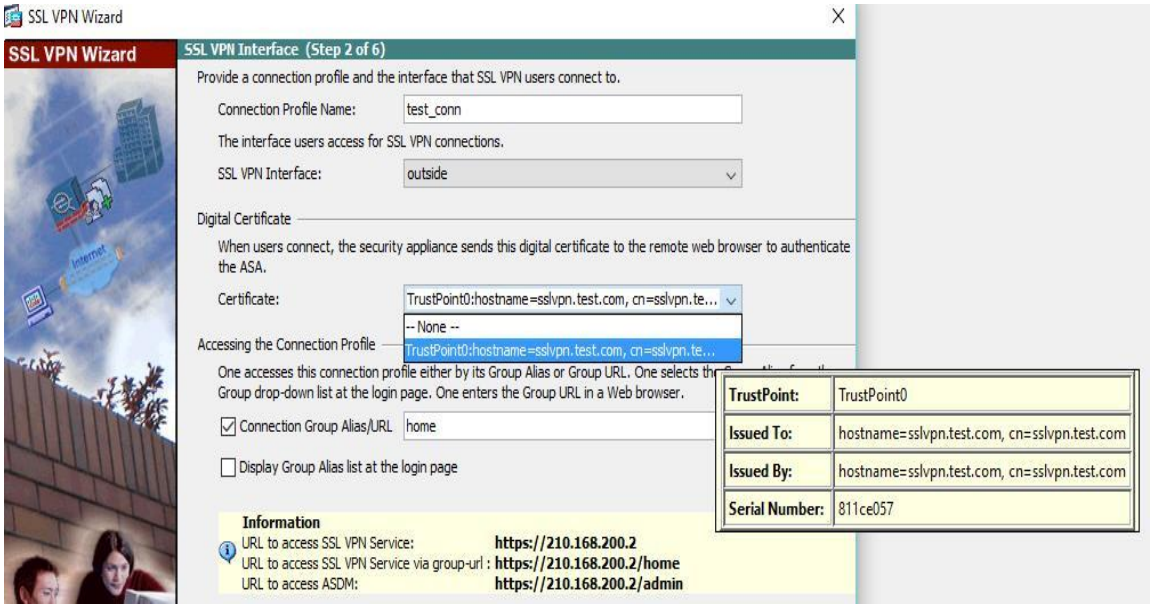
3. Δηλώνουμε ποιο κλειδί θα χρησιμοποιηθεί για την υπογραφή, ζητάμε την υπογραφή και τοποθετούμε το πιστοποιητικό στην outside interface του firewall.

```
ciscoasa(config-ca-trustpoint)# keypair sslvpnkey
ciscoasa(config-ca-trustpoint)# crypto ca enroll TrustPoint0 noconfirm

% The fully-qualified domain name in the certificate will be: sslvpn.test.com
ciscoasa(config)# ssl trust-point TrustPoint0 outside
```

Εικόνα 158. Τοποθέτηση πιστοποιητικού στην εξωτερική interface του firewall

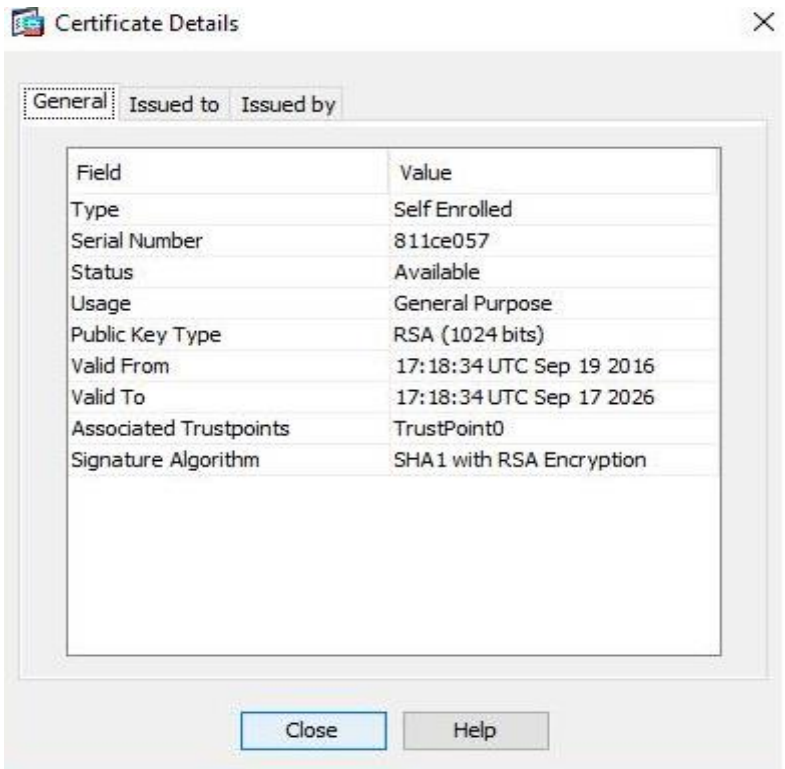
Στη συνέχεια, μπορούμε να περάσουμε στο ASDM. Από εκεί, θα ακολουθήσουμε τον Configuration Wizard στον οποίο αποκτούμε πρόσβαση από το ASDM από το menu Wizards -> VPN Wizards -> clientless SSL VPN Wizard.

Στο πρώτο βήμα απλά ορίζουμε ένα profile name, επιλέγουμε την εξωτερική interface του firewall που την έχουμε ονομάσει outside και επιλέγουμε το ψηφιακό πιστοποιητικό που δημιουργήσαμε πριν λίγο. Επίσης, παρατηρούμε ότι στο κάτω μέρος, εκτός από το βασικό URL, εμφανίζει και άλλα δυο, το ένα που είναι ίδιο με το πρώτο, αλλά χρησιμοποιεί το ψευδώνυμο που δώσαμε και το τρίτο, για να αποκτήσει πρόσβαση ο administrator.



Εικόνα 159. Ρύθμιση SSL VPN μέσα από το ASDM (βημα 1)

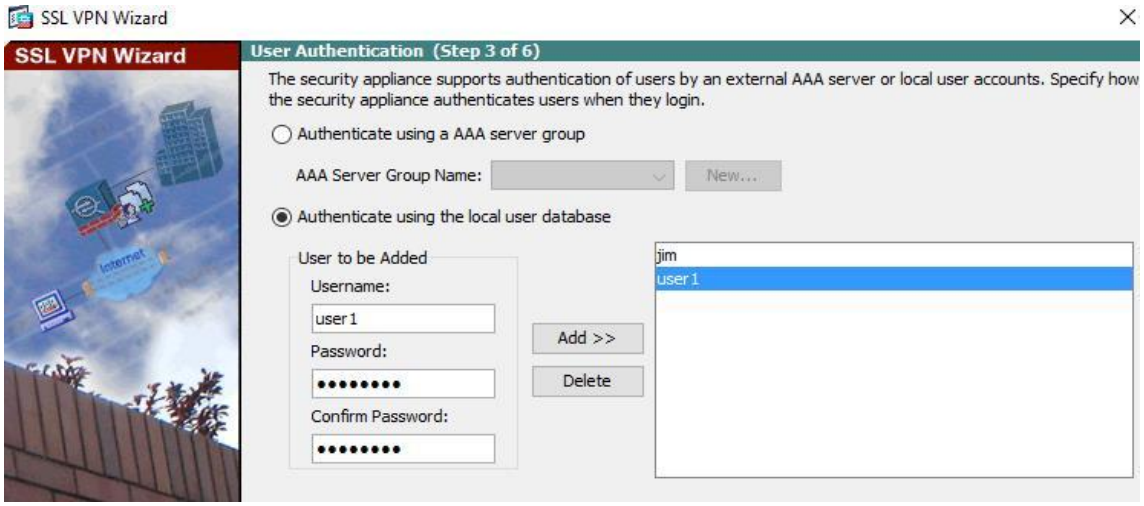
Την εικόνα του πιστοποιητικού που δημιουργήσαμε, μπορούμε να τη δούμε και μέσα από το ASDM, στο path Configuration -> Device Management -> Certificate Management -> Identity Certificates.



Εικόνα 160. Εικόνα με λεπτομέριες πιστοποιητικού που δημιουργήσαμε

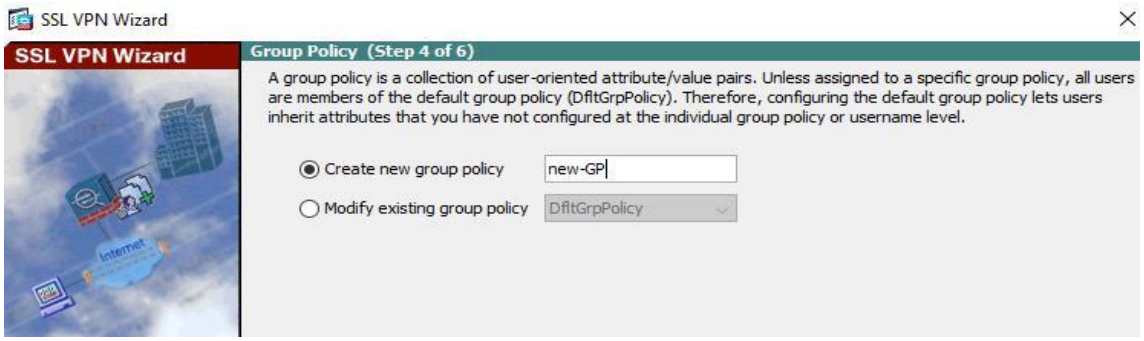
Αμέσως μετά, μιας και δεν έχουμε κάποιον Radius ή TACACS+ Server για αυθεντικοποίηση χρηστών, θα ορίσουμε χειροκίνητα τους χρήστες και θα τους προσθέσουμε

στην εφαρμογή. Παρατηρούμε ότι υπάρχει ήδη ο χρήστης jim ο οποίος είναι και ο administrator με τους κωδικούς του οποίου κάναμε είσοδο και στο ASDM.

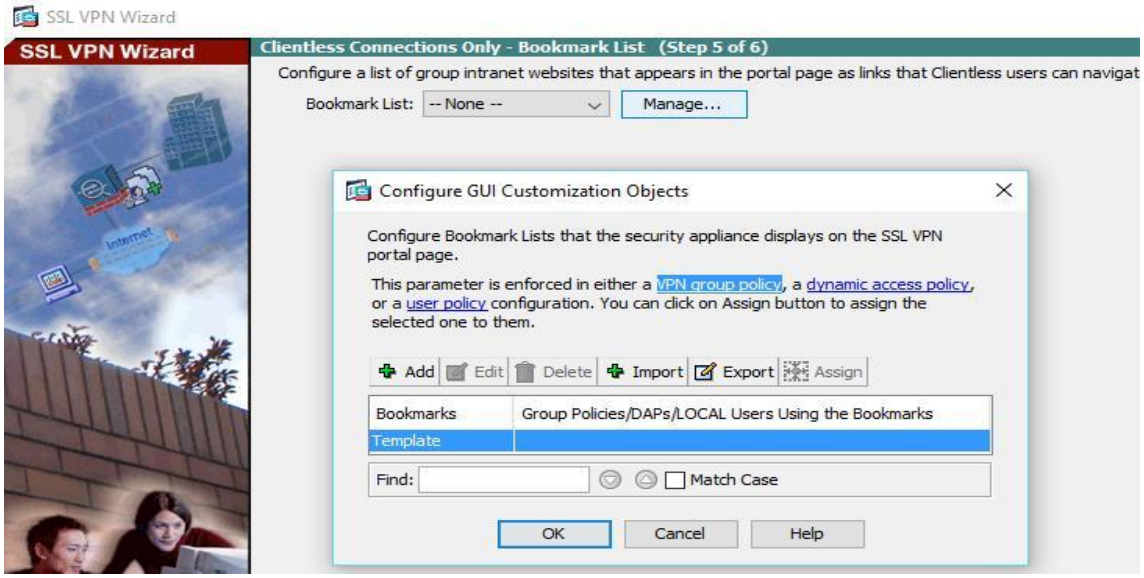


Εικόνα 161. Ρύθμιση SSL VPN μέσα από το ASDM (βημα 2)

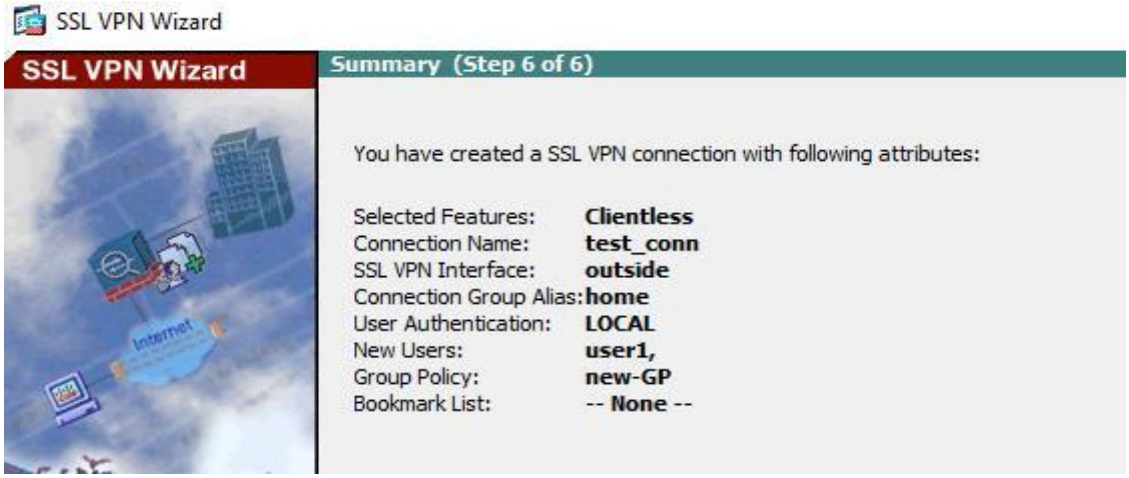
Στα δυο επόμενα βήματα απλά δημιουργούμε ένα νέο Group Policy που θα κάνει υπερισχύσει του ήδη υπάρχοντος. Όλοι οι χρήστες υιοθετούν τις ιδιότητες του νέου group policy. Στο συγκεκριμένο παράδειγμα, δε θα παραμετροποιήσουμε το policy αφού δεν έχουμε κάποιες ιδιαίτερες απαιτήσεις. Τέλος, αν έχουμε δημιουργήσει κάποια bookmark που θα φαίνονται στην εφαρμογή, τα προσθέτουμε (δεν είναι υποχρεωτικό). Στην τελική εικόνα φαίνεται η σύνοψη που εμφανίζεται πριν εισάγουμε το configuration στο firewall.



Εικόνα 162. Ρύθμιση SSL VPN μέσα από το ASDM (βημα 3)

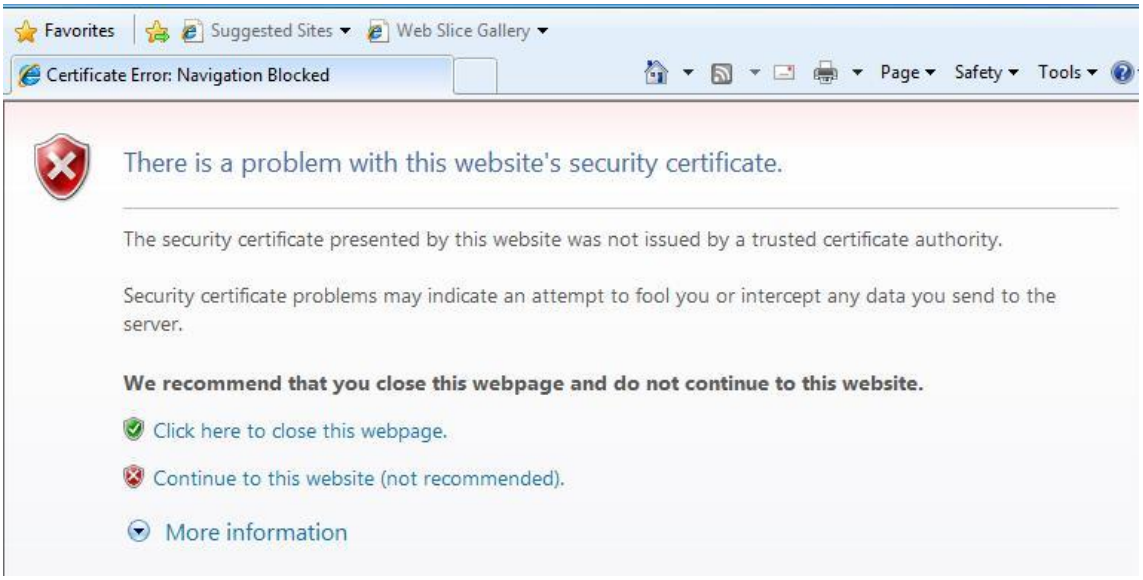


Εικόνα 163. Ρύθμιση SSL VPN μέσα από το ASDM (βημα 4)



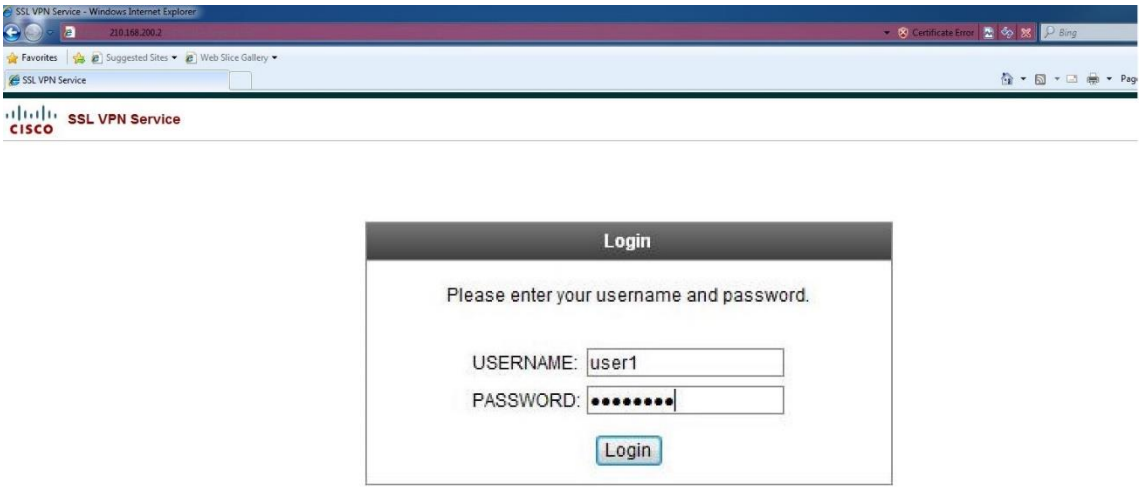
Εικόνα 164. Σύνοψη ρυθμίσεων

Αφού ολοκληρώσουμε τα βήματα μέσω wizard, είναι ώρα να πάμε στη VM που έχουμε δημιουργήσει, να ανοίξουμε έναν browser και να προσπαθήσουμε να αποκτήσουμε πρόσβαση στην εφαρμογή μας. Το URL που θα εισάγουμε είναι το *https://210.168.200.2*. Επειδή το certificate δεν έχει εκδοθεί από κάποια επίσημη CA που εμπιστευόμαστε, θα μας εμφανίσει μήνυμα για το αν θέλουμε να απομακρυνθούμε από τη σελίδα ή αν θέλουμε συνεχίσουμε και να αποδεχτούμε το πιστοποιητικό.



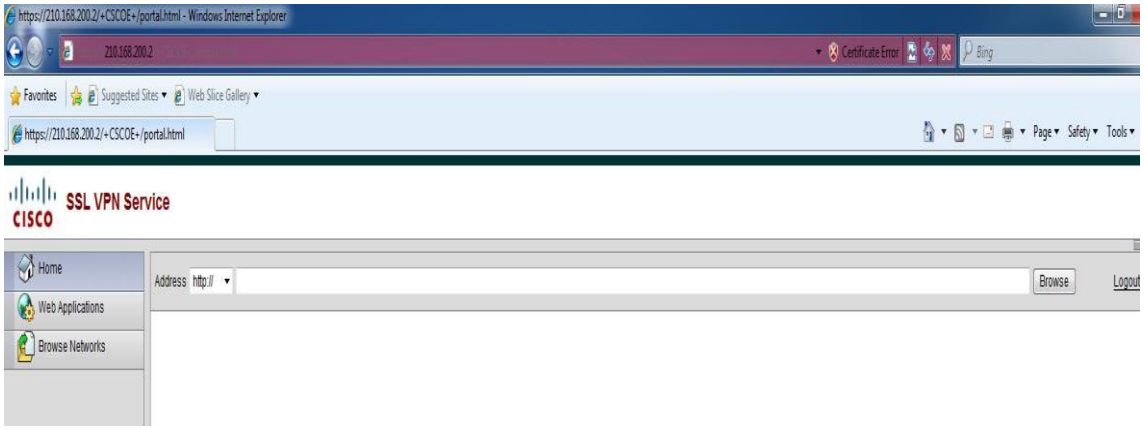
Εικόνα 165. Εικόνα του client όταν προσπαθεί να εισέλθει στην εφαρμογή. Το πιστοποιητικό είναι self-signed και γι'αυτό εμφανίζεται η προειδοποίηση.

Επιλέγουμε να συνεχίσουμε και αμέσως μετά το σύστημα μας ζητάει να εισάγουμε username και password. Φυσικά για να αποκτήσουμε πρόσβαση θα πρέπει να εισάγουμε τα user credentials που ορίσαμε στο configuration του firewall.



Εικόνα 166. Καταχώρηση username/password για είσοδο στην σελίδα

Αφού τα εισάγουμε σωστά, αποκτούμε πρόσβαση στην εφαρμογή. Στο συγκεκριμένο παράδειγμα το interface είναι εντελώς άδειο, μιας και πρόκειται για test εφαρμογή.



Εικόνα 167. Interface test εφαρμογής

5.2.2. Υλοποίηση με CLI (Command Line Interface)

Σε αυτό το κομμάτι θα δούμε τις αντίστοιχες εντολές που θα πρέπει να εισάγουμε στο CLI για να έχουμε το ίδιο αποτέλεσμα με το παραπάνω. Το πρώτο κομμάτι, δηλαδή η δημιουργία αρχής πιστοποίησης και η δημιουργία του self-signed digital certificate, είναι ακριβώς το ίδιο και δε χρειάζεται να το επαναλάβουμε.

Ξεκινάμε, δημιουργώντας ένα νέο group policy το οποίο στη συνέχεια θα χρησιμοποιήσουμε στη θέση του default και ορίζουμε να είναι internal.

```
ciscoasa(config)# group-policy new-GP internal
```

Εικόνα 168. Δημιουργία νεου group policy

Στη συνέχεια, θα ορίσουμε ότι θα χρησιμοποιήσουμε το self-signed certificate, θα το ενεργοποιήσουμε στην outside interface και θα ενεργοποιήσουμε το SSL VPN (webvpn) στην ίδια interface.

```
ciscoasa(config)# ssl trust-point TrustPoint0 outside
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
```

Εικόνα 169. Ενεργοποίηση SSL VPN και χρήση του Certificate δημιουργήσαμε στην εικόνα 157 από την CA TrustPoint0

Αμέσως μετά θα ορίσουμε τα χαρακτηριστικά του νέου group policy (ότι είναι, δηλαδή, clientless) και, αν έχουμε, θα προσθέσουμε και τα bookmarks. Φυσικά το σύστημα θα μας ενημερώσει ότι δεν έχουμε δημιουργήσει bookmarks και δε θα λάβει υπόψη την εντολή.

```
ciscoasa(config-webvpn)# group-policy new-GP attributes
ciscoasa(config-group-policy)# vpn-tunnel-protocol ssl-clientless
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# url-list value home
ERROR: No url-list "home" exists.
ciscoasa(config-group-webvpn)# exit
ciscoasa(config-group-policy)# exit
```

Εικόνα 170. Ρύθμιση SSL VPN ως clientless

Στο προτελευταίο βήμα, θα ορίσουμε το tunnel για remote access, σε αντιστοιχία με τα site-to-site που ορίζαμε ως τώρα, και θα δηλώσουμε ότι θα χρησιμοποιήσουμε το policy που δημιουργήσαμε στην αρχή.

```
ciscoasa(config)# tunnel-group test_conn type webvpn
ciscoasa(config)# tunnel-group test_conn general-attributes
ciscoasa(config-tunnel-general)# default-group-policy new-GP
```

Εικόνα 171. Ορισμός remote access tunnel και χρήση του group policy που δημιουργήσαμε στην εικόνα 168

Τέλος, ορίζουμε το url που θα πρέπει να εισάγει ο χρήστης για να εισέλθει στην εφαρμογή και του δίνουμε και ψευδώνυμο.

```
ciscoasa(config-tunnel-general)# tunnel-group test_conn webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias home enable
ciscoasa(config-tunnel-webvpn)# group-url https://210.168.200.2 enable
```

Εικόνα 172. Ορισμός URL για είσοδο του χρήστη στην εφαρμογή.

Η εισαγωγή των χρηστών είναι πολύ απλή και ολοκληρώνεται με την πιο κάτω εντολή.

```
ciscoasa(config)# username user password password
```

Εικόνα 173. Εισαγωγή χρήστη στο σύστημα

5.2.3 Debugging και εντολές ελέγχου ορθής διαμόρφωσης

Σε αντίθεση με το IPsec VPN, στο SLL VPN δεν έχουμε πολλά πράγματα να ελέγξουμε. Από τη μεριά του χρήστη, το μόνο που μπορούμε να κάνουμε είναι να ελέγξουμε την συνδεσιμότητα (ping), αν έχουμε πρόσβαση στο internet και φυσικά αν εισάγουμε σωστά το username και το password. Από τη μεριά του firewall μπορούμε να επιβεβαιώσουμε ότι όλα είναι σωστά απλά κοιτώντας ξανά αν οι εντολές που δώσαμε είναι σωστές και δεν έχουμε ξεχάσει κάτι (για την περίπτωση που το configuration έγινε μέσα από CLI).

6. Συμπεράσματα

Συνοψίζοντας, αξίζει τα σταθούμε στα παρακάτω.

- Η ραγδαία αύξηση της χρήσης του Internet άλλαξε το τοπίο με αποτέλεσμα εκτός από νέους τύπους κακόβουλων χρηστών να εμφανιστούν και άλλοι τρόποι επιθέσεων.
- Οι κίνδυνοι του Internet αλλά και το γεγονός ότι το IPv4 από μόνο του δεν προσφέρει κάποια ασφάλεια, ήταν οι δυο κύριοι λόγοι που οι μισθωμένες γραμμές έκαναν την εμφάνισή τους.
- Η εναλλακτική του IPv4, το IPv6, που έχει ενσωματωμένη το IPsec δε μπορεί ακόμη να χρησιμοποιηθεί ευρέως και βρίσκεται σε υβριδική μορφή.
- Το κόστος, η ταχύτητα των δεδομένων, η μεγάλη ανάπτυξη του Internet καθώς και των δυνατοτήτων των ISP σήμαναν το τέλος των μισθωμένων γραμμών και την ανάπτυξη των Virtual Private Networks (VPN).
- Τα βασικά χαρακτηριστικά ενός VPN είναι το κόστος, η επεκτασιμότητα, η ευελιξία, η εύκολη διαχείριση και, σαφώς, η ασφάλεια.
- Οι δυο κυριότερες μορφές VPN, είναι το SLL και το IPsec VPN.
- Αν και το SSL VPN έχει σαφώς πιο εύκολη εφαρμογή, καθώς οι εντολές είναι λιγότερες αλλα και επειδή οι όποιες ενέργειες, γίνονται από τη μεριά του end-point (server, firewall, εφαρμογή κτλ.), αυτό δε σημαίνει και το τέλος του IPsec VPN.
- Το κάθε ένα χρησιμοποιείται από διαφορετικούς χρήστες και εξυπηρετεί διαφορετικές ανάγκες οι οποίες είναι τόσο σημαντικές στους εκάστοτε χρήστες που δεν είναι δυνατόν να επικρατήσει το ένα από τα δυο. Σαφώς πιο πιθανό είναι, στο μέλλον, να έχουμε έναν νέο τύπο VPN που να έχει τα χαρακτηριστικά και των δυο και να τα αντικαταστήσει πλήρως.
- Στο πρακτικό κομμάτι της εργασίας χρησιμοποιήσαμε εργαλεία (ASDM, CCP) που χρησιμοποιούν και στον πραγματικό κόσμο οι network administrators, χωρίς την ανάγκη να έχουμε μπροστά μας το αντίστοιχο hardware.
- Ακριβώς επειδή το λογισμικό ήταν εικονικό και δεν είχαμε το 100% των δυνατοτήτων του (οι ελλείψεις ήταν ελάχιστες αλλά υπαρκτές), χρειάστηκε να κάνουμε ενέργειες που στην πραγματικότητα δε θα χρειαζόντουσαν, όπως η εγκατάσταση loopback adapters. Επίσης, και πάλι λόγω αυτών των ελαχίστων περιορισμών, χρειάστηκε να παρεκκλίνουμε λίγο από την πραγματική αναπαράσταση του IPsec VPN με την χρήση firewall ASA χρησιμοποιώντας σαν end-point την εξωτερική interface του firewall. Παρόλα αυτά η διαδικασία είναι ακριβώς η ίδια και το αποτέλεσμα ανταποκρίνεται στην πραγματικότητα.
- Χρησιμοποιήσαμε, όπου μπορούσαμε, τα πρωτόκολλα δρομολόγησης που είθισται να χρησιμοποιούνται και στην πραγματικότητα (iBGP και eBGP). Στα σημεία που αυτό δεν κατέστη δυνατό λόγω παλαιότητας του firmware του firewall, χρησιμοποιήσαμε στατική δρομολόγηση.
- Έγινε και χρήση GUI για την ευκολότερη διαμόρφωση των τοπολογιών, αν και σε πολλές περιπτώσεις ο συνδυασμός του GUI και του CLI ήταν αναπόφευκτος.

7. Βιβλιογραφία

1. Demystifying the IPsec Puzzle - Sheila Frankel
2. The Practice of Network Security: Deployment Strategies for Production Environments - Allan Liska
3. Packet-sniffer: A comparative study - Dr. Charu Gandhi, Gaurav Suri, Rishi P. Golyan, Pupul Saxena, Bhavya K. Saxena
4. An introduction to keyloggers: Rats and Malware - Rafay Baloch
5. Beginner's guide to Internet Protocol addresses - www.icann.org
6. Building VPNs: with IPsec and MPLS - Tan Nam Kee
7. A technical guide to IPsec virtual private networks - Tiller, James. S
8. Security Mechanisms for the IPv4 to IPv6 Transition - Abidah Hj Mat Taib, Rahmat Budiarto
9. Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks - Marc Blanchet
10. IPsec: Securing VPNs - Carlton Davis
11. IPsec VPN Design - Vijay Bollapragada, Mohamed Khalid, Scott Wainner
12. IPsec Virtual Private Network Fundamentals - James Henry Carmouche
13. VPNs Illustrated: Tunnels, VPNs, and IPsec - Jon C. Snader
14. VPNs: A Beginner's Guide - John Mairs
15. Firewall policies and VPN configurations - Henmi, Anne., Lucas, Mark., Singh, Abhishek., Cantrell, Chris.
16. Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services - Jazib Frahim, Omar Santos, Andrew Ossipov
17. Firewall Fundamentals - Wes Noonan, Ido Dubrawsky
18. SSL VPN: Understanding, evaluating and planning secure, web-based remote access: A comprehensive overview of SSL VPN technologies and design strategies - Joseph Steinberg, Tim Speed, J. Steinberg, T. Speed
19. Recent Advances in Networking - Hammed Haddadi, Olivier Bonaventure
20. Anti-Replay Window Protocols for Secure IP - Mohamed G. Gouda, Chin-Tser Huang, Eric Li
21. Computer Networks (5th edition) – Andrew S. Tanenbaum, David J. Wetheral
22. Computer Networking: A Top-Down Approach (6th Edition) - James F. Kurose, Keith W. Ross
23. http://www.esecurityplanet.com/network-security
24. http://searchtelecom.techtarget.com
25. http://www.kb.juniper.net/InfoCenter
26. www.cisco.com
27. www.ciscopress.com
28. www.enterprisenetworkingplanet.com
29. www.networkworld.com
30. www.quora.com
31. www.searchsecurity.com
32. www.ietf.org
33. www.ieee.org
34. www.technet.microsoft.com
35. www.gns3.com

8. Παράρτημα

Σε αυτό το κομμάτι της μεταπτυχιακής εργασίας θα παραθέσουμε τα configuration files από routers/firewalls που θα αποδεικνύουν τις κινήσεις που κάναμε στα προηγούμενα βήματα. Για να μειωθεί το μέγεθος των αρχείων έχουν διαγραφεί αρκετά από τα κενά ενδιάμεσα στις "γραμμές" του configuration, όπου αυτό είναι εφικτό.

8.1. IPsec VPN με IOS Routers

Παρατίθενται τα start-up configuration files από τα τέσσερα routers του παραδείγματος. Τρία από αυτά, το Athens, το Thessaloniki και το CA_Server, έχουν ένα επιπλέον configuration file , ένα private file που περιέχει αρχεία που ναι μεν χρησιμοποιούνται για τη σωστή λειτουργία του router, περιέχουν όμως πληροφορίες που δεν πρέπει να είναι εμφανείς σε κάποιον. Και ποιες πληροφορίες μπορεί να είναι αυτές; Μα φυσικά τα RSA key pairs.

8.1.1. Router Athens

8.1.1.1. Private configuration

kerberos password
crypto RSA-key-pair Athens.thesis.com 0 1470863560
30820275 02010030 0D06092A 864886F7 0D010101 05000482 025F3082 025B0201
00028181 00BB23F1 891769CA B05A0D1B DE84EB1C DE1D4F22 BF14BDEF 35BD3C91
3484B907 CFCD5C83 DE1A4CCF F74C35D8 59BDA219 AE0E4956 1A659428 07816B92
3E5E3326 D255FA84 2B7584EC 6CA502E5 8D2EC40F D9BB6E32 8A7A078F 2AA7FB45
2A340E7F FC38F795 E1DE2695 05862649 F3697792 198E4259 5B33267C 6853D339
C8033C4E A5020301 00010281 803E7B24 B489DDA7 6FB3D136 A1D7AD0C 0958ADC8
4315F0C8 421FF96D DDA40687 0629619F 2173947B C6EC69F9 DF14825F A28E608B
DFEA5449 FD1F87C3 DF10E271 2E2C98EF F5EABBD0 5F9A62A9 9A8B9F5C B177C242
6B42CE0E 5CD98FF4 DF4769A0 B48A2F83 5D5D17C4 B83756F7 947AD14D 95DF605A
D50C8147 CA362576 8A8BB89B 81024100 DF462E30 121BB5FD 799A073C A825CDE8
034616F6 8A521816 F9B99B8F D687D7E5 656AC94B F949BC50 4EC05DFC A19E0419
348F172A 5ADDE7C8 1A65EEA2 6B03FFE1 024100D6 91EEAFFF D6A36062 501FB093
CB0748BF 6CE34BE6 2582BE16 41C640AF 27D16011 43D86D50 737B4F4C D16B463A
734E875A 6349FD5F C8F5156E A1087571 0F374502 402CDC7D 0B4B9825 C8F855EA
7E558AC3 048B23DA 194F518F 658E67AC CA09E0E1 9046005E D1D514EB B177214F
C122F80C FAC384BC B2D5EF20 53247AB6 A80BB892 01024050 F6A5C301 5D632E66
4A677AC0 79B698EB AA51A5FD 04A06DCB 862C2192 360B1A1D C9A4EBB2 94B0ADBE
85B2DDC0 066C5644 73FCA23F B75B4B28 005969BF 2C87A502 405EAC45 3A7116B6
4AF3F7A7 8F38BF51 DECF9EEC 4B97CB7E 1F429EC7 51C8E5FC C87588A5 FAB82097
D8BF28A2 8D9D9882 FAE22A3C 011FEE28 BC2CDBCC 570E2216 1C
quit
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00BB23F1
891769CA B05A0D1B DE84EB1C DE1D4F22 BF14BDEF 35BD3C91 3484B907 CFCD5C83

```
 DE1A4CCF F74C35D8 59BDA219 AE0E4956 1A659428 07816B92 3E5E3326 D255FA84
 2B7584EC 6CA502E5 8D2EC40F D9BB6E32 8A7A078F 2AA7FB45 2A340E7F FC38F795
 E1DE2695 05862649 F3697792 198E4259 5B33267C 6853D339 C8033C4E A5020301 0001
 quit
end
```

8.1.1.2. Start-up configuration

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Athens
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name thesis.com
!
crypto pki trustpoint ca_server
 enrollment url http://10.1.1.1:80
 revocation-check none
!
crypto pki certificate chain ca_server
 certificate 04 nvram:testthesisco#7373.cer
 certificate ca 01 nvram:testthesisco#7373CA.cer
!
ip tcp synwait-time 5
!
crypto isakmp policy 1
 encr aes 256
 group 5
 lifetime 3600
!
crypto IPsec transform-set MYSET esp-aes esp-sha-hmac
mode tunnel
!
```

```
crypto map MYMAP 1 IPsec-isakmp
 set peer 210.169.200.1
 set transform-set MYSET
 set pfs group2
 match address 100
!
interface Loopback1
 ip address 172.16.10.1 255.255.255.0
!
interface GigabitEthernet1/0
 ip address 210.168.200.1 255.255.255.252
 negotiation auto
 crypto map MYMAP
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 network 172.16.10.0 mask 255.255.255.0
 network 210.168.200.0 mask 255.255.255.252
 neighbor 210.168.200.2 remote-as 100
 no auto-summary
!
no ip http server
no ip http secure-server
!
access-list 100 permit ip 172.16.10.0 0.0.0.255 192.168.10.0 0.0.0.255
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

```
line vty 0 4
 login
!
ntp clock-period 17179280
ntp peer 10.1.1.1
!
end
```

8.1.2. Router Thessaloniki

8.1.2.1. Start-up configuration

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Thessaloniki
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name thesis.com
!
crypto pki trustpoint ca_server
 enrollment url http://10.1.1.1:80
 revocation-check none
!
crypto pki certificate chain ca_server
 certificate 05 nvram:testthesisco#7373.cer
 certificate ca 01 nvram:testthesisco#7373CA.cer
!
ip tcp synwait-time 5
!
crypto isakmp policy 1
 encr aes 256
 group 5
 lifetime 3600
!
```

```
crypto IPsec transform-set MYSET esp-aes esp-sha-hmac
mode tunnel
!
crypto map MYMAP 1 IPsec-isakmp
 set peer 210.168.200.1
 set transform-set MYSET
 set pfs group2
 match address 100
!
interface Loopback1
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet1/0
 ip address 210.169.200.1 255.255.255.252
 negotiation auto
 crypto map MYMAP
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 network 192.168.10.0
 network 210.169.200.0 mask 255.255.255.252
 neighbor 210.169.200.2 remote-as 100
 no auto-summary
!
no ip http server
no ip http secure-server
!
access-list 100 permit ip 192.168.10.0 0.0.0.255 172.16.10.0 0.0.0.255
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
ntp clock-period 17179869
ntp peer 10.1.1.1
!
end
```

8.1.2.2. Private configuration

```
kerberos password
crypto RSA-key-pair Thessaloniki.thesis.com 0 1470863797
 30820276 02010030 0D06092A 864886F7 0D010101 05000482 02603082 025C0201
 00028181 00B5BE39 FB9C917A E8B228C3 86674B6B 5B02C7E0 D58F798B D2AF25D5
 7234EEE4 AEA9E925 9B7A9867 54829C26 94227518 F82E7ADC CD780615 4B3BB6FD
 F25C02F3 2B012E3C 23C7752D 410D890B 92987116 40E750A5 7A9EE54D 627EECC6
 0137FAD4 74FC3904 1C91CC23 2EF90BAC 3AB7BADE CF8C4451 50DE536F 0E2387B7
 5AABB3EA B7020301 00010281 803CD86B E71DFAE2 B046FD38 C0A5926D 65B1DFA3
 193C888F D4404925 55AFFD0E D89F0FEC 444A5DFD B2206C10 CA6562D8 B2363571
 F8E426FD 380BCCEE E61601F2 D0B116C2 744E5F5C A5C8DBEF EC17239A 8ED8521D
 C6F7AD97 7A0DC6EC BA4F3578 4706C3ED E54ABB35 865F4547 94AB4331 E2C0F03A
 37EF2F45 9EB1A474 85011754 B9024100 E9B31726 AD1A18D1 A9B67C0C D0C275FF
 952499C1 6CF192E0 AFCE3660 CC604962 C62FA136 D4D8B92A 6935DB30 F8A9C62B
 84A37EF1 8EAF672E A7E2C124 74095353 024100C7 15EBD6F9 9EC67B57 E6C28882
 702C2E1B 13ED77DC D47B12FC 99A321D9 B0C9AC89 E48241EA BA96F470 85F70155
 F755146D 26108625 E4378030 B08BBD34 80228D02 410081F4 D13EF4AB BA797D02
 B960F705 EC504043 A62CE5C4 408529BE 6686D5A0 05AF23BE 80CBD8F8 DB9F35FA
 78F57692 125D48D9 125289A2 08A2ED41 2F5E7218 6D790240 07AC62A0 B0925C18
 18F53DFE 40F8CDDB 21140D8D 1727E16E 83E9F00D B7F44671 AE06EEB6 57B3C569
 BA848F56 AFD78EA1 F0EB0CAB FEFDE2DD C002AE00 26EBE169 02405E24 E15D5E77
 08B91F14 443ECD85 AAE4A1D0 DFBAB173 2C79CD59 34C52ACD BF5DA2AC B4CD88D2
 CF9D4F40 5F4AA756 25DFD1EF 8E5EF55C 09B4242B CB41E786 871B
 quit
 30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B5BE39
 FB9C917A E8B228C3 86674B6B 5B02C7E0 D58F798B D2AF25D5 7234EEE4 AEA9E925
 9B7A9867 54829C26 94227518 F82E7ADC CD780615 4B3BB6FD F25C02F3 2B012E3C
 23C7752D 410D890B 92987116 40E750A5 7A9EE54D 627EECC6 0137FAD4 74FC3904
 1C91CC23 2EF90BAC 3AB7BADE CF8C4451 50DE536F 0E2387B7 5AABB3EA B7020301 0001
 quit
end
```

8.1.3. Router CA_Server

8.1.3.1. Start-up configuration

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CA_Server
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name thesis.com
!
crypto pki server ca_server
 issuer-name cn=test.thesis.com c=greece l=athens
 grant auto
!
crypto pki trustpoint ca_server
 revocation-check crl
 rsakeypair ca_server
!
crypto pki certificate chain ca_server
 certificate ca 01 nvram:testthesisco#7373CA.cer
!
ip tcp synwait-time 5
!
interface Serial4/0
 ip address 10.1.1.1 255.255.255.0
 serial restart-delay 0
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 10.1.1.0 mask 255.255.255.0
 neighbor 10.1.1.2 remote-as 100
```

```
 no auto-summary
!
ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
ntp master 3
!
end
```

8.1.3.2. Private configuration

```
kerberos password
crypto RSA-key-pair test 0 1470855451 1 0
 308204BE 02010030 0D06092A 864886F7 0D010101 05000482 04A83082 04A40201
 00028201 0100C460 008E4A66 2FAF6588 4EABB65B 45B5553F 5330EF85 5D26628E
 06D5FDDA 9DA46C31 0FD297C7 0F947B69 8C6532F3 0E38774E 0399C393 39AA297F
 3B29D99F B786A2A1 50356CC9 6C1EC647 8E3363F2 F89210D7 CB08B475 22B54127
 B91AC249 EBD0BDC9 50CA3EFE 814A35C2 3BA6E36A 42BDDA86 26FCD4B5 34297C54
 2E3C5983 DEA0A48B CDDC5B56 A76AB029 C1033F8E D6A63101 4CD2B451 A4B5D83A
 6EFF07F3 7182B3AE CCD2F630 754F779B 782C0AB5 184A3D9B 56E91ADE 40B99461
 0074F844 2D773F13 52B268B1 D99AA9E3 9DD771FF D72DF8AC 0000C0D2 E6698D3B
 101AFB16 7C4A717C 1D97CCF3 F40D4EF3 F3A89C27 9BBC23E7 BF8B23FA E7DA7AA4
 D0D9E2AA F4BF0203 01000102 82010100 933D744D 3C45A04D 7FF09324 36E7FABD
```

7AFCAF30 CAF7111F FDD78612 9F7372AD DD1D7042 B3E0E2B2 AF52359D 8F7524DD
7BBEF7FE 2BE150E4 6096F052 71C54AC3 5D5F5C97 A248E893 AE91EA72 67E7BF2F
2E07CF49 689D4777 E631959E 15BD7D5E 175F41FF 52FA5B10 BC7C3563 EDB237F6
C849BC23 E88D315E 45C58CA1 5D70FDD3 DE94C926 DA03660B 35867992 0E057CB1
63AF8541 174805EE 40EAAFE8 2BBC618E B8FCD7EB 15CAFF89 ABF3BBC6 C306612D
C85CC5E0 3946CECE 94919D15 CE49C5B6 7CA8BB7C 685268D7 206761D5 1CF832AE
43C5BF95 2FC3B2C8 C05360B9 444D37C2 31A6BE20 1A021831 20B5D626 6175A0B6
DD99C108 446262E0 3BB81E60 AC263931 02818100 EE247518 E423E20D 97407617
573A57FB 6B3DD46A FDD170C5 0DFA413F 1E31C78E 00F87B71 55548291 24494161
3638851B A19BABC1 A7BF2BC0 88789BC6 C1A7CBF8 E7E9D3FE C415CBF0 9FFF901E
BAC3416E 9047C926 15599FEA 028DB700 098A1092 18119135 557F01BE 603FD34D
7B4A28E6 5CA14E2C BC582E84 9378B8E7 F39BB697 02818100 D319BFDD 98BF6024
19A06DDC 3BD0176A 9CEA2870 265B9FD9 0F839D37 A65707AD 9280B735 F39EC629
14901758 0A5007E4 F64A5FE5 066BAE0C 3A09ECBE DDE8454C 15EE1E7C F1297B06
0FCBC66D E519F133 A6530E8D 5C71693B F5F47085 00B22231 7D126161 1884EC74
E8126442 1A5BA9D0 D7DABD3B 836265F7 6EA62169 851EE019 02818042 59FE1655
5A7A1D77 4B0A9C2E 3D9F4DF9 EF5C4403 3C5BC34B C5B27037 A57F085D D4DDF011
EA5E06BA A97E81EB 6D8C08CA DA68DCA8 3467A859 5DE1695B 83B91D3C E0B5A482
55E060C6 F399E036 013935E9 15574239 28A399BB E4685CA6 4BC59A2F 029606DA
2F6CF8F2 30565B7C 42896AC5 DC5BBFB3 2A8EAB79 BB65299B 82833902 8181009D
87D79FFB FEC435EC 51C5E9D5 50C248B2 F4225D1E A2BD3473 D959974F B01E70AE
A5131355 CBA440BF B18F5A09 C8133C0F 770CFC91 C0054FE6 77C58DE1 77154F64
06200648 C9159F3E 66689B55 9DF85AFC C17A588F 25AACC2E 0CCD72D3 441B3427
0B7253CC C254DA20 DCA8A893 96D7B09B 840636C5 22C6C8D0 6F74FB93 75A8F102
81802C11 9D57D4A0 6FEEB76D 5A4F2C17 60609255 21AD2A23 D202674B E9DF4F19
F1BE81A0 43BFA554 0D846631 465F3BF8 5AB34DEB 57B068CB B4E8BCD4 BA056FA5
E8C285D9 CEB8C16F 0253D3EA 7F938FEA E2A56DD8 09AB6AD6 614079CE D7716817
49D37A38 17846DC5 AF79A0AB 16F7F1F1 724C9288 030932C1 951E2304 5003C25C 163E
quit
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C46000 8E4A662F AF65884E ABB65B45 B5553F53 30EF855D 26628E06 D5FDDA9D
A46C310F D297C70F 947B698C 6532F30E 38774E03 99C39339 AA297F3B 29D99FB7
86A2A150 356CC96C 1EC6478E 3363F2F8 9210D7CB 08B47522 B54127B9 1AC249EB
D0BDC950 CA3EFE81 4A35C23B A6E36A42 BDDA8626 FCD4B534 297C542E 3C5983DE
A0A48BCD DC5B56A7 6AB029C1 033F8ED6 A631014C D2B451A4 B5D83A6E FF07F371
82B3AECC D2F63075 4F779B78 2C0AB518 4A3D9B56 E91ADE40 B9946100 74F8442D
773F1352 B268B1D9 9AA9E39D D771FFD7 2DF8AC00 00C0D2E6 698D3B10 1AFB167C
4A717C1D 97CCF3F4 0D4EF3F3 A89C279B BC23E7BF 8B23FAE7 DA7AA4D0 D9E2AAF4
BF020301 0001
Quit

crypto RSA-key-pair ca_server 0 1470855801
30820278 02010030 0D06092A 864886F7 0D010101 05000482 02623082 025E0201

00028181 00B3B8AE CFE537B5 3DB4524C 9AC482D0 9DE44CDB 52B99485 E03A2573
5953EDA0 A7283347 8C3F0A7A ED474217 BB3337D8 AC02C7E2 83B0B6DE 2BB5A05E
577E4CCF 18FF951A E6AD1533 DEFEA59A AFFAC8CD 20AE1636 9327200E E3AC4A95
6B384C8C 0A0D0D04 EB4621E6 321434C8 9D61666A A22922CD 4A7523B3 00127C26
5EF85FFC 97020301 00010281 8100AAA3 928F5FD2 B9E9E159 36D4C7FA 70BB4975
D3D442D2 0B1EAFF6 B903BA95 67B0EE91 69C07666 ABFAB86A BF7F858C E3D3C63C
250CE66F 6A98D3B5 757DDB34 707872A5 8B5237A3 14F4AC6E 44551A4B EAC1AAD6
8A429BC8 6DCFB2B3 03ED1718 15F918FB 501CE743 9151E0A3 D65DA273 06D66E68
EB45EA94 6CD2E549 FAFB88C5 7B290241 00E49C3E 96BADBA0 A800A2C3 3070B227
675CA002 DC78F470 0B2E2F2E 2B484CE3 238050AE 09C97BB8 72C048A2 4CEAC7AE
7119C4E9 553F1E64 B4C977E8 641F6579 85024100 C940F4CC E76B87B8 94AB7590
894A4DC6 3ADCB349 843F5EAE 7E667BAD 03BCC6CA FB38EB09 764B86B3 5E486EDD
53AD2004 B8A91E3D 28B6DD5D 61F81790 7B8B0A6B 02410095 0BE9228C A1349554
14C9FD82 FC240497 B71B2673 15AB171E FD53B494 66CC9010 D0892788 5D495C47
5113BFE2 325DE10F 53FA6CC1 C2271657 63FDF789 20B7A102 4049AA9A 30EAC0C4
943EEF28 00791096 B969D061 5C16A96F 89E5C0B3 A2980CA0 A3AA23A2 7CFB2D18
284DE9AB 931E4EEF BA6AB194 DD042B33 8A3C1328 E4FD23DE F3024100 D2134CF2
8B2806A4 40513624 09BDF4C1 6C3C085D 41D63E69 AE1DFEF5 0E1E9511 E5D2E1DB
6062C3E2 AF60E289 7D49D720 B03F1836 B423FF9D F8C317F3 032B
D906
quit
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B3B8AE
CFE537B5 3DB4524C 9AC482D0 9DE44CDB 52B99485 E03A2573 5953EDA0 A7283347
8C3F0A7A ED474217 BB3337D8 AC02C7E2 83B0B6DE 2BB5A05E 577E4CCF 18FF951A
E6AD1533 DEFEA59A AFFAC8CD 20AE1636 9327200E E3AC4A95 6B384C8C 0A0D0D04
EB4621E6 321434C8 9D61666A A22922CD 4A7523B3 00127C26 5EF85FFC 97020301 0001
quit
end

8.1.4. Router Internet

8.1.4.1. Start-up configuration

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Internet
!
boot-start-marker
boot-end-marker
!
no aaa new-model
```

```
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 210.168.200.2 255.255.255.252
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 210.169.200.2 255.255.255.252
 negotiation auto
!
interface Serial4/0
 ip address 10.1.1.2 255.255.255.0
 serial restart-delay 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 10.1.1.0 mask 255.255.255.0
 network 210.168.200.0 mask 255.255.255.252
 network 210.169.200.0 mask 255.255.255.252
 neighbor 10.1.1.1 remote-as 200
 neighbor 210.168.200.1 remote-as 300
 neighbor 210.169.200.1 remote-as 400
 no auto-summary
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
```

```
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
ntp clock-period 17181657
ntp peer 10.1.1.1
!
End
```

8.2. IPsec VPN με ASA

8.2.1. Firewall Start-up configuration

```
ASA Version 8.4(2)
!
hostname FirewallPatra
enable password 8Ry2YjIyt7RRXU24 encrypted
password 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 210.169.200.1 255.255.255.252
!
interface GigabitEthernet1
 nameif management
 security-level 0
 ip address 10.10.10.1 255.255.255.0
!
interface GigabitEthernet2
 nameif inside
```

```
 security-level 100
 ip address 192.168.10.1 255.255.255.0

ftp mode passive
access-list MYLIST extended permit ip host 210.169.200.1 172.16.10.0 255.255.255.0
pager lines 24
logging enable
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

route outside 0.0.0.0 0.0.0.0 210.169.200.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto IPsec ikev1 transform-set MYSET esp-aes-256 esp-sha-hmac
crypto map IPSEC 1 match address MYLIST
crypto map IPSEC 1 set peer 210.168.200.1
crypto map IPSEC 1 set ikev1 transform-set MYSET
crypto map IPSEC interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 3600
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
```

```
no threat-detection statistics tcp-intercept
tunnel-group 210.168.200.1 type IPsec-l2l
tunnel-group 210.168.200.1 IPsec-attributes
 ikev1 pre-shared-key *****
!
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
crashinfo save disable
Cryptochecksum:ba879f0b9eade1ca04d1608bf4b60403
```

8.2.2. Router Athens Start-up configuration

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Athens
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
!
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key 6 Ky2#$4TipL address 210.169.200.1
!
crypto IPsec transform-set MYSET esp-aes 256 esp-sha-hmac
!
crypto map MYMAP 1 IPsec-isakmp
```

```
 set peer 210.169.200.1
 set transform-set MYSET
 match address 100
!
interface Loopback1
 ip address 172.16.10.1 255.255.255.0
!
interface GigabitEthernet1/0
 ip address 210.168.200.1 255.255.255.252
 negotiation auto
 crypto map MYMAP
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 172.16.10.0 mask 255.255.255.0
 network 210.168.200.0 mask 255.255.255.252
 neighbor 210.168.200.2 remote-as 100
 no auto-summary
!
ip route 192.168.10.0 255.255.255.0 210.168.200.2
ip route 210.169.200.0 255.255.255.252 210.168.200.2
!
no ip http server
no ip http secure-server
!
access-list 100 permit ip 172.16.10.0 0.0.0.255 host 210.169.200.1
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

8.2.3. Router Internet Start-up configuration

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Internet
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
!
interface GigabitEthernet1/0
 ip address 210.168.200.2 255.255.255.252
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 210.169.200.2 255.255.255.252
 negotiation auto

router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 210.168.200.0 mask 255.255.255.252
 neighbor 210.168.200.1 remote-as 200
 no auto-summary
!
no ip http server
no ip http secure-server
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
```

```
!
End
```

8.3. SSL VPN

8.3.1. Router Start-up configuration

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 33.33.33.1 255.255.255.0
 duplex half
!
interface GigabitEthernet1/0
 ip address 210.168.200.1 255.255.255.0
 negotiation auto
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
 shutdown
!
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
```

8.3.2. Firewall Start-up configuration

```
ASA Version 8.4(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 210.168.200.2 255.255.255.0
!
interface GigabitEthernet1
 nameif management
 security-level 0
 ip address 10.10.10.1 255.255.255.0
!
ftp mode passive
pager lines 24
mtu outside 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-649.bin
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 10.10.10.2 255.255.255.255 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ca trustpoint TrustPoint0
 enrollment self
 fqdn sslvpn.test.com
 subject-name CN=sslvpn.test.com
 keypair sslvpnkey
 crl configure
crypto ca certificate chain TrustPoint0
 certificate 811ce057
    308201eb 30820154 a0030201 02020481 1ce05730 0d06092a 864886f7 0d010105
    0500303a 31183016 06035504 03130f73 736c7670 6e2e7465 73742e63 6f6d311e
    301c0609 2a864886 f70d0109 02160f73 736c7670 6e2e7465 73742e63 6f6d301e
    170d3136 30393139 31373138 33345a17 0d323630 39313731 37313833 345a303a
    31183016 06035504 03130f73 736c7670 6e2e7465 73742e63 6f6d311e 301c0609
    2a864886 f70d0109 02160f73 736c7670 6e2e7465 73742e63 6f6d3081 9f300d06
    092a8648 86f70d01 01010500 03818d00 30818902 818100bb 06caa0b0 d79004e3
    8011646c 87e98807 f2bbd918 cb29bd8b a092a2d7 f66ed103 a146f054 1bb47cf2
    26a3a38b c2346427 87f13fd6 838325d1 ab0063e9 599e26ec 1bf6f043 ced34cf2
    8f2a49f0 f90e8c64 7c707b89 bb0bb311 e39fd6dc c79a17f7 c2368499 09534b3b
    197183e9 7e42aadc f45a690f ffa7b8d4 3a33cd74 29088d02 03010001 300d0609
    2a864886 f70d0101 05050003 8181000d fd449af4 7aea6bdc 8ef9c679 ddf0a291
    863867e0 9546f9ca 6cf18794 7a7de1b4 1695f826 2282d78d 0bd2bc33 b7d5f7f3
    718684f7 7213109f 8be10b31 8190b8ac bc7357ef a959a300 4a44b5a3 7e1d66aa
    dacf310e 1ad6c5fe 3886ee92 70888643 1f3fdc23 bfb7e744 6b693c22 fa3f9aa5
    045194f4 e7b4dd91 6710e53a 80a7ed
  quit
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
```

```
no threat-detection statistics tcp-intercept
ssl trust-point TrustPoint0 outside
webvpn
 enable outside
group-policy new-GP internal
group-policy new-GP attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  url-list none
username jim password T28PmZJh9ryTSu7B encrypted privilege 15
username user1 password NcPLCME0rhZMzney encrypted privilege 0
username user1 attributes
 vpn-group-policy new-GP
tunnel-group test_conn type remote-access
tunnel-group test_conn general-attributes
 default-group-policy new-GP
tunnel-group test_conn webvpn-attributes
 group-alias home enable
 group-url https://210.168.200.2/home enable
!
crashinfo save disable
Cryptochecksum:76a30b4ef4cadbaa5e8af74eba58a2b3
: end
```