ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ
Τμήμα Εφαρμοσμένης Πληροφορικής στην Οικονομία και στην Διοίκηση

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Θέμα: «ΣΧΕΔΙΑΣΜΟΣ, ΥΛΟΠΟΙΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΕΝΟΣ IPSec VPN ΔΙΚΤΥΟΥ-ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΔΡΑΣΤΙΚΟΥ ΣΤΑΘΜΟΥ ΠΛΗΡΟΦΟΡΗΣΗΣ (INFOKIOSK)»

Σπουδαστής: **Δημήτριος Τόλης**

Α.Μ 11987

Επιβλέπων : Δρ. Αριστογιάννης Γαρμπής
Επίκουρος Καθηγητής

Αθήνα Σεπτέμβριος 2009

ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ

ΣΧΕΔΙΑΣΜΟΣ,ΥΛΟΠΟΙΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΕΝΟΣ IPSec VPN ΔΙΚΤΥΟΥ-ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΔΡΑΣΤΙΚΟΥ ΣΤΑΘΜΟΥ ΠΛΗΡΟΦΟΡΗΣΗΣ (INFOKIOSK)

Δημήτριος Τόλης

Αθήνα Σεπτέμβριος 2009

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κ. Αριστογιάννη Γαρμπή, για την συμπαράστασή του και την συνδρομή του στην εκπόνηση αυτής της πτυχιακής εργασίας, αλλά κυρίως για την υποδειγματική του παρουσία και διδασκαλία όλα αυτά τα χρόνια της φοίτησης μας στη σχολή.

ΠΡΟΛΟΓΟΣ

Σκοπός της πτυχιακής εργασίας είναι η μελέτη ενός Ιδεατού Ιδιωτικού Δικτυού (Virtual Private Network - VPN). Η εργασία χωρίζετε σε δυο μέρη. Το πρώτο είναι το κυρίως κομμάτι της πτυχιακής και εξετάζει την δημιουργία VPN με την χρησιμοποίηση της σουίτας πρωτοκόλλων IPSec (Internet Protocol Security). Η εργασία περιγράφει ένα παράδειγμα υλοποίησης μιας IPsec site-to-site VPN σύνδεσης ανάμεσα σε δυο linux μηχανήματα στα οποία έχει εγκατασταθεί το StrongSwan. Και οι δυο υπολογιστές λειτουργούν ως VPN gateways. Το StrongSwan είναι ένα λογισμικό ανοιχτού κώδικα που υλοποιεί το IPSec πρωτόκολλο. Μεταξύ άλλων υποστηρίζει το IKEv2 πρωτόκολλο, παρέχει αυθεντικοποίηση μέσω X.509 πιστοποιητικών και είναι συμβατό με την τεχνολογία NAT-T. Το δεύτερο μέρος σχετίζεται με την απομακρυσμένη διαχείριση ενός νεοαποκτηθέντος διαδραστικού σταθμού πληροφόρησης (Infokiosk Friendlyway Impress 40") που προμηθεύτηκε το Τ.Ε.Ι Μεσολογγίου.

Εταιρίες και οργανισμοί μπορούν να χρησιμοποιήσουν ένα VPN δίκτυο για να επικοινωνήσουν με ασφάλεια μέσω ενός δημόσιου δικτύου από το οποίο επιτρέπεται η διέλευση ομιλίας, βίντεο και δεδομένων. Επίσης εξασφαλίζει την επικοινωνία κάθε απομακρυσμένου γραφείου/καταστήματος ή ακόμα και με κάθε στέλεχος της εταιρίας που βρίσκεται εκτός γραφείου, με τα κεντρικά γραφεία της επιχείρησης σε ένα "ιδιωτικό περιβάλλον".

Το IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών μέσα από ένα δημόσιο προσβάσιμο μέσο. Το IPsec είναι το πιο δημοφιλές και καλοσχεδιασμένο πρωτόκολλο στην εποχή μας. Είναι βασισμένο στις προδιαγραφές που ανέπτυξε η ομάδα εργασίας της Internet Engineering Task Force (IETF). Το IPsec σχεδιάστηκε με στόχο να παρέχει υψηλής ποιότητας επιπέδου ασφάλεια βασισμένη στην κρυπτογράφηση, σε IPv4 και IPv6 δίκτυα. Οι προσφερόμενες υπηρεσίες ασφάλειας που προσφέρει περιλαμβάνουν έλεγχο πρόσβασης, ακεραιότητας των δεδομένων, αυθεντικοποίηση της προέλευσης των δεδομένων, προστασία από replay επιθέσεις, εμπιστευτικότητα (κρυπτογράφηση). Στο IPSec οι παραπάνω υπηρεσίες υλοποιούνται σε επιπέδου δικτύου προσφέροντας προστασία στο IP πρωτόκολλο αλλά επίσης και σε πρωτόκολλα ανώτερων στρωμάτων.

Εάν και τα VPN μπορούν να μειώσουν το ρίσκο της επικοινωνίας μέσα από ένα δημόσιο προσβάσιμο μέσο δεν μπορούν όμως και να το εξαλείψουν. Για παράδειγμα, μια VPN υλοποίηση μπορεί να έχει κενά ασφαλείας εξαιτίας αδυναμιών ενός αλγορίθμου ή λογισμικού που χρησιμοποιήθηκε. Επίσης, μπορεί να έγινε η παραμετροποίηση ενός VPN δικτύου με λανθασμένες ρυθμίσεις.

Στο τέλος, το IPSec VPN δίκτυο που θα υλοποιηθεί αξιολογείται με βάση ορισμένα κριτήρια όπως: η απόδοση, το κόστος και πότε συμφέρει μια εταιρία να επενδύσει στην δημιουργία VPN σε σύγκριση με hardware VPN επιλογές που κυκλοφορούν στην αγορά.

ABSTRACT

The purpose of this project is to study Virtual Private Network (VPN). The project is separated in two parts. The first one is the main part which involves a VPN construction by using Internet Protocol Security (IPsec). The project describes an example implementation for IPsec site-to-site VPN and step-by-step procedure that can be used to set up a VPN connection between two Linux computers with the StrongSwan. Both computers act as VPN gateways. StrongSwan is an open source IPsec implementation for the Linux operating system. It supports IKEv2 key exchange protocol, provides authentication based on X.509 certificates and it is compatible with NAT-T technology. The second part describes Infokiosk remote control (Infokiosk Friendlyway Impress 40") of TEI.

Companies and organizations use a VPN to communicate confidentially over a public network and can be used to send voice, video or data. It's an excellent option for remote workers and organizations with global offices and partners to share data in a private manner.

IPSec is a framework of open standards for ensuring private communications over public networks. IPSec is the most well known VPN protocol today, developed by IETF in order to provide security over the standard IP networks. IPSec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols

Although VPNs can reduce the risks of networking, they cannot totally eliminate them. For example, a VPN implementation may have flaws in algorithms or software, or a VPN may be set up with insecure configuration settings and values.

At the end of the project the IPSec VPN network is evaluated in terms of performance cost and when a company is benefitted by investing to the construction of VPN in compassion with hardware VPN solutions available in the market.

Α΄ ΜΕΡΟΣ

Πίνακας περιεχομένων

Ευρετήριο Σχημάτων

Ευρετήριο Πινάκων

Παραρτήματα

Β΄ ΜΕΡΟΣ

Πίνακας περιεχομένων

Ευρετήριο Σχημάτων

Παραρτήματα

πιστωτικών καρτών κ.α.) να "ταξιδεύουν" στο διαδίκτυο χωρίς καμία ασφάλεια. Μέσα σε ορισμένα λεπτά, με τα εργαλεία που υπάρχουν σε αφθονία στο διαδίκτυο, ακόμα και ένας χρήστης με περιορισμένες γνώσεις θα μπορούσε να βρεθεί με έναν "θησαυρό" δεδομένων στα χέρια του. Οπότε, καθιστάτε σαφές ότι η ασφάλεια τέτοιου είδους συνδέσεων είναι ένα κρίσιμο σημείο για την επιβίωση τους.

Η ανάπτυξη και ο σχεδιασμός των VPNs όμως, έγινε με γνώμονα αυτή την παράμετρο παρέχοντας μηχανισμούς κρυπτογράφησης των δεδομένων. Σήμερα ο λόγος που η τεχνολογία VPN είναι τόσο δημοφιλής οφείλεται στο ότι είναι ένα προϊόν που προσφέρει ένα πολύ αυξημένο επίπεδο ασφάλειας σε συνδυασμό με το μικρό κόστος του, συγκριτικά με τεχνολογίες που προσφέρουν τα ίδια αποτελέσματα.

Το κόστος είναι ένα ακόμα λόγος για την εξάπλωση την VPN. Οι επιχειρήσεις για να καλύψουν αυτές τις ανάγκες πριν από την δημιουργία των VPN χρησιμοποιούσαν δίκτυα μισθωμένων γραμμών, που είχαν σαν μειονέκτημα τα υψηλά μηνιαία τέλη για την παροχή αυτών των υπηρεσιών. Εν αντίθεση, τα VPNs χρησιμοποιούν το διαδίκτυο ως μέσο σύνδεσης , ελαχιστοποιώντας το κόστος. Σύμφωνα με μελέτη της Infinities (εταιρία διαχείρισης δικτύων και παροχής συμβουλευτικών υπηρεσιών) το κόστος LAN-to-LAN σύνδεσης μειώνεται κατά 20% με 40% σε σχέση με αυτό των δικτύων μισθωμένων γραμμών. Επιπλέον η αντίστοιχη μείωση του κόστους για απομακρυσμένη πρόσβαση πέφτει κατά 60% με 80%. Η λίστα όμως με τα πλεονεκτήματα της χρήσης VPNs δεν σταματούν εδώ διότι προσφέρουν μειωμένα έξοδα διαχείρισης συγκρινόμενα με αυτά της ιδιοκτησίας και λειτουργίας ιδιωτικού δικτύου. Οι επιχειρήσεις μπορούν να αναθέσουν τη λειτουργία μέρους ή και όλου του WAN τους σε κάποιον πάροχο υπηρεσιών έτσι ώστε να επικεντρωθούν στη δουλειά τους και να μην διαχειρίζονται το WAN δίκτυο ή αυτό που παρέχει δυνατότητα απομακρυσμένης πρόσβασης και τέλος προσφέρουν απλοποίηση των δικτυακών τοπολογιών μειώνοντας έτσι το φόρτο διαχείρισης: η χρησιμοποίηση ενός IP backbone μειώνει δραστικά τα μόνιμα εικονικά κυκλώματα (PVCs) που σχετίζονται με πρωτόκολλα σύνδεσης όπως τα Frame Relay και ATM δημιουργώντας μια εντελώς μπερδεμένη δικτυακή τοπολογία την ίδια στιγμή που μειώνουν τη συνθετότητα και το κόστος του δικτύου.

Παρ όλα αυτά, η υλοποίηση Virtual Private Network βρίσκεται ακόμα σε στάδιο ανάπτυξης, με ότι αυτό και εάν συνεπάγεται. Μάλιστα συμφώνα με το Internetworking Technologies Handbook της Cisco τα Virtual private networks (VPNs) είναι ένα αρκετά "δονκιχωτικό" θέμα (quixotic subject) διότι δεν υπάρχει ένα μοναδικά καθορισμένο προϊόν, ούτε μια γενική παραδοχή μεταξύ των κατασκευαστών σχετικά με το από τι αποτελείται εάν VPN. Αυτός είναι άλλωστε και ο λόγος για την ύπαρξη πολλών πρωτοκόλλων για την υλοποίηση ενός VPN. Επιπλέον ένα VPN σύστημα μπορεί να πραγματοποιηθεί τόσο με software όσο και σε hardware μηχανήματα.

Ένα από πρωτόκολλα με την χρήση του οποίου μπορούμε να υλοποιήσουμε VPN δίκτυο είναι το IPSec (Internet Protocol Security suite). Θεωρείτε το πιο καλοσχεδιασμένο και ασφαλές πρωτόκολλο και είναι αυτό που θα χρησιμοποιηθεί για την υλοποίηση του VPN δικτύου στην παρούσα εργασία. Η υλοποίηση θα βασιστεί σε open source λογισμικό, με στόχο όσο είναι εφικτό, την κατασκευή ενός VPN συστήματος με μηδαμινό κόστος. Στο τέλος θα πραγματοποιηθεί σύγκριση μεταξύ του open source VPN που θα έχει δημιουργηθεί σε σχέση με εμπορικές λύσεις που βασίζονται σε hardware επιλογές, για να αξιολογηθεί η αξία της εργασίας.

Το παρακάτω κεφάλαιο ασχολείται με την δημιουργία ενός πλαισίου αναφοράς για τα VPNs, τα απαραίτητα συστατικά στοιχειά που συνθέτουν τα VPNs και γίνεται αναφορά των διαφορετικών αρχιτεκτονικών που υπάρχουν. Ο κύριος όμως σκοπός του είναι η θεωρητική προσεγγίσει της λειτουργιάς του IPSec, οπού και βασίζεται η υλοποίηση της πτυχιακής.

ΚΕΦΑΛΑΙΟ 2

2. Τι είναι τα Virtual Private Networks

Ένα virtual private network (VPN) είναι ένα δίκτυο ιδιωτικών δεδομένων που χρησιμοποιεί την υπάρχουσα δημόσια τηλεπικοινωνιακή υποδομή, παρέχει ιδιωτικότητα χρησιμοποιώντας πρωτόκολλα διόδου (tunneling protocol) και άλλες διαδικασίες ασφαλείας. Μάλιστα, συμφώνα με την Internet Engineering Task Force (IETF)[1], που αναπτύσσει και προωθεί Internet standards, έχει ορίσει τα VPNs ως "εξομοίωση ενός προσωπικού Wide Area Network (WAN), χρησιμοποιώντας ένα κοινόχρηστο ή δημόσια προσβάσιμο μέσο επικοινωνίας, όπως το Internet και τα IP δίκτυα". Ένα virtual private network μπορεί να κατασκευαστεί με ένα σύστημα ιδιόκτητων ή μισθωμένων γραμμών (leased lines) που μονό η εταιρία θα μπορεί να χρησιμοποιεί. Ο κυρίως σκοπός ενός VPN είναι να δώσει στην επιχείρηση τις ίδιες δυνατότητες με τις ιδιωτικές γραμμές σε πολύ όμως, χαμηλότερο κόστος, εξαιτίας της χρησιμοποίησης του δημόσιου τηλεπικοινωνιακού δικτύου. Για να το φανταστούμε καλυτέρα ας σκεφτούμε τις τηλεπικοινωνιακές εταιρίες. Παρέχουν στους πελάτες τους ιδιωτικές τηλεφωνικές γραμμές χρησιμοποιώντας το δημόσιο δίκτυο. Με ένα ιδεατό ιδιωτικό δίκτυο έχουμε τις ίδιες δυνατότητες με την διαφορά ότι έχουμε ταυτόχρονη μεταφορά φωνής και ψηφιακών δεδομένων από την ίδια γραμμή με το ίδιο επίπεδο ασφάλειας. Γενικά τα VPNs δίκτυα παρέχουν:

- Ασφάλεια απόρρητου (Confidentiality) → Τα δεδομένα στέλνονται κρυπτογραφημένα
- Πιστοποίηση αυθεντικοποίησης (Authentication) → αυτός που στέλνει τα δεδομένα είναι έγκυρος και αυτός που τα παίρνει σωστός
- Ακεραιότητα δεδομένων (Data integrity) → Τα δεδομένα στέλνονται χωρίς να τροποποιηθεί το περιεχόμενο τους
- Προστασία από διάφορες επιθέσεις δικτύου (Network attacks). (π.χ replay attack και flooding)

2.1 VPN τεχνολογίες

Υπάρχουν τρείς κύριες κατηγορίες VPN τεχνολογιών: trusted VPNs, secure VPNs, και hybrid VPNs. Πρέπει να σημειωθεί ότι τα secure VPNs και τα trusted VPNs δεν ανήκουν στην ίδια οικογένεια από τεχνικής πλευράς και μπορούν να συνυπάρξουν σε ένα μονό σύστημα VPN.

2.1.1 Trusted VPNs

Με το πέρασμα τον χρονών, οι υλοποιήσεις αξιόπιστων ιδεατών εικονικών δικτύων (trusted VPNs) έχουν μετακινηθεί από τα μισθωμένα ιδιωτικά κυκλώματα των τηλεπικοινωνιακών κατασκευαστών σε μισθωμένα ιδιωτικά IP δίκτυα από τους τηλεπικοινωνιακούς παρόχους.

[1] Η IETF είναι ένας οργανισμός που αναπτύσσει και προωθεί δικτυακά πρότυπα (Internet standard), βλέπε http://www.ietf.org/

Ένα μισθωμένο κύκλωμα περνάει μέσα από έναν ή και περισσότερους διαμεταγωγείς (switches), που οποιοιδήποτε από αυτούς θα μπορούσε να αποτελεί κίνδυνο στα χέρια ενός κακόβουλου χρηστή. Οι VPN πελάτες εμπιστεύονται τον VPN πάροχο τους για να διατηρεί και να διαχειρίζεται την ακεραιότητα των κυκλωμάτων και για να εφαρμόζει τις καλύτερες τεχνικές για την αποφύγει κατασκόπευσης της κίνησης του δικτύου τους.

Αυτά λοιπόν ονομάζονται trusted VPNs και οι κύριες τεχνολογίες που χρησιμοποιούνται για την υλοποίηση τους σε IP δίκτυα είναι ATM[2], Frame Relay[3] κυκλώματα και Multiprotocol Label Switching (MPLS)[4].

Το ATM και το Frame Relay λειτουργούν στο επίπεδο data link του OSI μοντέλου[5]. (Το πρώτο επίπεδο είναι το Physical Layer και το τρίτο το network layer.). Το MPLS εξομοιώνει ορισμένες ιδιότητες δικτύων μεταγωγής κυκλώματος πάνω σε δίκτυο μεταγωγής πακέτου και εξαιτίας αυτής της ιδιομορφίας του, επικρατεί η άποψη ότι λειτούργει στο επίπεδο 2.5 του OSI μοντέλου, δηλαδή ανάμεσα στο data link και στο network layer. Το MPLS αρχίζει να υπερκαλύπτει το ATM και το frame relay για την υλοποίηση trusted VPNs από τις μεγάλες εταιρίες και τους τηλεπικοινωνιακούς παρόχους.

2.1.2 Secure VPNs

Με την αλματώδη αύξηση του διαδικτύου και την ένταξη του πλέον ως ένα βασικό εργαλείο για τις επιχειρήσεις, τα θέματα που αφορούν στην ασφάλεια έγιναν κρίσιμο ζήτημα τόσο για τους πελάτες όσο και για τους τηλεπικοινωνιακούς παρόχους. Τα trusted VPNs δεν παρείχαν ουσιαστική ασφάλεια και έτσι οι κατασκευαστές άρχισαν να δημιουργούν πρωτόκολλα που θα επέτρεπαν την κρυπτογράφηση των δεδομένων από την μια άκρη του δικτύου και την αποκρυπτογράφηση τους από την άλλη άκρη. Η κρυπτογραφημένη αυτή κίνηση, θα μπορούσε να περιγραφεί ως μια σήραγγα (tunnel) μεταξύ των δυο δικτύων. Έτσι, ακόμα και εάν ένας κακόβουλος χρήστης καταφέρει και υποκλέψει την κίνηση, δεν θα μπορέσει να την διαβάσει ή να την τροποποίηση χωρίς να γίνει αντιληπτό από τον νόμιμο παραλήπτη, ο όποιος και θα την απορρίψει. Τα δίκτυα που κατασκευάζονται χρησιμοποιώντας κρυπτογράφηση λέγονται secure VPNs.

---

[2] Ο ασύγχρονος τρόπος μεταφοράς (Asynchronous Transfer Mode, ATM) είναι ένας τρόπος μεταγωγής και διασύνδεσης των ευζωνικών δημόσιων δικτύων για τη μεταφορά πληροφοριών σε κυψέλες (cells) των 53 ψηφιοσυλλαβών (bytes), για περισσότερες πληροφορίες βλέπε, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/atm.pdf

[3] Το FRAME RELAY είναι τεχνολογία WAN που επιτρέπει σε εταιρίες και οργανισμούς να διασυνδέουν τα τοπικά τους δίκτυα χρησιμοποιώντας ως δίκτυο κορμού το δημόσιο δίκτυο, για περισσότερες πληροφορίες βλέπε, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Frame-Relay.pdf

[4] Το MPLS είναι μια τεχνολογία που προσβλέπει στον αποδοτικό προσδιορισμό, δρομολόγηση, προώθηση, και μεταγωγή της ροής της κυκλοφορίας μέσα στο δίκτυο. Καθορίζεται από το RCF 3031, για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc3031.txt

[5] Το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή μοντέλο αναφοράς OSI είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων η οποία καθορίστηκε από την πρωτοβουλία Ανοικτή Διασύνδεση Συστημάτων – OSI. Είναι γνωστό και ως μοντέλο των επτά επιπέδων, για περισσότερες πληροφορίες βλέπε, http://el.wikipedia.org/wiki/Μοντέλο_αναφοράς_OSI

Τα ασφαλή (Secure VPNs) μπορούν να χρησιμοποιήσουν το πρωτόκολλο IPSec με κρυπτογράφηση, το IPSec μέσα σε ένα επίπεδου data link tunneling πρωτόκολλο (Layer 2 Tunneling Protocol-L2TP), το SSL 3.0 ή το Transport Layer Security (TLS) με κρυπτογράφηση, Layer Two Forwarding (L2F) ή Point-to-Point Tunneling Protocol (PPTP).

Το IPSec είναι ένα πρωτόκολλο κρυπτογράφησης και ταυτοποίησης IP πακέτων στο network layer. Έχει ένα σύνολο πρωτοκόλλων κρυπτογράφησης που εξυπηρετούν δυο σκοπούς: να προσφέρουν ασφάλεια στα δεδομένα του διακινούνται στο δίκτυο και στην ανταλλαγή κλειδιών κρυπτογράφησης. Πολλοί ειδικοί σε θέματα ασφάλειας στο διαδίκτυο , όπως ο Bruce Schneier (Counterpane Internet Security), υποστηρίζουν ότι το πρωτόκολλο IPSec είναι το προτιμότερο για την κατασκευή VPNs από τα τέλη της δεκαετίας του 1990. Το IPSec υποστηρίζεται από τα Windows XP, 2000, 2003 και Vista. Σε Linux με kernel 2.6 και έπειτα, σε Mac OS X, NetBSD, FreeSwan, OpenSwan, StrongSwan, σε Solaris, AIX and HP-UX, και σε VxWorks. Σκοπός της εργασίας αυτής άλλωστε, είναι η υλοποίηση VPN με IPSec με λογισμικό ανοιχτού κωδικα[6] εξαιτίας των παραπάνω πλεονεκτημάτων. Το πρωτόκολλο IPSec θα αναλυθεί σε βάθος στην συνεχεία.

Το PPTP πρωτόκολλο: χρησιμοποιείτε ευρύτατα στα Windows, διότι είναι δωρεάν και εύκολο στην εγκατάσταση και παραμετροποίηση του. Το μειονέκτημα του όμως είναι ότι δεν είναι το πιο ασφαλές συγκριτικά με τα αλλά πρωτόκολλα για την δημιουργία ασφαλών VPNs. Το πρόβλημα έγκειται στο γεγονός ότι η ασφάλεια αυτού, εξαρτάται από το password του εισάγει ο χρήστης.

Ένα πιο παλιό πρωτόκολλο έχει αναπτυχτεί από την Cisco, το οποίο ονομάζεται Layer 2 Tunneling Protocol (L2TP). Συνδυάζει στοιχειά από το L2F και το PPTP για να δημιουργήσει ένα επίπεδου data link πρωτόκολλο. Αυτό παρέχει την δημιουργία ενός tunnel, αλλά όχι ασφάλεια και αυθεντικοποίηση (authentication) του χρηστή. Το L2TP μπορεί να μεταφέρει PPP sessions. Η Cisco όπως και πολλές open-source υλοποιήσεις για Linux χρησιμοποιούν το L2TP.

Ο συνδυασμός L2TP και IPSec προσφέρει L2TP tunnel με την ασφάλεια του IPSec. Αυτό πρακτικά σημαίνει ότι η ανταλλαγή ασφαλών κλειδιών κρυπτογράφησης γίνεται πιο εύκολα συγκριτικά με μια υλοποίηση που βασίζεται αποκλειστικά σε IPSec. Η Microsoft έχει αναπτύξει και προσφέρει δωρεάν ένα L2TP/IPSec VPN client για τα Windows 98, ME και NT από το 2002.

Στο κεφάλαιο 2,3 αναλύεται σε βάθος το πρωτόκολλο IPSec ενώ το κεφάλαιο 4 ασχολείται με εναλλακτικά VPN πρωτόκολλα (PPTP, L2TP, SSL κ.α).

2.1.3 Hybrid VPNs

Ένα secure VPN μπορεί να υπάρχει σαν ένα μέρος ενός trusted VPN, δημιουργώντας έναν τρίτο τύπο VPN που είναι πολύ νέος στην αγορά και ονομάζετε υβριδικό VPN (hybrid VPN).Τα ασφαλή μέρη ενός υβριδικού VPN μπορούν να ελέγχονται από τον πελάτη (χρησιμοποιώντας εξοπλισμό από secure VPN στο χώρο του) ή από τον ίδιο προμηθευτή που παρέχει το ασφαλές μέρος του hybrid VPN. Υπάρχουν περιπτώσεις οπου ολόκληρο το hybrid VPN ασφαλίζετε με secure VPN, αλλά συνήθως μόνο ένα μέρος του είναι ασφαλές.

[6] Για περισσότερες πληροφορίες σχετικά με λογισμικό ανοικτού κώδικα βλέπε, http://www.opensource.org/

2.2 Τοπολογίες VPN

Τα VPN χωρίζονται σε τρεις κατηγορίες: απομακρυσμένης πρόσβασης (remote access), intranets και extranets:

- Τα remote access VPNs συνδέουν τηλεργαζόμενους, κινούμενους χρήστες ή ακόμα και μικρότερα απομακρυσμένα γραφεία με περιορισμένη κίνηση από και προς το WAN της επιχείρησης και των συλλογικών υπολογιστικών της πόρων.
- Τα intranet VPNs συνδέουν σταθερά σημεία, παρακλάδια και γραφεία σπιτιών με το WAN της επιχείρησης.
- Τα extranet VPNs επεκτείνουν την περιορισμένη πρόσβαση στους υπολογιστικούς πόρους της επιχείρησης στους διαφόρους συνεργάτες της που μπορεί να είναι προμηθευτές ή πελάτες επιτρέποντας πρόσβαση σε διαμοιράσιμη πληροφορία.

Κάθε τύπος VPN έχει διαφορετικά θέματα ασφάλειας και ποιότητας παρεχόμενων υπηρεσιών να αντιμετωπίσει.

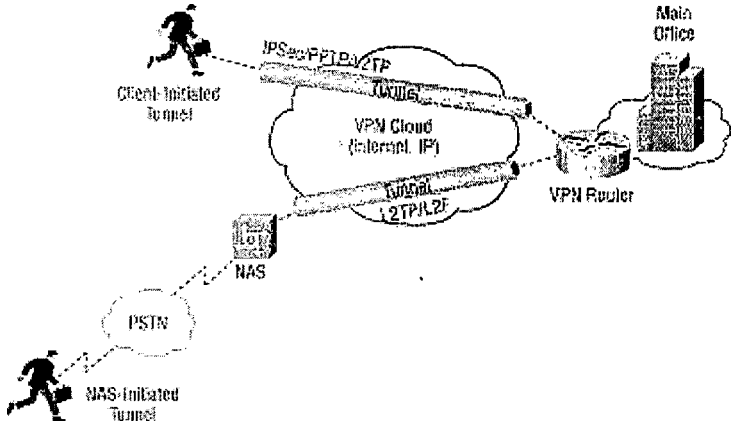
2.2.1 VPNs Απομακρυσμένης Πρόσβασης

Τα VPN απομακρυσμένης πρόσβασης επεκτείνουν το δίκτυο σε τηλεργαζόμενους, κινούμενους χρήστες ή ακόμα και μικρότερα απομακρυσμένα γραφεία με περιορισμένη κίνηση από και προς το WAN της επιχείρησης και των συλλογικών υπολογιστικών της πόρων. Επιτρέπουν στους χρήστες να συνδεθούν στα intranets και extranets των συνεργατών τους όταν, από όπου και όπως αυτοί θέλουν. Τα VPNs απομακρυσμένης πρόσβασης δίνουν την δυνατότητα σύνδεσης μέσα από μία διαμοιρασμένη μορφή χρησιμοποιώντας τις ίδιες πολιτικές όπως και το ιδιωτικό δίκτυο. Οι μέθοδοι πρόσβασης ποικίλουν: ασύγχρονες κλήσεις, ISDN, DSL, κινητό IP καθώς επίσης και καλωδιακές τεχνολογίες. Τα πλεονεκτήματα της μετάβασης στα VPN για απομακρυσμένους χρήστες είναι:

- Μειωμένα κεφάλαια για απόκτηση modem και αναγκαίου εξοπλισμού υλοποίησης του VPN
- Δυνατότητα χρήσης τοπικών τηλεφωνικών γραμμών και όχι υπεραστικών ή του νούμερου 800, ελαχιστοποιώντας έτσι σε μεγάλο βαθμό το κόστος σύνδεσης
- Μεγαλύτερη διαβάθμιση και ευκολία ανάπτυξης για νέους χρήστες
- Επιστροφή της επιχείρησης στο σκοπό της και όχι στη συντήρηση του μέσου

Όταν σχεδιάζεται ένα VPN σύστημα, είναι πολύ σημαντικό να αποφασιστεί από πού θα ξεκινήσει η διαδικασία του tunneling και της κρυπτογράφησης. Οι επιλογές είναι δυο: στον dialup client ή στον server πρόσβασης (Network Access Server-NAS). Στο σχεδιάγραμμα *2-1* το μοντέλο λειτουργίας όπου έχουμε έναρξη σύνδεσης από client το κρυπτογραφημένο τούνελ εγκαθιδρύεται στον client χρησιμοποιώντας IPSec, L2TP, PPTP κάνοντας έτσι το δίκτυο του παροχέα υπηρεσιών απλά ένα μέσο μεταφοράς στο δίκτυο των συνεργατών. Ένα πλεονέκτημα του μοντέλου αυτού είναι το ότι η χρήση του πρωτοκόλλου POP για την κλήση στον παροχέα υπηρεσιών είναι ασφαλισμένη. Ένα ζήτημα που πρέπει να προσεχθεί στην περίπτωση αυτή είναι το αν

θα ενεργοποιηθεί το λογισμικό ασφάλειας του συστήματος ή θα προτιμηθεί κάποιο συμπληρωματικό πακέτο ασφάλειας. Η επιλογή της δεύτερης λύσης έχει μεν όλα τα θετικά στοιχεία που απορρέουν από την εφαρμογή ειδικού πακέτου ασφάλειας αλλά έχει και το αρνητικό της ανάγκης εγκατάστασης και συντήρησής του.



***Σχήμα 2-1**: VPN Απομακρυσμένης Πρόσβασης*

Στο δεύτερο μοντέλο, τώρα, κάποιος server (NAS) ξεκινά τη σύνδεση, οπότε θέματα που αφορούν το λογισμικό που τρέχει στον client περιορίζονται αισθητά. Ο απομακρυσμένος χρήστης επικοινωνεί με το POP server του παροχέα υπηρεσιών χρησιμοποιώντας μία PPP/SLIP[7] σύνδεση, πιστοποιείται από τον παροχέα υπηρεσιών ο οποίος σε απάντηση ξεκινά ένα ασφαλές κρυπτογραφημένο τούνελ με την επιχείρηση από το POP κάνοντας χρήση των L2TP ή L2F. Με την αρχιτεκτονική αυτή όλη η "εξυπνάδα" του VPN βρίσκεται στη πλευρά του server του παροχέα υπηρεσιών καθώς δεν υπάρχει λογισμικό τελικού χρήστη στην επιχείρηση που να χρειάζεται συντήρηση μειώνοντας έτσι την ανάγκη διαχείρισης των απομακρυσμένων συνδέσεων. Το μειονέκτημα, ωστόσο, αυτού του σεναρίου είναι η ανυπαρξία ασφάλειας στο τοπικό δίκτυο που ενώνει τον client με το δίκτυο του παροχέα υπηρεσιών. Για την επιλογή του τελικού μοντέλου που ταιριάζει σε μια επιχείρηση πρέπει να γίνει στάθμιση όλων αυτών των παραγόντων.

2.2.2 Intranet VPNs

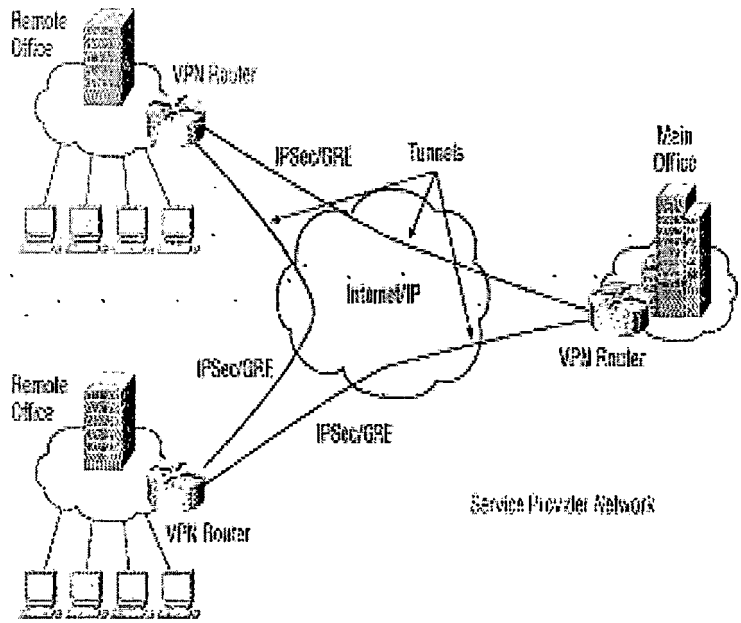
Τα Intranet VPNs (*Σχήμα 2-2*) είναι η εναλλακτική λύση στη δομή WAN αφού μπορούν να αυξήσουν ή να αντικαταστήσουν τις ιδιωτικές γραμμές ή άλλες ιδιωτικές WAN υποδομές ενεργοποιώντας διαμοιρασμένες υποδομές που παρέχονται από τους παροχείς υπηρεσιών. Τα Intranet VPNs χτίζονται πάνω στο Internet ή σε IP, Frame Relay ή ATM του δικτύου του παροχέα υπηρεσιών.

---

[7] Το Serial Line Internet Protocol (SLIP) είναι πρωτόκολλο επικοινωνίας που επιτρέπει έναν υπολογιστή, κάνοντας χρήση μίας κανονικής τηλεφωνικής γραμμής και ενός modem για να συνδεθεί στο Internet. Καθορίζεται από το RFC 1055, για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc1055.txt Το Point-to-Point Protocol (PPP) είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται στην κυκλοφορία των δεδομένων στον ISP από τα διάφορα modems και ISDN links. Καθορίζεται από το rfc 1661, για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc1661.txt

Όταν τα Intranet VPNs έχουν κατασκευαστεί πάνω σε IP WAN υποδομή χρησιμοποιούν IPSec ή GRE[8] για τη δημιουργία ασφαλών tunnel για τη μεταφορά της κίνησης του WAN δικτύου. Όταν συνδυάζονται με τους μηχανισμούς QoS (WFQ, WRED, GTS, CAR) του παροχέα υπηρεσιών, τότε διασφαλίζεται η αποδοτικότερη χρήση του εύρους ζώνης και αξιόπιστη διασύνδεση. Τα πλεονεκτήματα των Intranet είναι:

- Μειωμένο κόστος WAN εύρους ζώνης
- Εύκολη σύνδεση απομακρυσμένων sites
- Αυξημένο χρόνο λειτουργίας (uptime) με την ενεργοποίηση της υπηρεσίας πλεοναζόντων WAN διασυνδέσεων στους παροχείς υπηρεσιών.



***Σχήμα 2-2**: Intranet VPN*

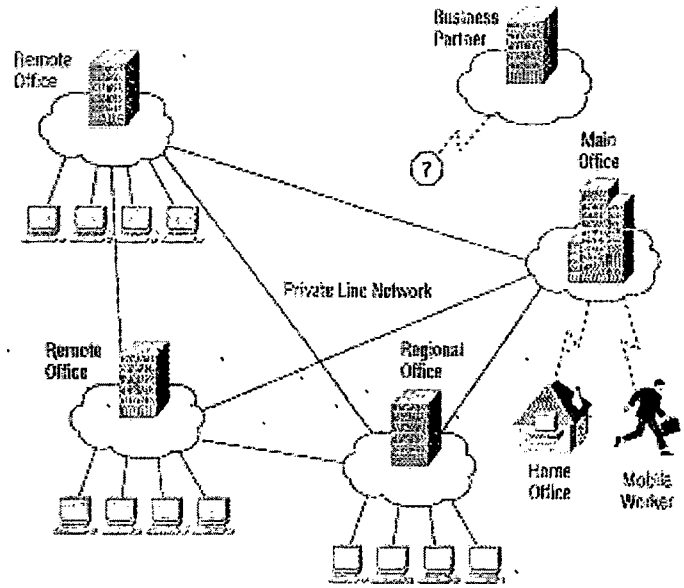
Με την δημιουργία ενός Intranet VPN χρησιμοποιώντας την υπάρχον υποδομή (διαδίκτυο), πετυχαίνουμε την πιο αποδοτική σχέση μεταξύ των χρημάτων που δαπανήθηκαν και των αποτελεσμάτων που παίρνουμε. Τα επίπεδα των υπηρεσιών, ωστόσο, δεν εγγυώνται με την χρήση του διαδικτύου. Όταν υλοποιούμε ένα intranet VPN, θα πρέπει να σταθμίζουμε ποία είναι τα υπέρ και ποία τα κατά των διαφόρων λύσεων. Εάν για παράδειγμα θέλαμε εγγυημένη ποιότητα διασύνδεσης τότε θα ήταν καλύτερα να στήναμε το VPN πάνω από κάποιο IP/frame Relay/ATM δίκτυο ενός παροχέα υπηρεσιών.

---

[8] Για περισσότερες πληροφορίες σχετικά με το GRE, βλέπε RFC 2784, Generic Routing Encapsulation (GRE), διαθέσιμο στο http://www.ietf.org/rfc/rfc2784.txt

2.2.3 Extranet VPNs

Στην χρήση ιδιωτικών γραμμών ή ιδιωτικού Frame Relay/ATM βασίζονται σήμερα τα WAN δίκτυα. Το μέρος της απομακρυσμένης σύνδεσης στο δίκτυο είναι επίσης μια ιδιωτική λύση με τις εταιρίες να αναπτύσσουν και να διαχειρίζονται τα δικά τους συστήματα απομακρυσμένης πρόσβασης. Εφαρμογές extranet συνήθως δεν υποστηρίζονται ή πραγματοποιούνται σε συγκεκριμένες περιπτώσεις που απαιτείται, λόγο του υψηλού κόστους τους.



***Σχήμα 2-3**: Extranet VPN*

Ένα τέτοιο ιδιωτικό δίκτυο περιορίζει την επεκτασιμότητα του σε απομακρυσμένους χρήστες και συνεργάτες, καθότι είναι δύσκολο στη διαχείριση και επιπλέον ακριβό στο εύρος ζώνης και στη διαχείριση του. Η μετανάστευση από ένα ιδιωτικό δίκτυο σε VPN επικεντρώνεται στο κάθε ξεχωριστό τμήμα του δικτύου-intranet και απομακρυσμένης πρόσβασης και επεκτείνει το δίκτυο στους συνεργάτες της επιχείρησης.

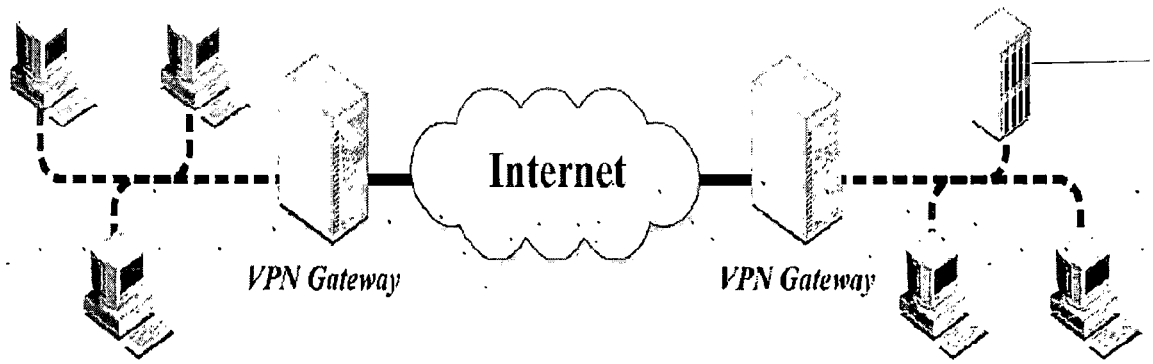
Με την χρήση του πρωτοκόλλου IPSec πρόκειται να γίνει η υλοποίηση VPN συστήματος σε αυτή την εργασία, οπότε στα παρακάτω κεφάλαια θα εστιάσουμε στην τεχνική του ανάλυση από θεωρητικής πλευράς.

2.3 VPN αρχιτεκτονικές

Υπάρχουν τρεις βασικές VPN αρχιτεκτονικές, η καθεμιά περιγράφεται παρακάτω:

2.3.1 Gateway-to-Gateway αρχιτεκτονική

VPN βασισμένα σε IPSec χρησιμοποιούνται για να παρέχουν ασφαλείς επικοινωνίες δικτύων μεταξύ δύο δικτύων. Αυτό συνήθως γίνεται με την εγκατάσταση και παραμετροποίηση ενός VPN gateway σε κάθε δίκτυο ώστε να «κατασκευαστεί μια VPN σύνδεση» μεταξύ των δυο gateways. Τα δεδομένα που χρειάζονται να κρυπτογραφηθούν, περνάνε μέσα από το VPN δίκτυο διαμέσου των δυο gateways. VPN gateway μπορεί να είναι μια συσκευή που έχει ως αποκλειστική λειτουργία την δημιουργία VPNs ή μπορεί να είναι άλλες δικτυακές συσκευές όπως, firewall ή routers. Στο σχεδιάγραμμα *2-4* παρουσιάζετε μια gateway-to-gateway αρχιτεκτονική. Να σημειωθεί ότι για την υλοποίηση του IPSec VPN σεναρίου της παρούσας πτυχιακής επιλέχτηκε αυτό το μοντέλο. (Η αρχιτεκτονική αυτή είναι γνωστή ως και Site-to-Site VPN).



Σχήμα 2-4: *Gateway-to-Gateway αρχιτεκτονική*

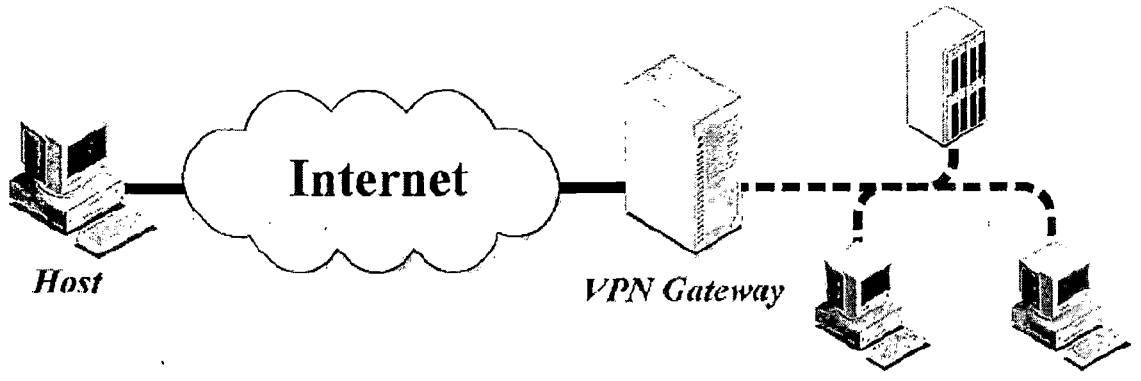
Σε αυτό το μοντέλο οι δυο VPN gateways ανταλλάσουν πληροφορίες για να δημιουργήσουν μια IPSec σύνδεση. Η δρομολόγηση στο κάθε δίκτυο διαμορφώνεται έτσι ώστε υπολογιστές από το ένα δίκτυο, να μπορούν να επικοινωνήσουν με υπολογιστές από το άλλο δίκτυο, αφού τα δεδομένα δρομολογούνται αυτόματα στην IPSec σύνδεση που έχει δημιουργηθεί.

Τα μειονέκτημα της gateway-to-gateway αρχιτεκτονικής είναι ότι τα δεδομένα που μεταφέρονται από τον υπολογιστή στον VPN gateway, στο κάθε δίκτυο και αντίστροφα, δεν κρυπτογραφούνται.

2.3.2 Host-to-Gateway αρχιτεκτονική

Η host-to-gateway αρχιτεκτονική χρησιμοποιείται συνήθως για να παρέχει ασφάλεια σε τοπολογίες απομακρυσμένης πρόσβασης (remote access). Σε αυτή την περίπτωση η εταιρία εγκαθιστά ένα VPN gateway στο δίκτυο της και κάθε απομακρυσμένος χρήστης μπορεί να δημιουργήσει μια VPN σύνδεση ανάμεσα σε έναν τοπικό υπολογιστή και το VPN gateway της εταιρίας. Και σε αυτή την περίπτωση VPN gateway μπορεί να είναι μια συσκευή που έχει ως αποκλειστική λειτουργία την

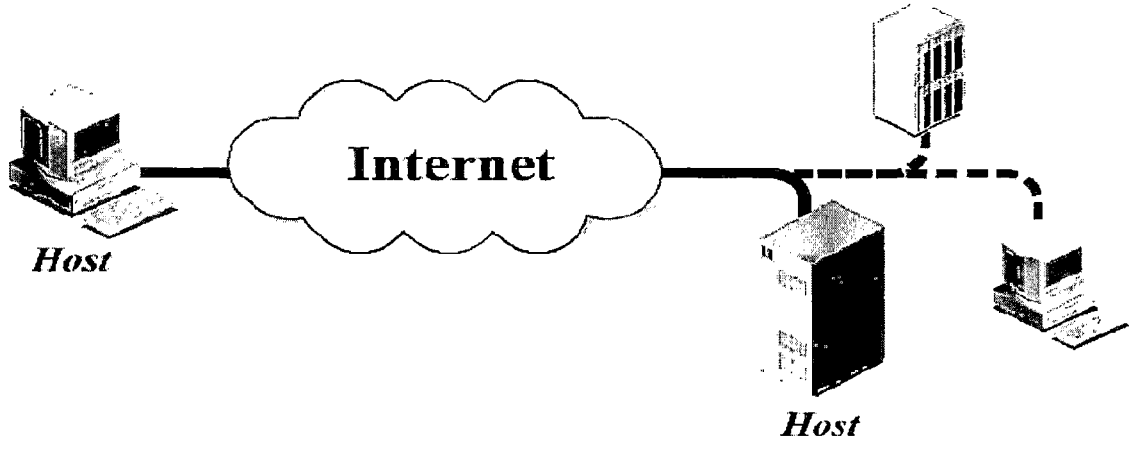
δημιουργία VPNs ή μπορεί να είναι άλλες δικτυακές συσκευές όπως, firewall ή routers. (Η αρχιτεκτονική αυτή είναι γνωστή ως και Roadwarrior VPN).



Σχήμα 2-5: *Host-to-Gateway αρχιτεκτονική*

2.3.3 Host-to-Host αρχιτεκτονική

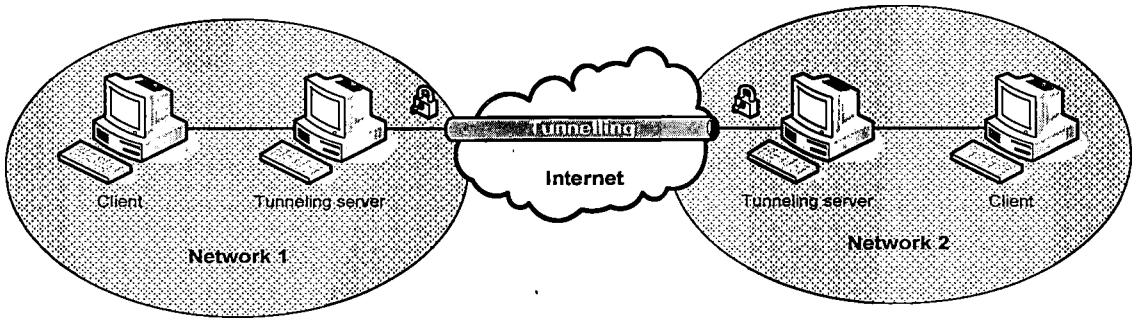
Η host-to-host αρχιτεκτονική χρησιμοποιείται λιγότερο και συνήθως σε ειδικές περιπτώσεις, όπως για απομακρυσμένη διαχείριση ενός server από τον διαχειριστή του συστήματος. Σε αυτή την περίπτωση, η εταιρία διαμορφώνει τον server έτσι ώστε να παρέχει VPN υπηρεσίες και οι υπολογιστές που χρησιμοποίει ο διαχειριστής του δικτύου να λειτουργούν ως clients. Στο επόμενο σχεδιάγραμμα παρουσιάζετε αυτό το μοντέλο.



Σχήμα 2-6: *Host-to-Host αρχιτεκτονική*

2.4 VPN tunneling

Ένα VPN σύστημα είναι βασισμένο στο σκεπτικό του Tunneling. Ο όρος tunneling θα εξηγηθεί με την βοήθεια του παρακάτω σχεδιαγράμματος:



Σχήμα 2-7: *VPN tunneling*

Συμφωνά με το *Σχήμα 2-7*, κάθε πακέτο ανεξαρτήτως από ποιο δίκτυο ξεκινά μπαίνει στο tunnel για να μεταφερθεί μέχρι την άλλη άκρη του δικτυού (tunneling). Το tunneling είναι ένας τρόπος με τον οποίο τα δεδομένα μεταφέρονται με ασφάλεια μεταξύ των δύο δικτύων. Όλα τα δεδομένα που μεταβιβάζονται είναι κατακερματισμένα σε μικρότερα πακέτα και στη συνέχεια διέρχονται από τη σήραγγα. Η διαδικασία αυτή είναι διαφορετική από την κανονική μεταφορά δεδομένων μεταξύ κόμβων. Κάθε πλαίσιο που διέρχεται από τη σήραγγα θα είναι κρυπτογραφημένο και θα έχει μια πρόσθετη επικεφαλίδα (header) η οποία χρησιμοποιείται για τη δρομολόγηση πακέτων προς τη σωστή κατεύθυνση (encapsulation). Στο *Σχήμα 2-7* ο client από το network 1 στέλνει ένα πακέτο στο tunneling server. Εκεί το πακέτο δεδομένων (δεδομένα και header) κρυπτογραφείται πριν την αποστολή. Έπειτα εσωκλείεται σε ένα νέο πακέτο χρησιμοποιώντας έναν νέο header .Το αρχικό πακέτο αποστέλλεται στο Internet κρυπτογραφημένο, από το ένα άκρο του tunnel στο άλλο. Κατά την λήψη του από τον tunneling server στο network 2, αφαιρείται η επιπλέον επικεφαλίδα (de-capsulated) και τα δεδομένα αποκρυπτογραφούνται. Η σήραγγα που δημιουργήθηκε για την μεταφορά των πακέτων είναι μια λογική διαδρομή μεταξύ της πηγής και του προορισμού μεταξύ των δύο δικτύων και λειτούργει ως μια point-to-point σύνδεση μεταξύ των τερματικών στάθμών, επιτρέποντας στα δυο δίκτυα να επικοινωνούν απευθείας. Το tunneling πρωτόκολλο κρυπτογραφεί τα αρχικά δεδομένα ώστε να μην μπορούν να διαβαστούν από τρίτους. Η ενθυλάκωση (encapsulation) της VPN κίνησης δεδομένων ονομάζεται tunneling.

2.4.1 Είδη tunneling

Υπάρχουν δυο ειδή tunneling:

- Voluntary tunneling: με το voluntary tunneling, ο client αρχίζει την διαδικασία σύνδεσης του με έναν VPN server. Απαραίτητη όμως προϋπόθεση είναι, να υπάρχει ήδη σύνδεση μεταξύ του server και του client. Αύτη την σύνδεση χρησιμοποιεί ο client για να δημιουργήσει ένα tunnel με τον VPN server.

- Compulsory tunneling: σε αυτή την περίπτωση, μια σύνδεση δημιουργείται μεταξύ είτε δυο VPN servers, είτε μεταξύ δυο VPN δρομολογητών-VPN access devices. Ο client καλεί τον απομακρυσμένο VPN server για να δημιουργηθεί το tunnel μέσω του όποιου θα διέρχονται τα πακέτα, διαμέσου του τοπικού δικτυού ή του διαδικτύου.

VPN tunnels μπορούν να δημιουργηθούν στα επόμενα επίπεδα του Open Systems Interconnection (OSI) μοντέλου.

- Επίπεδο 2 - Data-Link επίπεδο (Point-to-Point Tunneling Protocol (PPTP) και Layer 2 Tunneling Protocol (L2TP)
- Επίπεδο 3 - Network επίπεδο : (IPSec)

2.5 Ασφάλεια και κρυπτογράφηση στα VPNs

Τα ιδεατά ιδιωτικά δίκτυα προκειμένου να ασφαλίσουν την κίνηση δεδομένων που διέρχονται μέσα από αυτά, χρησιμοποιούν κρυπτογράφηση και τεχνικές κρυπτογράφησης κατά μήκος του tunnel που έχει δημιουργηθεί.

Η ασφάλεια απορρήτου εξασφαλίζεται με την χρήση μυστικών κλειδιών για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων, ενώ η πιστοποίηση αυθεντικοποίησης σχετίζετε με τις πιστοποιήσεις που εκδίδονται μεταξύ των ακρών επικοινωνίας.

Η κρυπτογράφηση των δεδομένων είναι απόρια ορισμένων αλγορίθμων που παράγουν το τελικό αποτέλεσμα. Οι αλγόριθμοι αυτοί χωρίζονται σε δυο μεγάλες κατηγορίες και ανάλογα κατηγοριοποιούν το είδος της κρυπτογράφησης σε συμμετρική και ασύμμετρη κρυπτογράφηση.

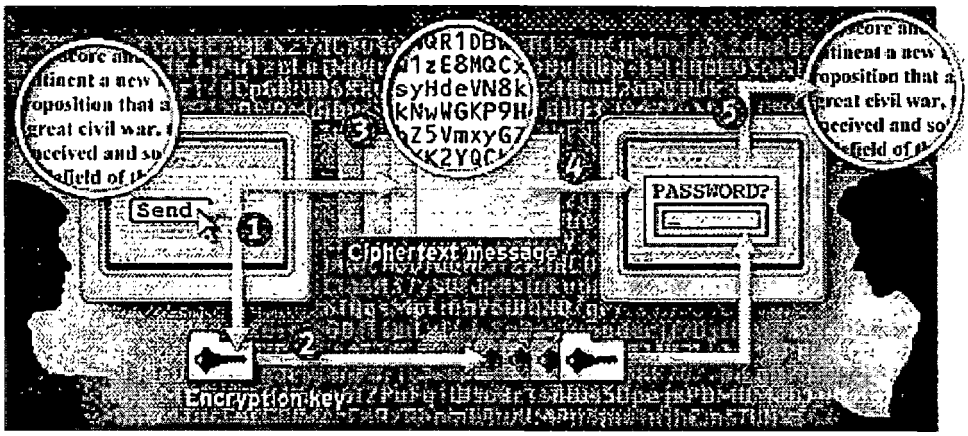
2.5.1 Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιηθεί. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή (IDEA, CAST5, BLOWFISH, TWOFISH,), με πιο γνωστό τον Data Encryption Standard (DES) και τον 3DES, ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών.

Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos[9], του MIT (Massachusetts Institute of Technology).



Σχήμα 2-8: Συμμετρική κρυπτογράφηση

Στο παραπάνω σχεδιάγραμμα ο αποστολέας και ο παραλήπτης έχουν το ίδιο πρόγραμμα κρυπτογράφησης.

1. Για να αποσταλεί ένα κρυπτογραφημένο μήνυμα, δημιουργείται πρώτα το κείμενο και έπειτα παράγουμε το κλειδί κρυπτογράφησης που θα χρησιμοποιηθεί και την κωδικοποίηση του κειμένου.

2. Το κλειδί θα δρομολογηθεί στον παραλήπτη αλλά από διαφορετική διαδρομή από αυτή που θα αποσταλεί το κείμενο. Το κλειδί μπορεί να έχει την μορφή είτε κωδικού είτε αρχείου.

3. Το πρόγραμμα κρυπτογράφησης χρησιμοποιώντας τον αλγόριθμο που έχει επιλεγεί και το κλειδί μετατρέπει το κείμενο σε κρυπτογραφικό κώδικα.

4. Ο αποστολέας στέλνει το κρυπτογραφημένο κώδικα στον παραλήπτη.

5. Ο παραλήπτης μόλις το λάβει ανοίγει το κρυπτογραφημένο κώδικα με την ίδια εφαρμογή που χρησιμοποιεί τον αλγόριθμο και το κλειδί για να αποκρυπτογραφήσει το κείμενο για να μπορέσει να το διαβάσει.

2.5.2 Ασύμμετρη κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

---

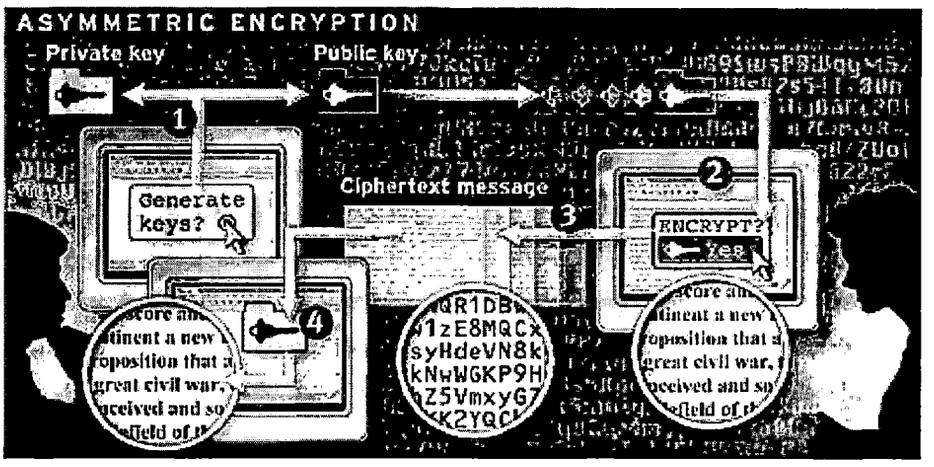
[9] Kerberos είναι ένα πρωτόκολλο δικτύου που χρησιμοποιεί συμμετρική κρυπτογραφία για να παρέχει έλεγχο ταυτότητας για client-server εφαρμογές, για περισσότερες πληροφορίες βλέπε, http://web.mit.edu/Kerberos/

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.



***Σχήμα 2-9**: Ασύμμετρη κρυπτογράφηση*

Στο παραπάνω σχεδιάγραμμα ο αποστολέας και ο παραλήπτης χρησιμοποιούν το ίδιο πρόγραμμα κρυπτογράφησης.

1. Εάν κάποιος θέλει να στείλει εάν κρυπτογραφημένο κείμενο, θα πρέπει πρώτα να φτιάξει ένα δημόσιο και ένα ιδιωτικό κλειδί με την εφαρμογή που

χρησιμοποιεί. Έπειτα θα πρέπει να στείλει το δημόσιο κλειδί στον παραλήπτη.

2. Ο αποστολέας χρησιμοποιώντας έναν ασύμμετρο αλγόριθμο και το δημόσιο κλειδί, κωδικοποιεί το κείμενο σε κρυπτογραφημένο κώδικα.

3. Στην συνεχεία το στέλνει στον παραλήπτη.

4. Ο αποστολέας στέλνει το κρυπτογραφημένο κώδικα στον παραλήπτη.

5. Ο παραλήπτης μόλις το λάβει ανοίγει το κρυπτογραφημένο κώδικα με την ίδια εφαρμογή, η οποία αποκρυπτογραφεί το κείμενο χρησιμοποιώντας το δικό του ιδιωτικό κλειδί.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ότι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής.

ΚΕΦΑΛΑΙΟ 3

3. Ανάλυση του Internet Protocol Security (IPSec) suite

Το πρωτόκολλο IPSec αναπτύχτηκε από την Internet Engineering Task Force με σκοπό την διασφάλιση της επικοινωνίας ανάμεσα σε δύο δικτυακές συσκευές, τόσο υπό την έννοια του να μην είναι δυνατή η υποκλοπή της πληροφορίας που ανταλλάσουν μεταξύ τους, όσο και υπό την έννοια της διασφάλισης της ακεραιότητας της επικοινωνίας αυτής. Για τον σκοπό αυτό, το πρωτόκολλο χρησιμοποιεί ένα ευέλικτο πλαίσιο το οποίο μπορεί να χρησιμοποιήσει μια πληθώρα από μεθόδους κρυπτογράφησης και συναρτήσεων κατακερματισμού ανάλογα με τις εκάστοτε ανάγκες. Ορίζεται από το RFC 4301[10], ως ένα επίπεδου τρία tunneling πρωτόκολλο το οποίο με την χρησιμοποίηση κρυπτογραφικών μεθόδων παρέχει αυθεντικοποίηση (Authentication), ακεραιότητα δεδομένων (Data integrity), ασφάλεια απορρήτου (Confidentiality), προστασία από διάφορες επιθέσεις δικτύου (Network attacks) (πχ replay attack και flooding). Επιπλέον, υπάρχει η δυνατότητα συνεννόησης μεταξύ των συσκευών που επικοινωνούν με IPSec ώστε να υπάρξει μια κοινή συμφωνία σχετικά με το ποιες μέθοδοι θα χρησιμοποιηθούν πριν η επικοινωνία ξεκινήσει. Για την ταυτοποίηση των δύο άκρων που επικοινωνούν μεταξύ τους, υπάρχουν ποικίλα σχήματα (μοιρασμένα εκ των προτέρων κλειδιά, πιστοποιητικά κτλ.) κάθε ένα από τα οποία έχει συγκεκριμένα πλεονεκτήματα και μειονεκτήματα.

3.1 Αρχιτεκτονική του IPSec

Οι λειτουργίες που εκτελεί το IPSec μπορούν να κατηγοριοποιηθούν σε δυο επίπεδα. Το πρώτο σχετίζετε με τα δεδομένα (data plane) και το άλλο με το επίπεδο του ελέγχου (control plane). Το επίπεδο με τα δεδομένα υλοποιείται με την χρησιμοποίηση δυο IPSec πρωτοκόλλων: το πρωτόκολλο αυθεντικοποίησης επικεφαλίδας Authentication Header (AH)[11] και το πρωτόκολλο Ασφαλούς Ενθυλάκωσης Πακέτου (Encapsulating Security Payload-ESP)[12]. Τα δυο αυτά πρωτόκολλα εκτελούν ενέργειες σχετικά με τον χειρισμό των πακέτων, όπως είναι η κρυπτογράφηση και αποκρυπτογράφηση τους. Αυτές οι ενέργειες πραγματοποιούνται απ' ευθείας από το κέλυφος του λειτουργικού συστήματος καθώς απαιτείται γρήγορη επεξεργασία με την μικρότερη δυνατή λανθάνουσα κατάσταση (latency)[13].

---

[10] Τα πρωτόκολλα IPSec καθορίζονταν από τα RFC 1825 & 1829 το 1995. Το 1998 αντικαταστάθηκαν από το RFC 2401 και το RFC 2412 ώσπου το 2005 τα RFC 4301 και RFC 4309 διαδέχτηκαν όλα τα προηγούμενα.

[11] AH είναι ένα IP protocolμε αριθμό 51. Η AH έκδοση 2 καθορίζετε από το RFC 2402, IP Authentication Header, διαθέσιμο στο http://www.ietf.org/rfc/rfc2402.txt

[12] ESP είναι ένα IP protocol με αριθμό 50. The ESP version έκδοση 2 καθορίζετε από το RFC 2406, IP Encapsulating Security Payload (ESP), διαθέσιμο στο http://www.ietf.org/rfc/rfc2406.txt

[13] Latency: είναι το διάστημα που μεσολαβεί μεταξύ ερεθίσματος και αντίδρασης.

Όσον αφορά το επίπεδο ελέγχου, αυτό υλοποιείτε με την χρήση του πρωτοκόλλου Internet Key Exchange (IKE)[14], και αφορά την ανταλλαγή των πληροφοριών πιστοποίησης και άλλες πληροφορίες μεταξύ των δυο άκρων του tunnel.

3.2 Το πρωτόκολλο Authentication Header (AH)

Το πρωτόκολλο AH παρέχει προστασία στην ακεραιότητα των δεδομένων και της επικεφαλίδας (header) των πακέτων που μεταφέρονται, καθώς επίσης και αυθεντικοποίηση του χρηστή. Προαιρετικά, μπορεί να προσφέρει και προστασία από διάφορες επιθέσεις του δικτύου, όπως replay attack. Δεν παρέχει όμως, κανένα μηχανισμό κρυπτογράφησης. Στην αρχική έκδοση του IPSec χρησιμοποιούταν σε συνδυασμό με το ESP πρωτόκολλο, διότι το ESP παρείχε μόνο μεθόδους κρυπτογράφησης.

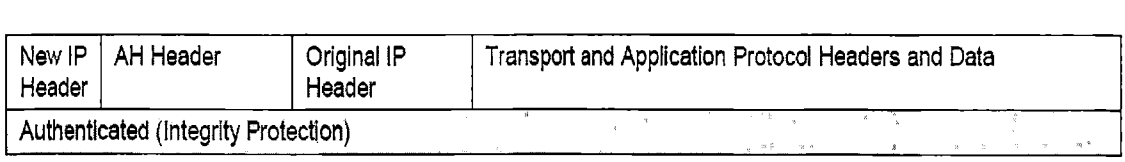
Έπειτα από την έλευση της δεύτερης έκδοσης του IPSec που πρόσθετε δυνατότητες αυθεντικοποίησης (authentication) στο Encapsulating Security Payload, το πρωτόκολλο AH άρχισε σιγά, σιγά να χάνει την αξία του και μάλιστα ορισμένα IPSec λογισμικά δεν υποστηρίζουν πλέον καθόλου το authentication header. Παρ' όλα αυτά το AH έχει ακόμα αξία διότι, παρέχει αυθεντικοποίηση σε ορισμένα πεδία ενός πακέτου, που το ESP δεν μπορεί.

3.2.1 Καταστάσεις Authentication Header

Υπάρχουν δυο καταστάσεις για το AH. Η πρώτη είναι η κατάσταση διόδου (tunnel mode) και η δεύτερη είναι η κατάσταση μεταγωγής (transport mode).

Σε κατάσταση διόδου: το AH δημιουργεί μια νέα IP επικεφαλίδα για κάθε πακέτο ενώ αντίθετα σε κατάσταση μεταγωγής όχι. Στην IPSec αρχιτεκτονική χρησιμοποιεί μια πύλη (gateway) και θα πρέπει η IP διεύθυνση είτε της προέλευσης (source) είτε του προορισμού (destination) να είναι η διεύθυνση του gateway.

Σε κατάσταση μεταγωγής: επειδή το transport mode δεν μπορεί να τροποποιήσει την αρχική IP κεφαλίδα (header), καθώς και επίσης ούτε να δημιουργήσει μια νέα, για αυτό τον λόγο χρησιμοποιείται στις host-to-host αρχιτεκτονικές. Όπως φαίνεται και στα σχήματα *3-1και 3-2* το AH πρωτόκολλο παρέχει προστασία ακεραιότητας των δεδομένων σε ολόκληρο το πακέτο, ασχέτως εάν χρησιμοποιείται tunnel mode ή transport mode.



Σχήμα 3-1: *AH Tunnel Mode Πακέτο*

[14] Το IKE καθορίζετε από το RFC 2409, The Internet Key Exchange (IKE), διαθέσιμο στο http://www.ietf.org/rfc/rfc2409.txt. Η προεπιλεγμένη UDP πόρτα που χρησιμοποίει το IKE είναι η 500

IP Header	AH Header	Transport and Application Protocol Headers and Data
Authenticated (Integrity Protection)		

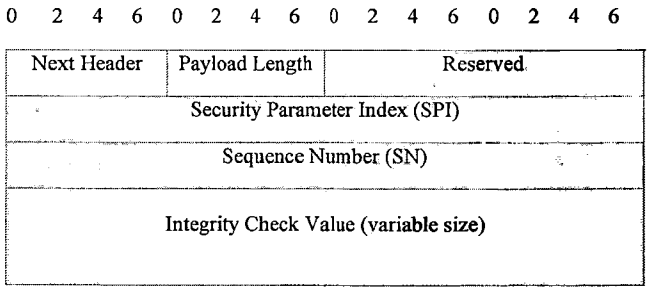
Σχήμα 3-2: *AH Transport Mode Πακέτο*

3.2.2 Διαδικασία προστασίας ακεραιότητας δεδομένων

Κατά την διαδικασία προστασίας ακεραιότητας των δεδομένων το πρώτο βήμα είναι η δημιουργία ενός hash με την βοήθεια ενός hash αλγορίθμου, ή όπως αλλιώς ονομάζεται Message Authentication Code (MAC) αλγόριθμος. Αυτός παράγει έναν hash βασισμένο σε ένα κείμενο και σε ένα κρυφό κλειδί που μοιράζεται στις δυο άκρες που θέλουν να ανταλλάξουν δεδομένα. Προσθέτετε ο hash στο πακέτο, και αυτό στέλνετε στον παραλήπτη. Έπειτα, ο παραλήπτης αναπαράγει το hash χρησιμοποιώντας το κρυφό κλειδί και επικυρώνει ότι οι δυο hashes ταιριάζουν. Με αυτόν τον τρόπο επιτυγχάνεται η προστασία της ακεραιότητας των δεδομένων. Το IPSec για να εκτελέσει αυτή την διαδικασία χρησιμοποιεί αλγορίθμους hash κώδικα επικύρωσης μηνυμάτων (Hash Message Authentication Code)[15]. Για παράδειγμα HMAC-MD5 και HMAC-SHA-1.

Το πρόβλημα όμως που παρουσιάζεται με την παραπάνω διαδικασία είναι ότι ορισμένα πεδία της IP επικεφαλίδας, όπως είναι το Time To Live (TTL) και το checksum, ενδέχεται να μεταβληθεί η τιμή τους κατά την δρομολόγηση. (Η τιμή TTL σε ένα TCP πακέτο αναλύετε στο κεφάλαιο 6.2). Έτσι, όταν το πακέτο με το hash φτάσει στον παραλήπτη και αυτός προσπαθήσει να το ταιριάξει με το δικό του hash, θα καταλάβει ότι το πακέτο άλλαξε κατά την μεταφορά του και ότι παραβιάστηκε η ακεραιότητα του. Για την αποφυγή αυτού του προβλήματος τα πεδία αυτά οπού αλλάζουν νόμιμα, κατά την μεταφορά εξαιρούνται από την διαδικασία υπολογισμού της ακεραιότητας των δεδομένων. Άλλωστε, αυτή είναι και η αιτία που το πρωτόκολλο AH παρουσιάζει ασυμβατότητες με την τεχνολογία μετάφρασης της διεύθυνσης δικτυού-Network Address Translation-NAT. (Η τεχνολογία NAT και το πρόβλημα ασυμβατότητας που δημιουργείτε αναλύονται στο τέλος αυτού του κεφαλαίου).

3.2.3 Ανάλυση της επικεφαλίδας Authentication Header



Σχήμα 3-3: *Τα πεδία από τα οποία αποτελείται το Authentication Header*

[15] Για περισσότερες πληροφορίες σχετικά με το HMAC, βλέπε RFC 2104, HMAC: Keyed-Hashing for Message Authentication http://www.ietf.org/rfc/rfc2104.txt

Το AH προστίθεται σε κάθε πακέτο. Όπως δείχνει και το *Σχήμα 3-3*, κάθε authentication header αποτελείτε από έξι πεδία:

- **Next Header**. Σε αυτό το πεδίο περιέχετε ο αριθμός του IP πρωτοκόλλου για το επόμενο πακέτο καθαρών δεδομένων (payload)[16].
- **Payload Length**. Εδώ περιέχονται πληροφορίες για το μήκος του payload
- **Reserved**. Αυτή η τιμή είναι δεσμευμένη για μελλοντική χρήση, και είναι 0.
- **Security Parameters Index (SPI)**. Σε αυτό το πεδίο η SPI τιμή επιλέγετε τυχαία σε κάθε τερματικό άκρο, κάθε IPSec σύνδεσης, και προσδιορίζει μοναδικά κάθε σύνδεση. Ο παραλήπτης χρησιμοποιεί την SPI τιμή, μαζί με την IP διεύθυνση προορισμού και προαιρετικά με τον τύπο του IPSec πρωτοκόλλου, για να προσδιορίσει ποιον Συσχετισμό Ασφάλειας (Security Association–SA[17]) πρόκειται να χρησιμοποιήσει. Αυτό ουσιαστικά λέει στον παραλήπτη, ποιον αλγόριθμο και ποιο IPSec πρωτόκολλο έχει το πακέτο.
- **Sequence Number**. Είναι ο αριθμός που μηδενίζεται με την εγκατάσταση μιας νέας SA και που αυξάνει κατά ένα σε κάθε πακέτο που εκπέμπεται. Χρησιμοποιείται για να αποφεύγεται η κατά λάθος επανεκπομπή του ίδιου πακέτου.
- **Authentication Information**. Στην περιοχή αυτή υπολογίζεται η Τιμή Ελέγχου Ακεραιότητας (Integrity Check Value, ICV). Είναι η τιμή με την οποία γίνεται η αυθεντικοποίηση της ταυτότητας του χρήστη, δηλ. η «καρδιά» του πρωτοκόλλου AH.

3.2.4 Τρόπος λειτουργίας Authentication Header

Για να δούμε συνολικά πως λειτούργει το πρωτόκολλο AH θα χωρίσουμε την επεξεργασία που πραγματοποιείται σε μια δυο κομμάτια: την επεξεργασία εξερχόμενων και εισερχόμενων πακέτων.

Επεξεργασία εξερχόμενων: Σε αυτή την περίπτωση όταν ένα πακέτο προς εκπομπή φτάσει στο στρώμα του IPSec, ελέγχεται μέσω της βάσης δεδομένων SPD[18], η πολιτική ασφαλείας που ακολουθεί ο σταθμός για την κατηγορία πακέτων στην οποία ανήκει το συγκεκριμένο πακέτο.

---

[16] Payload τα πακέτα που διακινούνται στο διαδίκτυο περιέχουν δεδομένα και άλλες πληροφορίες που προσδιορίζουν τον αποστολέα και τον παραλήπτη του πακέτου. Το payload είναι τα δεδομένα χωρίς τις υπόλοιπες πληροφορίες.

[17] Security Association, SA Το μονοπάτι επικοινωνίας δύο σταθμών που προστατεύεται από κάποιο πρωτόκολλο ασφαλείας.(είτε SA - Tunnel Mode, είτε Transport Mode, βλέπε "*Δίκτυα Ευρείας Ζώνης", Ι.Σ. Βενιέρης, 2001*

[18] Security Policy Database (SPD). Είναι η βάση στην όποια αποθηκεύονται πληροφορίες οι οποίες κατηγοριοποιούν την διερχόμενη κίνηση σε αυτή που απαιτεί IPSec προστασία (protect), σε αυτή που δεν απαιτεί IPSec προστασία (bypass) και σε αυτή που απορρίπτεται.(discard).

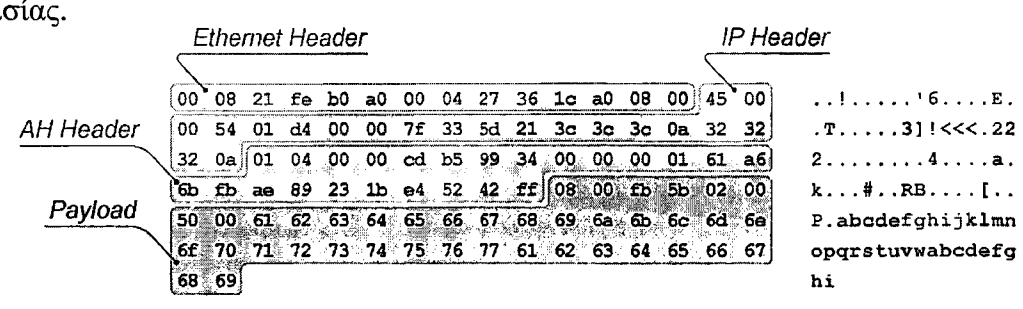
Αν το πακέτο πρέπει να "ασφαλιστεί", εφαρμόζονται σε αυτό τα αντίστοιχα πρωτόκολλα (AH, ESP).

Με την επιλογή του κατάλληλου συσχετισμού ασφάλειας και την εγκατάσταση αυτού, η πρώτη πράξη είναι να μηδενιστεί η τιμή του Sequence Number. Η επιλογή του κατάλληλου συσχετισμού SA γίνεται μέσα από τη Βάση Δεδομένων Συσχετισμού Ασφάλειας (Security Association Database, SAD)[19], που υπάρχει σε κάθε σταθμό. Σε αυτή, κάθε συνδυασμός υπηρεσιών ασφαλείας που μπορεί να εφαρμοστεί σε ένα πακέτο, αντιστοιχεί και σε μία SA. Οι υπηρεσίες που στηρίζονται από την κάθε SA προκύπτουν από την τιμή SPI του εκάστοτε πρωτοκόλλου ασφαλείας.
Η Τιμή Ελέγχου Ακεραιότητας (ICV) υπολογίζεται σύμφωνα με μεταβλητές που περιέχονται στην επικεφαλίδα IP, στην επικεφαλίδα AH και σε επικεφαλίδες ανωτέρων στρωμάτων.

Επεξεργασία εισερχόμενων: Στην επεξεργασία εισερχόμενων πακέτων, με την παραλαβή του πακέτου από το δίκτυο, ο τερματικός σταθμός διαβάζει την διεύθυνση IP του αποστολέα, το πρωτόκολλο ασφαλείας (AH) και την τιμή SPI. Από τον συνδυασμό των τριών αποφαίνεται για το ποια SA από την SAD πρέπει να χρησιμοποιηθεί. Η SA στην οποία καταλήγει, του καθορίζει τα επόμενα βήματα:

1. Αν υποστηρίζεται η υπηρεσία αποφυγής επανάληψης πακέτου, ο σταθμός ελέγχει την τιμή Sequence Number, η οποία αν συμπίπτει με την τιμή κάποιου προηγούμενου πακέτου, το καινούργιο πακέτο απορρίπτεται.
2. Υποδεικνύεται ο αλγόριθμος με τον οποίο θα υπολογιστεί εκ νέου η τιμή ICV, καθώς και κάποιο πιθανό κλειδί για την κωδικοποίησή της. Με το ίδιο σκεπτικό με τον αποστολέα για τον μηδενισμό κάποιων μεταβλητών, ο παραλήπτης υπολογίζει την τιμή του ICV, την κωδικοποιεί και την συγκρίνει με αυτή που ήρθε στο πακέτο. Αν οι δύο τιμές συμπίπτουν, το πακέτο γίνεται δεκτό.
3. Αν το πακέτο είχε σταλεί από λάθος διεύθυνση, ο παραλήπτης θα είχε αποφανθεί για μια SA η οποία δεν θα είχε χρησιμοποιηθεί. Θα χρησιμοποιούσε άλλο αλγόριθμο υπολογισμού του ICV, θα κατέληγε σε διαφορετικό ICV από αυτό με το οποίο ήρθε το πακέτο και τελικά θα απέρριπτε το πακέτο.

Παρακάτω παρουσιάζετε ένα απλό παράδειγμα για την καλύτερη κατανόηση της διαδικασίας.



Σχήμα 3-4: *Δείγμα AH Transport Mode πακέτου*

[19] Association Database καθορίζετε από το RFC 2401, βλέπε http://www.ietf.org/rfc/rfc2401.txt

3.2.5 Συμπερασματικά για το πρωτόκολλο AH

- Το πρωτόκολλο AH παρέχει προστασία ακεραιότητας δεδομένων για όλα τα πακέτα (επικεφαλίδα και δεδομένα), με μόνη εξαίρεση ορισμένα πεδία από την IP επικεφαλίδα που νόμιμα αλλάζουν την τιμή τους κατά την μετάδοση.

- Δημιουργούνται ασυμβατότητες με την τεχνολογία NAT διότι, το AH περιέχει την IP διεύθυνση του προορισμού και αφετηρίας στους υπολογισμούς που πρέπει να γίνουν για την προστασία ακεραιότητας δεδομένων

- Το AH παρέχει μόνο αυθεντικοποίηση και όχι κρυπτογράφηση και πλέον οι περισσότερες υλοποιήσεις IPSec γίνονται με την δεύτερη έκδοση του, στην οποία το ESP μπορεί να παρέχει και αυτό προστασία ακεραιότητας δεδομένων. Η χρήση του AH έχει μειωθεί σημαντικά και πλέον ορισμένες υλοποιήσεις IPSec δεν υποστηρίζουν καθόλου το AH.

3.3 Πρωτόκολλο Ασφαλούς Ενθυλάκωσης Πακέτου (ESP)

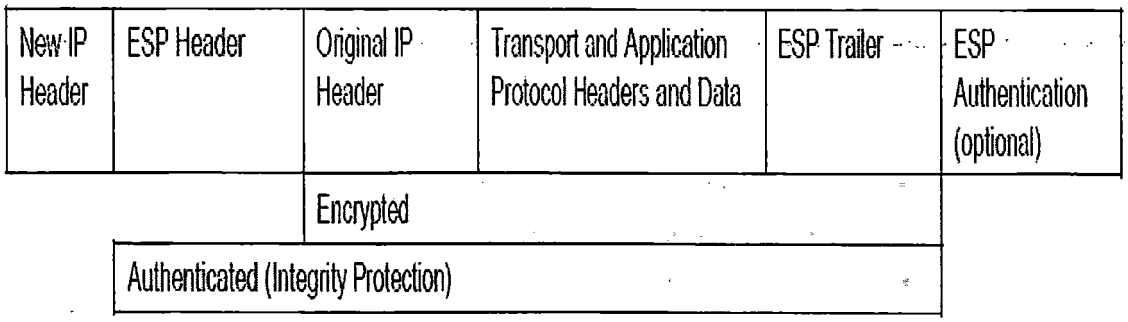
Το Encapsulating Security Payload (ESP) είναι το δεύτερο κύριο πρωτόκολλο του IPSec. Στην αρχική του έκδοση παρείχε μόνο κρυπτογράφηση των δεδομένων ενός πακέτου. Όπου χρειάζονταν αυθεντικοποίηση αυτή γίνονταν σε συνδυασμό με το πρωτόκολλο AH, όπως αναφέρθηκε στο κεφάλαιο 3.2. Στην δεύτερη έκδοση όμως του ESP προστέθηκε η δυνατότητα πιστοποίησης για να παρέχει ακεραιότητα των δεδομένων, αν και όχι για όλα τα πεδία της IP επικεφαλίδας. Επιπλέον το ESP μπορεί να απενεργοποιηθεί μέσω του αλγορίθμου Null ESP Encryption. Σε αυτό το κεφάλαιο θα ασχοληθούμε με τα χαρακτηριστικά της δεύτερης έκδοσης του πρωτοκόλλου ESP.

3.3.1 Καταστάσεις Encapsulation Security Payload

Υπάρχουν δυο καταστάσεις στο ESP, όπως και στο AH: κατάσταση (tunnel), κατάσταση μεταγωγής (transport).

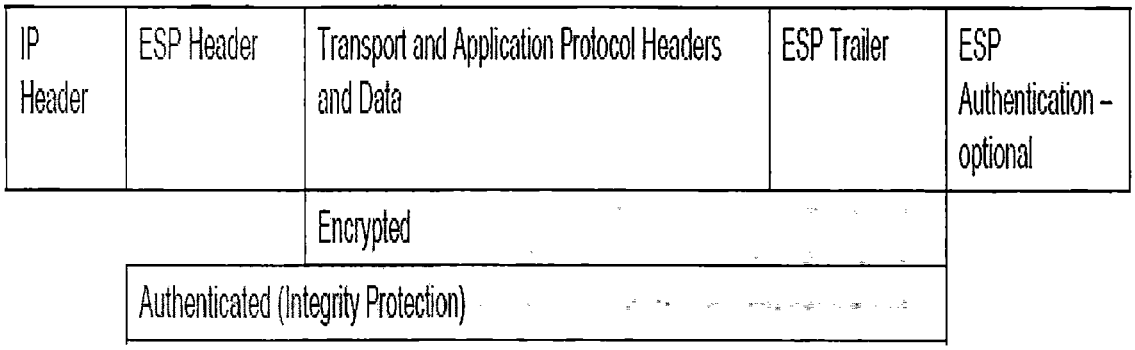
Κατάσταση διόδου: Η κατάσταση tunnel χρησιμοποιείται πολύ περισσότερο απ' ότι η κατάσταση μεταγωγής. Εδώ το ESP δημιουργεί μια νέα IP επικεφαλίδα για κάθε πακέτο. Η νέα IP επικεφαλίδα συγκαταριθμεί τα δυο τερματικά άκρα του ESP tunnel (σαν αφετηρία και προορισμό του πακέτου). Όπως απεικονίζετε και στο *Σχήμα 3-6*, το ESP μπορεί μόνο να κρυπτογραφεί και/ή να παρέχει προστασία ακεραιότητας και στα δεδομένα και στην αρχική IP επικεφαλίδα κάθε πακετου[21]. Με την κρυπτογράφηση τα δεδομένα δεν μπορούν να διαβαστούν και να τροποποιηθούν από κανέναν άλλο. Με την χρησιμοποίηση της προστασίας ακεραιότητας δεδομένων, κάθε πακέτο θα έχει ένα πεδίο ESP Authentication μετά από το ESP trailer.

[21] Είτε ESP κρυπτογράφηση είτε η ESP πιστοποίηση (αλλά όχι και τα δυο μαζί) μπορούν να τεθούν σε null, απενεργοποιώντας αυτή την δυνατότητα



Σχήμα 3-6: *Πακέτο με ESP σε κατάσταση tunneling*

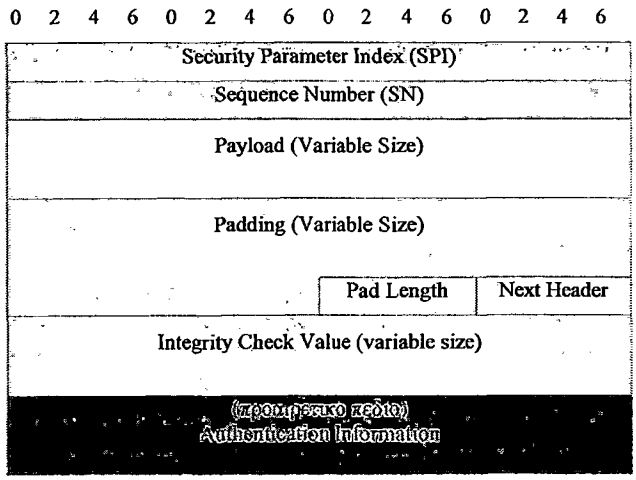
Κατάσταση μεταγωγής: Στην κατάσταση αυτή, το ESP χρησιμοποιεί την αρχική IP επικεφαλίδα αντί να δημιουργήσει μια καινούργια. Στο *Σχήμα 3-7* απεικονίζετε αυτό, το ESP μπορεί μόνο να κρυπτογραφεί και/ή να παρέχει προστασία ακεραιότητας δεδομένων, αλλά δεν δημιουργεί καινούργια IP επικεφαλίδα.
Το αρχικό πακέτο επεξεργάζεται και ύστερα εισέρχεται η ESP επικεφαλίδα μετά από την IP επικεφαλίδα. Στην περίπτωση όπου το πακέτο έχει και άλλες IPSec επικεφαλίδες, τότε η ESP επικεφαλίδα προστίθεται πριν από αυτές. Στο τέλος του πακέτου εισέρχονται άλλα δύο πεδία το ESP trailer και τα προαιρετικά δεδομένα εξακρίβωσης γνησιότητας. Το ESP στην κατάσταση μεταγωγής δεν παρέχει κρυπτογράφηση και εξακρίβωση γνησιότητας στην επικεφαλίδα IP. Το πλεονέκτημα είναι το χαμηλό υπολογιστικό φορτίο. Στο επόμενο σχήμα φαίνεται πως είναι αυτού του είδους τα πακέτα.



Σχήμα 3-7: *Πακέτο με ESP σε κατάσταση μεταφοράς*

3.3.2 Ανάλυση του πακέτου Encapsulating Security Payload

Το πρωτόκολλο ESP προσθέτει μια επικεφαλίδα (header) και ένα trailer γύρω από κάθε «καθαρή πληροφορία» (payload) ενός πακέτου. Στο *Σχήμα 3-8* απεικονίζονται τα πεδία που αποτελούν το ESP πακέτο.



Σχήμα 3-8: *Τα πεδία από τα οποία αποτελείται το ESP*

- **SPI:** Η τιμή SPI, η διεύθυνση IP και το πρωτόκολλο ασφαλείας (ESP) ορίζουν μονοσήμαντα τον SA που χρησιμοποιείται.
- **Sequence Number**: Είναι η μεταβλητή που αυξάνει κατά ένα σε κάθε πακέτο που αποστέλλεται και χρησιμοποιείται για την υποστήριξη της υπηρεσίας αποφυγής λανθασμένων επαναλήψεων πακέτων.

Τα επόμενα πεδία αφορούν την «καθαρή πληροφορία» του πακέτου. Αποτελείται από τα δεδομένα, τα οποία είναι κρυπτογραφημένα, και το Initialization Vector (IV), το οποίο δεν έχει κρυπτογραφηθεί. Το (IV) χρησιμοποιείται κατά την κρυπτογράφηση και η τιμή του είναι διαφορετική για κάθε πακέτο. Έτσι στην περίπτωση που δυο πακέτα έχουν το ίδιο περιεχόμενο, το IV θα προκαλέσει την κρυπτογράφηση των δυο πακέτων με διαφορετικό όμως, αποτέλεσμα. Αυτή η δυνατότητα κάνει το πρωτόκολλο ESP να είναι λιγότερο ευάλωτο στη ανάλυση της κρυπτογράφησης (cryptanalysis).

Το τρίτο μέρος του πακέτου είναι trailer που προστίθεται από το ESP, το οποίο περιέχει τουλάχιστον δυο πεδία και προαιρετικά μπορεί να προστεθεί ακόμα ένα.

- **Padding**: Πολλές φορές ο αλγόριθμος που απαιτείται για την κωδικοποίηση της πληροφορίας, απαιτεί αυτή να έχει μήκος πολλαπλάσιο κάποιου αριθμού bytes. Αν αυτό δεν ικανοποιείται από την αρχική πληροφορία, προστίθενται στο padding τόσα μηδενικά όσα χρειάζονται για να ικανοποιηθεί η συνθήκη.
- **Padding Length**: Είναι η τιμή που δείχνει το μήκος του padding σε bytes.
- **Authentication Data (προαιρετικό)**: Και εδώ περιέχεται ο Αριθμός Ελέγχου Ακεραιότητας (Integrity Check Value - ICV) όπως και στο AH. Αυτό σημαίνει ότι το πρωτόκολλο ESP έχει την ιδιότητα πιστοποίησης της ακεραιότητας των δεδομένων, αφού σε αυτήν την περίπτωση η τιμή ICV υπολογίζεται επάνω σε όλο το πακέτο (επικεφαλίδα και δεδομένα).

3.3.3 Τρόπος λειτουργίας ESP

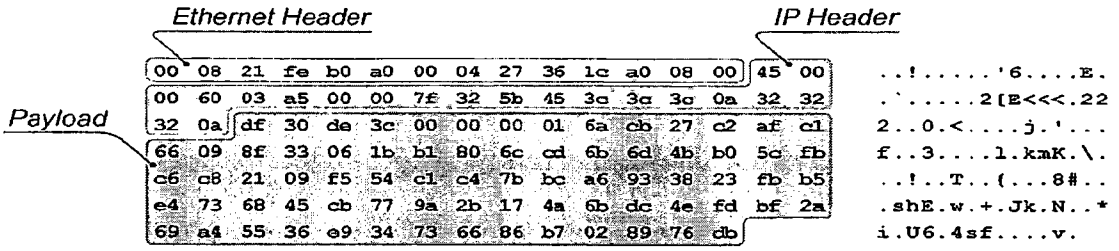
Με την ιδία λογική, όπως και με το πρωτόκολλο AH, έτσι στο ESP, θα χωρίσουμε την επεξεργασία που πραγματοποιείται σε δυο κομμάτια: την επεξεργασία εξερχόμενων και εισερχόμενων πακέτων.

Επεξεργασία εξερχόμενων πακέτων: Το πακέτο προς αποστολή φτάνει στο στρώμα IPSec. Αυτό συμβουλεύεται την πολιτική ασφαλείας από την βάση SPD για τον τύπο του πακέτου, καταλήγει σε συγκεκριμένη SA και εφαρμόζει το πρωτόκολλο ESP στο πακέτο. Σε αυτό το στάδιο συγχωνεύει στα δεδομένα (data) οτιδήποτε υπάρχει μετά την επικεφαλίδα ESP (πρωτόκολλα ανώτερου στρώματος -κατάσταση μεταφοράς-, πρωτόκολλα ανώτερου στρώματος μαζί με IP header -κατάσταση tunnel-, και τέλος προσθέτει ότι χρειάζεται στο πεδίο Padding. Έπειτα, κωδικοποιεί το διαμορφωμένο πακέτο. Η κωδικοποίηση γίνεται πάνω στις περιοχές data, padding, padding length και next header. Δεν περιλαμβάνεται η επικεφαλίδα ESP και το Authentication Data. Ο αλγόριθμος κωδικοποίησης ορίζεται από τον SA. Στην συνεχεία υπολογίζεται η τιμή του Sequence Number ανεξάρτητα από το εάν είναι επιλεγμένη η υπηρεσία αποφυγής επαναλήψεων και τελευταίο βήμα είναι ο υπολογισμός της τιμής ICV στο Authentication data εάν είναι επιλεγμένη η υπηρεσία πιστοποίησης δεδομένων για το πρωτόκολλο ESP.

Επεξεργασία εισερχόμενων πακέτων: Με τον που φτάνει ένα πακέτο, το IPsec του παραλήπτη διαβάζει τη μεταβλητή SPI, τη διεύθυνση IP του αποστολέα και το πρωτόκολλο ESP, συμβουλεύεται την SPD και καταλήγει στην SA που έχει χρησιμοποιηθεί. Στη συνέχεια, με οδηγό την SA προχωρεί στα εξής βήματα:

- Αν είναι επιλεγμένη η υπηρεσία αποφυγής επαναλήψεων ελέγχει την τιμή Sequence Number.
- Αν είναι επιλεγμένη η υπηρεσία πιστοποίησης του πακέτου, υπολογίζεται ξανά η τιμή ICV σύμφωνα με τον αλγόριθμο που ορίζει ο SA και συγκρίνεται με αυτή που περιέχεται στο πακέτο. Σημειώνεται ότι τόσο στον αποστολέα όσο και στον παραλήπτη, η τιμή ICV υπολογίζεται πάνω σε κωδικοποιημένα δεδομένα.
- Αποκωδικοποιούνται τα κρυπτογραφημένα δεδομένα με την βοήθεια του αλγόριθμου που ορίζει ο SA, και τελικά λαμβάνεται το γνήσιο πακέτο.

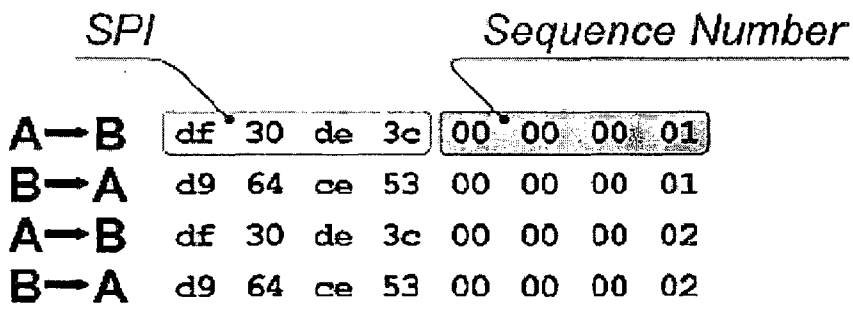
Στην συνεχεία παρουσιάζετε ένα απλό παράδειγμα για να γίνει πιο κατανοητή η λειτουργία του πρωτοκόλλου ESP.



Σχήμα 3-9: *Πακέτο ESP*

Στο *Σχήμα 3-9* έχουμε τα bytes που αποτελούν ένα ESP πακέτο και την μετάφραση του με τον ASCII κώδικα, όπως στο κεφάλαιο 3.2.4. Η αλφανουμερική ακολουθία που ήταν ορατή στα δεδομένα που ήταν προστατευμένα με AH, εδώ δεν εμφανίζετε εξαιτίας της κρυπτογράφησης που έχει γίνει. Τα ESP πακέτα περιέχουν πέντε πεδία: Ethernet επικεφαλίδα, IP επικεφαλίδα, ESP επικεφαλίδα, κρυπτογραφημένα δεδομένα (payload and ESP trailer), και (προαιρετικά) authentication πληροφορίες. Από τα κρυπτογραφημένα δεδομένα δεν είναι δυνατόν να προσδιοριστεί από ποια κατάσταση αυτό το πακέτο προήρθε, είτε κατάσταση μεταγωγής, είτε κατάσταση tunnel. Επειδή όμως, η IP επικεφαλίδα δεν έχει κρυπτογραφηθεί, το πεδίο του IP πρωτοκόλλου στην επικεφαλίδα, μας αποκαλύπτει ποιο πρωτόκολλο χρησιμοποιήθηκε (στην περίπτωση μας ESP). Όπως είδαμε στα σχήματα *3-6* και *3-7* το πεδίο που δεν έχει κρυπτογραφηθεί και στις δυο καταστάσεις (tunnel and transport) είναι το ίδιο.

Από το *Σχήμα 3-9* είναι δύσκολο να καταλάβουμε εάν η ESP επικεφαλίδα είναι κρυπτογραφημένη ή όχι. Στο παρακάτω *Σχήμα, 3-10*, που απεικονίζει τα τέσσερα πρώτα πακέτα που ανταλλάσσουν ο υπολογιστής A και ο υπολογιστής B σε μια σύνδεση με ESP βλέπουμε ότι το πεδίο του SPI και του sequence αριθμού λειτουργεί με το ίδιο σκεπτικό όπως με το AH. Ο κάθε υπολογιστής χρησιμοποιεί διαφορετική SPI τιμή για τα πακέτα του, που αντιστοιχούν στην ESP σύνδεση κάθε υπολογιστή. Επίσης στην αρχή κάθε υπολογιστής θέτει τον sequence αριθμό στην τιμή 1 και έπειτα με το δεύτερο πακέτο αυξάνει την τιμή στο 2.



Σχήμα 3-10: *Πεδία της ESP επικεφαλίδας από δείγματα πακέτων*

3.3.4 Συμπερασματικά για το πρωτόκολλου ESP

Σε κατάσταση διόδου, το ESP μπορεί να παρέχει κρυπτογράφηση και προστασία ακεραιότητας δεδομένων για ένα IP πακέτο που έχει ενθυλακωθεί, καθώς επίσης και αυθεντικοποίηση της επικεφαλίδας ESP. Η κατάσταση tunnel μπορεί να είναι συμβατή με την τεχνολογία NAT.

Σε κατάσταση μεταγωγής, το ESP παρέχει κρυπτογράφηση και προστασία ακεραιότητας για την «καθαρή πληροφορία» (payload) και για το αρχικό IP πακέτο, όπως επίσης προστασία ακεραιότητας και για τη επικεφαλίδα ESP . Δεν είναι όμως συμβατό με την τεχνολογία NAT.

Η πιο συνηθισμένη κατάσταση που χρησιμοποιείται στο IPSec είναι η ESP tunnel κατάσταση. Επειδή κρυπτογραφεί την επικεφαλίδα του IP, τροποποιεί την αληθινή διεύθυνση πηγής (source) και προορισμού (destination) του πακέτου. Επίσης, το ESP μπορεί να προσθέσει "γέμισμα" (padding) στα πακέτα που δυσκολεύει την ανάλυση της κρυπτογράφησης.

Εάν και το ESP μπορεί να παρέχει κρυπτογράφηση ή προστασία ακεραιότητας δεδομένων ή και τα δυο μαζί, παρόλα αυτά η βέλτιστη πρακτική θα ήταν η ESP κρυπτογράφηση να μην χρησιμοποιείται χωρίς προστασία ακεραιότητας.

3.4 Πρωτόκολλο Ανταλλαγής Κλειδιών

Το πρωτόκολλο διαχείρισης κλειδιών IKE (Internet Key Exchange) αναπτύχτηκε για την ρύθμιση των συσχετίσεων ασφάλειας, security associations (SA) για το IPSec, και για την αυτοματοποιημένη δημιουργία και ανανέωση κρυπτογραφικών κλειδιών. Το IKE χρησιμοποιεί πέντε διαφορετικούς τύπους ανταλλαγής κλειδιών για να δημιουργήσει SA, για την μεταφορά των πληροφοριών σχετικά με την κατάσταση της σύνδεσης και τυχόν λαθών που ίσως εμφανιστούν. Επίσης, καθορίζει καινούργιες ομάδες Diffie-Hellman, που είναι ο βασικός αλγόριθμος που χρησιμοποιείται για την ανταλλαγή κλειδιών.

Ο αλγόριθμος Diffie-Hellman είναι ένας μηχανισμός ανταλλαγής κλειδιών που αναπτύχθηκε από τους Diffie και Hellman το 1976. Με αυτόν γίνεται δυνατό, δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές κανάλι. Είναι ένας κρυπτογραφικός αλγόριθμος δημοσίου κλειδιού. Το πρωτόκολλο έχει δύο παραμέτρους (αριθμούς): p και g. Το p είναι ένας πολύ μεγάλος πρώτος αριθμός και το g είναι ένας αριθμός με την ιδιότητα $g^k \neq 1 \bmod p$ για όλους τους k από 1 μέχρι p-2 (δηλαδή, στοιχείο-γεννήτορας (generator) στο σώμα των ακεραίων Modulo p). Τα p,g τα γνωρίζουν όλοι – είναι δημοσίως γνωστά. Ας υποθέσουμε τώρα ότι δύο χρήστες, ο A και ο B, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο A παράγει μία τυχαία τιμή x και ο B μία τυχαία τιμή y (όπου τα x,y είναι μικρότερα του p). Τα x,y κρατούνται μυστικά – μόνο ο A δηλαδή γνωρίζει το x και μόνο ο B το y. Στη συνέχεια ο A υπολογίζει τον αριθμό $x' = g^x \bmod p$ και ο B τον αριθμό $y' = g^y \bmod p$. Κατόπιν, ο ένας στέλνει στον άλλον τις τιμές αυτές. Τέλος, ο A κάνει τον υπολογισμό $(y')^x = g^{xy} \bmod p$ και ο B κάνει με την σειρά του τον υπολογισμό $(x')^y = g^{xy} \bmod p$. Συνεπώς και οι δύο υπολογίζουν τον ίδιο αριθμό – ο οποίος θα είναι το μυστικό κλειδί που θα χρησιμοποιήσουν. Η ασφάλεια του πρωτοκόλλου αυτού βασίζεται στο γεγονός ότι ένας επιτιθέμενος, ο οποίος παρακολουθεί το τι ανταλλάσσουν οι A και B, δεν μπορεί από τα x', y' να υπολογίσει το μυστικό κλειδί: για να το κάνει αυτό θα πρέπει να ξέρει είτε το x είτε το y. Όμως, όταν τα p και g είναι πολύ μεγάλα, το να ξέρει κανείς το x' ή το y' δεν του αρκεί για να βρει το x ή το y.

Στο IPSec, το IKE παρέχει τον μηχανισμό μέσω του οποίου κατασκευάζονται ασφαλείς IPSec συνδέσεις. Σε αυτό το κεφάλαιο γίνεται περιγραφή των τριών, πιο συνηθισμένων τύπων IKE ανταλλαγής κλειδιών (main mode, aggressive mode, quick mode) και εξετάζετε ο τρόπος λειτουργιάς τους μαζί με το πρωτόκολλο IPSec. Στο τέλος του κεφαλαίου γίνεται αναφορά και στην δεύτερη έκδοση του IKE και στις διαφορές που έχει από την πρώτη έκδοση.

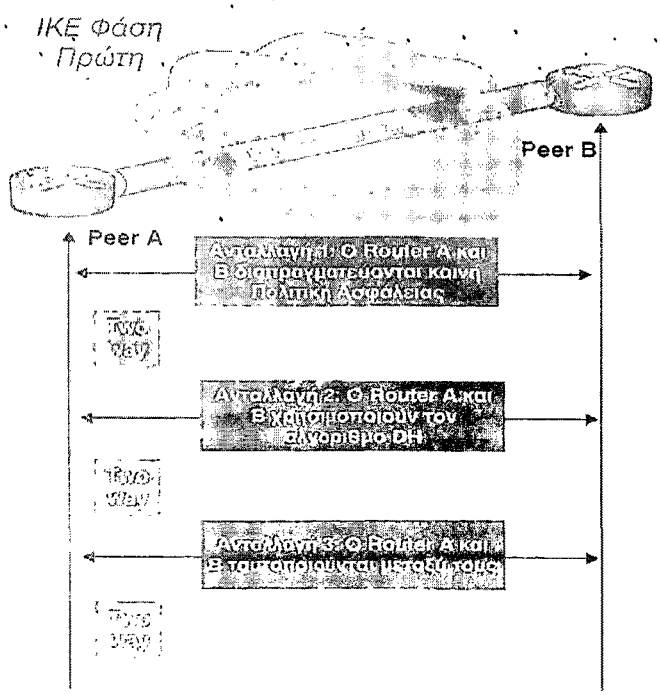
3.4.1 Πρώτη φάση του πρωτοκόλλου IKE

Ο ρόλος του πρωτοκόλλου IKE στην πρώτη φάση ανταλλαγής είναι να δημιουργήσει ένα ασφαλές κανάλι επικοινωνίας μεταξύ των δυο IPSec άκρων μέσου του οποίου να μεταφέρονται IPsec συσχετίσεις ασφάλειας.

Το ασφαλές κανάλι που δημιουργείτε ονομάζετε IKE SA και πρέπει να ολοκληρωθεί με επιτυχία ειδάλλως το IKE δεν μπορεί να προχωρήσει στα επόμενα βήματα αφού εδώ παρέχετε αμφίδρομη κρυπτογράφηση και αυθεντικοποίηση για τις επόμενες φάσεις τις IKE ανταλλαγής. Η πρώτη φάση του IKE μπορεί να πραγματοποιηθεί με δυο τρόπους: είτε τον κύριο τρόπο (main) είτε τον επιθετικό (aggressive).

3.4.1.1 Main mode

Στον κύριο τρόπο έχουμε συνολικά τρεις ανταλλαγές μηνυμάτων από κάθε συμβαλλόμενο μέρος μιας IPSec επικοινωνίας (*Σχήμα 3-11*).



Σχήμα 3.11: *Πρώτη Φάση IKE ανταλλαγής*

Στην πρώτη ανταλλαγή κάθε μέρος προτείνει τις παραμέτρους που πρόκειται να χρησιμοποιηθούν για την συσχέτιση ασφάλειας. Τέσσερεις από αυτές τις παραμέτρους, είναι υποχρεωτικές, και όλες μαζί αναφέρονται ως «σουίτα προστασίας» protection suite. Οι παράμετροι αυτοί είναι:

- Αλγόριθμος κρυπτογράφησης.
- Αλγόριθμος προστασίας ακεραιότητας.
- Μέθοδος αυθεντικοποίησης. Υπάρχουν αρκετοί μέθοδοι για την αυθεντικοποίηση των δυο συμβαλλόμενων μερών, όπως:

  - **Προμοιρασμένα Κλειδιά (Pre-Shared):** Σε κάθε ένα από τα συμβαλλόμενα μέρη δίνεται το ίδιο μυστικό κλειδί εκ των προτέρων ώστε να το χρησιμοποιήσουν για να παράγουν μια τιμή βάση της οποίας θα δημιουργηθούν στην συνέχεια τα κρυφά κλειδιά. Τα κλειδιά θα παρέχουν προστασία για να κατασκευαστεί το ασφαλές κανάλι επικοινωνίας στη πρώτη φάση του IKE. Η επιτυχής ολοκλήρωση της πρώτης φάσης, αποτελεί απόδειξη ότι το κάθε άκρο έχει το Pre-Shared κλειδί, το όποιο εξυπηρετεί στην πιστοποίηση του ένα άκρου στο άλλο.

  - **Ψηφιακές υπογραφές (Digital Signatures).** Κάθε συμβαλλόμενο μέρος έχει τη δική το ψηφιακή υπογραφή, η οποία περιέχει το δημόσιο κλειδί. Το έναν άκρο χρησιμοποιεί το αντίστοιχο ιδιωτικό κλειδί για να υπογράψει ψηφιακά τα στοιχεία πριν τα στέλνει στο άλλο άκρο, το οποίο ελέγχει την υπογραφή χρησιμοποιώντας το όμοιο δημόσιο κλειδί. Οι αλγόριθμοι που χρησιμοποιούνται σε αυτή την περίπτωση είναι RSA και ο Digital Signature Standard (DSS) .

  - **Κρυπτογράφηση Δημόσιου Κλειδιού (Public Key Encryption):** Σε αυτή την μέθοδο κάθε άκρο κρυπτογραφεί τα δεδομένα με το δικό του ιδιωτικό κλειδί και αποκρυπτογραφεί τα δεδομένα με το δημόσιο κλειδί. Ο RSA αλγόριθμος συνήθως χρησιμοποιείται σε αυτή την περίπτωση.

  - **Εξωτερική πιστοποίηση (External Authentication):** Αυτή η μέθοδος, αν και δεν καθορίζετε σε αυτή την έκδοση του IKE, παρ' όλα αυτά χρησιμοποιείται από ορισμένες υλοποιήσεις IPSec με την εξωτερική πιστοποίηση σε servers και υπηρεσιες[22] όπως το Kerberos στην πέμπτη έκδοση του.

Diffie-Hellman (DH) Group: Το *Σχήμα 3-12* απεικονίζει τον πίνακα[23] που αντιστοιχίζει κάθε αριθμό ομάδας DH με ένα μήκος κλειδιού και με έναν τύπο παραγωγής. (Ο όρος MODP παραπέμπει στην εκθετική αύξηση του πρώτου συντελεστή, ενώ όρος EC2N στις ελλειπτικές καμπύλες. Είναι τεχνικές παραγωγής του κρυπτοσυστήματος

---

[22] Το Extensible Authentication Protocol (EAP), το οποίο επιτρέπει στο IPsec να χρησιμοποιήσει υπηρεσίες εξωτερικής πιστοποίησης όπως είναι το Kerberos and Remote Authentication Dial In User Service (RADIUS), βλέπε http://www.ietf.org/rfc/rfc2865.txt

[23] Το RFC 2409 καθορίζει τις ομάδες από την 1 μέχρι την 4. Το RFC 3526, More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE), καθορίζει τις υπόλοιπες ομάδες που εμφανίζονται στον πίνακα, βλέπε, http://www.ietf.org/rfc/rfc2409.txt, http://www.ietf.org/rfc/rfc3526.txt

Group Number	Generator	Modulus or Field Size
1	MODP	768-bit modulus
2	MODP	1024-bit modulus
3	EC2N	155-bit field size
4	EC2N	185-bit field size
5	MODP	1536-bit modulus
14	MODP	2048-bit modulus
15	MODP	3072-bit modulus
16	MODP	4096-bit modulus
17	MODP	6144-bit modulus
18	MODP	8192-bit modulus

Σχήμα 3-12: *Ορισμός ομάδων Diffie-Hellman*

Πιο αναλυτικά:

Πρώτη Ανταλλαγή: Εδώ καθορίζονται οι αλγόριθμοι ασφάλειας (κρυπτογράφησης) καί αυθεντικοποίησης ταυτότητας οι οποίοι πρόκειται να χρησιμοποιηθούν στα επόμενα βήματα: Για κάθε ένα άκρο δημιουργείται μία ξεχωριστή Συσχέτιση Ασφαλείας (SA) με πληροφορίες που περιλαμβάνουν τους αλγόριθμους κρυπτογράφησης και αυθεντικοποίησης που υποστηρίζονται από το κάθε άκρο της συνομιλίας, τον αλγόριθμο παραγωγής κοινού μυστικού κλειδιού (συμφωνία αρχικών παραμέτρων του Diffie-Hellman αλγορίθμου), τον χρόνο διάρκειας της πρώτης IKE φάσης, τον τρόπο αυθεντικοποίησης που θα χρησιμοποιηθεί (π.χ. Προμοιρασμένα κλειδιά) κ.ά. Στο τέλος της παραπάνω διαδικασίας καθένα από τα δυο άκρα του IPSec διαθέτει μία κοινή IKE SA.
Επίσης, σε αυτό το στάδιο γίνεται και η ανταλλαγή των cookies. Παρέχουν ένα επίπεδο ασφάλειας εναντίων των επιθέσεων άρνησης υπηρεσιών (denial of service)[24] διότι τα cookies είναι μερικώς βασισμένα στην IP διεύθυνση του άλλου υπολογιστή και σε ένα μηχανισμό μέτρησης του χρόνου.

Το *Σχήμα 3-13* παρουσιάζει το αρχικό μήνυμα κατά την πρώτη ανταλλαγή στο main mode όπως αναπαριστάται στο Wireshark[25]. Σε αυτό το μήνυμα παρατηρούμε την αρχική τιμή του cookie, το mode που χρησιμοποιείται (εδώ το main mode), ποιος αλγόριθμος κρυπτογράφησης και hash θα πρέπει κανονικά να χρησιμοποιηθεί (DES-CBC) και ποια μέθοδος κρυπτογράφησης (PSK).

[24] Οι DOS επιθέσεις έχουν ως σκοπό να διακόψουν (άρνηση) της χρήσης του Internet ή/και του δικτύου στους νόμιμους χρήστες του. Για περισσότερες πληροφορίες βλέπε, http://en.wikipedia.org/wiki/Denial-of-service_attack

[25] Το wireshark είναι το δημοφιλέστερο λογισμικό ανοιχτού κώδικα για την ανάλυση των δικτύων, η επίσημη ιστοσελίδα του είναι: http://www.wireshark.org/

```
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0x04874D4D109ECCF4
    Responder cookie: 0x0000000000000000
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...0 = No encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 84
    Security Association payload
        Next payload: NONE (0)
        Length: 56
        Domain of interpretation: IPSEC (1)
        Situation: IDENTITY (1)
        Proposal payload # 1
            Next payload: NONE (0)
            Length: 44
            Proposal number: 1
            Protocol ID: ISAKMP (1)
            SPI size: 0
            Number of transforms: 1
            Transform payload # 1
                Next payload: NONE (0)
                Length: 36
                Transform number: 1
                Transform ID: KEY_IKE (1)
                Encryption-Algorithm (1): DES-CBC (1)
                Hash-Algorithm (2): MD5 (1)
                Group-Description (4): Default 768-bit MODP group (1)
                Authentication-Method (3): PSK (1)
                Life-Type (11): Seconds (1)
                Life-Duration (12): Duration-Value (28800)
```

Σχήμα 3-13: *Αρχικό μήνυμα της πρώτης ανταλλαγής στο Main Mode*

Δεύτερη Ανταλλαγή: Όταν επέλθει συμφωνία με τις προτεινόμενες παραμέτρους, εκτελείται ο αλγόριθμος για την παραγωγή του κοινού μυστικού κλειδιού (Diffie-Hellman) μέσω του οποίου δημιουργείτε ένα κλειδί που είναι κοινό και στα δύο μέρη. Ο αλγόριθμος είναι σημαντικός για τις διαδικασίες που αφορούν το IPSec πρωτόκολλο επειδή το κοινό μυστικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα χρησιμοποιώντας τους βασικούς αλγορίθμους κρυπτογράφησης που διευκρινίζονται στα IPSec SA (π.χ. στον DES). Στο παρακάτω *Σχήμα 3-14* απεικονίζετε το αρχικό μήνυμα από την δεύτερη ανταλλαγή. Το περιεχόμενο αυτών των μηνυμάτων διαφέρει ανάλογα με την μέθοδο αυθεντικοποίησης που χρησιμοποιείται.

```
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0x04874D4D109ECCF4
    Responder cookie: 0x38945FD052E53D60
    Next payload: Key Exchange (4)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...0 = No encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 152
    Key Exchange payload
        Next payload: Nonce (10)
        Length: 100
        Key Exchange Data
    Nonce payload
        Next payload: NONE (0)
        Length: 24
        Nonce Data
```

Σχήμα 3-14: *Αρχικό μήνυμα της δεύτερης ανταλλαγής στο Main Mode.*

Τρίτη Ανταλλαγή: Στην τρίτη ανταλλαγή, κάθε άκρο ταυτοποιεί το άλλο με την χρήση των κατάλληλων αλγόριθμων. Όπως και στην δεύτερη ανταλλαγή έτσι και εδώ, το περιεχόμενο των μηνυμάτων διαφέρει ανάλογα με την μέθοδο αυθεντικοποίησης. Άσχετα όμως από την μέθοδο που χρησιμοποιήθηκε, τα μηνύματα αυτά είναι κρυπτογραφημένα με βάση τις πληροφορίες που ανταλλάχτηκαν στο προηγούμενο βήμα. Στο *Σχήμα 3-15* έχουμε την αναπαράσταση του μηνύματος της τρίτης ανταλλαγής με την βοήθεια του Wireshark.

```
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xC4874D4D109ECCF4
    Responder cookie: 0x38945FD052E53D60
    Next payload: Identification (5)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...1 = Encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 60
    Encrypted payload (32 bytes)
```

Σχήμα 3-15: *Αρχικό μήνυμα της τρίτης ανταλλαγής στο Main Mode*

Συνοψίζοντας για τον main mode μπορούμε να πούμε ότι χρησιμοποιεί συνολικά έξι ανταλλαγές μηνυμάτων. Κάθε μια από αυτές τις ανταλλαγές εξυπηρετεί διαφορετικό σκοπό. Στην πρώτη γίνεται η διαπραγμάτευση των IKE συσχετίσεων ασφάλειας (SA), στην δεύτερη πραγματοποιείται η ανταλλαγή του κλειδιού, και στην τελευταία αυθεντικοποιούνται τα συμβαλλόμενα μέρη, το ένα στο άλλο.

3.4.1.2 Aggressive mode

Με αυτό τον τρόπο οι παραπάνω ανταλλαγές που περιγράφηκαν στο κεφάλαιο 3.4.1.1 συμπτύσσονται σε μια μόνο ανταλλαγή με τρία στάδια (αποστολέας - δέκτης, δέκτης - αποστολέας, αποστολέας - δέκτης) και για αυτό τον λόγο γίνονται με μεγαλύτερη ταχύτητα. Το μειονέκτημα του όμως είναι, ότι με την μεγαλύτερη ταχύτητα που προσφέρει μειώνεται το επίπεδο της ασφάλειας. Επιπλέον, η ταυτότητα της πληροφορίας που διακινείτε δεν είναι πάντοτε κρυφή με αποτέλεσμα κάποιος τρίτος να μπορεί να δει ποια είναι τα συμβαλλόμενα μέρη που διαπραγματεύονται. Ένα ακόμα θέμα είναι ότι πρέπει υποχρεωτικά όλες οι συσκευές που χρησιμοποιούν το πρωτόκολλο IPSec να υποστηρίζουν το main mode, ενώ όμως, η υποστήριξη του aggressive mode είναι προαιρετική. Γενικότερα, προτείνεται η χρησιμοποίηση του main mode για την ολοκλήρωση της πρώτης φάσης ανταλλαγής.

3.4.2 Δεύτερη φάση του πρωτοκόλλου IKE

Η δεύτερη φάση IKE πραγματοποιείται αμέσως μετά την ολοκλήρωση της πρώτης φάσης. Σκοπός εδώ είναι η δημιουργία IPSec Συσχέτισης Ασφαλείας (SA). Η IPSec SA διαφέρει από την IKE SA διότι δεν είναι αμφίδρομη. Αυτό σημαίνει ότι η σύνδεση IPSec μεταξύ των δυο συστημάτων απαιτεί δυο συσχετίσεις ασφάλειας. Η IPSec SA δημιουργείτε μέσω ενός μόνο τώρα τρόπου που ονομάζεται γρήγορος τρόπος (quick mode). Με το quick mode υπάρχουν τρία μηνύματα για τον καθορισμό των SA. Η επικοινωνία σε αυτό το στάδιο είναι κρυπτογραφημένη έτσι όπως έχει καθοριστεί από το προηγούμενο βήμα (IKE SA). Το *Σχήμα 3-16* δείχνει μια

αναπαράσταση του Quick Mode μηνύματος. Στην αυτή την φάση εκτελούνται παρακάτω ενέργειες:

- **Διαπραγμάτευση μιας κοινής πολιτικής IPSec**: Εδώ καθορίζονται οι τρόποι χρήσης των αλγόριθμων κρυπτογράφησης (π.χ. αν θα είναι σε κατάσταση μεταγωγής (transport mode) ή σε κατάσταση διόδου (tunnel mode), αν θα χρησιμοποιηθεί AH ή ESP κ.α.)

- **Δημιουργία IPSec Συσχέτισης Ασφαλείας:** Στην δεύτερη IKE φάση κάθε στιγμή μπορεί να δημιουργηθεί ένα νέο IPSec SA στη περίπτωση που το προηγούμενο τερματιστεί, είτε λόγω αδυναμίας συμφωνίας των συμβαλλομένων μερών για τις παραμέτρους επικοινωνίας είτε λόγω παρέλευσης του προκαθορισμένου χρόνου λειτουργίας ενός IPSec SA.

- **Χρήση Κλειδιών**. Τα κοινά μυστικά κλειδιά που δημιουργήθηκαν στη πρώτη φάση χρησιμοποιούνται για τις λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων που μεταφέρονται μεταξύ των δύο IPSec συμβαλλομένων μερών.

```
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0x04874D4D109ECCF4
    Responder cookie: 0x38945FD052E53D60
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags
        .... ...1 = Encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x7DEA6802
    Length: 164
    Encrypted payload (136 bytes)
```

Σχήμα 3-16: *Δείγμα Quick Mode μηνύματος*

Μόλις ολοκληρωθεί και το τρίτο μήνυμα, οι IPSec συσχετίσεις ασφάλειας έχουν ολοκληρωθεί. Όλες οι SA αποθηκεύονται σε μια βάση δεδομένων που ονομάζετε SAD - Security Association Database. Σε αυτή την βάση υπάρχουν οι παρακάτω πληροφορίες για κάθε προστατευμένη σύνδεση.

- Η IP διεύθυνση της πηγής
- Η IP διεύθυνση του προορισμού
- Το SPI
- Το πρωτόκολλο ασφάλειας IPsec (AH or ESP)
- Mode (transport or tunnel)

- Ο αλγόριθμος κρυπτογράφησης για το ESP (πχ, AES-CBC)
- Ο αλγόριθμος για την προστασία ακεραιότητας δεδομένων (πχ, HMAC-MD5)
- Τα κρυφά κλειδιά που έχουν χρησιμοποιηθεί από τους αλγορίθμους
- Το μήκος του κλειδιού

Στην πρώτη έκδοση του πρωτοκόλλου IKE υπάρχουν ορισμένα προβλήματα που παρουσιάζονται παρακάτω:

1. **Πολυπλοκότητα**
   - Το IKE πρωτόκολλο είναι αρκετά περίπλοκο και γι' αυτό άλλωστε καθορίζετε σε τρία διαφορετικά RFC (RFC2409, RFC2408, RFC2407).
   - Χρησιμοποιεί 8 τύπους ανταλλαγής στη πρώτη φάση.
     - Τέσσερις μεθόδους πιστοποίησης (Προχειρισμένα κλειδιά, ψηφιακές υπόγραφες, κρυπτογράφηση δημόσιου κλειδιού, εξωτερική πιστοποίηση).
     - Δυο modes (main mode, aggressive mode)
     - Η πολυπλοκότητα δημιούργησε προβλήματα στη λειτουργικότητα του IKE.
2. **Το IKE είναι ευάλωτο σε επιθέσεις Denial Of Service**
3. **Υπάρχει καθυστέρηση μέχρι την αρχικοποίηση του IPSec SA**

Εξαιτίας των προβλημάτων αυτών η IEFT σχεδίασε την δεύτερη έκδοση του, το IKE version 2.

3.4.3 IKE Version 2

Τα πλεονεκτήματα της δεύτερης έκδοσης του πρωτοκόλλου IKE είναι τα έξης:

- Καθορίζετε μόνο από ένα RFC[26]
- Απλοποιεί το πρωτόκολλο αντικαθιστώντας τις οκτώ διαφορετικές αρχικές ανταλλαγές που αναφέρθηκαν στο προηγούμενο κεφάλαιο, σε μόνο μια με τέσσερις ανταλλαγές μηνυμάτων
- Ενισχύει την αξιόπιστη μεταφορά των μηνυμάτων, προσθέτοντας μηχανισμό που επιβεβαιώνει ότι το μήνυμα παραδόθηκε στον προορισμό του
- Παρέχει επιπλέον ασφάλεια απέναντι σε επιθέσεις Denial Of Service.
- Επιλύει θέματα σχετικά με την συμβατότητα του IKE με την τεχνολογία NAT και με ζητήματα απομακρυσμένης πρόσβασης.

[26] Το IKEv2 καθορίζετε από το rfc 4306. Για περισσότερες πληροφορίες βλέπε, http://tools.ietf.org/html/rfc4306

Η δεύτερη έκδοση του IKE είναι ένα σχετικά νέο πρωτόκολλο που κυκλοφόρησε μόλις το 2006 και αναμένετε τα επόμενα χρόνια να καθιερωθεί ως το βασικό πρωτόκολλο ανταλλαγής κλειδιών. Το IKEv2 θα ενισχύσει την λειτουργία του IPSec και άλλων προϊόντων VPN και θα προωθήσει την χρήση του IPSec σε νέα πεδία, όπως είναι «κινητά με IP» (Mobile IP).

3.4.4 Συμπερασματικά για το πρωτόκολλο IKE

- Το IPsec χρησιμοποιεί το IKE για να δημιουργήσει συσχετίσεις ασφάλειας, οι οποίες είναι μια λίστα από τιμές που καθορίζουν τις συνδέσεις που προστατεύονται από το πρωτόκολλο IPSec. Στην πρώτη φάση δημιουργείτε μια IKE SA (συσχέτιση ασφάλειας) και στην δεύτερη δημιουργείτε μια IPSec SA (συσχέτιση ασφάλειας).

- Στην πρώτη φάση του IKE υπάρχουν δυο τρόποι: ο κύριος τρόπος (main mode) και ο επιθετικός τρόπος (aggressive mode). Στο main mode πραγματοποιείται η διαπραγμάτευση της IKE SA μέσα από έξι ανταλλαγές μηνυμάτων, ενώ στο aggressive mode μόνο σε μια.

- Η δεύτερη φάση του IKE έχει μόνο ένα τρόπο που ονομάζετε «γρήγορος τρόπος» (quick mode). Σε αυτό το βήμα καθορίζετε η IPSec SA με την χρησιμοποίηση τριών μηνυμάτων.

- Η δεύτερη έκδοση του πρωτοκόλλου IKE, απλοποίησε την πολυπλοκότητα του στην ανταλλαγή των κλειδιών και επίλυσε αρκετά σημαντικά ζητήματα, όπως η συμβατότητα του IKE με την τεχνολογία NAT.

3.5 IPSec και η τεχνική «Μεταγλώττισης Διευθύνσεων Δικτύου»

Η τεχνική μεταγλώττισης διευθύνσεων δικτύου (Network Address Translation-NAT) σχεδιάστηκε για την απλοποίηση και διατήρηση των IP διευθύνσεων. Η λειτουργία της έγκειται ότι παρέχει έναν μηχανισμό που επιτρέπει την χρησιμοποίηση ιδιωτικών διευθύνσεων σε εσωτερικά δίκτυα, και την «μεταγλώττιση» τους σε δημόσιες διευθύνσεις που μπορούν να δρομολογηθούν στο διαδίκτυο. Το σύστημα NAT λειτουργεί σε κάποιον δρομολογητή, ο οποίος συνδέει συνήθως δύο δίκτυα και μεταφράζει τις ιδιωτικές διευθύνσεις του εσωτερικού δικτύου σε διευθύνσεις που μπορούν να δρομολογηθούν προτού τα πακέτα προωθηθούν σε άλλο δίκτυο. Σαν μέρος αυτής της λειτουργίας το NAT μπορεί να ρυθμιστεί να κάνει γνωστή μόνο μία διεύθυνση στον έξω κόσμο για ολόκληρο το δίκτυο που συνδέει με αυτόν. Αυτό το χαρακτηριστικό παρέχει επιπλέον ασφάλεια αφού κρύβει ολόκληρο το εσωτερικό δίκτυο πίσω από μία διεύθυνση. Το NAT είναι κάτι ανάλογο των εσωτερικών (extension numbers) αριθμών σε τηλεφωνικά κέντρα. Οι διευθύνσεις που δεν δρομολογούνται στο διαδίκτυο και ονομάζονται ιδιωτικές είναι:

- 10.0.0.0 – 10.255.255.255 (16,777,216 κόμβοι)
- 172.16.0.0 – 172.31.255.255 (1,048,576 κόμβοι)
- 192.168.0.0 – 192.168.255.255 (65,536 κόμβοι)

Η τεχνολογία NAT είναι πολύ χρήσιμη σε επιχειρήσεις, μικρά γραφεία και σε ιδιώτες εξαιτίας τις ασφάλειας και ευελιξίας που προσφέρει. Δυστυχώς, όπως αναφερθείτε και στο κεφάλαιο 3.2.2 υπάρχουν ορισμένα σημαντικά ζητήματα ασυμβατότητας μεταξύ του πρωτοκόλλου IPSec και της τεχνολογίας NAT, διότι ο μηχανισμός βάση του οποίου λειτούργει το NAT, τροποποιεί την IP διεύθυνση του πακέτου, που έχει ως αποτέλεσμα την παραβίαση της προστασίας ακεραιότητας των δεδομένων που προστατεύει το IPSec. Ποιο συγκεκριμένα, επειδή το NAT αλλάζει την IP διεύθυνση πηγής (source) και προορισμού (destination), που χρησιμοποιείται για τον υπολογισμό του HMAC αλγορίθμου για το πεδίο της τιμής ελέγχου ακεραιότητας (ICV), αυτό προκαλεί την παραγωγή λάθους αποτελέσματος του ICV και το πακέτο απορρίπτεται. Το πρόβλημα παρουσιάζετε στο πρωτόκολλο AH, όπου όλη η IP επικεφαλίδα είναι προστατευμένη. Στο πρωτόκολλο ESP αν και η IP διεύθυνση πηγής και προορισμού δεν περιέχεται στον υπολογισμό του ICV, παρόλα αυτά μπορεί να υπάρξει δυσλειτουργία στο ESP όταν είναι σε κατάσταση μεταγωγής (transport mode) με τον υπολογισμό τις τιμής TCP checksum. Έχουν διατυπωθεί ορισμένες λύσεις για να ξεπεραστεί αυτό το πρόβλημα που περιλαμβάνουν τα παρακάτω:

- Η τεχνική NAT να χρησιμοποιείται προτού εφαρμοστεί το πρωτόκολλο IPSec. Αυτό μπορεί να πραγματοποιηθεί βάζοντας τις συσκευές με μια συγκεκριμένη σειρά ή με την χρήση IPSec gateways.
- Η χρήση UDP ενθυλάκωσης[27] στα ESP πακέτα. Αυτή η λύση μπορεί να πραγματοποιηθεί σε κατάσταση διόδου (tunnel mode) ESP ή με το πρωτόκολλο Layer 2 Tunneling Protocol (L2TP) σε κατάσταση μεταγωγής (transport mode) στο ESP. Ο τρόπος λειτουργίας του βασίζεται ότι επισυνάπτεται μια UDP επικεφαλίδα σε κάθε πακέτο, η οποία παρέχει μια IP διεύθυνση και μια UDP «θύρα» port, που μπορεί να χρησιμοποιηθεί στο NAT. Με αυτό τον τρόπο το πρόβλημα επιλύεται στις περισσότερες των περιπτώσεων. Επιπλέον, για να καταστεί εφικτό το IKE να μπορεί να διαπραγματευτεί την UDP ενθυλάκωση σχεδιάστηκε η τεχνική IPsec NAT Traversal (NAT-T)[28]. Με αυτή την τεχνική κατά την πρώτη φάση της IKE ανταλλαγής, και τα δυο συμβαλλόμενα μέρη κάνουν γνωστό, το ένα στο άλλο, ότι υποστηρίζουν το NAT-T μέσα από ένα vendor ID που ανταλλάσουν. Έπειτα, «ψάχνουν» να βρουν εάν υπάρχουν NAT λειτουργιές μεταξύ των δυο IPSec άκρων, στέλνοντας το καθένα ένα hash με κανονική τους IP διεύθυνση πηγής, την οποία και συγκρίνουν με αυτή που έχουν τώρα. Εάν είναι διαφορετικές σημαίνει ότι έχει μεταφραστεί η διεύθυνση τους άρα «τρέχουν» το NAT. Στην συνεχεία το πρωτόκολλο IKE προωθεί την κίνηση του από την UDP θύρα 500 στην θύρα 4500, για να αποφύγει τυχόν παρεμβολές από NAT συσκευές.

Η UDP ενθυλάκωση και το NAT-T βοήθησαν πολύ για να ξεπεραστεί το πρόβλημα άλλα ακόμα και τώρα πολλές IPSec συσκευές και εφαρμογές δεν είναι συμβατά με τις τεχνικές αυτές.

---

[27] Για περισσότερες πληροφορίες βλέπε, RFC 3948, UDP Encapsulation of IPsec Packets, διαθέσιμο στο http://www.ietf.org/rfc/rfc3948.txt

[28] Το NAT-T καθορίζετε από το rfc 3947, Negotiation of NAT-Traversal in the IKE, που είναι διαθέσιμο στο http://www.ietf.org/rfc/rfc3947.txt

3.6 Συμπεράσματα για το πρωτόκολλο IPSec

Σαν γενικό συμπέρασμα που μπορούμε να εξάγουμε έπειτα από την θεωρητική προσέγγιση του IPSec, είναι ότι θεωρείται ένας πλήρες πρωτόκολλο αφού περιλαμβάνει έναν αριθμό από αλγορίθμους αυθεντικοποίησης και κρυπτογράφησης στο επίπεδο του IP, καθώς επίσης είναι έτοιμο για μελλοντικές τροποποιήσεις (flexibility, scalability). Επειδή όμως το IPSec είναι ένα σύνολο πρωτοκόλλων αυτό το κάνει να είναι πολύ περίπλοκο στην υλοποίηση του και στην περίπτωση που δεν έχει κατανοηθεί καλά μπορεί να προκύψουν σημαντικά ζητήματα. Υπάρχουν αρκετοί τρόποι για να κατασκευαστεί ένα σύστημα VPN με IPSec, όπως είδαμε στα προηγούμενα κεφαλαία, άλλα ο προτεινόμενος είναι η χρησιμοποίηση του πρωτοκόλλου ESP σε tunnel mode. Προσφέρει μεγαλύτερο επίπεδο ασφάλειας περιορίζοντας τα ζητήματα ασυμβατότητας.

ΚΕΦΑΛΑΙΟ 4

4. Εναλλακτικά VPN πρωτόκολλα

Αν και το IPSec είναι ένα ολοκληρωμένο πρωτόκολλο που καλύπτει πολλές ανάγκες, πρέπει να σημειωθεί ότι υπάρχουν και άλλα VPN πρωτόκολλα, και κατηγοριοποιούνται ανάλογα με το επίπεδο που λειτουργούν στο TCP/IP μοντέλο (όπως φαίνεται στο πίνακα *4-1*).

Επίπεδο εφαρμογών (Application Layer): Αυτό το επίπεδο στέλνει και λαμβάνει δεδομένα για συγκεκριμένες εφαρμογές, όπως είναι το Simple Mail Transfer Protocol (SMTP), TELNET, Domain Name System (DNS).
Επίπεδο μεταφοράς (Transport Layer): Το στρώμα μεταφοράς είναι υπεύθυνο για την μεταφορά μηνυμάτων, με έλεγχο σφαλμάτων (error control), κατάτμηση (fragmentation) και ρύθμιση ροής (flow control). Η μετάδοση μηνυμάτων μεταξύ δυο οντοτήτων μπορεί να κατηγοριοποιηθεί ως εξής: 1. Connection-oriented, π.χ. TCP, δηλαδή η μεταφορά δεδομένων γίνεται μέσω σύνδεσης, η οποία οριοθετείται από ένα σήμα έναρξης και ένα σήμα τέλους ή διακοπής. 2. connectionless, π.χ. UDP, δηλαδή δεν υπάρχει η έννοια της σύνδεσης προτού αρχίσει η μεταφορά των δεδομένων.
Επίπεδο δικτυού (Network Layer): Αυτό το επίπεδο είναι υπεύθυνο για την δρομολόγηση πακέτων διαμέσου ενός δικτύου δικτύων (internetwork) ή διαδικτύου. Το βασικό πρωτόκολλο είναι το IP (Internet Protocol).
Επίπεδο ζεύξης δεδομένων (Data Link): Αυτό το επίπεδο καθορίζεται από πρωτόκολλα τα οποία ρυθμίζουν τη μετάδοση δεδομένων σε ένα τηλεπικοινωνιακό κανάλι αποτελούμενο από ένα μοναδικό φυσικό μέσο. Το πιο γνωστό πρωτόκολλο αυτού του επιπέδου είναι το Ethernet.

Πίνακας 4-1: *Επίπεδα του TCP/IP μοντέλου*

4.1 VPN πρωτόκολλα επιπέδου ζεύξης δεδομένων

Σε αυτή την κατηγορία τα VPN πρωτόκολλα λειτουργούν κάτω από το επίπεδο δικτύου στο TCP/IP μοντέλο και αυτό σημαίνει ότι διάφορα πρωτόκολλα δικτύου μπορούν να χρησιμοποιηθούν, όπως το IP, IPX, NetBEUI. Πολλά VPN πρωτόκολλα όπως το IPSec υποστηρίζουν μονό το IP. Για αυτόν τον λόγο τα VPN πρωτόκολλα επιπέδου ζεύξης δεδομένων προσφέρουν μια εφικτή επιλογή για την προστασία των δικτύων του δεν «παίζουν» με το IP.

4.1.1 Πρωτόκολλο PPTP

Το Point-to-Point Tunneling Protocol[29] σχεδιάστηκε από μια ομάδα κατασκευαστών (3Com, Ascend Communications, Microsoft, ECI Telematics και US Robotics). Σε αυτό το πρωτόκολλο δημιουργείτε μια Point-to-Point δίοδος (tunnel) όπου μέσα εκεί κρυπτογραφούνται τα PPP frames, και μεταφέρονται χρησιμοποιώντας μια τροποποιημένη έκδοση του πρωτοκόλλου Generic Routing Encapsulation (GRE). Επίσης, δημιουργείτε μια επιπλέον ξεχωριστή σύνδεση, στην TCP θύρα 1723 που ελέγχει και διαχειρίζεται το tunnel. Το PPTP δεν παρέχει από μονό του αυθεντικοποίηση και προστασία ακεραιότητας των δεδομένων γι' αυτό πρέπει να χρησιμοποιείται σε συνδυασμό είτε με το πρωτόκολλο CHAP[30] (Challenge Handshake Authentication Protocol), είτε με το πρωτόκολλο MPPE[31] (Microsoft Point-to-Point Encryption) για να παρέχει ασφάλεια απορρήτου. Το πρωτόκολλο MPPE αναπτύχτηκε από την Microsoft για να παρέχει μεγαλύτερο επίπεδο ασφάλειας. Για τον ίδιο λόγο άλλωστε η Microsoft σχεδίασε και το MS-CHAP[32] διότι και το CHAP και το PAP[33] έχουν γνωστές αδυναμίες. Από τα παραπάνω γίνεται φανερό από το PPTP είναι ένα πολύ απλό πρωτόκολλο για την δημιουργία tunnel σε ένα VPN δίκτυο.

Αρχικά η απλότητα του PPTP ήταν και το πλεονέκτημα του, αλλά σε ένα δυναμικό περιβάλλον όπως είναι αυτό του διαδικτύου, με καθημερινές μεταβολές και την εξέλιξη κακόβουλων συστημάτων και προγραμμάτων, η απλότητα στην υλοποίηση του μετατράπηκε σε μειονέκτημα. Το επίπεδο της ασφάλειας που προσφέρει είναι σαφώς μικρότερο απ' ότι το πρωτόκολλο IPSec και για τις επιχειρήσεις όπου η ασφάλεια αποτελεί ένα κρίσιμο ζήτημα η χρησιμοποίηση του δεν είναι προτείνετε.

4.1.2 Πρωτόκολλο L2F

Το 1996 η Cisco εξαιτίας της μεγάλης ανάπτυξης των dial-up υπηρεσιών , σχεδίασε το δικό της πρωτόκολλο που το ονόμασε, Layer Two Forwarding [L2F][34].

---

[29] Για περισσότερες πληροφορίες σχετικά με το PPTP, βλέπε RFC 2637, Point-to-Point Tunneling Protocol, διαθέσιμο στο http://www.ietf.org/rfc/rfc2637.txt

[30] Το Challenge-Handshake Authentication Protocol (CHAP) είναι πρωτόκολλο ελέγχου ταυτότητας μέσω ανταλλαγής χειραψίας. Καθορίζετε από το RFC 1994, για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc1994.txt

[31] Για περισσότερες πληροφορίες σχετικά με το MPPE, βλέπε RFC 3078, Microsoft Point-to-Point Encryption (MPPE) Protocol, διαθέσιμο στο http://www.ietf.org/rfc/rfc3078.txt

[32] Υπάρχει ένα κείμενο που ασχολείται με αδυναμίες του πρωτοκόλλου MS-CHAP το «Exploiting known security holes in Microsoft's PPTP Authentication Extensions (MS-CHAPv2)» από τον Jochen Eisinger που έχει αναπτύξει και ένα πρόγραμμα και τεκμηρίωση της άποψης του, διαθέσιμα στο http://penguin-breeder.org/pptp/download/

[33] Το Password Authentication Protocol (PAP) είναι μια μέθοδος πιστοποίησης χρήστη που χρησιμοποιείται από PPP servers. Καθορίζετε από το RFC 1334, για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc1334.txt

[34] Για περισσότερες πληροφορίες σχετικά με το L2F βλέπε, RFC 2341, Cisco Layer Two Forwarding (Protocol) L2F, διαθέσιμο στο http://www.ietf.org/rfc/rfc2341.txt

Το πρόβλημα ήταν ότι λόγο των πολλών και διαφορετικών πρωτοκόλλων που υπήρχαν χρειαζόταν ένας τρόπος για να δημιουργείται μία εικονική dial-up σύνδεση, όπου οποιοδήποτε από τα μη-IP πρωτόκολλα να μπορεί να χρησιμοποιεί τα πλεονεκτήματα που παρέχει το διαδίκτυο. Για τη χρήση του χρειάζεται την ύπαρξη Access Server και Router (δρομολογητή). Επιτρέπει πάνω από μία ταυτόχρονες συνδέσεις κατά τη δημιουργία των tunnel. Χρησιμοποιεί το PPP για την πιστοποίηση ταυτότητας του χρήστη αλλά επίσης υποστηρίζει TACACS+ (Terminal Access Controller Access Control System)[35] και RADIUS (Remote Authentication Dial-in User Service)[36]. Έχει δύο επίπεδα πιστοποίησης: το πρώτο από το ISP όταν δημιουργεί το tunnel και το δεύτερο όταν γίνεται η σύνδεση με την επιχείρηση. Ορισμένα από τα πλεονεκτήματα που προσφέρει είναι:

- Ανεξαρτησία πρωτοκόλλων (IPX, SNA[37])
- Δυναμικά και ασφαλή tunnels
- Υπηρεσίες χρέωσης (accounting)
- Αυθεντικοποίηση (PPP, CHAP, TACACS ή RADIUS)

4.1.3 Πρωτόκολλο L2TP

Το Layer Two Tunneling Protocol (L2TP)[38] είναι το αποτέλεσμα της συγχώνευσης των πρωτοκόλλων PPTP και L2F ύστερα από συμφωνία των εταιριών που τα ανέπτυξαν. Συνδυάζει πολλά χαρακτηριστικά και πλεονεκτήματα άλλων πρωτοκόλλων και επίσης την υποστήριξη μεγάλων εταιριών.

Είναι ευέλικτο μιας και λειτουργεί στο δεύτερο επίπεδο του μοντέλου OSI και δίνει τη δυνατότητα χρήσης των πρωτοκόλλων IPX και NETBEUI[39] καθώς επίσης και των τεχνολογιών ATM και Frame Relay.

---

[35] Είναι ένα πρωτόκολλο πιστοποίησης απομακρυσμένης πρόσβασης. Για περισσότερες πληροφορίες βλέπε http://tools.ietf.org/html/rfc1492 και http://tools.ietf.org/html/rfc0927

[36] Είναι ένα πρωτόκολλο δικτύου που παρέχει κεντρική πρόσβαση, εξουσιοδότηση, και καταγραφή των ενεργειών του χρηστή. Για περισσότερες πληροφορίες βλέπε, http://tools.ietf.org/html/rfc2865

[37] Το Systems Network Architecture (SNA) Αναπτύχθηκε από την IBM, με σκοπό να εξυπηρετήσει την επικοινωνία μεταξύ υπολογιστών — σταθμών εξυπηρέτησης και υπολογιστών —τερματικών, σύμφωνα με το σχήμα πελάτη – εξυπηρετητή, για περισσότερες πληροφορίες βλέπε, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/IBM-SNA-Protocols.html

[38] Για περισσότερες πληροφορίες σχετικά με το L2TP βλέπε, RFC 2661, Layer Two Tunneling Protocol L2TP, διαθέσιμο στο http://www.ietf.org/rfc/rfc2661.txt

[39] Το NetBIOS Extended User Interface (NetBEUI) είναι ένα πρωτόκολλο δικτύου που χρησιμοποιείται συνήθως σε μικρά τοπικά δίκτυα (LAN) με 1 έως 200 υπολογιστές. Το NetBEUI είναι γρήγορο και μικρό, λειτουργεί σωστά μέσα σε ένα LAN, όμως δεν έχει δυνατότητα δρομολόγησης, δηλαδή δεν μπορεί να χρησιμοποιηθεί από υπολογιστές που δεν βρίσκονται στο ίδιο τοπικό δίκτυο ή υποδίκτυο για επικοινωνία. Στις περισσότερες περιπτώσεις, το NetBEUI έχει αντικατασταθεί από το TCP/IP

Με το Layer Two Tunneling Protocol υπάρχουν τέσσερα είδη tunneling του μπορούν να δημιουργηθούν:

- voluntary tunnel
- compulsory tunnel — εισερχόμενη κλήση
- compulsory tunnel — απομακρυσμένη κλήση
- L2TP multi-hop σύνδεση

Το πρωτόκολλο δεν ασχολείται καθόλου με την ταυτοποίηση των συναλλασσόμενων μερών μέσα στην επιπέδου 2 σύνδεση και την κρυπτογράφηση ή γενικότερα με την ασφάλεια των δεδομένων που μεταδίδονται μέσα από το tunnel. Για τον λόγο αυτό, στις περιπτώσεις όπου το tunnel περνά μέσα από δίκτυα τρίτων, που όλα τα δεδομένα που μεταφέρει μπορεί να υποκλαπούν, συνηθίζεται η ενθυλάκωσή του σε έναν άλλο μηχανισμό ο οποίος προσφέρει κρυπτογράφηση και ακεραιότητα, όπως π.χ. το IPSec. Γενικότερα μπορούμε να πούμε ότι επειδή το L2TP χρησιμοποιεί πολλά χαρακτηριστικά του IPSec για να επιτύχει μεγαλύτερη ασφάλεια, θεωρείται ότι παρέχει υπηρεσίες όχι μόνο δεύτερου αλλά και τρίτου επιπέδου.

4.2 Πρωτόκολλα επιπέδου μεταφοράς

Το πρωτόκολλο Secure Socket Layer (SSL)[40] έχει αναπτυχτεί από την Netscape Communications Corporation το 1994. Παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ ενός πελάτη και ενός διακομιστή για την ανταλλαγή πληροφοριών μέσω Internet. Η έκδοση που χρησιμοποιείται ευρέως είναι η 3. Το Transport Layer Security πρωτόκολλο αποτελεί τη συνέχεια του Secure Sockets Layer (SSL) πρωτοκόλλου αλλά δεν είναι ευρέως διαδεδομένο λόγω της ασυμβατότητας του με το SSL.

Χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού και παρέχει:

- Εμπιστευτικότητα
- Ακεραιότητα
- Αυθεντικοποίηση διακομιστή, και
- Προαιρετικά, αυθεντικοποίηση πελάτη.

Το βασικό του πλεονέκτημα είναι ότι είναι ανεξάρτητο από τα πρωτόκολλα επιπέδου εφαρμογής. Το SSL διατηρεί το κανάλι επικοινωνίας ανοιχτό μέχρι μια από τις δύο οντότητες να αιτηθεί τερματισμό της επικοινωνίας (π.χ. να κλείσει το παράθυρο του browser) όπου σε αυτή την περίπτωση η σύνοδος τερματίζεται.

Το SSL απαιτεί τόσο ο server όσο και ο browser του πελάτη να το υποστηρίζουν. Ο χρήστης μπορεί να επαληθεύσει μια προστατευμένη από το SSL επικοινωνία εξετάζοντας το URL το οποίο θα πρέπει να ξεκινά με την ακολουθία "https://" αντί του "http://".

---

[40] Για περισσότερες πληροφορίες βλέπε, RFC 2818, HTTP Over TLS, διαθέσιμο στο http://www.ietf.org/rfc/rfc2818.txt

Ένας άλλος τρόπος είναι από την ύπαρξη κλειδαριάς ή ενός κλειδιού στον browser τα οποία υποδηλώνουν την προστασία των δεδομένων.

Το πρωτόκολλο SSL είναι οικείο στους περισσότερους χρήστες, ακόμα και σε εκείνους χωρίς ιδιαίτερο υπόβαθρο τεχνικών γνώσεων. Είναι ήδη εγκατεστημένο σε οποιοδήποτε Η/Υ που είναι συνδεδεμένος στο διαδίκτυο και χρησιμοποιεί έναν standard browser χωρίς κάποια ιδιαίτερη ρύθμιση. Το SSL VPN είναι ανεξάρτητο από το λειτουργικό σύστημα και επιτρέπει την κλιμάκωση στον έλεγχο πρόσβασης στις εφαρμογές, καθιστώντας το ιδανικό για «κινητούς» χρήστες που επιθυμούν να έχουν πρόσβαση από ένα μη «ασφαλές» άκρο (endpoint).[41]

4.3 Πρωτόκολλα επιπέδου εφαρμογών

Το Secure Shell (SSH)[42] είναι ένα πρόγραμμα αντικατάστασης του απλού telnet με την διαφορά ότι παρέχει αρκετά καλή αυθεντικοποίηση και κρυπτογράφηση κατά την απομακρυσμένη σύνδεση ενός υπολογιστή με έναν άλλον σε μη ασφαλή δίκτυα. Το SSH χρησιμοποιείται για την προστασία των κωδικών και άλλων πληροφοριών.

Είναι δηλαδή μια κρυπτογραφημένη διασύνδεση telnet, εννοώντας ότι οτιδήποτε στέλνεται στον κεντρικό υπολογιστή ή λαμβάνεται από αυτόν είναι κρυπτογραφημένο και δεν φαίνεται στους άλλους στο δίκτυο. Ορισμένες επιχειρήσεις έχουν επεκτείνει την χρήση του αφού δημιουργούν SSH tunnels μεταξύ των συμβαλλόμενων μερών, και έπειτα περνάνε από εκεί την κίνηση που επιθυμούν. Με αυτό τον τρόπο, μέσα από ένα και μόνο tunnel, υπάρχει η δυνατότητα να περνούν τα δεδομένα πολλαπλών εφαρμογών. VPN βασισμένα σε SSH απαιτούν ειδικευμένες γνώσεις για την εγκατάσταση και παραμετροποίηση των clients software και επειδή ο server πρέπει να είναι απ' ευθείας προσβάσιμος από το διαδίκτυο για να μπορέσει ο χρήστης να αυθεντικοποιηθεί και να εισέρθει στο σύστημα, αυτό αποτελεί μια εν δυνάμει αδυναμία.

4.4 Συγκριτική μελέτη IPSec και εναλλακτικών VPN πρωτοκόλλων

Σε αυτό το κεφάλαιο μελετήθηκαν τα εναλλακτικά πρωτόκολλα που υπάρχουν για μια υλοποίηση ενός VPN συστήματος πέραν του IPSec. Όλα τους έχουν πλεονεκτήματα και μειονεκτήματα ανάλογα με τον σκοπό της χρήσης τους και εξυπηρετούν συγκεκριμένες ανάγκες. Στον *Πίνακα 4.1* παρουσιάζετε μια σύγκριση των πρωτοκόλλων.

---

[41] Υπάρχει μια εργασία από τον Moxie Marlinspike που ασχολείται με αδυναμίες του πρωτοκόλλου SSL το « New Tricks For Defeating SSL In Practice» Έχει αναπτύξει και ένα πρόγραμμα για την τεκμηρίωση της άποψης του, διαθέσιμα https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf και στο http://www.thoughtcrime.org/software/sslstrip/index.html

[42] Για περισσότερες πληροφορίες σχετικά με το Secure Shell, βλέπε http://www.ssh.com/ και http://www.openssh.com/

Πρωτόκολλο	Πλεονεκτήματα	Μειονεκτήματα	Περιπτώσεις που μπορούν να χρησιμοποιηθούν αντί του IPSec
IPSEC	Υποστηρίζεται από πολλά λειτουργικά συστήματα Παρέχει ισχυρή κρυπτογράφηση και ακεραιότητα δεδομένων Υποστηρίζει πολλά πρωτόκολλα πιστοποίησης	Προστατεύει μόνο επικοινωνίες βασισμένες στο πρωτόκολλο IP Απαιτείται η εγκατάσταση και διαμόρφωση client software Δεν παρέχει προστασία στις επικοινωνίες μεταξύ των client και των IPSec gateway	
PPTP	Μπορεί να παρέχει προστασία και σε επικοινωνίες που βασίζονται στο IP πρωτόκολλο	Έχει γνωστά προβλήματα ασφάλειας Δεν προσφέρει ισχυρή μέθοδο αυθεντικοποίησης Υποστηρίζει μόνο μια session ανά tunnel	Καμιά
L2F	Μπορεί να παρέχει προστασία και σε επικοινωνίες που βασίζονται στο IP πρωτόκολλο Μπορεί να χρησιμοποιήσει πρωτόκολλα πιστοποίησης όπως το RADIUS	Απαιτείτε η συμμέτοχη του τηλεπικοινωνιακού παρόχου Δεν παρέχει προστασία μεταξύ του client και του τηλεπικοινωνιακού παρόχου Δεν προσφέρει κρυπτογράφηση. Το κομμάτι αυτό καλύπτεται με τις PPP υπηρεσίες κρυπτογράφησης οι οποίες έχουν γνωστές αδυναμίες	Καμία

L2TP	Μπορεί να παρέχει προστασία και σε επικοινωνίες που βασίζονται στο IP πρωτόκολλο	Απαιτείται η εγκατάσταση και διαμόρφωση client software	Καμιά
SSL	Υποστηρίζετε από όλους τους Web browsers	Μπορεί να υποστηρίξει μόνο επικοινωνίες βασισμένες στο TCP/IP Απαιτεί ότι οι application servers και οι clients υποστηρίζουν το SSL	Στην προστασία της επικοινωνίας για ένα μικρό αριθμό, βασισμένο σε HTTP εφαρμογών που δεν απαιτείτε η χρήση ισχυρής πιστοποίησης.
SSH+ άλλα επιπέδου εφαρμογών VPNs	Μπορούν να παρέχουν προστασία σε συγκεκριμένες εφαρμογές.	Μπορούν να παρέχουν προστασία σε ένα μέρος ή και σε όλα τα δεδομένα μιας όμως μόνο εφαρμογής. Συχνά εδώ χρησιμοποιούνται ιδιωτικοί μηχανισμοί πιστοποίησης που ενδέχεται να έχουν σοβαρές αδυναμίες	Παρέχουν προστασία για συγκεκριμένες εφαρμογές που έχουν σχεδιαστεί για να χρησιμοποιούν αποδεδειγμένα ισχυρούς αλγόριθμους κρυπτογράφησης και αυθεντικοποίησης.

Πινάκας 4-2: *Σύγκριση του IPSec και εναλλακτικών πρωτοκόλλων για VPN*

Στον πίνακα που ακολουθεί (*4.2*) υπάρχουν οι TCP και UDP αριθμοί των θυρών και τα IP πρωτόκολλα που αντιστοιχούν στο IPSec και στα υπόλοιπα πρωτόκολλα που παρουσιαστήκαν νωρίτερα.

Πρωτόκολλο	IP πρωτόκολλο- Αριθμός θύρας
IPSec	50-(Authentication Header, για AH συνδέσεις) 51-(Encapsulating Security Payload, για ESP συνδέσεις) 17-(UDP), θύρα 500 (για Internet Key Exchange, είτε χρησιμοποιείται είτε όχι το NAT-Traversal) 17-(UDP), θύρα 4500 (για Internet Key Exchange χρησιμοποιώντας το NAT-Traversal)
PPTP	47-(Generic Routing Encapsulation) 6-(TCP), θύρα 1723
L2F	17-(UDP), θύρα 1701
L2TP	17-(UDP), θύρα 1701

SSL/TLS	6-(TCP), θύρα 443
SSH+άλλα επιπέδου εφαρμογών VPNs	Διαφέρει ανάλογα με την εφαρμογή

Πινάκας 4-3: *Πρωτόκολλα με τον αντίστοιχο αριθμό τους και θύρες τους*

4.5 Συμπεράσματα

Στα προηγούμενα κεφαλαία μελετήθηκαν και παρουσιαστήκαν πρωτόκολλα για την υλοποίηση ενός VPN δικτύου με κεντρικό άξονα το IPSec πρωτόκολλο ανοικτών προδιαγραφών. Προσεγγίσαμε την λειτουργία τους θεωρητικά και παρουσιάστηκε πως δημιουργείτε ένα tunnel από το οποίο διέρχεται όλη η κίνηση των δεδομένων, είδαμε τα πρωτόκολλα που χρησιμοποιούνται και τον τρόπο με τον οποίο λειτουργούν. Τέλος, με βάση την ανάλυση που έχει γίνει μέχρι τώρα πάνω στο IPSec, θα υλοποιηθεί ένα VPN σενάριο θεμελιωμένο με «πείραμα και την απόδειξη του». Για την υλοποίηση θα χρησιμοποιηθεί το ESP πρωτόκολλο σε tunnel mode, η τεχνική NAT-T και το πρωτόκολλο ανταλλαγής κλειδιών IKEv2. Στο επόμενο κεφαλαίο θα γίνει περιγραφή του σεναρίου, των παραμέτρων και των «συστατικών» μέσω των οποίων θα υλοποιηθεί το IPSec VPN δίκτυο.

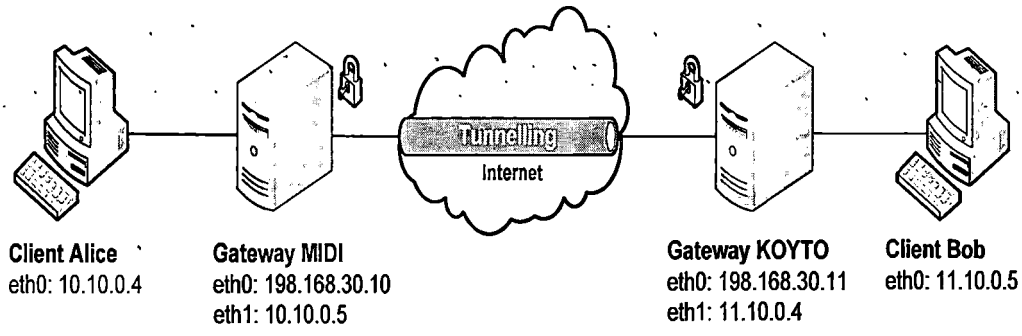
ΚΕΦΑΛΑΙΟ 5

5. Μεθοδολογία

Αυτό το κεφάλαιο ασχολείται με την πρακτική πλευρά της εργασίας, που είναι η υλοποίηση ενός σεναρίου VPN δικτύου με το πρωτόκολλο IPSec. Θα παρουσιαστούν αναλυτικά οι τεχνικές προδιαγραφές, το περιβάλλον πάνω στο οποίο πρόκειται να «στηθεί» το VPN σύστημα, και άλλα πρακτικά ζητήματα.

5.1 IPSec VPN σενάριο

Στο παρακάτω σχήμα παρουσιάζεται η τοπολογία του δικτύου που έχει εγκατασταθεί στο εργαστήριο:



Σχήμα 5-1: *Τοπολογία του VPN δικτύου*

Συμφώνα με το παραπάνω σχήμα το σύστημα μας αποτελείτε από τέσσερα στοιχεία δυο gateways servers (MIDI, KOYTO) και δυο clients (Client Alice, Client Bob). Συνολικά υπάρχουν δυο ξεχωριστά δίκτυα που το καθένα έχει ένα gateway και έναν client. Το πρώτο τοπικό δίκτυο έχει IP διευθύνσεις από το δίκτυο κλάσης A 10.10.0.0/16 και το δεύτερο από το δίκτυο κλάσης A 11.10.0.0/16. Οι gateways-Nat servers έχουν πρόσβαση στο διαδίκτυο μέσω μιας δεύτερης Ethernet κάρτας που έχουν, με IP διευθύνσεις από το δίκτυο 198.168.30.0/24. Κάθε client συνδέεται μόνο με τον gateway που υπάρχει στο δίκτυο του και έχει πρόσβαση στο διαδίκτυο μέσω αυτού. Περισσότερες λεπτομέρειες σχετικά με τις τεχνικές προδιαγραφές του συστήματος περιέχονται στο Παράρτημα Α.
Μια IPSec VPN σύνδεση έχει κατασκευαστεί και λειτουργεί ανάμεσα στους δυο gateways. Ο στόχος είναι να δημιουργηθεί ένα ιδεατό δίκτυο, διαμέσου του tunnel, που θα επιτρέπει στους δυο clients να επικοινωνούν έμμεσα με την βοήθεια των δυο gateways.

5.2 Περιβάλλον εργασίας

Με τον όρο περιβάλλον εργασίας εννοούμε το λειτουργικό σύστημα που θα χρησιμοποιηθεί για την δημιουργία του VPN δικτύου. Η επιλογή του OS (Operating System) είναι πρωταρχικής σημασίας όταν «στήνουμε» ένα δίκτυο. Φυσικά, η προσοχή μας εστιάζετε στην επιλογή του κατάλληλου OS για τους gateways εξαιτίας της ζωτικής τους σημασίας. Σε αυτήν την εργασία έχει επιλεγεί η χρήση ενός πασίγνωστου λειτουργικού συστήματος που χρησιμοποιεί τον πυρήνα του Linux και δεν είναι άλλο από το Ubuntu Server Edition 8.04 LTS[43]. Χτισμένο πάνω στη σταθερή βάση του Debian[44] - γνωστό για τις στιβαρές του εγκαταστάσεις server - το Ubuntu Server Edition έχει μια ισχυρή κληρονομιά αξιόπιστης απόδοσης και προβλέψιμης ανάπτυξης. Η έκδοση Ubuntu Server Edition 8.04 LTS, με υποστήριξη μακράς διάρκειας, προσφέρει υποστήριξη για διάφορες συνήθεις διαμορφώσεις. Ένα βασικό χαρακτηριστικό που πηρέ από το Debian είναι αυτό της by default ασφάλειας. Ο Ubuntu Server δεν έχει ανοιχτές πόρτες μετά την εγκατάσταση του και περιέχει μόνο το απαραίτητο λογισμικό για το στήσιμο ενός ασφαλούς server. Είναι κατασκευασμένο υπό την GPL άδεια, δηλαδή ο πηγαίος κώδικάς του είναι διαθέσιμος στον καθένα (opensource). Οι λόγοι που επιλέχτηκε αυτό το λειτουργικό σύστημα έναντι άλλων (πχ Windows Server 2003, 2008) οφείλεται στ' ότι είναι φτηνότερο, γρηγορότερο, πολύ πιο ευέλικτο και προσαρμόσιμο από κάθε άλλη έκδοση των Windows. Η συντήρησή του είναι φτηνότερη σε σχέση με αυτή των WinNT (το συγκεκριμένο πλεονέκτημα, επί της ευκαιρίας, είναι πλεονέκτημα και κάθε άλλου συστήματος Unix). Επίσης είναι φτηνότερο και από οποιαδήποτε άλλη εμπορική έκδοση Unix. Εύκολη η συντήρησή του από οποιοδήποτε σημείο του Internet. Έχει καλύτερη υποστήριξη υλικού (hardware) από τα FreeBSD, SCO και Solaris/X86. Ο πηγαίος κώδικάς του είναι διαθέσιμος και αυτό μεταφράζετε πως τυχόν bugs διορθώνονται πολύ γρήγορα.

Στους clients το σκεπτικό για την επιλογή του λειτουργικού συστήματος είναι, να εξεταστεί στην πράξη, ότι το IPSec είναι ένα πρωτόκολλο που λειτουργεί στο επίπεδο δικτύου και να αναλυθεί το κατά πόσο η λειτουργία του γίνεται αντιληπτή από τον τελικό χρήστη (client Alice, client Bob). Επιπλέον, να εξεταστεί εάν υπάρχουν ασυμβατότητες μεταξύ των διαφορετικών OS μεταξύ των gateways και των clients. Για να καλυφτούν οι παραπάνω ανάγκες χρησιμοποιήθηκαν στους clients Windows XP Service Pack 3.

5.3 Επιλογή λογισμικού

Το λογισμικό που επιλέχτηκε για την υλοποίηση του IPSec VPN σεναρίου στην παρούσα πτυχιακή εργασία είναι το StrongSwan.

---

[43] Η επίσημη ιστοσελίδα του Ubuntu είναι: http://www.ubuntu.com/ και η ιστοσελίδα απ' οπου «κατέβηκε» η έκδοση που χρησιμοποιήθηκε για τους δυο server είναι: http://www.ubuntu.com/getubuntu/download-server

[44] Η επίσημη ιστοσελίδα του Debian είναι: http://www.debian.org/

Το StrongSwan είναι ένα λογισμικό ανοιχτού κώδικα, απόγονος του προγράμματος FreeS/WAN. Υπεύθυνος για αυτό το εγχείρημα είναι ο Andreas Steffen ο οποίος είναι καθηγητής στην ασφάλεια επικοινωνιών στο University of Applied Sciences στο Rapperswil στην Ελβετία.

Το StrongSwan εστιάζετε στους ισχυρούς μηχανισμούς επικύρωσης που χρησιμοποιούν τα πιστοποιητικά δημόσιων κλειδιών X.509[45] και προαιρετικά στην ασφαλή αποθήκευση των ιδιωτικών κλειδιών στις έξυπνες κάρτες (smartcards) με το πρότυπο PKCS#11[46]. Επίσης, υποστηρίζει καταλόγους ανάκλησης πιστοποιητικών (certificate revocation lists)[47] και το πρωτόκολλο OCSP (Online Certificate Status Protocol)[48]. Ένα μοναδικό γνώρισμα του λογισμικού είναι η χρησιμοποίηση ορισμένων ιδιωτικών X.509 πιστοποιητικών με την βοήθεια των οποίων υλοποιεί προχωρημένες τεχνικές ελέγχου πρόσβασης.
Η έκδοση StrongSwan 4.3 είναι το μοναδικό λογισμικό ανοιχτού κώδικα για IPSec, που υποστηρίζει το πρωτόκολλο IKE Version 2 (κεφάλαιο 3) και αυτός είναι ο βασικός λόγος που επιλέχτηκε σε αυτή την εργασία. Επιπλέον είναι συμβατό με διάφορους VPN clients, μεταξύ των οποίων και τα Microsoft Windows. Παρακάτω παρουσιάζετε το γενεαλογικό δέντρο του StrongSwan.

5.3.1 Το γενεαλογικό δέντρο του StrongSwan

Σε μια εποχή όπου η IETF προσπαθούσε να σχεδιάσει τα IPSec πρωτόκολλα, ένας νέος επιχειρηματίας εν ονόματι John Gilmore ανέπτυξε το FreeS/WAN project. Ο σκοπός αυτού ήταν να καταστήσει το IPSec ως το κύριο πρωτόκολλο για υλοποίηση VPN σε ολόκληρο το διαδίκτυο. Η πρώτη έκδοση του παρουσιάστηκε τον Απρίλιο του 1999. Το FreeS/WAN εισήγαγε μια νέα μέθοδο κρυπτογράφησης γνώστη ως Opportunistic Encryption[49].

---

[45] Το X.509 είναι το πιο διαδεδομένο πρότυπο για τη δημιουργία ψηφιακών πιστοποιητικών (Digital Certificates). Καθορίζετε από το RFC 4158. Για περισσότερες πληροφορίες βλέπε, http://tools.ietf.org/html/rfc4158

[46] Το PKCS#11 είναι ένα πρότυπο που καθορίζει μια διεπαφή προγραμματισμού εφαρμογών (API) που ονομάζετε Cryptoki, σε συσκευες που φυλάσσουν κρυπτογραφικές πληροφορίες και εκτελούν κρυπτογραφικές λειτουργίες. Για περισσότερες πληροφορίες βλέπε, http://www.rsa.com/rsalabs/node.asp?id=2133

[47] Λίστες ανάκλησης πιστοποιητικών (CRL) χρησιμοποιούνται στις περιπτώσεις που κάποια πιστοποιητικά πρέπει να οριστούν μη αξιόπιστα και να ακυρωθούν, πριν την ημερομηνία λήξης τους. Για περισσότερες πληροφορίες βλέπε, http://www.rsa.com/rsalabs/node.asp?id=2283

[48] Το Online Certificate Status Protocol (OCSP) είναι ένα πρωτόκολλο που χρησιμοποιείται για να καθοριστεί εάν ένα πιστοποιητικό θεωρείται έγκυρο και αξιόπιστο. Καθορίζετε από το RFC 2560. Για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc2560.txt

[49] Opportunistic Encryption (OE) αναφέρεται σε κάθε σύστημα που, όταν συνδέεται με ένα άλλο, προσπαθεί να κρυπτογραφήσει το κανάλι επικοινωνίας και εάν δεν καταστεί αυτό επιτυχές συνεχίζει χωρίς κρυπτογράφηση. Για περισσότερες πληροφορίες βλέπε http://en.wikipedia.org/wiki/Opportunistic_encryption

Με αυτή την μέθοδο σε κάθε IP διεύθυνση αντιστοιχεί ένα δημόσιο και ένα ιδιωτικό κλειδί. Τα δημόσιά κλειδιά φυλάσσονται στον DNS server. Κάθε φορά που κάποιος θέλει να επικοινωνήσει με κάποιον, ζητάει το δημόσιο κλειδί, εφαρμόζει την κρυπτογράφηση, και στέλνει το πακέτο. Το πακέτο μπορεί να αποκρυπτογραφηθεί μόνο από το ιδιωτικό κλειδί. Η απάντηση θα γίνει με τον ίδιο τρόπο. Έτσι, η πληροφορία διάφανα κρυπτογραφείται, και αποκρυπτογραφείται μόνο από τον τελικό παραλήπτη.

Στο FreeS/WAN αυτή η τεχνική κρυπτογράφησης γίνονταν με την χρήση ακατέργαστων κλειδιών αυθεντικοποίησης που προέρχονταν από τον κρυπταλγόριθμο RSA[50], τα οποία και αποθηκεύονταν στον παγκόσμιο Σύστημα Ονομάτων Τομέα ή αλλιώς στο Domain Name System (DNS)[51]. Το πρόβλημα όμως ήταν ότι εξαιτίας των περιορισμών που υπήρχαν σχετικά με τα RSA κλειδιά, το FreeS/WAN δεν ήταν συμβατό με ένα αρκετά μεγάλο αριθμό λογισμικών για VPN και με διάφορα λογισμικά που χρησιμοποιούσαν πιστοποιητικά X.509.

Το 2000 ο John Gilmore άρχισε να εξελίσσει το FreeS/WAN ώστε να είναι πλήρως συμβατό με το πιστοποιητικό X.509 και παράλληλα πρόσθεσε επιπλέον χαρακτηριστικά (PKCS#11 smart card) στον πηγαίο κώδικα του λογισμικού. Εξαιτίας όμως πολιτικών λόγων, οι ανωτέρω αλλαγές δεν ενσωματώθηκαν ποτέ στο FreeS/WAN.

Το 2002 Ken Bantoft πρόσθεσε αρκετές αλλαγές μεταξύ των οποίων ήταν: εναλλακτική αλγόριθμοι κρυπτογράφησης, το X.509, την ανίχνευση εάν κάποιο από τα συμβαλλόμενα μέρη του tunnel έχει χάσει την σύνδεση του (Dead Peer Detection - DPD)[52],κ.α. Αυτή την νέα διανομή του FreeS/WAN (Super FreeS/WAN) την μοίρασε στο διαδίκτυο οπου είχε μεγάλη απήχηση σε λογισμικά firewall ανοιχτού κώδικα (IPCop). Ο Ken Bantoft διατήρησε αυτή την Super FreeS/WAN διανομή με το όνομα Openswan 1.x. Το αρχικό FreeS/WAN 1.x «έτρεχε» σε Linux με Kernel 2.0, 2.2 και 2.4 αλλά με την με την συμβολή του Herbert Xu το FreeS/WAN 2.x κατάφερε να «τρέχει» και σε Linux με 2.6 kernel. Το 2004 ο John Gilmore αποφάσισε να σταματήσει το όλο εγχείρημα του, διότι ο κύριος σκοπός του είχε επιτευχτεί με την τελευταία έκδοση του FreeS/WAN 2.0.6.

Μόλις σταμάτησε η εξέλιξη του FreeS/WAN ο Michael Richardson που ήταν υπεύθυνος έργου, μαζί με τον Ken Bantoft και Paul Wouters ίδρυσαν την Xelerance Inc που σαν κύριο στόχο είχε να αποκτήσει καθ' ολοκληρία το Openswan project. Εξαιτίας όμως διαφόρων λόγων, ο Andreas Steffen, αποφάσισε να αναπτύξει μια νέα διανομή για την δημιουργία VPN με IPSec που την ονόμασε StrongSwan.

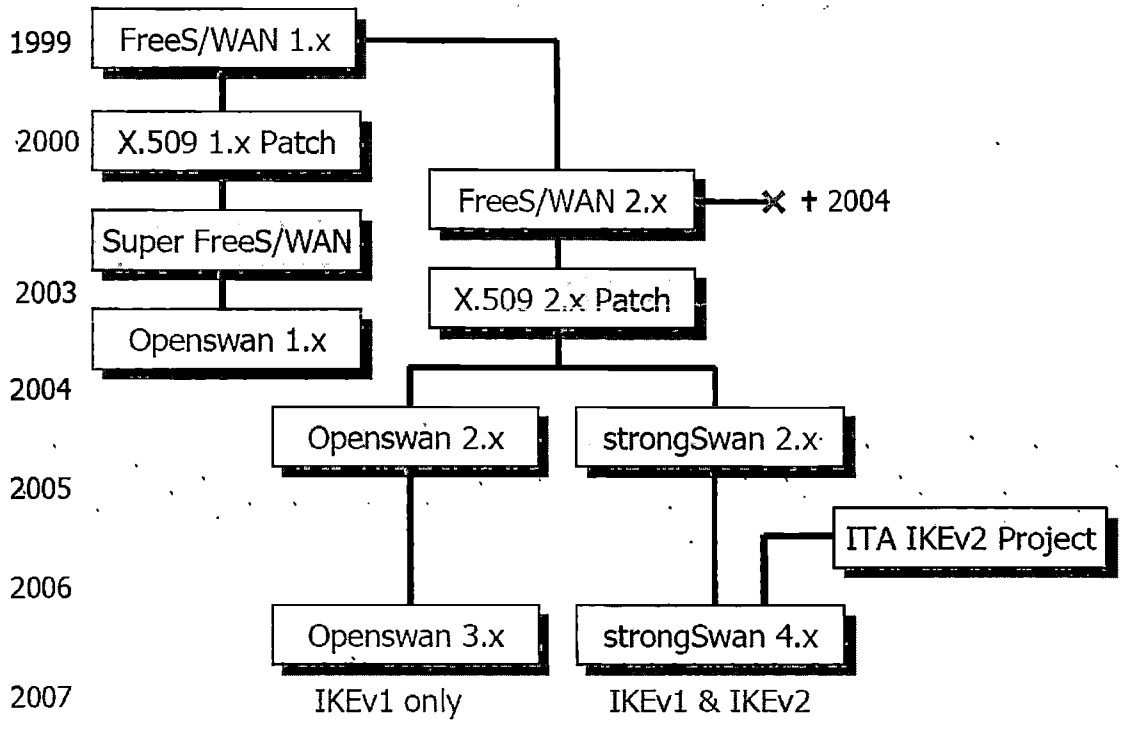
---

[50] Ο RSA είναι ένας κρυπταλγόριθμος ασύμμετρου κλειδιού, το όνομα του οποίου προέρχεται από τους δημιουργούς του, Ron **R**ivest, **A**di **S**hamir και Len **A**dleman. Για περισσότερες πληροφορίες βλέπε, http://en.wikipedia.org/wiki/RSA

[51] Το Domain Name System ή DNS (Σύστημα Ονομάτων Τομέα) είναι ένα σύστημα με το οποίο αντιστοιχίζονται οι διευθύνσεις IP σε ονόματα τομέων (Domain Names). Καθορίζετε από το RFC 1034. Για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc1034.txt

[52] Για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc3706.txt

Συνέπεια όλων αυτών ήταν, το Openswan 2.x, που υποστήριζε τον εν δυνάμει μη ασφαλές «επιθετικό τρόπο» (aggressive mode, βλέπε κεφ. 3.4.1.2) ανταλλαγής κλειδιών και το StrongSwan 2.x, που εστίαζε στην ισχυρή πιστοποίηση, να γίνουν οι επίσημοι διάδοχοι του προγράμματος FreeS/WAN. Στο παρακάτω *Σχήμα 5-2* παρουσιάζετε εικονογραφημένα το γενεαλογικό δέντρο του λογισμικού που πρόκειται να χρησιμοποιηθεί για την υλοποίηση της παρούσας εργασίας.



Σχήμα 5-2: *Το γενεαλογικό δέντρο του StrongSwan*

5.4 Ανάλυση του VPN δικτύου

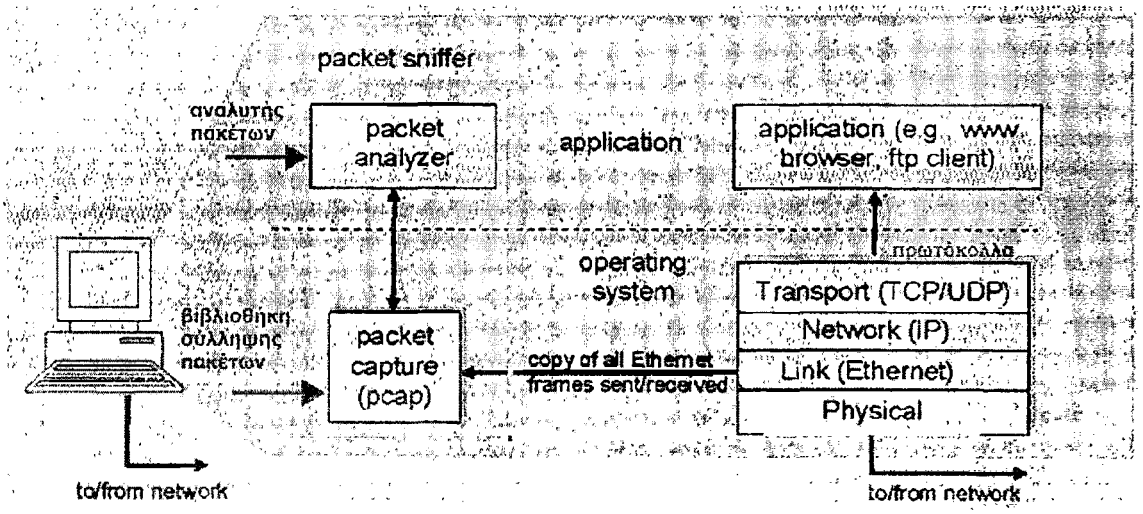
Για την ανάλυση της κίνησης στο διαδίκτυο κατά την διάρκεια του VPN συστήματος, απαιτείται ένα λογισμικό με δυνατότητα παρακολούθησης των πακέτων που μεταδίδονται, γνωστό και ως Packet sniffer ή απλώς sniffer.
Ο τρόπος λειτουργιάς τους έχεις ως εξής: Οι περισσότεροι προσωπικοί υπολογιστές συνδέονται σε ένα τοπικό δίκτυο (LAN - Local Area Network), που σημαίνει ότι μοιράζονται μία σύνδεση με άλλους υπολογιστές. Αν το δίκτυο δεν χρησιμοποιεί switches (μεταγωγείς) - μεταγωγέας είναι μια συσκευή που φιλτράρει και ξαναστέλνει τα πακέτα ανάμεσα στους τομείς ενός LAN - η κίνηση που προορίζεται για έναν τομέα μεταδίδεται σε κάθε μηχάνημα του δικτύου. Επακόλουθα, κάθε υπολογιστής στην πραγματικότητα βλέπει τα δεδομένα που προέρχονται από ή προορίζονται για τους γειτονικούς υπολογιστές, αλλά τα αγνοεί.

Το sniffer αναγκάζει τον υπολογιστή, συγκεκριμένα την κάρτα δικτύου (Network Interface Card - NIC), να αρχίσει να προσέχει και αυτά τα πακέτα, τα οποία προορίζονται για άλλους υπολογιστές. Για να το καταφέρει αυτό θέτει τη NIC σε

ειδική λειτουργία, γνωστή ως promiscuous mode[53]. Όταν η NIC βρίσκεται σε αυτή τη λειτουργία, μια κατάσταση που συνήθως απαιτεί δικαιώματα ανώτερου χρήστη (root), ένα μηχάνημα μπορεί να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του.

Υπάρχουν πολλές δυνατότητες, που καθορίζουν την τύχη των πακέτων:

- Τα πακέτα μετριούνται. Με αυτό τον τρόπο, προσθέτοντας στη συνέχεια το συνολικό μέγεθός τους για μία ορισμένη χρονική περίοδο (συμπεριλαμβάνοντας τις επικεφαλίδες των πακέτων), εξάγεται μια καλή ένδειξη για το πόσο φορτωμένο είναι το δίκτυο. Το πρόγραμμα μπορεί να παρέχει γραφικές απεικονίσεις της σχετικής κίνησης του δικτύου.
- Τα πακέτα μπορούν να εξετασθούν λεπτομερώς. Είναι δυνατόν να γίνει σύλληψη συγκεκριμένων πακέτων, ώστε να διαγνωσθεί και να αντιμετωπιστεί ένα πρόβλημα.



Σχήμα 5-3: *Δομή packet sniffer*

Για αυτό τον σκοπό χρησιμοποιήθηκε ένα λογισμικό ανοιχτού κώδικα γνωστό ως, Wireshark, έκδοση 1.0.7. Το Wireshark αποτελεί ένα από τα διασημότερα προγράμματα παγκοσμίως για την ανάλυση των δικτύων. Αυτό το εργαλείο παρέχει πληροφορίες για το δίκτυο σχετικά με τα δεδομένα που διακινούνται σ'αυτό.
Όπως πολλά άλλα δικτυακά προγράμματα, το Wireshark χρησιμοποιεί τη δικτυακή βιβλιοθήκη pcap για την σύλληψη (ανάλυση) των πακέτων.
Η δύναμη του Wireshark πηγάζει από:

- Την ευκολία εγκατάστασής του.
- Την απλότητα της χρήσης του μέσω της γραφικής διεπαφής του (GUI).
- Το μεγάλο αριθμό της λειτουργικότητας του.

---

[53] Για περισσότερες πληροφορίες βλέπε, http://en.wikipedia.org/wiki/Promiscuous_mode

Το Wireshark ονομαζόταν Ethereal μέχρι το 2006, όταν ο επικεφαλής προγραμματιστής, αποφάσισε την αλλαγή τού ονόματός του, λόγω δικαιωμάτων χρήσης που προϋπήρχαν για το όνομα Ethereal, το οποίο ήταν κατοχυρωμένο στην εταιρεία από την οποία αποφάσισε να αποχωρήσει το 2006.

5.5 Web και video servers

Με σκοπό την καλύτερη ανάλυση και εξαγωγή το δυνατόν καλύτερων αποτελεσμάτων, εγκαταστάθηκε στους υπολογιστές "Alice " και "Bob" ο Apache[54] HTTP web server. Με την εγκατάσταση του Apache web server είναι εφικτό να μεταφέρουμε αρχεία ανάμεσα στους δυο clients και να υπολογίσουμε τα στατιστικά του δικτύου. Η έκδοση που χρησιμοποιήθηκε ήταν η 2.2.11. Επιπλέον, εγκαταστάθηκε και video server, ώστε να έχουμε video streaming μέσω του διαδικτύου. Επιλέχτηκε το λογισμικό ανοιχτού κώδικα VideoLan[55], η έκδοση 0.9, η οποία περιέχει το VLS (VideoLan Server) και το VLC (VideoLan Client) και εγκαταστάθηκε στους δυο clients.

[54] Για περισσότερες πληροφορίες σχετικά με τον Apache web server βλέπε, http://httpd.apache.org/. Ένας πλήρης οδηγός εγκατάστασης και παραμετροποίησης υπάρχει εδώ http://httpd.apache.org/

[55] Για περισσότερες πληροφορίες σχετικά με τον VLC player βλέπε, http://www.videolan.org/. Ένας πλήρης οδηγός για την παραμετροποίηση του video streaming υπάρχει εδώ, http://wiki.videolan.org/Documentation:Streaming_HowTo

ΚΕΦΑΛΑΙΟ 6

6. Εμπειρική προσέγγιση της λειτουργιάς του IPSEC

Αυτό το κεφάλαιο θα είναι κατ' ουσία συμπληρωματικό στην θεωρητική προσέγγιση της λειτουργιάς του IPSec που παρουσιάστηκε στα κεφαλαία 2 και 3. Έχοντας πλέον ως δεδομένο ότι έχουμε υλοποιήσει το VPN δίκτυο μας (Παράρτημα Β και Γ) θα παρατηρήσουμε την συμπεριφορά του δικτύου μας, και πιο συγκεκριμένα την διαδικασία του tunneling και την επικεφαλίδα του πρωτοκόλλου ESP. Τέλος θα παρουσιαστούν διαγράμματα που θα βοηθήσουν την κατανόηση αυτών των όρων.

6.1 Ανάλυση της κίνησης του IPSec VPN

Πριν να προσπαθήσει ένα πρόγραμμα-πελάτης (client) να συνδεθεί με έναν server, ο server πρέπει πρώτα να δεσμεύσει μια port και να την ανοίξει ώστε να δέχεται συνδέσεις: αυτό καλείται passive open. Όταν γίνει αυτό, ο client μπορεί να αρχίσει τη σύνδεση (active open). Για να γίνει μια σύνδεση, γίνεται μια τριμερείς "χειραψία" ανάμεσα στα συμμετέχοντα μέρη, το λεγόμενο three-way handshake.

Οι υπολογιστές στις δυο άκρες του συστήματος μας "Alice" και "Bob" πραγματοποιούν την three-way handshake διαδικασία και με την βοήθεια του wireshark παρουσιάζετε παρακάτω.

No.	Source	Destination	Protocol	Info
1	10.10.0.4	11.10.0.5	TCP	34480 > 80 [SYN] Seq=0 Len=0 MSS=1460 TSV=6522154 TSER=0 WS=2
2	11.10.0.5	10.10.0.4	TCP	80 > 34480 [SYN, ACK] Seq=0 Ack=1 Win=23168 Len=0 MSS=1460 TSV=6521974 TSER=6522154 WS=2
3	10.10.0.4	11.10.0.5	TCP	34480 > 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0

Σχήμα 6-1: *Three-way handshake ανάμεσα στο "Client Alice" και "Client Bob"*

Στον παραπάνω πίνακα αρχικά αποστέλλεται ένα πακέτο με το SYN bit ενεργοποιημένο. Ο client θέτει το πεδίο αριθμού ακολουθίας στην TCP επικεφαλίδα (TCP header) στον αρχικό αριθμό ακολουθίας του (ISN - initial sequence number). Ο gateway στο άλλο άκρο απαντάει με SYN (για να στείλει και το δικό του ISN) και ACK (που έχει το ISN+1 του client) του πρώτου πακέτου του client για να αποδεχτεί τη σύνδεση. Όταν ο client πάρει ένα πακέτο SYN/ACK απαντάει, αυτή τη φορά, με ένα πακέτο ACK. Σε αυτό το σημείο, τα δύο μέρη συνδέονται και μπορούν πλέον να σταλούν τα δεδομένα. Η παραπάνω κίνηση που μεταδίδεται από τον κάθε client στον αντίστοιχο gateway, δεν είναι κρυπτογραφημένη. Με δεδομένο όμως ότι το tunnel μεταξύ των gateways έχει δημιουργηθεί, τα δεδομένα όταν θα φτάσουν στο σημείο να «ταξιδέψουν» μέσα στο tunnel, θα κρυπτογραφηθούν σαν ESP πακέτα.

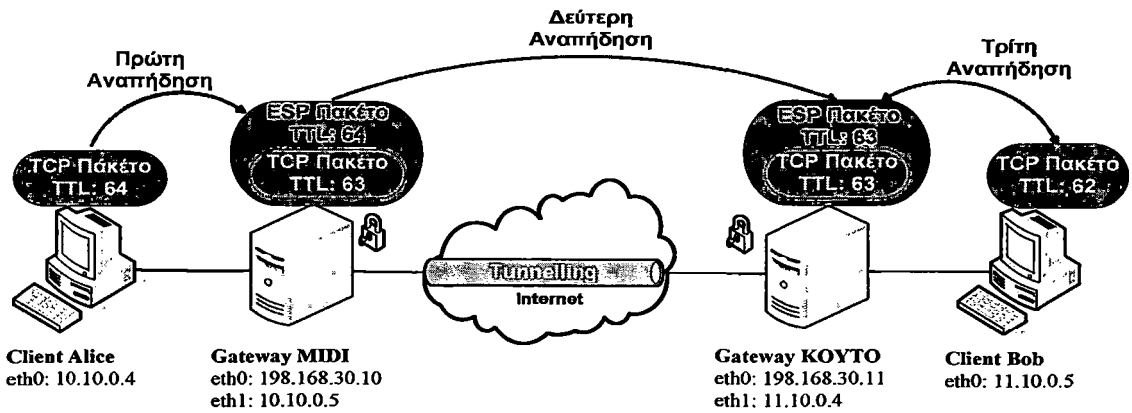
No.	Source	Destination	Protocol	Info
1	198.168.30.10	198.168.30.11	ESP	ESP (SPI=0x595c35ec)
2	198.168.30.11	198.168.30.10	ESP	ESP (SPI=0x6d7ecf2c)
4	198.168.30.10	198.168.30.11	ESP	ESP (SPI=0x595c35ec)

Σχήμα 6-2: *Ανάλυση πακέτων ανάμεσα στον "Gateway Midi" και "Gateway Koyto"*

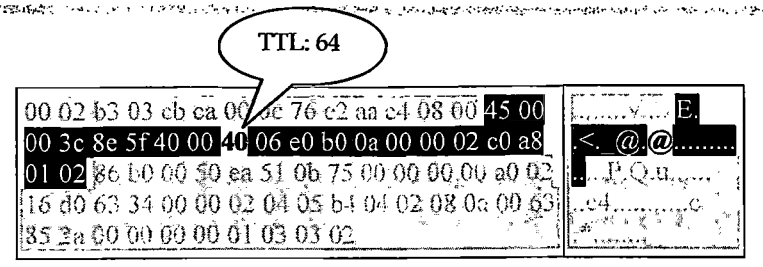
Κατά τη διάρκεια του three-way handshake, τα δύο μέρη διαπραγματεύονται επίσης όλες τις ειδικές επιλογές που θα χρησιμοποιηθούν κατά τη διάρκεια της σύνδεσης TCP, όπως ECN κα.

6.2 Η τιμή TTL (time to live) και Network hops

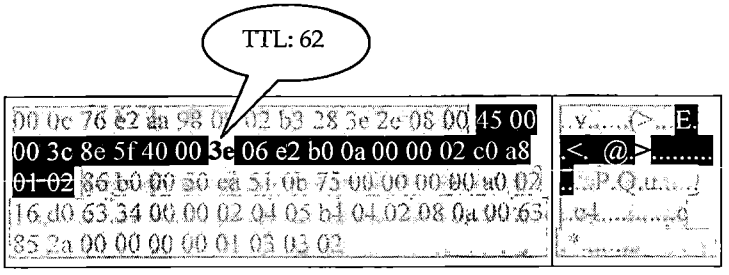
Ένα κύριο χαρακτηριστικό της tunneling διαδικασίας είναι ο αριθμός των αναπηδήσεων που παίρνει ένα πακέτο για να φτάσει στον τελικό του προορισμό (network hops) και η τιμή Time To Live (TTL) που βρίσκεται στην IP επικεφαλίδα. Στο σενάριο αυτής της εργασίας, κανονικά ο αριθμός των αναπηδήσεων για κάθε έναν από τους δυο client είναι τρεις, αλλά εξαιτίας ότι στο tunnel αλλάζει προσωρινά η IP διεύθυνση, οι αναπηδήσεις μειώνονται σε δυο (*Σχήμα 6-3*). Η αρχική IP διεύθυνση χρησιμοποιείται μονό για τις αναπηδήσεις από τον "Client Alice" στο "Gateway Midi" και αντίστοιχα από το "Client Bob" στο "Gateway Koyto". Κατά την λειτουργία του tunnel η αρχική επικεφαλίδα γίνεται μέρος του Encapsulating Security Payload (ESP) πακέτου, με τα πεδία του να παραμένουν ανεπηρέαστα. Συγκρίνοντας τα αρχικά TCP πακέτα από τον "Client Bob" στο "Client Alice", προκύπτει ότι όντως η TTL τιμή έχει μειωθεί κατά 2 (*Σχήμα 6-4, 6-5*), επιβεβαιώνοντας την λειτουργία του IPSec, όπως έχουμε δει και στο κεφάλαιο 3.2.2, σε κατάσταση διόδου (tunnel). Στην περίπτωση που είχε επιλεχτεί η κατάσταση μεταγωγής (transport mode) τότε η τιμή του TTL θα μειώνονταν κατά τρεις μονάδες, αφού η αρχική IP επικεφαλίδα ενθυλακώνεται μέσα στο ESP πακέτο.



Σχήμα 6-3: *Αριθμός αναπηδήσεων και η τιμή TTL κατά την διαδικασία tunneling*



Σχήμα 6-4: *TCP πακέτο στον "Client Bob" με TTL 64*



Σχήμα 6-5: *TCP πακέτο στον "Client Alice" με TTL 64*

Η παρατήρηση αυτή είναι πολύ σημαντική διότι σε ορισμένες περιπτώσεις οπου η διαδικασία tunneling είναι σε λειτουργία, στο δίκτυο προστίθεται επιπλέον φόρτος χωρίς να υπάρχει συγκεκριμένος λόγος. Πιο συγκεκριμένα σε περιπτώσεις οπου ένα πακέτο δεν έχει επαρκείς TTL αναπηδήσεις για να φτάσει στον τελικό του προορισμό, αλλά κατορθώνει να φτάσει μέχρι την άκρη του tunnel, τότε το πακέτο θα ενθυλακωθεί σε ένα ESP πακέτο και θα σταλθεί μέσα στο tunnel. Αυτό θα έχει σαν αποτέλεσμα επιπλέον φόρτο για το tunneling δίκτυο και για τους gateways, ασχέτως από το γεγονός ότι θα απορριφτεί μόλις γίνει η αποθυλάκωση – decapsulation του πακέτου. Επομένως το πρόβλημα είναι οτι στις άκρες του tunnel δεν υπάρχει κάποιος μηχανισμός που θα λαμβάνει υπόψη εάν το πακέτο μπορεί πραγματικά να φτάσει στον προορισμό του.

ΚΕΦΑΛΑΙΟ 7

7. Ανάλυση της απόδοσης του VPN IPSec δικτύου

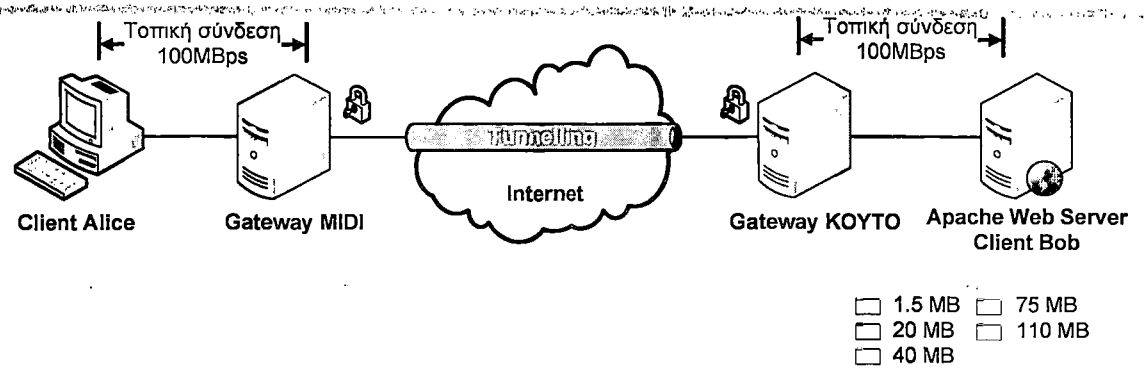
Σκοπός αυτού του κεφαλαίου είναι να αξιολογηθεί η απόδοση του IPSec VPN δικτύου σε διαφορετικά σενάρια, εκ των οποίων είναι η μεταφορά αρχείων, εφαρμογών με μικρά πακέτα και υπηρεσιών πραγματικού χρόνου (real time services). Τέλος, για κάθε σενάριο αντίστοιχα, γίνεται αναφορά κατά πόσο η λειτουργία του IPSec είναι αποδοτική η όχι.

7.1 Επιπλέον φόρτος από την λειτουργία του IPSec

Μπορούμε να θεωρήσουμε ότι όταν το επιθυμητό ζητούμενο είναι η αύξηση του προσφερόμενου επιπέδου ασφάλειας σε οποιαδήποτε δραστηριότητα, αυτό θα έχει ορισμένες αρνητικές επιπτώσεις. Με την ιδία λογική και το πρωτόκολλο IPSec περάν όλων των πλεονεκτημάτων που προσφέρει, έχει και μειονεκτήματα.

Είναι αναμενόμενο ότι η λειτουργία του IPSec θα κάνει το δίκτυο πιο αργό, εξαιτίας των επιπλέον διεργασιών που απαιτούνται τόσο κατά την «κατασκευή» του tunnel όσο και από την μεταφορά των δεδομένων μέσα από αυτό. Πιο συγκεκριμένα, για την διαδικασία της ενθυλάκωσης κάθε πακέτο θα πρέπει να κρυπτογραφηθεί, να υπολογιστεί το hash checksum, και να προστεθούν οι επιπλέον επικεφαλίδες που απαιτεί το IPSec, αναλόγως με τι έχουμε επιλέξει. Αυτή η διαδικασία θα πρέπει να επαναληφτεί, από την αντίθετη μεριά, όταν το πακέτο φτάσει την άλλη μεριά του tunnel. Το παραγόμενο αποτέλεσμα, θα είναι μια σύνδεση με αυξημένο επίπεδο ασφάλειας αλλά παράλληλα θα υπάρχει και μια χρονοκαθυστέρηση στην ροή των πακέτων κατά το tunneling. Εδώ να σημειώσουμε ότι ο χρόνος της καθυστέρησης εξαρτάται επίσης και από την υπολογιστική ισχύ των hardware συσκευών.

Όπως προαναφέρθηκε, ο στόχος σε αυτό το κεφάλαιο είναι ο προσδιορισμός του επιπλέον φόρτου από την λειτουργία του IPSec. Για αυτό τον σκοπό η απόδοση του δικτύου αξιολογείται πριν και μετά από την έναρξη της διαδικασίας του IPSec. Η αξιολόγηση πραγματοποιήθηκε με την εκτέλεση μεταφορών αρχείων στον «Client Alice», χρησιμοποιώντας τον Apache web server που έχει εγκατασταθεί στον «Client Bob» (*Σχήμα 7-1*). Για την μεταφορά των αρχείων χρησιμοποιήθηκαν διαφορετικού μεγέθους αρχεία, 1.5MB, 20MB, 40MB, 75MB και 110MB. Το εύρος ζώνης (bandwidth) της γραμμής που χρησιμοποιήθηκε είναι 1024 KB/s. Όλες οι δόκιμες που διεξήχθησαν επανελήφθησαν αρκετές φόρες ώστε να εξαχθεί ο μέσος όρος για την απόδοση του δικτύου.



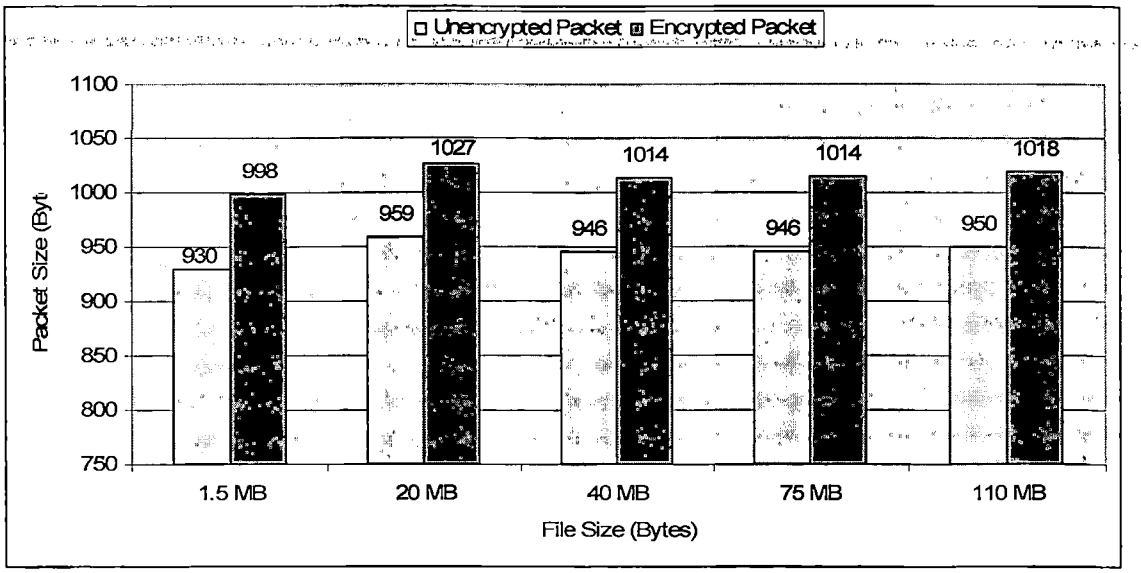
Σχήμα 7-1: *Τοπολογία του δικτύου για την μεταφορά αρχείων*

Πράγματι, τα πρώτα αποτελέσματα που παρουσιάζονται στον παρακάτω πίνακα (*Πινάκας 7-1*) πιστοποιούν αυτό που περιμέναμε. Το IPSec προσθέτει επιπλέον καθυστέρηση στην μεταφορά των αρχείων. Εξαιτίας κυρίως, του ότι έχουμε ένα σταθερό μέγεθος αρχείων, θα πρέπει να μεταφερθούν περισσότερα δεδομένα λόγω των πρόσθετων επικεφαλίδων που εισάγονται από το IPSec. Επιπλέον, η κρυπτογράφηση και η ενθυλάκωση των πακέτων επιβαρύνει τον χρόνο μεταφοράς.

	Απαιτούμενος χρόνος		**Διαφορά (σε δευτερόλεπτα)**	**Διαφορά (Σε ποσοστό %)**
	Ενεργοποιημένο το IPSec	**Απενεργοποιημένο το IPSec**		
Αρχεία πολύ μικρού μεγέθους (1.5 MB)	13.909 δευτ	13.305 δευτ	0.60 δευτ	4.5%
Αρχεία μικρού μεγέθους (20 MB)	173.414 δευτ	165.968 δευτ	7.45 δευτ	4.5%
Αρχεία μεσαίου μεγέθους (40MB)	355.665 δευτ	340.083 δευτ	15.58 δευτ	4.6%
Αρχεία μεγάλου μεγέθους (75MB)	659.789 δευτ	630.188 δευτ	29.60 δευτ	4.7%
Αρχεία πολύ μεγάλου μεγέθους (110 MB)	1015.986 δευτ	972.349 δευτ	43.64 δευτ	4.5%

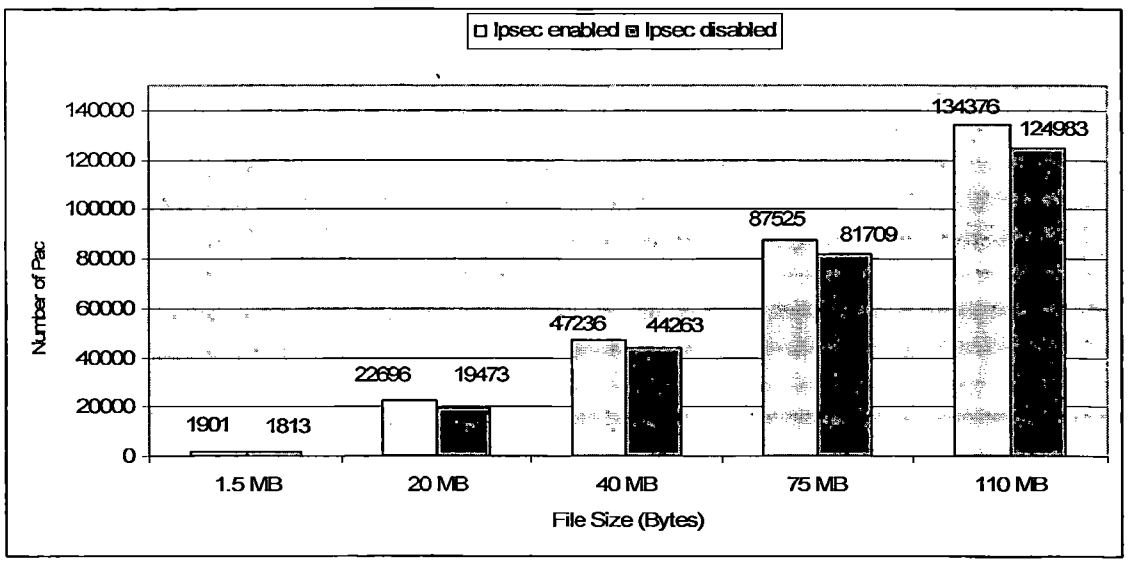
Πινάκας 7-1: *Απόδοση του IPSec κατά την μεταφορά αρχείων*

Ενδιαφέρον θα είχε να βλέπαμε το πόσο είναι ο επιπλέον φόρτος που προσθέτει η IPSec διαδικασία, εκφρασμένο σε αριθμητική μονάδα. Απάντηση σε αυτή την ερώτηση μας δίνει το επόμενο σχήμα. Πιο συγκεκριμένα, μας δείχνει ότι η διαδικασία του tunneling απαιτεί 68 bytes να επισυναφτούν σαν μια πρόσθετη επικεφαλίδα σε κάθε ένα πακέτο.



Σχήμα 7-2: *Επιπλέον φόρτος σε κάθε πακέτο εξαιτίας της κρυπτογράφησης*

Η πρόσθετη επικεφαλίδα υπονοεί το γεγονός, ότι ο αριθμός πακέτων που απαιτείται για να διαβιβαστεί το αρχείο είναι μεγαλύτερος όταν είναι σε λειτουργία το IPSec. Το *Σχήμα 7-3* παρουσιάζει τον αριθμό των πακέτων του μεταφερθήκαν προτού και μετά το IPSec ενεργοποιηθεί.



Σχήμα 7-3: *Ο αριθμός των πακέτων που διαβιβαστήκαν με και χωρίς το IPSec*

Αν και η πρόσθετη καθυστέρηση θα πρέπει να θεωρηθεί ως μια σημαντική επιβάρυνση αυτό θα πρέπει να εξετάζετε κατά περίπτωση ανάλογα με την «ευαισθησία» της κάθε εφαρμογής σε τυχόν καθυστερήσεις. Ειδικότερα, οι εφαρμογές για μεταφορά αρχείων δεν είναι επιρρεπής σε καθυστερήσεις. Τέλος, ο επιπλέον φόρτος σε όλες τις περιπτώσεις ήταν γύρω στο 4,5% (*Πινάκας 7-1*). Ομοίως και στην απόδοση του δικτύου εκφρασμένο με όρους της διεκπεραιωτής ικανότητας (throughput) η επιβάρυνση είναι επίσης αμελητέα (*Πινάκας 7-2*).

	Ενεργοποιημένο το IPSec	Απενεργοποιημένο το IPSec	Διαφορά στην διεκπεραιωτική ικανότητα
Αρχεία πολύ μικρού μεγέθους (1.5 MB)	0.970 MBit/δευτ	1.010 MBit/δευτ	-0.040 MBit/δευτ
Αρχεία μικρού μεγέθους (20 MB)	0.957 MBit/δευτ	0.996 MBit/δευτ	-0.039 MBit/δευτ
Αρχεία μεσαίου μεγέθους (40MB)	0.958 MBit/δευτ	0.998 MBit/δευτ	-0.040 MBit/δευτ
Αρχεία μεγάλου μεγέθους (75MB)	0.957 MBit/δευτ	0.997 MBit/δευτ	-0.040 MBit/δευτ
Αρχεία πολύ μεγάλου μεγέθους (110 MB)	0.959 MBit/δευτ	0.996 MBit/δευτ	-0.037 MBit/δευτ

Πινάκας 7-2: *Οι επιπτώσεις της λειτουργιάς του IPSec στην διεκπεραιωτή ικανότητα του δικτύου*

Μελετώντας τα δεδομένα που έχουμε έως τώρα, συμπεραίνουμε ότι το IPSec αποδίδει πολύ καλά σε ότι άφορα τις μετρήσεις που έγιναν και αφορούν την απόδοση του δικτύου. Οι επιβάρυνση από το IPSec είναι σχεδόν ασήμαντη και το συνολικό throughput επηρεάζετε με μικρό βαθμό. Συνολικά μπορούμε να πούμε ότι όλο το πρόβλημα έγκειται στις πρόσθετες επικεφαλίδες που εισάγονται και αυτό φαίνεται περισσότερο σε πακέτα μικρού μεγέθους. Αυτή η περίπτωση θα αναλυθεί περαιτέρω στο ακόλουθο τμήμα.

7.2 Ανάλυση απόδοσης του IPSec για πακέτα μικρού μεγέθους

Σε αυτό το κεφάλαιο θα εξετάσουμε σε βάθος την επιβάρυνση που προκαλεί το IPSec σε πακέτα πολύ μικρού μεγέθους όπως είναι για παράδειγμα τα πακέτα μηνυμάτων ελέγχου διαδικτύου (network control messages).

Αυτά τα πακέτα χρησιμοποιούνται με σκοπό να βοηθήσουν τον έλεγχο και την διαχείριση του δικτύου. Το κύριο χαρακτηριστικό αυτών είναι ότι έχουν πολύ μικρό μέγεθος και συνήθως μεταδίδονται αυτόματα σε περιοδικά χρονικά διαστήματα. Στην εργασία για τις δοκιμές επιλέχτηκε το γνωστό σε όλους μας, Πρωτόκολλο Μηνυμάτων Ελέγχου Διαδικτύου ή αλλιώς ICMP, χρησιμοποιώντας την εντολή "Ping" μεταξύ των δυο clients. Η αξιολόγηση εστιάστηκε στο μέγεθος των επιπλέον επικεφαλίδων που εισάγονται στο αρχικό πακέτο, και όχι στην καθυστέρηση που αυτές προκαλούν.

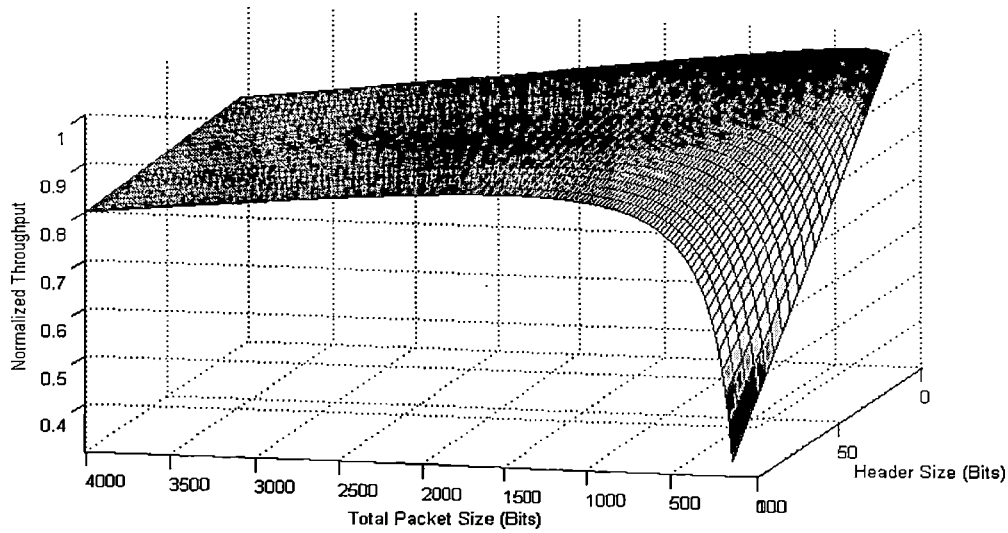
Τα αποτελέσματα στον *Πίνακα 7-3* είναι εντυπωσιακά διότι δείχνουν ότι το ICMP μήνυμα όταν το IPSec είναι ενεργοποιημένο είναι 70% μεγαλύτερο από ότι θα ήταν σε κανονικές συνθήκες.

	Μέγεθος του πακέτου ESP	Μέγεθος του πακέτου χωρίς κρυπτογράφηση	Διαφορά	ESP κεφαλίδα % επί των καθαρών δεδομένων
Μήνυμα ICMP	166 Bytes	98 Bytes	68 Bytes	70% Bytes

Πινάκας 7-3: *Η επιβάρυνση που προσθέτει η IPSec διαδικασία σε μικρού μεγέθους πακέτα*

Επίσης, θα πρέπει να επισημάνουμε ότι στις μέρες μας ορισμένες και μάλιστα πολύ δημοφιλείς επιθέσεις στο διαδίκτυο βασίζονται σε network control messages. Μεταξύ αυτών συγκαταλέγονται, Denial of Service (DoS) επιθέσεις (Smurf attack[56], ICMP flood κ.α.), οι οποίες χρησιμοποιούν ICMP μηνύματα για να «πλημυρίσουν» το δίκτυο με πακέτα πολύ μικρού μεγέθους. Σε αυτές τις περιπτώσεις η χρησιμοποίηση του IPSec θα ήταν προβληματική.

Το συνολικό κόστος από την επιβάρυνση πολλών επικεφαλίδων σε πολύ μικρά πακέτα είναι ότι η διεκπαιρεωτική ικανότητα του δικτύου μειώνεται σημαντικά. Το *Σχήμα 7-4* μας παρουσιάζει εικονογραφημένα τα παραπάνω σε ένα 3D διάγραμμα. Το διάγραμμα δείχνει την διεκπαιρεωτική ικανότητα του δικτύου σε σχέση με το συνολικό μέγεθος ενός πακέτου και της επικεφαλίδας του πακέτου. Όπως φαίνεται, με τα πολύ μικρά πακέτα η επιβάρυνση εξαιτίας των πρόσθετων bits της επικεφαλίδας είναι αρκετά σημαντική. Στον αντίποδα, με τα μεγάλα αρχεία, αυξάνεται η πιθανότητα να απορριφθούν πακέτα που έχει ως αποτέλεσμα την υποβάθμιση της διεκπαιρεωτικής ικανότητας του δικτύου.



Σχήμα 7-4: *Τρισδιάστατο διάγραμμα της διεκπαιρεωτικής ικανότητας του δικτύου σε σχέση με το συνολικό μέγεθος ενός πακέτου και της επικεφαλίδας του πακέτου*

[56] Smurf attack είναι ένα είδος D.O.S. επίθεσης που σχετίζεται με το πρωτόκολλο TCP/IP. Σε αυτή την επίθεση στέλνεται ένας υπέρογκος αριθμός από ping requests συνήθως στον router του δικτύου, χρησιμοποιώντας ψεύτικες (spoofed) IP διευθύνσεις μέσα από το ίδιο το δίκτυο. Για περισσότερες πληροφορίες βλέπε, http://www.cert.org/advisories/CA-1998-01.html

Συνεπώς, το βέλτιστο throughput του δικτύου επιτυγχάνεται για τη μικρότερη δυνατή επικεφαλίδα με ένα λογικό μέγεθος πακέτου. Προηγουμένως, στην περίπτωση μεταφοράς αρχείων, το μέγεθος των πακέτων ήταν λογικό και το μόνο πρόβλημα ήταν το πρόσθετο μέγεθος των επικεφαλίδων, οι οποίες έδωσαν μια αμελητέα χαμηλότερη τιμή στο throughput του δικτύου. Εντούτοις για τα μηνύματα ελέγχου δικτύων το πρόβλημα είναι χειρότερο. Το πολύ μικρό μέγεθος πακέτων, σε συνδυασμό με μια κανονική επικεφαλίδα δίνει μια χαμηλή ρυθμοαπόδοση του δικτύου. Ενεργοποιώντας και το IPSec, το μέγεθος των επικεφαλίδων γίνεται μεγαλύτερο, δίνοντας το χειρότερο δυνατό throughput στο δίκτυο. (η μπλε χαμηλότερη δεξιά γωνία του διαγράμματος).

Ένα ακόμα παράδειγμα οπου θα είναι πρόβλημα η λειτουργιά του IPSec εξαιτίας των πολύ μικρών πακέτων που χρησιμοποιούνται, είναι στην τεχνολογία Voice over IP (VoIP)[57]. Η τεχνολογία VoIP χρησιμοποίει το πρωτόκολλο real-time transport (RTP)[58]. Μια VoIP εφαρμογή αναμένετε να μεταδίδει πακέτα των 60 bytes κάθε 10ms, με την προϋπόθεση ότι χρησιμοποίει G729 κωδικοποιητή[59]. Για κάθε ένα μόνο VoIP frame, 68 επιπλέον bytes πρόσθετης επικεφαλίδας απαιτούνται από την IPSec λειτουργία. Γίνεται προφανές, ότι ο επιπλέον φόρτος που εισάγεται είναι μεγαλύτερος από το αρχικό frame, με αποτέλεσμα το δίκτυο να επιβαρύνεται κατά 113%. Για παράδειγμα, κάθε λεπτό η VoIP εφαρμογή θα δημιουργήσει δεδομένα μεγέθους 351kB, εκ των οποίων θα απαιτούνται 398kB IPSec επικεφαλίδες.

Γενικότερα, όλη η ανωτέρω ανάλυση μας υποδεικνύει ότι το IPSec δεν συστήνεται για χρήση με πολύ μικρά σε μέγεθος πακέτα. Οι πρόσθετες επικεφαλίδες του IPSec που απαιτούνται είναι πάρα πολύ μεγάλες έναντι των αρχικών πακέτων, καθιστώντας το δίκτυο αναποτελεσματικό.

7.3 Ανάλυση απόδοσης του IPSec σε Video Streaming

Έως τώρα έχουμε παρατηρήσει ότι το IPSec επιβαρύνει το δίκτυο και ειδικότερα τα μικρότερα πακέτα όπως είναι τα μηνύματα ελέγχου διαδικτύου και VoIP εφαρμογές. Σε αυτό το σημείο θα αξιολογήσουμε την απόδοση του IPSec σε ένα σενάριο υπηρεσιών πραγματικού χρόνου όπως είναι το video streaming. Σε αυτή την περίπτωση δεν θα εστιάσουμε την προσοχή μας στην επιβάρυνση που προκαλούν στο δίκτυο οι επιπλέον επικεφαλίδες αλλά στην καθυστέρηση της μετάδοσης των πακέτων. Είναι απαραίτητο όταν χρησιμοποιούμε video streaming εφαρμογές τα πακέτα μας να παραδίδονται σε συγκεκριμένο χρόνο, ειδάλλως θα δημιουργούνται προβλήματα.

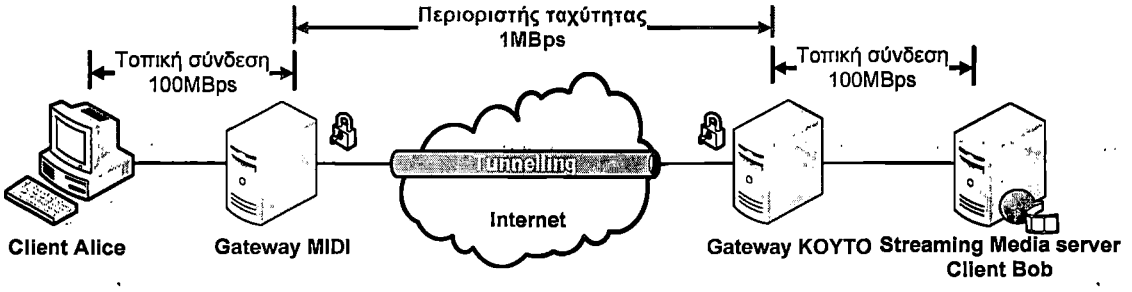
---

[57] Η τεχνολογία VoIP ή ΦεΔΠ δηλαδή "Φωνή επί διαδικτυακού πρωτοκόλλου", χαρακτηρίζει μια ομάδα πρωτοκόλλων-τεχνολογιών (H.323, SIP), η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα πλέον και στην ουσία χωρίς κόστος. Για περισσότερες πληροφορίες βλέπε, http://www.voip-info.org/wiki/view/IETF

[58] RTP – συντομογραφία για το Real Time Transport Protocol (Πρωτόκολλο μεταφοράς σε πραγματικό χρόνο). Ορίζει ένα τυπικό μορφότυπο πακέτου για την παράδοση ήχου και εικόνας μέσω του διαδικτύου. Ορίζεται στο RFC 1889. Δημιουργήθηκε από τον όμιλο Audio Video Transport Working και δημοσιεύτηκε για πρώτη φορά το 1996. Για περισσότερες πληροφορίες βλέπε, http://www.ietf.org/rfc/rfc1889.txt

[59] Το G.729 είναι ένας αλγόριθμος συμπίεσης στοιχείων για τη φωνή που συμπιέζει την ψηφιακή φωνή σε πακέτα διάρκειας των 10ms. Για περισσότερες πληροφορίες βλέπε, http://www.voip-info.org/wiki/view/ITU+G.729

Το παρακάτω σχήμα απεικονίζει την τοπολογία του δικτύου για το video streaming σενάριο.



Σχήμα 7-5: *Σενάριο video streaming*

Από τις δοκιμές που έγιναν παρατηρήθηκε ότι με την υπάρχον διαμόρφωση του IPSec είναι δυνατή η υλοποίηση του video streaming, χωρίς σημαντική επιβάρυνση.

	Μέγεθος κρυπτογραφημένου πακέτου	**Μέγεθος πακέτου χωρίς κρυπτογράφηση**	**Διαφορά**	**Επιβάρυνση % επί των αρχικών δεδομένων**
Μέσος όρος μεγέθους ενός πακέτου	1430 Bytes	1370 Bytes	60 Bytes	4.38%

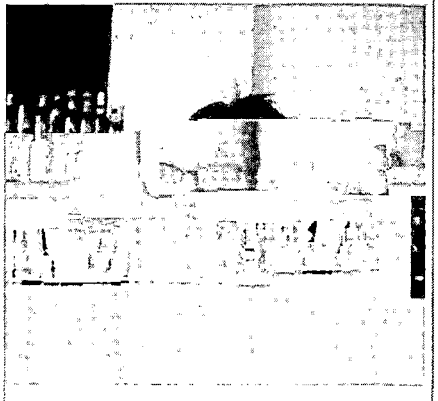
Πίνακας 7-4: *Επιπλέον φόρτος που εισάγει το IPSec στο αρχικό πακέτο*

Ένα ακόμα σημαντικό ζήτημα που πρέπει να σημειωθεί είναι ότι γενικότερα τα VPN συστήματα στηρίζονται στο διαδίκτυο για να μεταδώσουν τα δεδομένα τους. Το πρόβλημα είναι, ότι το video streaming απαιτεί ένα εγγυημένο εύρος ζώνης, ενώ το διαδίκτυο είναι ένα δημόσιο κοινόχρηστο δίκτυο και αυτή η διαθεσιμότητα εύρους ζώνης δεν μπορεί να εγγυηθεί. Έχουν αναπτυχτεί διάφορα standards για την παροχή υπηρεσιών εγγυημένης ποιότητας (quality of service-QoS)[60] που ως στόχο έχουν, να βελτιώσουν την ικανότητα δημόσιων προσβάσιμων δικτύων ώστε να μπορούν να υποστηρίξουν εφαρμογές πραγματικού χρόνου[61]. Το εύρος ζώνης για την μεταφορά αρχείων με το πρωτόκολλο FTP μπορεί να κυμαίνετε όπως μας δείχνει το *Σχήμα 7-6*.

---

[60] Η υπηρεσία παροχής ποιότητας (Quality of Service-QoS) περιλαμβάνει το σύνολο των αλγορίθμων που προσπαθούν να παρέχουν διαφορετικά επίπεδα ποιότητας στα διάφορα είδη κίνησης δικτύου. Για περισσότερες πληροφορίες βλέπε, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html

[61] Πληροφορίες σχετικά με υλοποίηση QoS σε IPsec πακέτα βλέπε, Lars Völker, Marcus Schöller, Martina Zitterbart: "Introducing QoS mechanisms into the IPsec packet processing", 32nd IEEE Conference on Local Computer Networks (LCN 2007), IEEE, p. 360--367, Dublin, Ireland, Oct 2007.

Περιγραφή	Αρχικό video	Streamed video
The video streaming αρχίζει κανονικά και όλα φαίνεται να πηγαίνουν καλά		
Το διαθέσιμο εύρος ζώνης μειώνεται σε 950 Kbit/sec. Αμέσως ορισμένες παραμορφώσεις παρουσιάζονται στα frames του video		
Έπειτα από μερικά δευτερόλεπτα η εικόνα του video παραμορφώνεται σε μεγάλο βαθμό, σε σημείο να μην μπορούμε να διακρίνουμε τίποτα		
Η παραμόρφωση συνεχίζεται έπειτα από μερικά ακόμα δευτερόλεπτα. Αυξάνουμε το διαθέσιμο εύρος ζώνης σε 1024 Kbit/sec για να παρατηρήσουμε την αντίδραση του video streaming		

Αύξηση της ταχύτητας βελτιώνει σχεδόν ακαριαία την ποιότητα του video.		
Έπειτα από μερικά μόλις δευτερόλεπτα η εικόνα έχει επανέλθει πλήρως σε φυσιολογικά επίπεδα. Ρυθμίζουμε πάλι την ταχύτητα σε 950 Kbit/sec		
Σχεδόν αμέσως αφού μειώσαμε την ταχύτητα, άρχισαν να ξαναεμφανίζονται παραμορφώσεις στο video		
Έπειτα από μερικά δευτερόλεπτα η εικόνα παραμορφώθηκε εντελώς		

Σχήμα 7-7: *Η διακύμανση της ποιότητας του video σε σχέση με το διαθέσιμο εύρος ζώνης*

Με τις παραπάνω δόκιμες καταλήγουμε στο συμπέρασμα ότι η αλλοίωση της ποιότητας στο video δεν είναι χαρακτηριστικό μόνο του IPSec, άλλα κάθε VPN πρωτοκόλλου που χρησιμοποίει το διαδίκτυο για να υλοποιήσει μια σύνδεση. Ουσιαστικά το πρόβλημα αρχίζει εκεί οπου στηρίζετε η φιλοσοφία και η σκέψη για τα VPN δίκτυα. Ο ορισμός ενός VPN, όπως είδαμε και στο κεφάλαιο 2, είναι " εξομοίωση ενός προσωπικού Wide Area Network (WAN), χρησιμοποιώντας ένα κοινόχρηστο ή δημόσια προσβάσιμο μέσο επικοινωνίας, όπως το Internet και τα IP δίκτυα." Εξ' ορισμού δηλαδή υπάρχει το πρόβλημα και σε αυτή την «ατέλεια» στηρίζονται εναλλακτικές λύσεις, όπως είναι οι μισθωμένες γραμμές (leased lines). Τα πλεονεκτήματα αυτών είναι ότι το εύρος ζώνης είναι πάντα εγγυημένα διαθέσιμο στον πελάτη, προσφέροντας μια αξιόπιστη και σταθερή επιλογή. Άλλωστε, αυτός είναι και ο λόγος που οι μισθωμένες γραμμές απαιτούν μεγάλο κόστος για την απόκτηση τους. Με την χρησιμοποίηση μισθωμένων γραμμών δεν υπάρχει πλέον ανταγωνισμός για το κοινόχρηστο διαθέσιμο εύρος ζώνης και σε περιπτώσεις οπου το υψηλό επίπεδο ασφάλειας κρίνεται απαραίτητο, σε συνδυασμό με την απαίτηση για μεγάλο και σταθερό εύρος ζώνης, με την υπάρχουσα τεχνολογία, οι μισθωμένες γραμμές κρίνονται ως μονόδρομος.

Τέλος, να σημειωθεί ότι το αποτέλεσμα των παραπάνω δοκιμών δεν είναι κατά της υλοποίησης VPN με IPSec, άλλα μια πρόταση για εναλλακτικές επιλογές κατασκευής VPN δικτύων, οι οποίες σε μερικές περιπτώσεις μπορεί να είναι και απαραίτητες.

ΚΕΦΑΛΑΙΟ 8

8. Αξιολόγηση του VPN IPSec δικτύου με αντίστοιχες εμπορικές επιλογές

Στο προηγούμενο κεφάλαιο αξιολογήθηκε η απόδοση του VPN IPSec δικτύου που έχει υλοποιηθεί στην παρούσα πτυχιακή. Σε αυτό το κεφάλαιο θα γίνει σύγκριση μεταξύ του IPSec συστήματος με αντίστοιχες hardware εναλλακτικές λύσεις που κυκλοφορούν στο εμπόριο. Οι πυλώνες στους οποίους θα στηριχτεί η ανάλυση είναι σχετικές με τις επιδόσεις και το κόστος υλοποίησης των εναλλακτικών λύσεων που θα παρουσιαστούν. Ο τελικός σκοπός είναι να παρουσιαστεί το τι μπορεί να προσφέρει μια υλοποίηση με λογισμικό ανοιχτού κώδικα και με ποιο αντίτιμο, σε αντιπαραβολή με hardware λύσεις.

Θα πρέπει να αναφερθεί ότι οι εναλλακτικές λύσεις που κυκλοφορούν στο εμπόριο δεν περιορίζονται μόνο σε hardware επιλογές άλλα και σε software. Αυτές οι λύσεις όμως ξεφεύγουν από τον σκοπό αυτής εργασίας διότι το κόστος υλοποίησης τους είναι αρκετά υψηλό και οι επιδόσεις του προσφέρουν, αμφιλεγόμενες, σε σχέση με hardware προτάσεις.

8.1 Σύγκριση χαρακτηριστικών

Σε αυτό το κομμάτι θα αναλυθούν τα χαρακτηριστικά των VPNs με λογισμικό ανοιχτού κώδικα έναντι άλλων εμπορικών λύσεων. Σαν γενικό κανόνα θα λέγαμε ότι το ελεύθερο λογισμικό προσφέρει απεριόριστες δυνατότητες χωρίς επιπλέον κόστος, αλλά με περιορισμένη υποστήριξη. Στον αντίποδα εμπορικές λύσεις παρέχουν εξαιρετικό επίπεδο υποστήριξης με το αντίστοιχο όμως τίμημα.

Το πρώτο κύριο χαρακτηριστικό που θα εξετάσουμε είναι ο αριθμός των χρηστών και των tunnel που μπορούν να υποστηρίξουν οι δυο πλευρές. Τα VPN με ΕΛ/ΛΑΚ (Ελεύθερο Λογισμικό/Λογισμικό Ανοικτού Κώδικα) θεωρητικά δεν επιβάλλουν κανένα περιορισμό στον αριθμό των χρηστών και tunnel που μπορούν να συνδεθούν και να κατασκευαστούν, με μόνο όριο την επαρκή υπολογιστική ισχύ του server για να ανταποκριθεί σε έναν τεράστιο αριθμό αιτημάτων. Σε αντίθεση, στα εμπορικά VPNs ο αριθμός των χρηστών και των tunnels είναι σε συνάρτηση με τον προϋπολογισμό κάθε επιχείρησης. Αυτό σημαίνει ότι το κόστος θα είναι μεγαλύτερο για κάθε επιπλέον χρήστη και tunnel, με την μορφή απόκτησης αδειών. Είναι επίσης δυνατό να καταβληθεί ένα πολύ υψηλό αντίτιμο για να υποστηρίζεται απεριόριστος αριθμός χρηστών, ενώ για την αύξηση των tunnel συνήθως θα πρέπει να γίνει αναβάθμιση στο υλικό ώστε να επεκταθούν οι δυνατότητες του gateway.

Δεύτερος κρίσιμος παράγοντας που μπορεί να επηρεάσει την επιλογή του πελάτη είναι η δυσκολία εγκατάστασης και το κόστος που απορρέει από αυτήν. Με λογισμικό ανοικτού κώδικα η εγκατάσταση ενός ασφαλούς VPN IPSec δικτύου είναι ιδιαίτερα περιπλοκή και δύσκολη εξαιτίας των πολλών και διαφορετικών παραμέτρων και εξαρτάται από την εμπειρία και την τεχνογνωσία του μηχανικού ή τον διαχειριστή δικτύου της εταιρίας. Επιπλέον είναι σχεδόν σίγουρο ότι θα προκύψουν ζητήματα ασυμβατότητας υλικών στις περισσότερες των περιπτώσεων.

Όσον άφορα τις λύσεις που κυκλοφορούν στο εμπόριο, η διαδικασία εγκατάστασης αναμένετε να είναι ευκολότερη και χωρίς ζητήματα ασυμβατότητας. Επίσης, πρόσθετο κόστος μπορεί να απαιτείται για την εγκατάσταση και παραμετροποίηση ενός VPN συστήματος από τον εμπορικό προμηθευτή, εκτός και εάν μπορεί να το αναλάβει ο διαχειριστής του δικτύου.

Τέλος, ο τρίτος παράγοντας που εξετάζετε είναι ο βαθμός υποστήριξης και οι αναβαθμίσεις που παρέχονται από τις δυο διαφορετικές VPN επιλογές υλοποίησης. Πολλές φόρες μάλιστα αυτός είναι ένας καθοριστικός παράγοντας για την τελική απόφαση του πελάτη. Η υποστήριξη που παρέχετε από το ελεύθερο λογισμικό είναι ίσως και το μεγαλύτερο μειονέκτημα γενικότερα ΕΛ/ΛΑΚ λύσεων. Αν και υπάρχει αρκετή υποστήριξη από τους υπεύθυνους για την ανάπτυξη ενός λογισμικού καθώς επίσης και από διάφορους ανθρώπους που ασχολούνται με το συγκεκριμένο λογισμικό, παρ' όλα αυτά μπορεί να υπάρχουν περιπτώσεις οπου καμία βοήθεια δεν θα παρασχεθεί για μακροπρόθεσμο διάστημα. Επίσης οι αναβαθμίσεις που προσφέρονται, κατά βάση, δεν είναι τόσο συχνές όσο με τις αντίστοιχες εμπορικές επιλογές. Το πλεονέκτημα όμως είναι ότι δεν απαιτείται η καταβολή χρημάτων για την υποστήριξη και για τις αναβαθμίσεις. Στην άλλη πλευρά, οι λύσεις του εμπορίου παρέχουν εξαιρετικό επίπεδο υποστήριξης των προϊόντων τους άλλα με το αντίστοιχο κόστος. Οι αναβαθμίσεις είναι συχνές και δεν προκύπτουν ζητήματα ασυμβατότητας, ενώ επίσης, συχνά οι εμπορικοί προμηθευτές προλαμβάνουν πιθανά προβλήματα προτού εμφανιστούν ή τουλάχιστον σε σύντομο χρονικό διάστημα. Όλα αυτά δίνουν ένα αίσθημα ασφάλειας στον πελάτη, κερδίζουν την προτίμηση και την εμπιστοσύνη του.

8.2 Σύγκριση κόστους

Σε αυτό το κεφάλαιο θα καθοριστεί ο προϋπολογισμός που πρέπει να δαπανήσει μια επιχείρηση για να υλοποιήσει μια από τις δυο επιλογές. Ο υπολογισμός του κόστους περιέχει, κατά προσέγγιση και τα έξοδα για την εγκατάσταση του εξοπλισμού χωρίς όμως να υπολογίζονται τυχόν άλλα έξοδα που θα προκύψουν από την διαχείριση των συστημάτων και την συντήρηση τους.

Η Cisco είναι κυρίαρχος στον χώρο οπου δραστηριοποιείται και για αυτό τον λόγο επιλέχτηκε να χρησιμοποιηθούν VPN hardware συσκευές της, ως σημείο αναφοράς. Στον επόμενο πίνακα (*8.1*), παρουσιάζονται συσκευές της Cisco μαζί με ορισμένα τεχνικά χαρακτηριστικά και το αντίστοιχο κόστος τους. Επίσης, στον *Πίνακα 8.2* παρουσιάζονται, ενδεικτικά, το κόστος απόκτησης αδειών για επιπλέον χρήστες για την συσκευή Cisco ASA 5510.

Cisco ISR and ASA Series		
Small Branch	Performance	
Cisco ISR 1800 / 1841 Price - $1,100-$2,100	L3 forwarding	75,000 pps
	VPN forwarding:	95 Mbps
	Max VPN tunnels	800
Cisco ISR 2801 Price - $1,800-$3,300	L3 forwarding	90,000 pps
	VPN forwarding:	145 Mbps
	Max VPN tunnels	1,500
Cisco ASA 5505 Price - $500-$2,700	L3 forwarding	85,000 pps
	VPN forwarding:	100 Mbps
	Max VPN tunnels	10 / 25
Small-Medium Branch, Small Enterprise		
Cisco ISR 2811 Price - $1,800-$4,300	L3 forwarding	120,000 pps
	VPN forwarding:	145 Mbps
	Max VPN tunnels	1,500
Cisco ISR 2821 Price - $2,800-$6,000	L3 forwarding	170,000 pps
	VPN forwarding:	145 Mbps
	Max VPN tunnels	1,500
Cisco ISR 2851 Price - $4,600-$9,500	L3 forwarding	220,0000 pps
	VPN forwarding:	145 Mbps
	Max VPN tunnels	1,500
Cisco ASA 5510 $2,500-$16,000	L3 forwarding	190,000 pps
	VPN forwarding:	170 Mbps
	Max VPN tunnels	250
Large Branch, Medium Enterprise		
Cisco ISR 3825 Price - $6,700-$12,500	L3 forwarding	350,000 pps
	VPN forwarding:	175 Mbps
	Max VPN tunnels	2,000
Cisco ISR 3845 Price - $9,150-$15,200	L3 forwarding	500,000 pps
	VPN forwarding:	185 Mbps
	Max VPN tunnels	2,500
Cisco ASA 5520 Price - $5,500-$16,000	L3 forwarding	320,000 pps
	VPN forwarding:	225 Mpbs
	Max VPN tunnels	750
Cisco ASA 5540 Price - $11,700-$23,000	L3 forwarding	500,000 pps
	VPN forwarding:	325 Mbps
	Max VPN tunnels	5,000
Enterprise, Service Provider Edge		
Cisco 7200VXR Price - $30,000-$36,000	L3 forwarding	2,000,000 pps
	VPN forwarding:	260 Mbps
	Max VPN tunnels	5,000
Cisco ASA 5550 Price - $13,500-$60,000	L3 forwarding	600,000 pps
	VPN forwarding:	425 Mbps
	Max VPN tunnels	5,000

Πινάκας 8-1: *Cisco συσκευές και οι αντίστοιχες τιμές τους.*
(ISR είναι συντομογραφία του Integrated Services Routers[63]
και το ASA είναι συντομογραφία Adaptive Security Appliance[64]*)*

---

[63] Integrated Services Routers (*ISR*) είναι ενιαίες συσκευές απλής χρήσης και διαχείρισης με πολλαπλές δυνατότητας όπως, ασύρματη δικτύωση, τείχος προστασίας, ποιότητα υπηρεσιών (QOS) κ.α. Για περισσότερες πληροφορίες, βλέπε, http://www.cisco.com/en/US/prod/routers/networking_solutions_products_genericcontent0900aecd806cab99.html

[64] Adaptive Security Appliance είναι συσκευές ασφαλείας της Cisco για περισσότερες πληροφορίες βλέπε, http://www.cisco.com/web/GR/solutions/smb/products/security/asa_5500_series_adaptive_security_appliances.html

	Κόστος Συσκευής	Χρήστες	Κόστος Απόκτησης Άδειας
Cisco ASA 5510 Adaptive Security Appliance	**$2,712.99**	**50**	**$329.99**
		150	**$784.99**
		250	**$2,685.99**
		500	**$4,003.99**

Πινάκας 8-2: *Κόστος απόκτησης αδειών για την συσκευή Cisco ASA 5510*

Για την υλοποίηση VPN με λογισμικό ανοιχτού κώδικα θα πρέπει να ληφθούν υπ' όψιν δυο παράγοντες για τον υπολογισμό του τελικού κόστους. Ο πρώτος είναι το κόστος για την εγκατάσταση και ο δεύτερος, το κόστος για τους gateways-servers. Στην πρώτη περίπτωση, το ποσό που θα δαπανηθεί εξαρτάται από το εάν η εγκατάσταση και παραμετροποίηση του συστήματος θα γίνει από εξωτερικό συνεργάτη ή ο υπεύθυνος για την διαχείριση του δικτύου της εταιρίας μπορεί να το αναλάβει μονός του. Εάν η εγκατάσταση πραγματοποιηθεί από εξωτερικό συνεργάτη, τότε το κόστος κατά προσέγγιση θα είναι $80 την ώρα και απαιτούνται περίπου πέντε εργάσιμες μέρες για κάθε σύστημα. Ο δεύτερος παράγοντας που επηρεάζει το κόστος είναι, εάν η εταιρία πρόκειται να χρησιμοποιήσει το υπάρχον σύστημα για το tunneling gateway, ή θα πρέπει να αποκτηθεί ένα καινούργιο σύστημα. Σε αυτή την περίπτωση, ίσως θα πρέπει να αγοραστούν καινούργιοι servers, καθώς η διαδικασία του tunneling προσθέτει επιπλέον φόρτο και αυτό ενδέχεται να επηρεάσει την απόδοση του συστήματος.

Περίπτωση	Κόστος Εγκατάστασης	Κόστος Server	Συνολικό Κόστος για κάθε Gateway
Ο διαχειριστής του δικτύου διαθέτει την απαιτουμένη εμπειρία και τεχνογνωσία για την εγκατάσταση και παραμετροποίηση του συστήματος Το μόνο επιπλέον κόστος θα είναι η απόκτηση των servers που θα χρειαστούν	-	$2000	**$2000**
Η εταιρία επιλεγεί την λύση του εξωτερικού συνεργάτη για την εγκατάσταση και παραμετροποίηση του VPN συστήματος Οι υπάρχον servers της εταιρίας επαρκούν για την δημιουργία του VPN δικτύου	$3200	-	**$3200**

Η εταιρία επιλέγει την λύση του εξωτερικού συνεργάτη για την εγκατάσταση και παραμετροποίηση του VPN δικτύου Απαιτείται η αγορά επιπλέον servers για την κάλυψη των αναγκών της εταιρίας	$3200	$2000	**$5200**

Πινάκας 8-3: *Συνολικό κόστος για την υλοποίηση VPN με λογισμικό ανοιχτού κώδικα*

Θα πρέπει να τονιστεί ότι τα ποσά που αναφέρονται στο παραπάνω πίνακα αφορούν την εγκατάσταση μόνο ενός tunnel gateway. Εάν για παράδειγμα μια εταιρία επιθυμεί την σύνδεση δυο γραφείων θα πρέπει να υπολογίσει το διπλάσιο κόστος.

Τα συμπεράσματα που εξάγονται από την παραπάνω ανάλυση είναι ότι η επιλογή ελεύθερου λογισμικού μειώνει κατά πολύ τα έξοδα που απαιτούνται για την εγκατάσταση ενός VPN δικτύου. Τα μειονεκτήματα όμως αυτής της λύσης είναι ότι απαιτεί εξειδικευμένο προσωπικό για την εγκατάσταση, παραμετροποίηση αλλά και την μετέπειτα διαχείριση του. Το γεγονός αυτό μπορεί να δημιουργήσει αρκετά προβλήματα στο μέλλον για μια εταιρία, γιατί στηρίζεται κατά μεγάλο βαθμό στον διαχειριστή του συστήματος και σε περίπτωση αποχώρησης του ίσως προκύψουν σημαντικά ζητήματα καθότι δεν υπάρχει υποστήριξη από τον προμηθευτή. Επίσης είναι σχεδόν σίγουρο ότι θα προκύψουν προβλήματα ασυμβατότητας και πιθανότατα θα πρέπει ο server να «ξαναστηθεί» από την αρχή. Για παράδειγμα, το IPSec δεν είναι συμβατό με kernel κάτω από 2.4. Στην άλλη πλευρά όμως, η επιλογή για υλοποίηση VPN με hardware, απαιτεί ένα πολύ μεγάλο κόστος αγοράς, εγκατάστασης και παραμετροποίησης του συστήματος αλλά παράλληλα είναι σταθερό, χωρίς προβλήματα ασυμβατότητας και με άμεση υποστήριξη. Το ερώτημα που εύλογα γενάτε είναι, ποια από τις δυο λύσεις είναι η ιδανική για να επιλέξει μια εταιρία. Η απάντηση ακολουθεί στο επόμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 9

9. Αποφασίζοντας την καταλληλότερη VPN επιλογή

Σε συνάρτηση πάντα με το κόστος που σχετίζεται με την κάθε επιλογή, το πιο σημαντικό κριτήριο για να ληφθεί η τελική απόφαση είναι, οι πραγματικές απαιτήσεις και οι ανάγκες που έχει η επιχείρηση συμπεριλαμβανομένου και του μεγέθους της.

9.1 Μικρού μεγέθους επιχειρήσεις

Το προφίλ μιας μικρής επιχείρησης στην παρούσα εργασία υποθέτεται ότι, απασχολεί περίπου 30 εργαζόμενους και εχει δυο ή τρία γραφεία. Δεν υπάρχει υπεύθυνος για την διαχείριση του δικτύου με μεγάλη εμπειρία και τεχνογνωσία και έτσι αναγκαστικά θα επιλεγεί η λύση του εξωτερικού συνεργάτη για την εγκατάσταση και παραμετροποίηση του συστήματος. Υποστήριξη θα πρέπει να παρέχεται σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα. Τυπικά εταιρίες τέτοιου μεγέθους αναζητούν ένα σύστημα που να πληρώσουν μια φορά το αντίτιμο που απαιτείται για την απόκτηση του εξοπλισμού, να το εγκαταστήσουν και να «παίζει» χωρίς προβλήματα. Η ιδανική λύση είναι η επιλογή ενός εμπορικού λογισμικού περιορισμένων δυνατοτήτων και η απόκτηση ενός μικρού αριθμού αδειών χρήσης.

9.2 Μεσαίου μεγέθους επιχειρήσεις

Το προφίλ μιας μεσαίας επιχείρησης στην παρούσα εργασία υποθέτεται ότι, απασχολεί περίπου 100 εργαζόμενους και έχει 15 με 20 γραφεία. Συνήθως σε αυτές τις εταιρίες υπάρχει ένα IT τμήμα οπου μπορεί να ανταποκριθεί στις απαιτήσεις για την εγκατάσταση και την διαχείριση του δικτύου ώστε να αποφευκτεί η λύση εξωτερικών συνεργατών. Επιπλέον, είναι μεγαλύτερη η πιθανότητα μια μεσαία εταιρία να αναπτυχτεί γρηγορότερα στο μέλλον και παράλληλα θα πρέπει και το VPN δίκτυο της, να είναι σε θέση να ανταποκριθεί άμεσα, εύκολα και οικονομικά στις διαφορές μεταβολές. Η λύση που καλύπτει πιο καλά τις ανάγκες αυτών των εταιριών είναι VPN με λογισμικό ανοιχτού κώδικα. Δεν χρειάζεται να πληρώσουν εξωτερικούς συνεργάτες για την εγκατάσταση και παραμετροποίηση του συστήματος, αν και η εγκατάσταση σε 15 με 20 γραφεία μπορεί να είναι χρονοβόρα.

9.3 Μεγάλου μεγέθους επιχειρήσεις

Το προφίλ μιας μεγάλης επιχείρησης στην παρούσα εργασία υποθέτεται ότι, απασχολεί περίπου 1000 εργαζόμενους και έχει 100 γραφεία. Σε αυτή την περίπτωση απαιτείται υψηλή απόδοση εξαιτίας του μεγάλου δικτύου. Ασχέτως με το κόστος, θα πρέπει να παρέχεται άμεση και υψηλού επιπέδου υποστήριξη ανά πάσα χρονική στιγμή. Επίσης θα πρέπει να παρέχονται συχνές αναβαθμίσεις για λόγους ασφαλείας και να γίνεται σε καθορισμένες περιόδους συντήρηση των συσκευών και εν γένει του δικτύου. Η πιο ιδανική και λογική λύση σε αυτές τις περιπτώσεις είναι η απόκτηση hardware εμπορικών VPN λύσεων. Κυρίως αυτή η επιλογή γίνεται διότι η ανάγκη για υποστήριξη είναι σε πολύ μεγάλο βαθμό. Τέλος, οι μεγάλες εταιρίες έχουν τόσα

πολλά γραφεία, που είναι παράλογο να χρησιμοποιηθεί το υπάρχον προσωπικό για μια τόσο χρονοβόρο εργασία.

9.4 Συμπέρασμα

Το θέμα που πραγματεύτηκε στην παρούσα πτυχιακή εργασία αφορούσε τα VPNs δίκτυα και πιο συγκεκριμένα αυτά που υλοποιούνται με την σουίτα πρωτοκόλλων IPSec. Η δημιουργία VPN, προσφέρει μια οικονομικά αποτελεσματική και αποδοτική πρόταση που επιτρέπει την ασφαλή σύνδεση απομακρυσμένων ιδιωτικών δικτύων μέσω του διαδικτύου. Αυτή η πρόταση είναι ιδιαιτέρως ενδιαφέρουσα για τις επιχειρήσεις, καθώς μπορούν να μειώσουν το κόστος αντικαθιστώντας τις μισθωμένες γραμμές με VPNs δίκτυα. Στην σημερινή εποχή τα VPNs είναι αρκετά δημοφιλή και αναμένετε να έχουν ακόμα πιο πρωταγωνιστικό ρόλο στο μέλλον. Οι απαιτήσεις για ασφάλεια στην μεταφορά δεδομένων με παράλληλη μείωση του κόστους είναι σημαντικό ζήτημα στο παρόν και ένα μείζον θέμα στο μέλλον. Πολλά άρθρα και μελέτες, έχουν γραφτεί και θεωρούν μονόδρομο την επιλογή VPNs για τις επιχειρήσεις του μέλλοντος. Εάν μάλιστα συνυπολογίσουμε και τις διεθνείς οικονομικές εξελίξεις γίνεται αντιληπτό τα πολλαπλά οφέλη που προσφέρει αυτή η τεχνολογία.

Το IPSec παρέχει κρυπτογράφηση στο επίπεδο του IP και για αυτό το λόγο αποτελεί ένα αξιοσημείωτο κομμάτι της συνολικής ασφάλειας. Σήμερα, θεωρείται μια αξιόπιστη και καλοσχεδιασμένη λύση με πολλές δυνατότητες. Σε όλη την εργασία αναλύθηκε διεξοδικά το IPSec και ο τρόπος λειτουργίας του. Επίσης υλοποιήθηκε ένα site-to-site IPSec VPN δίκτυο για την καλύτερη κατανόηση του και την εξαγωγή χρήσιμων αποτελεσμάτων. Κατά την διάρκεια της εγκατάστασης παρουσιαστήκαν αρκετά προβλήματα και χρειάστηκε να «ξαναστηθεί» ολόκληρο το σύστημα από την αρχή για να ξεπεραστούν αυτές οι δυσκολίες.

Η υλοποίηση του IPSec δικτύου, επέτρεψε την περαιτέρω αξιολόγηση του και έφερε στην επιφάνεια ορισμένα προβλήματα στην απόδοση του πρωτοκόλλου. Χαρακτηριστικό παράδειγμα είναι ότι το IPSec είναι αναποτελεσματικό με εφαρμογές που χρησιμοποιούν πακέτα πολύ μικρού μεγέθους. Το πρόβλημα είναι οι επιπλέον επικεφαλίδες που εισάγει σε κάθε πακέτο το IPSec, οι όποιες δημιουργούν πρόσθετο φόρτο, που ίσως ορισμένες φόρες είναι και μεγαλύτερου μεγέθους από ότι το αρχικό πακέτο. Αυτό είναι ένα πιθανό ζήτημα που θα πρέπει να ληφθεί υπ' όψιν καθώς επηρεάζει δημοφιλείς εφαρμογές όπως είναι οι εφαρμογές VoIP. Μια ακόμα αδυναμία του IPSec είναι ότι τα VPNs χρησιμοποιούν το διαδίκτυο για να μεταφέρουν δεδομένα. Αυτό μεταφράζετε στο ότι κάθε μειονέκτημα που έχει το διαδίκτυο (εκτός από την ασφάλεια) θα το έχουν και όλα τα VPNs δίκτυα, ασχέτως με τα πρωτόκολλα που επιλέχτηκαν για να κατασκευαστεί. Οι επιπτώσεις που απορρέουν από αυτή την αδυναμία είναι ότι εφαρμογές οπου απαιτούν εγγυημένο εύρος ζώνης για να λειτουργήσουν σωστά, π.χ όπως είναι το video streaming, δεν θα αποδώσουν τα αναμενόμενα εάν χρησιμοποιηθούν με VPNs δίκτυα. Επίσης, πολύς κόσμος πιστεύει ότι τα VPNs μπορούν να αντικαταστήσουν πλήρως τις μισθωμένες γραμμές. Δυστυχώς, αυτό είναι ακόμα αναληθές καθώς υπάρχουν περιπτώσεις όπου οι μισθωμένες γραμμές είναι μονόδρομος. Παρότι είναι μια πολύ οικονομική λύση για ασφαλείς συνδέσεις που προσφέρει μια πλειάδα από πλεονεκτήματα, τα VPNs

δίκτυα θα εξακολουθήσουν να έχουν ευάλωτα σημεία, όσο το μέσο που χρησιμοποιούν (διαδίκτυο) είναι ευάλωτο.

Κλείνοντας, η γενική άποψη που μου άφησε η ενασχόληση μου με τα VPNs είναι ότι η χρήση του πρωτοκόλλου IPSec και γενικότερα των VPNs θα πρέπει να σχετίζονται περισσότερο με το πολύ καλό επίπεδο ασφάλειας που προσφέρουν, πάρα με τα οικονομικά οφέλη που απορρέουν από την χρήση τους. Οι μισθωμένες γραμμές δεν μπορούν σε καμιά περίπτωση να αντικατασταθούν με VPNs, μέχρι ότου τα IP δίκτυα να βελτιωθούν στον τομέα παροχής ποιότητας υπηρεσιών (QoS). Παρόλα αυτά τα VPNs δίκτυα είναι μια τεχνολογία που θα γνωρίσουν ακόμα πιο μεγάλη ανάπτυξη στο μέλλον διότι έχουν σημαντικά πλεονεκτήματα, συνεχώς αναπτύσσονται και είναι λιγότερο δαπανηρά στη λειτουργία τους σε σχέση με τα ιδιωτικά δίκτυα από άποψη διαχείρισης, εύρους ζώνης και κεφαλαίου. Κατά συνέπεια ο χρόνος απόσβεσης ενός VPN δικτύου μετράται συνήθως σε μήνες αντί σε χρόνια. Ίσως, το πιο σημαντικό πλεονέκτημα από όλα να είναι ότι τα VPNs επιτρέπουν στις επιχειρήσεις να επικεντρωθούν στο αντικείμενο ενασχόλησής τους και όχι στο πώς να κρατήσουν το δίκτυό τους ζωντανό και αποδοτικό.

Β΄ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 1

1. Εισαγωγή

Σε αυτό το τμήμα θα καλυφτεί το δεύτερο μέρος της πτυχιακής εργασίας σχετικά με την απομακρυσμένη διαχείριση του διαδραστικού σταθμού πληροφόρησης (infokiosk) του ΤΕΙ Μεσολογγίου. Θα γίνει αναφορά στα infokiosk μηχανήματα (τι είναι, πως λειτουργούν), γιατί το Τεχνολογικό Ίδρυμα Μεσολογγίου προχώρησε στην απόκτηση ενός τέτοιου μηχανήματος και τι ανάγκες εξυπηρετεί. Τέλος, θα παρουσιαστεί η εγκατάσταση του λογισμικού μέσω του οποίου θα είναι εφικτή η απομακρυσμένη διαχείριση του Infokiosk, από τον επιστημονικό υπεύθυνο του γραφείου διασύνδεσης, Δρ. Αριστογιάννη Γαρμπή.

ΚΕΦΑΛΑΙΟ 2

2. Τι είναι οι διαδραστικοί σταθμοί πληροφόρησης

Το Infokiosk ή Διαδραστικός Σταθμός Πληροφόρησης είναι ένας ειδικά κατασκευασμένος υπαίθριος ή μη κλωβός, ο οποίος μέσω ενός υπολογιστικού συστήματος και κατάλληλου λογισμικού που διαθέτει, παρέχει στον χρήστη επιλεγμένες πληροφορίες σε ηλεκτρονική μορφή με χρήση τεχνολογίας πολυμέσων (multimedia). Οι διαδραστικοί σταθμοί πληροφόρησης μπορούν να εγκατασταθούν σε επίκαιρα σημεία και να λειτουργήσουν είτε σαν αυτόνομοι σταθμοί είτε διασυνδεδεμένοι μεταξύ τους σε δίκτυο. Επίσης τα Infokiosk μπορούν να είναι εξωτερικού ή εσωτερικού χώρου και να παρέχουν υπηρεσίες είτε στο γενικό κοινό είτε στο προσωπικό ενός συγκεκριμένου φορέα. Η επικοινωνία του συστήματος με τον χρήστη γίνεται με χρήση οθόνης αφής (touchscreen). Για την υποστήριξη πιο εξειδικευμένων εφαρμογών τα Infokiosk διαθέτουν επίσης, πληκτρολόγιο και touch pad.

Οι σταθμοί πληροφόρησης χρησιμοποιούνται για την ενημέρωση των επισκεπτών μίας περιοχής ενδιαφέροντος; ενός ειδικού θεματικού τμήματος, ή και ενός ορισμένου σημείου. Μπορούν να εγκατασταθούν σε οποιονδήποτε χώρο, εφόσον η αισθητική τους εναρμονίζεται με το περιβάλλον τους. Έχουν τη δυνατότητα να λειτουργούν σε κλειστούς αλλά και υπαίθριους χώρους, και είναι ανθεκτικοί στις περιβαλλοντικές συνθήκες. Επιπλέον, μπορούν να προσαρμοστούν στον διαθέσιμο χώρο και να τοποθετηθούν σε τοίχους, ειδικές βάσεις, ή ακόμα και επάνω σε πάγκους. Οι πληροφορίες δίνονται στον επισκέπτη μέσω οθόνης αφής ή πληκτρολογίου, τα οποία είναι ειδικά διαμορφωμένα έτσι ώστε να είναι εύκολα και ανθεκτικά στη χρήση. Παρουσιάζουν το περιεχόμενο τους με απλό και κατανοητό τρόπο, χρησιμοποιώντας επεξηγηματικά video, κείμενα, φωτογραφικό υλικό ή και ηχητικά μηνύματα. Παρέχουν τη δυνατότητα σύνδεσης με το διαδίκτυο (Internet), σε ένα ελεγχόμενο περιβάλλον με παράλληλη δυνατότητα εκμετάλλευσης του.
Τα βασικά πλεονεκτήματα των διαδραστικών σταθμών πληροφόρησης είναι:

- Διαθέτουν ποιοτική κατασκευή και αισθητική
- Προσαρμόζονται σε οποιονδήποτε χώρο εντός-εκτός
- Παρουσιάζουν οποιεσδήποτε πληροφορίες επιθυμούν οι επισκέπτες
- Παρέχουν τη δυνατότητα προβολής κειμένων, φωτογραφιών, ήχων, και video.

Οι σταθμοί πληροφόρησης τοποθετούνται στις εισόδους και τους εσωτερικούς χώρους ιδιωτικών επιχειρήσεων, Δημόσιων φορέων και οργανισμών, στις αίθουσες μουσείων, στις αίθουσες εκθέσεων και εμπορικών κέντρων, στις εισόδους και στις αίθουσες συμβουλίων, σε καταστήματα τραπεζών και γενικά σε κάθε δημόσιο εσωτερικό χώρο όπου ο χρήστης συναλλάσσεται καθημερινά.

2.1 Infokiosk - Προδιαγραφές και Κατασκευή

Οι διαδραστικοί σταθμοί πληροφόρησης είναι ειδικά κατασκευασμένοι και διαθέτουν υπολογιστικά συστήματα σύγχρονης τεχνολογίας. Οι κλωβοί είναι κατασκευασμένοι με ανοδιωμένο αλουμίνιο και ανοξείδωτο ατσάλι ειδικά επεξεργασμένο για την αντιχαρακτική τους προστασία. Οι οθόνες προβολής είναι υψηλής ευκρίνειας κατάλληλα κατασκευασμένες με προστασία έναντι χαράξεων και προστασία έναντι της σκόνης και των υγρών. Το εσωτερικό των σταθμών είναι εξοπλισμένο με υπολογιστικές μονάδες (ηλεκτρονικούς υπολογιστές) σύγχρονης τεχνολογίας οι οποίοι διαθέτουν κατάλληλα λογισμικά συστήματα (software). Στην οθόνη του σταθμού μεταφέρεται τα μήνυμα τα οποία μπορεί να είναι κείμενο, προβολή video, δημιουργία εφαρμογής για συγκεκριμένο θέμα, ανακοινώσεις και άλλα. Οι σταθμοί πληροφόρησης είναι εξοπλισμένοι με κατάλληλο ηχητικό σύστημα με δύο Hi-Fi ηχεία μέσω των οποίων η επικοινωνία και η ενημέρωση μπορεί να συνοδεύεται και με ήχο ή μουσική επένδυση. Στην οθόνη των σταθμών επίσης μπορούν να προβληθούν διάφορα θέματα τα οποία να συνοδεύονται από πανοραμικές εφαρμογές. Υπάρχει οθόνη αφής (touch screen) μέσω της οποίας ο χρήστης μπορεί αφ΄ ενός να πλοηγηθεί στο διαδίκτυο και αφ΄ ετέρου μπορεί να επιλέξει κάθε προεγκατεστημένη εφαρμογή για την ενημέρωσή του.

2.2 Διαδραστικός Σταθμός Πληροφόρησης στο ΤΕΙ Μεσολογγίου

Στο παλιό κτίριο της ΣΔΟ (Σχολή Διοίκησης και Οικονομίας), εγκαταστάθηκε πρόσφατα ένας καινούργιος διαδραστικός σταθμός πληροφόρησης για τους σπουδαστές και επισκέπτες του ΤΕΙ Μεσολογγίου. Το Γραφείο Διασύνδεσης του ιδρύματος[1] σε συνεργασία με το Εργαστήριο Ηλεκτρονικής Επιχειρηματικότητας-eBusiness Lab[2] του Τμήματος Εφαρμογών Πληροφορικής στη Διοίκηση και την Οικονομία[3] εγκατέστησαν ένα διαδραστικό σταθμό πληροφόρησης για την διευκόλυνση των σπουδαστών και των επισκεπτών του ΤΕΙ Μεσολογγίου. Ο σταθμός αυτός προσφέρει υπηρεσίες πληροφόρησης για όλα τα τμήματα του ΤΕΙ Μεσολογγίου καθώς και ενημερωτικό υλικό για την πόλη του Μεσολογγίου. Ο σταθμός είναι συνδεδεμένος στο διαδίκτυο και οι σπουδαστές, χρησιμοποιώντας την οθόνη αφής που έχει εγκατασταθεί, έχουν πρόσβαση σε όλες τις ηλεκτρονικές και διαδραστικές υπηρεσίες του ιδρύματος.

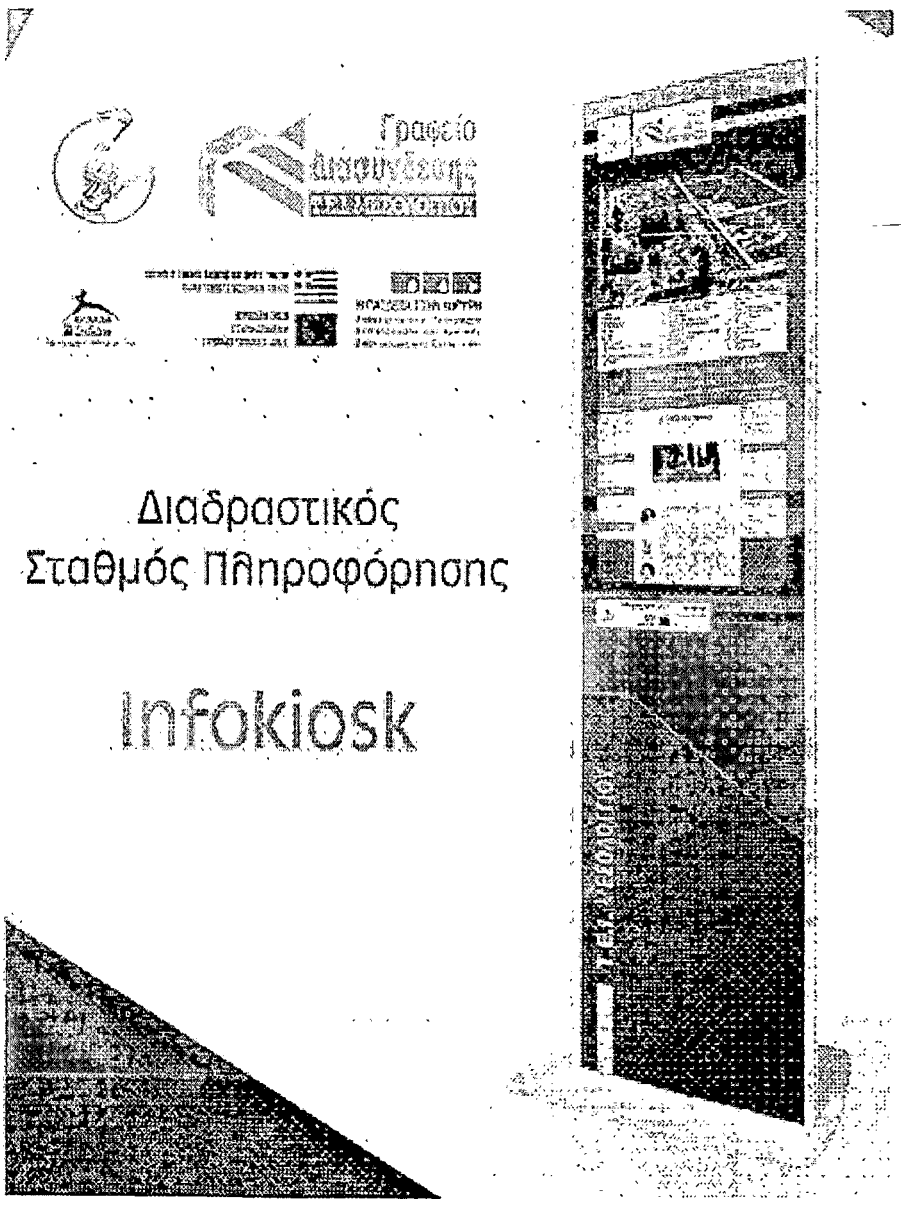
---

1 Η ιστοσελίδα του γραφείου διασύνδεσης είναι http://career.teimes.gr/career/

2 Η ιστοσελίδα του εργαστηρίου www.ebusiness-lab.gr

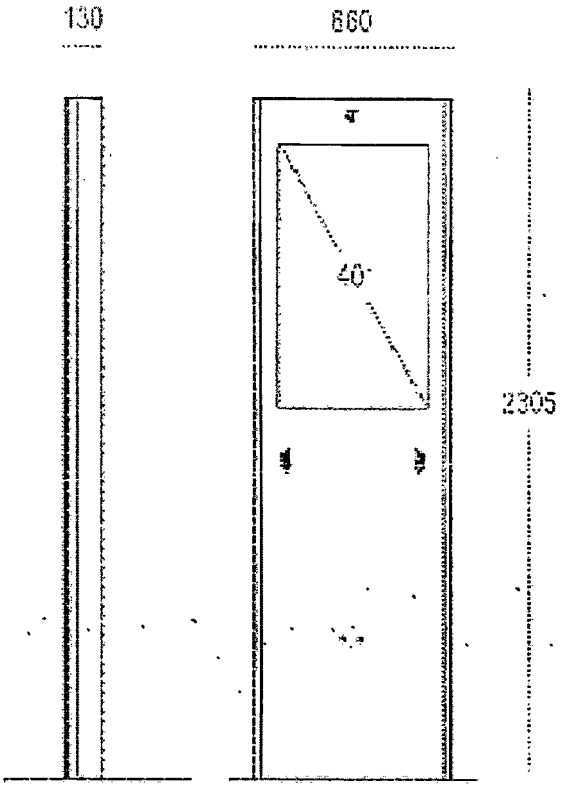
3 Η ιστοσελίδα του τμήματος Εφαρμογών Πληροφορικής στη Διοίκηση και Οικονομίας, www.epdo.teimes.gr

Με αυτό τον τρόπο οι σπουδαστές έχουν πρόσβαση στη συμπλήρωση αιτήσεων προς τις γραμματείες των τμημάτων για έκδοση πιστοποιητικών, στην ηλεκτρονική δήλωση μαθημάτων και συγγραμμάτων, ενημέρωση για τα αποτελέσματα των εξετάσεων και των βαθμών των εργαστηρίων και πρόσβαση στο υλικό όλων των μαθημάτων που βρίσκεται στο διαδίκτυο. Αυτή η προσπάθεια είναι η αρχή μιας σειράς από εφαρμογές που υλοποιούνται από το eBusiness Lab με στόχο την αναβάθμιση των υπηρεσιών που παρέχονται από απόσταση στο σύνολο των σπουδαστών του ΤΕΙ Μεσολογγίου.



Σχήμα 2-1: *Διαδραστικός Σταθμός Πληροφόρησης στο ΤΕΙ Μεσολογγίου*

Σχήμα 2-2: *Τεχνικά χαρακτηριστικά διαδραστικού σταθμού πληροφόρησης του ΤΕΙ Μεσολογγίου*



- **ΔΙΑΣΤΑΣΕΙΣ:** 230,5x66x13 (HxWxD in cm).
- **ΒΑΡΟΣ:** Impress 40'': 100 Kg.
- **ΟΘΟΝΗ:** 40'' TFT-LCD 1366x768 portrait.
- **Η/Υ:** Fujitsou Siemens Pentium 4 – 3,2 GHz, 80 GB HDD, 1 GByte RAM.
- **ΘΥΡΕΣ:** Δύο (2) σειριακές, μία (1) παράλληλη, έξι (6) USB.
- **ΣΥΝΔΕΣΗ:** ADSL modem router.
- **HI-FI SYSTEM:** Ηχητικό σύστημα με δύο ενσωματωμένα Hi – Fi ηχεία.
- **CD DRIVER:** CD / RW combo drive 24/24/8.
- **ΣΝΔΕΣΗ ΣΤΟ ΔΙΚΤΥΟ:** Ethernet 10/100, 1 Gbyte RAM.
- **ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ**: Windows XP Professional English.
- **ΛΟΓΙΣΜΙΚΟ**: Fw Secure Browser αντιβανδαλιστική προστασία λογισμικού, Fw Composer κατάτμηση οθόνης & διαχείριση multimedia.

ΚΕΦΑΛΑΙΟ 3

3. Εφαρμογή για απομακρυσμένη πρόσβαση

Για την υλοποίηση απομακρυσμένης πρόσβασης του διαδραστικού σταθμού πληροφόρησης από τον υπολογιστή του γραφείου διασύνδεσης, χρησιμοποιήθηκε το λογισμικό TeamViewer στην έκδοση 4.1.

Το TeamViewer είναι μια απλή, γρήγορη ασφαλής και φιλική στη σχεδίασή της εφαρμογή για τον απομακρυσμένο έλεγχο ενός υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο. Η απλότητα της έγκειται κυρίως σε δυο λόγους:

1. Εύκολο στην εγκατάσταση και την παραμετροποίηση του.
2. Μπορεί να επικοινωνεί με κάθε προορισμό περνώντας μέσα από τυχόν firewalls και proxies χωρίς να απαιτείται καμία διαμόρφωση από τον χρήστη.

Οι προσφερόμενες λειτουργίες του είναι αρκετές:

- Υπηρεσία άμεσων μηνυμάτων.
- Web Connector μέσω του οποίου γίνεται δυνατόν ο απομακρυσμένος έλεγχος υπολογιστών μέσω ενός φυλλομετρητή. (mozilla, internet explorer)
- Παρακολούθηση παρουσιάσεων μέσω ενός φυλλομετρητή.
- Κατηγοριοποίηση χρηστών σε δυο λίστες: Μαύρη λίστα και Άσπρη λίστα. Η μαύρη λίστα αναφέρεται σε χρήστες στους οποίους απαγορεύετε η πρόσβαση σε κάποιον υπολογιστή, ενώ η άσπρη λίστα, σε χρήστες στους οποίους επιτρέπεται να έχουν πρόσβαση.
- Το TeamViewer μπορεί να διαμορφωθεί αποκλειστικά για τοπικά δίκτυα. Η διαφορά είναι ότι δεν χρησιμοποιείται υποδομή δημόσιου κλειδιού (ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές αυθεντικοποίησης) αλλά συμμετρική κρυπτογράφηση. Το όφελος είναι ότι καταναλώνονται λιγότεροι υπολογιστικοί πόροι και έχουμε πιο γρήγορη αρχικοποίηση της σύνδεσης.
- Καταγραφή μιας συνεδρίας.
- Απομακρυσμένη επανεκκίνηση.
- Εγκαθίδρυση μιας VPN σύνδεσης.

3.1 Τρόπος λειτουργίας TeamViewer

Εάν συγκρίνουμε μια τηλεφωνική κλήση με μια σύνδεση TeamViewer, ο τηλεφωνικός αριθμός είναι ισοδύναμος με το στατικό ID που αποδίδει το TeamViewer και πάντα μένει το ίδιο.

Οι υπολογιστές μπορούν να αναγνωριστούν παγκοσμίως από ένα μοναδικό ID. Αυτό το ID παράγεται αυτόματα βασισμένο στην IP διεύθυνση κατά την πρώτη εκκίνηση

του TeamViewer και δεν αλλάζει. Όλες οι συνδέσεις είναι κρυπτογραφημένες και προστατευμένες από εξωτερικούς κινδύνους. Τεχνικές λεπτομέρειες σχετικά με την κρυπτογράφηση και την προστασία δεδομένων αναλύονται στο επόμενο κεφάλαιο.

Ο χρήστης εκτελεί την εφαρμογή, αυτόματα το TeamViewer παράγει το ID και το Password στον υπολογιστή του. Έπειτα δίνει τα στοιχεία πρόσβασης στον κάθε ενδιαφερόμενο που επιθυμεί να έχει απομακρυσμένη πρόσβαση στον υπολογιστή του. Ο τρόπος που θα επιλέξει ο χρήστης να επικοινωνήσει τα στοιχεία αυτά εξαρτάται αποκλειστικά από τον ίδιο, μπορεί να γίνει μέσω τηλεφώνου, μέσω φυσικής παρουσίας των συμβαλλόμενων μερών στον ίδιο χώρο κ.α. Έπειτα, κάθε άτομο που έχει επιλέξει ο χρήστης να έχει πρόσβαση στον υπολογιστή του, πληκτρολογεί τα στοιχεία αυτά και η σύνδεση εγκαθίσταται άμεσα.

3.2 Μέθοδος αυθεντικοποιήσης και κρυπτογράφησης

Όταν δημιουργείται μια συνεδρία το TeamViewer καθορίζει τον ιδανικό τύπο σύνδεσης. Καθώς ολοκληρώνεται το handshake μέσω των servers της εταιρείας δημιουργείται μια απευθείας σύνδεση μέσω των πρωτοκόλλων UDP ή TCP (ακόμα και εάν παρεμβάλλονται NATs και firewalls). Δεν χρειάζεται να ανοιχτούν πόρτες.

Το TeamViewer παρέχει κρυπτογράφηση με την χρησιμοποίηση του κρυπταλγόριθμου RSA και χρησιμοποιούνται δυο κλειδιά, ένα δημόσιο κατά την διάρκεια της κρυπτογράφησης και ένα κρυφό για την αποκρυπτογράφηση. Αυτή η τεχνολογία είναι παρεμφερείς με την λειτουργία του SSL και θεωρείται ασφαλής σύμφωνα με τα σημερινά standards. Το ιδιωτικό κλειδί δεν μεταφέρεται ποτέ στο δίκτυο, και έτσι διασφαλίζεται ότι δεν μπορούν να αποκρυπτογραφούν τα δεδομένα από πιθανούς κινδύνους.

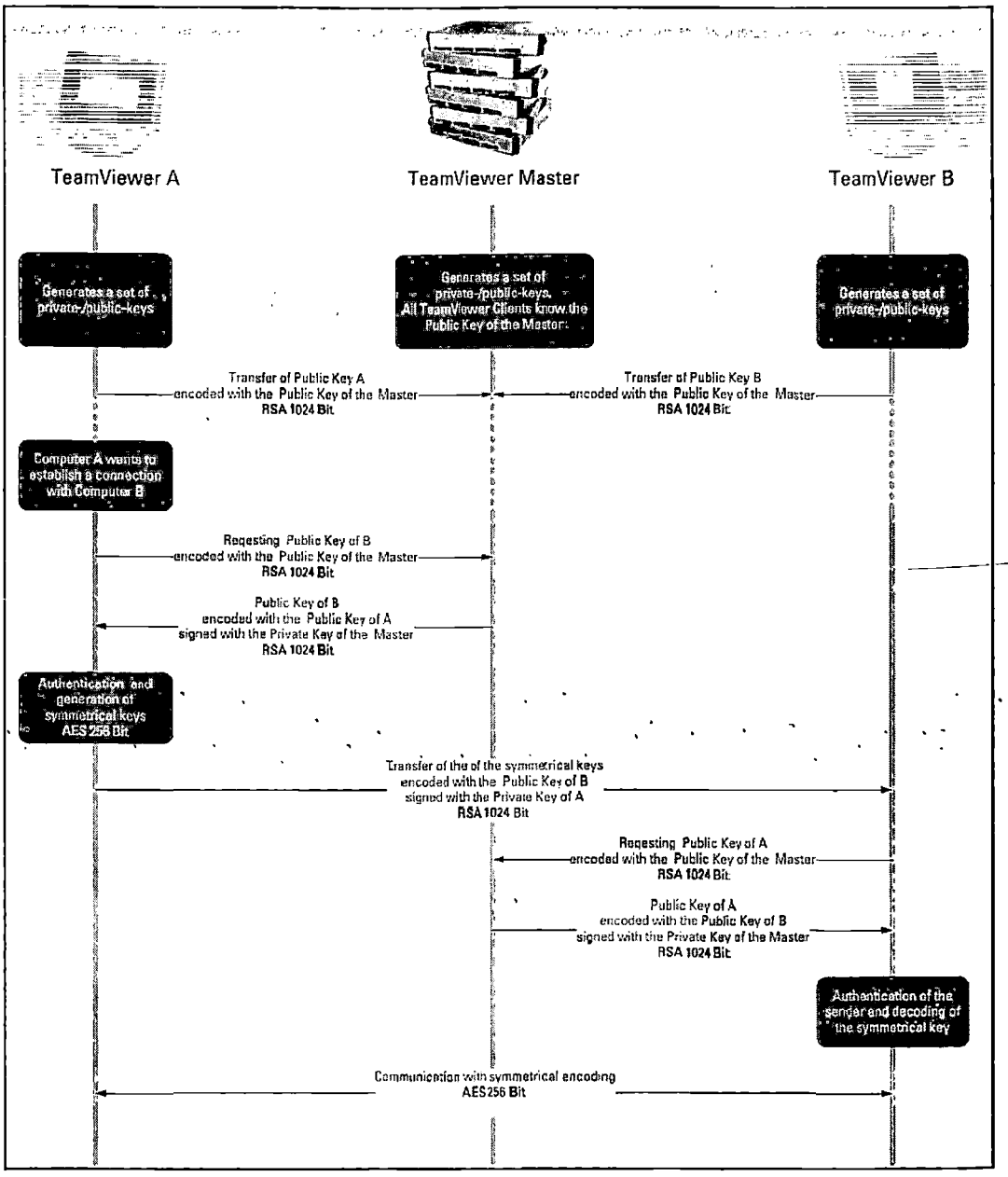
Κάθε πελάτης του TeamViewer έχει ήδη το δημόσιο κλειδί με το όποιο μπορεί να κρυπτογραφήσει τα μηνύματα προς τον master server και να τον αυθεντικοποίηση. Η υποδομή δημόσιου κλειδιού (PKI)[4] προσφέρει ένα πολύ υψηλό επίπεδο ασφάλειας και προστατεύει αποτελεσματικά από διαφόρων ειδών επιθέσεις (π.χ man in the middle attacks). Παρόλο που έχει κρυπτογραφηθεί το password δεν στέλνεται απευθείας παρά μόνο μέσω μιας challenge-response διαδικασίας και αποθηκεύεται τοπικά σε κάθε υπολογιστή.

Η διαδικασία κρυπτογράφησης και αυθεντικοποιήσης αναλυτικά:

1. Ο υπολογιστής Α παράγει ένα σύνολο με δημόσια και ιδιωτικά κλειδιά.

[4] Public Key Infrastructure (PKI)-Υποδομή Δημόσιου Κλειδιού είναι ένας συνδυασμός από λογισμικό, τεχνολογίες κρυπτογράφησης, διεργασίες και υπηρεσίες που καταστούν δυνατή την σύνθεση μιας υποδομής για ασφαλείς διαδικτυακές επικοινωνίες. Για περισσότερες πληροφορίες βλέπε, http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf

2. Στέλνει το δημόσιο κλειδί του, αφού πρώτα το έχει κρυπτογραφήσει με το δημόσιο κλειδί του TeamViewer master που είναι εξ' αρχής γνωστό σε κάθε TeamViewer client. Το μήκος του κλειδιού είναι 1024 bits και έχει κρυπτογραφηθεί με τον αλγόριθμο RSA.
3. TeamViewer master παράγει ένα σύνολο με δημόσια και ιδιωτικά κλειδιά.
4. Ο υπολογιστής Β παράγει ένα σύνολο με δημόσια και ιδιωτικά κλειδιά.
5. Στέλνει το δημόσιο κλειδί του όπως ακριβώς και ο υπολογιστής Α. (RSA 1024 bits)
6. Στην συνεχεία ο υπολογιστής Α αιτείται την εγκαθίδρυση μιας σύνδεσης με τον υπολογιστή Β
7. Στέλνει ένα αίτημα στο TeamViewer master ζητώντας το δημόσιο κλειδί του υπολογιστή Β. Το μήνυμα είναι κρυπτογραφημένο με το δημόσιο κλειδί του master. (RSA 1024 bits)
8. TeamViewer master απαντά με ένα μήνυμα με το δημόσιο κλειδί του υπολογιστή Β κρυπτογραφημένο με το δημόσιο κλειδί του υπολογιστή Α υπογεγραμμένο με το ιδιωτικό κλειδί του TeamViewer master (RSA 1024 bits)
9. Ο υπολογιστής Α αυθεντικοποιεί τον υπολογιστή Β και παράγει ένα συμμετρικό κλειδί. (AES 256)
10. Ο υπολογιστής Α στέλνει το συμμετρικό κλειδί κρυπτογραφημένο με το δημόσιο κλειδί του υπολογιστή Β υπογεγραμμένο με το ιδιωτικό κλειδί του υπολογιστή Α. (RSA 1024 bits)
11. Ο υπολογιστής Β στέλνει ένα μήνυμα στο TeamViewer master ζητώντας το δημόσιο κλειδί του υπολογιστή Α, κρυπτογραφώντας το μήνυμα με το δημόσιο κλειδί του master. (RSA 1024 bits)
12. TeamViewer master απαντά με ένα μήνυμα με το δημόσιο κλειδί του υπολογιστή Α κρυπτογραφημένο με το δημόσιο κλειδί του υπολογιστή Β υπογεγραμμένο με το ιδιωτικό κλειδί του TeamViewer master (RSA 1024 bits).
13. Ολοκλήρωση της αυθεντικοποίησης του αποστολέα και αποκρυπτογραφείται το συμμετρικό κλειδί.
14. Πραγματοποιείται η επικοινωνία των δυο συμβαλλόμενων μερών με συμμετρική κρυπτογράφηση. (AES 256)



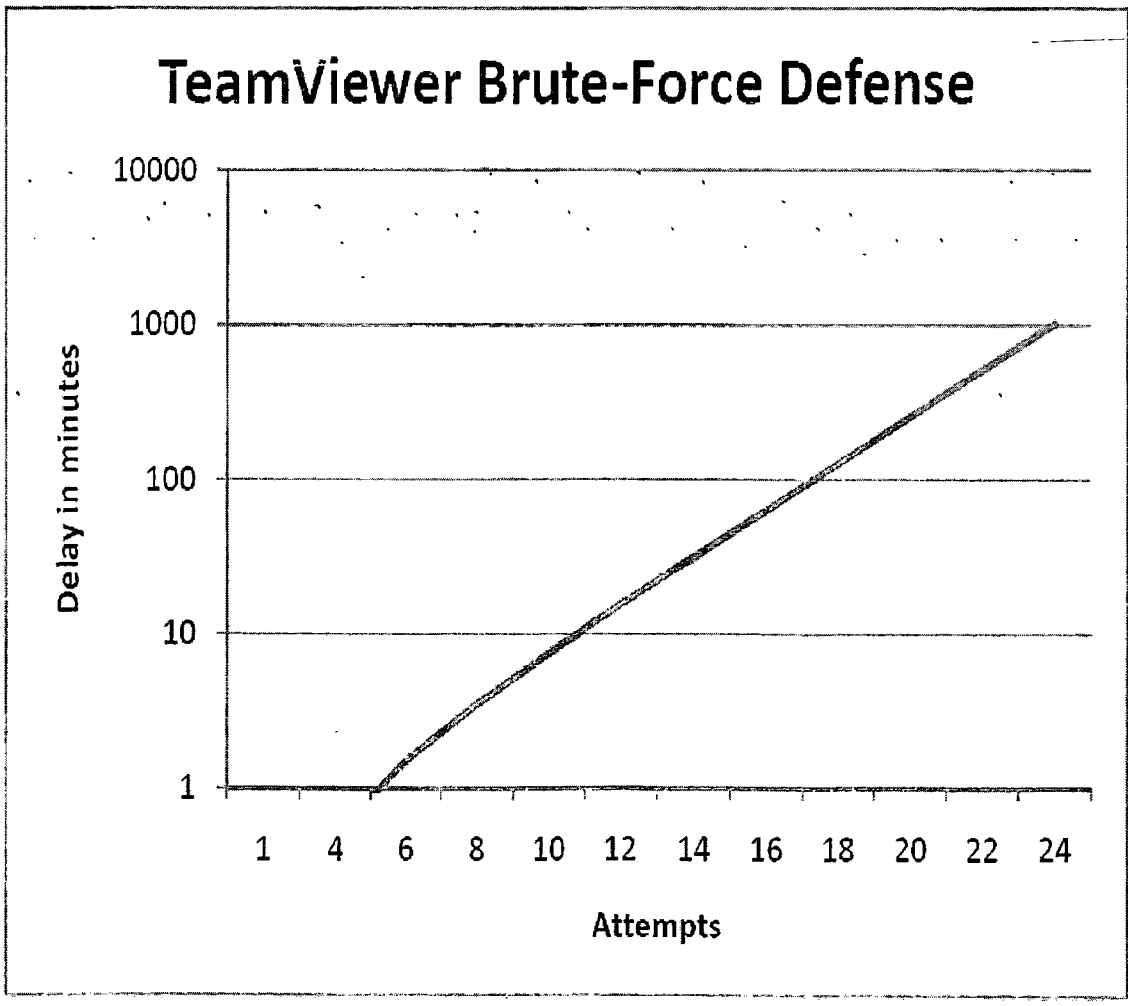
Σχήμα 3-1: *Διαδικασία κρυπτογράφησης και αυθεντικοποιήσης στο TeamViewer*

3.3 Επικύρωση των IDs που παράγονται από το TeamViewer

Τα IDs του TeamViewer παράγονται αυτόματα από το λογισμικό και βασίζονται στην IP διεύθυνση. Οι servers της εταιρίας που υλοποίησε την εφαρμογή ελέγχουν την εγκυρότητα του ID πριν από κάθε σύνδεση και έτσι αποφεύγετε η παραγωγή και η χρησιμοποίηση ενός ψεύτικου ID.

3.4 Προστασία από Brute Force επιθέσεις

Brute Force επίθεση ονομάζεται η προσπάθεια για εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Με την συνεχώς αυξανόμενη ισχύ των υπολογιστών ο χρονος που απαιτειται για να αποκαλυφθεί το αρχικό μήνυμα εχει μειωθεί αισθητά. Ο αμυντικός μηχανισμός που έχει αναπτυχτεί ενάντια σε brute force επιθέσεις, είναι ότι το λογισμικό αυξάνει εκθετικά το latency ανάμεσα στις προσπάθειες για την δημιουργία μιας νέας σύνδεσης. Για παράδειγμα, ο χρόνος που απαιτείται για 24 προσπάθειες είναι 17 ώρες. Ο μηχανισμός μέτρησης χρόνου του latency μηδενίζει μόνο μετά από μια επιτυχημένη σύνδεση. Το παρακάτω σχήμα απεικονίζει τις προσπάθειες που έγιναν σε μια επίθεση brute force και την εκθετική αύξηση στον χρόνο έπειτα από κάθε προσπάθεια.



Σχήμα 3-2: *Αμυντικός μηχανισμός του TeamViewer ενάντια σε επιθέσεις brute force*

Κεφάλαιο 4

4. Συμπέρασμα

Το ζήτημα που εξετάστηκε στο Β΄ μέρος της πτυχιακής είναι η απομακρυσμένη διαχείριση του διαδραστικού σταθμού πληροφόρησης του ΤΕΙ Μεσολογγίου με το λογισμικό TeamViewer. Τα κριτήρια για την επιλογή του συγκεκριμένου λογισμικού ήταν κυρίως η εύκολη εγκατάσταση, παραμετροποίηση και διαχείριση του. Δεν υπήρχε η ανάγκη για εξεζητημένη λύση που θα πρόσφερε ένα υψηλότερο επίπεδο ασφάλειας. Το TeamViewer όπως αναφέρθηκε και στο κεφάλαιο 3 είναι μια πολύ απλή εφαρμογή κατάλληλη για να καλύψει τις ανάγκες για τις οποίες εγκαταστάθηκε. Επίσης, η απομακρυσμένη διαχείριση του σταθμού γίνεται μέσα στο τοπικό δίκτυο του ΤΕΙ Μεσολογγίου και έτσι δεν μεταφέρονται δεδομένα μέσα από το διαδίκτυο. Τέλος, δεν συστήνεται η χρησιμοποίηση του TeamViewer σε περιπτώσεις οπου μεταφέρονται ευαίσθητα δεδομένα δια μέσου του διαδικτύου. Όταν προκύπτουν αντίστοιχες ανάγκες τότε συνδέσεις τύπου VPN, που εξετάστηκαν στο Α Μέρος της πτυχιακής, είναι μονόδρομος.

Παράρτημα Α– Προδιαγραφές συστήματος

	Client Alice	***Client Bob***	***Gateway MIDI***	***Gateway KOYTO***
Επεξεργαστής	Intel Celeron M 1.30GHz	Intel Duo Core Celeron E3200 2.4GHZ	Intel Core Duo T7100 Συχνότητα 1.83GHz	Intel Pentium 4 Συχνότητα 3.00GHz
Μνήμη RAM	1024 Mega Bytes		2048 Mega Bytes	
Σκληρός δίσκος *χωρητικότητας*	150 Giga Bytes		250 Giga Bytes	
Λειτουργικό Σύστημα	Windows XP Service Pack 3	Windows XP Service Pack 3	Ubuntu Server Edition 8.04 LTS	Ubuntu Server Edition 8.04 LTS
Τοπική Σύνδεση#1	*Με Gateway MIDI*	*Με Gateway KOYTO*	*Με Client Alice*	*Με Client Bob*
Τοπική Σύνδεση#2	-	-	Με το Διαδίκτυο	Με το Διαδίκτυο

Gateway Midi

Δημιουργία Αρχής Πιστοποίησης (CA)

1. ~$ cd && mkdir -p myCA/signedcerts && mkdir myCA/private && cd myCA
Η παραπάνω εντολή δημιουργεί ένα νέο υποκατάλογο στο home κατάλογο με την ονομασία **myCA.**

Μέσα στο νέο υποκατάλογο **myCA** δημιουργήθηκαν άλλοι δυο υποκατάλογοι, (**private, signedcerts**).
Ο ρόλος των παραπάνω νέων υποκαταλόγων είναι:

- ~/myCA :Περιέχει το πιστοποιητικό του Certificate Authority, μια βάση δεδομένων με τα πιστοποιητικά, τα παραγόμενα πιστοποιητικά, κλειδιά και αιτήσεις
- ~/myCA/signedcerts :Περιέχει αντίγραφα του κάθε υπογεγραμμένου πιστοποιητικού
- ~/myCA/private :Περιέχει το ιδιωτικό κλειδί

2. echo '01' > serial && touch index.txt
Με αυτή την εντολή δημιουργείται μια αρχική βάση δεδομένων πιστοποιητικών μέσα στο υποκατάλογο ~/myCA.

3. nano ~/myCA/ caconfig.cnf
Η εντολή αυτή δημιουργεί ένα νέο αρχείο με την ονομασία **caconfig.cnf**. Σε αυτό το αρχείο εισάγουμε το παρακάτω κείμενο:

```
# My sample caconfig.cnf file.
#
# Default configuration to use when one is not provided on the command line.
#
[ ca ]
default_ca      = local_ca
#
#
# Default location of directories and files needed to generate certificates.
#
[ local_ca ]
 dir            = /home/dimitris/myCA
 certificate    = $dir/cacert.pem
 database       = $dir/index.txt
 new_certs_dir  = $dir/signedcerts
```

```
 private_key      = $dir/private/cakey.pem
 serial           = $dir/serial
#
#
# Default expiration and encryption policies for certificates.
#
 default_crl_days    = 3650
 default_days        = 1825
 default_md          = md5
#
policy               = local_ca_policy
x509_extensions      = local_ca_extensions
#
#
# Default policy to use when generating server certificates.  The following
# fields must be defined in the server certificate.
[ local_ca_policy ]
 commonName              = supplied
 stateOrProvinceName     = supplied
 countryName             = supplied
 emailAddress            = supplied
 organizationName        = supplied
 organizationalUnitName  = supplied
#
#
# x509 extensions to use when generating server certificates.
#
[ local_ca_extensions ]
 subjectAltName     = IP:198.168.211.77
 basicConstraints   = CA:false
 nsCertType         = server
 #
 #
# The default root certificate generation policy.
#
[ req ]
 default_bits           = 2048
 default_keyfile        = /home/dimitris/myCA/private/cakey.pem
 dimitrisdefault_md     = md5
#
 prompt                 = no
 distinguished_name     = root_ca_distinguished_name
 x509_extensions        = root_ca_extensions
#
#
#
[ root_ca_distinguished_name ]
```

```
commonName              = midi
stateOrProvinceName     = Attica
countryName             = GR
emailAddress            = midi@teimes.com
organizationName        = Tei Mesologgiou
organizationalUnitName  = IT Department
#
[ root_ca_extensions ]
basicConstraints        = CA:true
```

4. export OPENSSL_CONF=~/myCA/caconfig.cnf

Η παραπάνω εντολή εξαναγκάζει το openssl tool να ψάξει για ένα configuration file σε μια εναλλακτική τοποθεσία (σε αυτή την περίπτωση, ~/myCA/caconfig.cnf).

5. openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM -days 1825

Η εντολή αυτή παράγει το πιστοποιητικό της Αρχής Πιστοποίησης και το αντίστοιχο κλειδί.

Σε αυτό το σημείο ο χρήστης πρέπει να εισάγει ένα κωδικό πρόσβασης. Το μήνυμα που εμφανίστηκε στην περίπτωση μας ήταν το παρακάτω:

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'cakey.pem '
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Η παραπάνω διαδικασία δημιούργησε ένα αυθυπόγραφο (self-signed) πιστοποιητικό σε PEM format και το RSA public/private κλειδί κρυπτογράφησης. Το πιστοποιητικό εχει ισχυ για 1825 μέρες. Η τοποθεσία και ο σκοπός των υπόλοιπων αρχείων που προκύπτουν είναι:

~/myCA/cacert.pem : Το δημόσιο πιστοποιητικό της CA
~/myCA /cakey.pem : Το ιδιωτικό κλειδί της CA

Δημιουργία αυθυπόγραφων πιστοποιητικών (self-signed) για το Gateway και Client.

Σε αυτό το σημείο πρέπει να αναφερθεί οτι υπάρχει η επιλογή να κρυπτογραφηθεί το ιδρωτικό κλειδί των πιστοποιητικών με έναν κωδικό πρόσβασης. Το πλεονέκτημα είναι, ότι το πιστοποιητικό είναι προστατευμένο ακόμα και σε περίπτωση κλοπής του.

Το μειονέκτημα όμως είναι, ότι απαιτείται πάντα να πληκτρολογείτε ο κωδικός πρόσβασης σε εφαρμογές που έχουν ενεργοποιημένο το SSL. Με αυτή την συνθήκη, ενώ το επίπεδο της ασφάλειας αυξάνει, παράλληλα υπάρχει η πιθανότητα να δημιουργηθούν προβλήματα. Για παράδειγμα, σε περίπτωση επανεκκίνησης ενός

server θα πρέπει να υπάρχει πάντα κάποιος άνθρωπος ώστε να πληκτρολογήσει τον κωδικό, ειδάλλως ο server δεν θα εκκινήσει ποτέ. Στην πτυχιακή εργασία επιλέχτηκε να μην κρυπτογραφηθεί το ιδιωτικό κλειδί χάριν ευκολίας.

Έκδοση πιστοποιητικού για το gateway Midi

6. nano ~/myCA/gatewaymidi.cnf
Η εντολή αυτή δημιουργεί ένα νέο αρχείο με την ονομασία **gatewaymidi.cnf**. Σε αυτό το αρχείο εισάγουμε το παρακάτω κείμενο:

```
#
# gatewaymidi
#
[ req ]
prompt                  = no
distinguished_name      = server_distinguished_name
[ server_distinguished_name ]
  commonName            = midi
  stateOrProvinceName   = Attica
  countryName           = GR
  emailAddress          = midi@teimes.com
  organizationName      = Tei Mesologgiou
  organizationalUnitName = IT Department
```

7. export OPENSSL_CONF=~/myCA/ gatewaymidi.cnf
Η παραπάνω εντολή εξαναγκάζει το openssl tool να ψάξει για ένα configuration file σε μια εναλλακτική τοποθεσία (σε αυτή την περίπτωση, ~/myCA/gatewaymidi.cnf).

8. openssl req -newkey rsa:1024 -keyout tempkey.pem -keyform PEM -out tempreq.pem -outform PEM
Η εντολή αυτή παράγει το πιστοποιητικό του gateway host και το αντίστοιχο κλειδί.

Σε αυτό το σημείο ο χρήστης πρέπει να εισάγει έναν κωδικό πρόσβασης. Το μήνυμα που εμφανίστηκε στην περίπτωση μας ήταν το παρακάτω:

```
Generating a 1024 bit RSA private key
.....++++++
....++++++
writing new private key to 'tempkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

9. openssl rsa < tempkey.pem > midi_key.pem
Με αυτή την εντολή μεταφράζεται το προσωρινό ιδιωτικό κλειδί σε ένα αποκρυπτογραφημένο κλειδί.
10. export OPENSSL_CONF=~/myCA/caconfig.cnf

Η παραπάνω εντολή εξαναγκάζει το openssl tool να ψάξει για ένα configuration file σε μία εναλλακτική τοποθεσία (σε αυτή την περίπτωση, ~/myCA/caconfig.cnf για να το επαναφέρει πίσω στην CA configuration).

11. openssl ca -in tempreq.pem -out midi_crt.pem
Η εντολή αυτή υπογράφει το πιστοποιητικό.

Ο χρήστης πρέπει να εισάγει τον κωδικό πρόσβασης της Αρχής Πιστοποίησης που δημιουργήθηκε προηγουμένως και τέλος να επιβεβαιώσει την υπογραφή του πιστοποιητικού. Στην περίπτωση μας, εμφανίστηκε το παρακάτω μήνυμα:

```
Using configuration from /home/dimitris/myCA/caconfig.cnf
Enter pass phrase for /home/dimitris/myCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'GR'
stateOrProvinceName   :PRINTABLE:'Attica'
organizationName      :PRINTABLE:'Tei Mesologgiou'
organizationalUnitName:PRINTABLE:'IT Department'
commonName            :PRINTABLE:'midi'
emailAddress          :IA5STRING:'midi@teimes.com'
Certificate is to be certified until Sep 16 11:25:17 2014 GMT (1825 days)
Sign the certificate? [y/n]:
```

12. rm -f tempkey.pem && rm -f tempreq.pem
Τέλος, η παραπάνω εντολή αφαιρεί το προσωρινό πιστοποιητικό του gateway και τα αρχεία του κλειδιού.

Με την ολοκλήρωση και του τελευταίου βήματος, έχουμε εκδώσει το αυθυπόγραφο πιστοποιητικό για το gateway host μαζί με το αντίστοιχο ζεύγος κλειδιών, τα όποια βρίσκονται μέσα στα αρχεία **midi_crt.pem**, **midi_key.pem**

Το αρχείο **midi_key.pem** περιέχει το ιδιωτικό κλειδί:


```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC6E4e1NgiZ5I0oqk5nMItSz2LDmQYv+UPIqxRll1cCuPwpI/qyiKp286d0848Ck
kyzGnLKQy9Xzvcz1ctWJWDoCuLCcS2k42mR3PjB9U1ZgSHSJXNS1TgRTcOVll8hsr50f12uPqlBz
uNI0cFAJOutsaHKlS/FTW7iGfBsqITJFwIDAQABAoGAdROiuGa2BLYkBukZCZ4mm0T3PGCE3x
x0BMd3vu/5BDKGHhCQRVLuBogJ3fD9Ez4f2jUS8qZRHGuRaGDlXl+IV4OYMlKiL/RVaifvt5Npo
atGX/25Yhiy2oho2ZDLpxSZMBKG8fXY6RQ0lW58RfXTO9S9bjK06sCPE6KvsRBll9ECQQDyHU
oaXRJRhyIzCalZW1uuG/a3dOE5z9ZWMOPHc4ya6v6fP4hL6yFNY8kWBMnLIiXOmtO6JWC6QrA
xwizYSMfAkEAxL2G6Zb1Zw3ec7tet9gldLuGSVvN9c+nlmosxTwiUtiEyb8Xeo0EAZiOpBG0OF1J
DKnFQGK66qO25IYjWNjTCQJAQWRW5Qc2JOQOqNOaTGlMWO7vJslqayaZcWQLzQdbvTpfOl
vwjFK2T/t+0hnx7j9RQOD025s5WFFfOrYecGOQJAMYL06eJIvfeajQuRabjmrDrpL5r/+SWaKltsCv
L4PFsrB86kbP4CDRjEhPvDnA+1647qCisOmTA8PcSYLqraaQJBAKRM5h9DJ4S7nhD31kQw0vkL
4/i1FtW3MFxmz0/hoIQ2E07ZyD/zymvZ6PnHOOhElNwBKSUQSjsqHhdQSSyQumg=
-----END RSA PRIVATE KEY-----
```


Το αρχείο **midi_crt.pem** περιέχει το πιστοποιητικό:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=Gr, ST=Attica, O=Tei Mesologgiou, OU=IT Department, CN=midi
        Validity
            Not Before: Sep 17 11:25:17 2009 GMT
            Not After : Sep 16 11:25:17 2014 GMT
        Subject: CN=midi, ST=Attica, C=GR/emailAddress=midi@teimes.com, O=T$
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ba:13:87:b5:36:08:99:e4:8d:28:aa:4e:67:30:
                    8b:52:cf:62:c3:99:06:2f:f9:43:c8:ab:14:65:97:
                    57:02:b8:fc:29:23:fa:b2:88:aa:76:f3:a7:74:f3:
                    8f:02:92:4c:b3:1a:72:ca:43:2f:57:ce:f7:33:d5:
                    cb:56:25:60:e8:0a:e2:c2:71:2d:a4:e3:69:91:dc:
                    f8:c1:f5:4d:59:81:21:d2:25:73:52:d5:38:11:4d:
                    c3:95:94:8f:21:b2:be:74:7f:5d:ae:3e:a9:41:ce:
                    e3:48:d1:c1:40:24:eb:ad:b1:a1:ca:95:2f:c5:4d:
                    6e:e2:19:f0:6c:a8:84:c9:17
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:198.168.211.77
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
    Signature Algorithm: md5WithRSAEncryption
        12:b0:92:3d:ec:42:f0:cc:92:78:fa:79:10:fd:d8:25:30:93:
        75:9c:a2:ac:7e:5a:02:04:10:f4:35:09:d2:0b:06:11:75:1b:
        f2:73:29:29:c7:93:91:d8:93:59:fa:1c:23:ce:d1:ba:b5:d8:
        10:33:96:50:e8:6b:20:c7:f4:cc:81:72:b2:1f:e3:c3:72:71:
        40:2a:91:b0:10:28:28:68:b9:d7:e1:e6:d4:56:fb:0e:5c:4c:
        b5:28:b0:2b:67:47:5a:9b:29:87:04:c5:fc:15:24:fc:31:8e:
        c2:17:5f:68:1b:ca:4d:d0:00:68:e6:50:db:65:1f:12:95:7d:
        39:e5:b2:2e:f4:eb:02:8d:ad:19:2b:c8:27:63:ea:6c:c4:6b:
        c6:4a:57:7e:e6:7e:5d:65:dc:63:cd:34:c9:71:2f:15:4a:96:
        74:0a:28:9f:c2:9f:89:e3:b8:d9:d7:d6:e1:42:05:84:cb:65:
        e0:7e:d6:c8:62:0a:76:bb:cc:5b:5f:8c:1d:d4:ab:aa:04:1b:
        04:7a:6e:5f:a5:d2:83:4e:45:c5:18:48:0b:5a:41:1b:bf:70:
        af:57:ba:2e:87:ac:4d:7c:96:1b:9a:de:a7:f7:25:6f:f8:3c:
        51:80:af:3c:4f:df:09:75:6c:fc:4a:2e:c7:e3:2d:b5:3d:34:
        c9:34:17:95

-----BEGIN CERTIFICATE-----
MIIDMDCCAhigAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgzELMAkGA1UEBhMCR3IxDzA
NBgNVBAgTBkF0dGljYTEYMBYGA1UEChMPVGVpIE1lc29sb2dnaW91MRYwFAYDVQQLEw
1JVCBEZXBhcnRtZW50MREwDwYDVQQDEwhkaW1pdHJpczEeMBwGCSqGSIb3DQEJARYPZ
GltaUB0ZWltZXMuY29tMB4XDTA5MDkxNzExMjUxN1oXDTE0MDkxNjExMjUxN1owgYMxET
APBgNVBAMTCGRpbWl0cmlzMQ8wDQYDVQQIEwZBdHRpY2ExCzAJBgNVBAYTAkdSMR4
wHAYJKoZIhvcNAQkBFg9kaW1pQHRlaW1lcy5jb20xGDAWBgNVBAoTD1RlaSBNZXNvbG9nZ
2lvdTEWMBQGA1UECxMNSVQgRGVwYXJ0bWVudDCBnzANBgkqhkiG9w0BAQEFAAOBjQA
wgYkCgYEAuhOHtTYImeSNKKpOZzCLUs9iw5kGL/lDyKsUZZdXArj8KSP6soiqdvOndPOPApJM
sxpyykMvV873M9XLViVg6AriwnEtpONpkdz4wfVNWYEh0iVzUtU4EU3DlZSPIbK+dH9drj6pQc7
jSNHBQCTrrbGhypUvxU1u4hnwbKiEyRcCAwEAAaMxMC8wDwYDVR0RBAgwBocExqjTTTAJ
BgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQQFAAOCAQE
```

```
AErCSPexC8MySePp5EP3YJTCTdZyirH5aAgQQ9DUJ0gsGEXUb8nMpKceTkdiTWfocI87RurXYE
DOWUOhrIMf0zIFysh/jw3JxQCqRsBAoKGi51+Hm1Fb7DlxMtSiwK2dHWpsphwTF/BUk/DGOwhd
faBvKTdAAaOZQ22UfEpV9OeWyLvTrAo2tGSvlJ2PqbMRrxkpXfuZ+XWXcY800yXEvFUqWdAo
on8KfieO42dfW4UIFhMtl4H7WyGIKdrvMW1+MHdSrqgQbBHpuX6XSg05FxRhIC1pBG79wr1e6L
oesTXyWG5rep/clb/g8UYCvPE/fCXVs/Eoux+MttT00yTQXlQ==
-----END CERTIFICATE-----
```

Έκδοση πιστοποιητικού για Client Alice

nano ~/myCA/clientalice.cnf
Η εντολή αυτή δημιουργεί ένα νέο αρχείο με την ονομασία **clientalice.cnf**. Σε αυτό το αρχείο εισάγουμε το παρακάτω κείμενο:

```
#
# clientalice
#
[ req ]
prompt                  = no
distinguished_name      = client_distinguished_name
[ client_distinguished_name ]
  commonName            = alice
  stateOrProvinceName   = Attica
  countryName           = GR
  emailAddress          = alice@teimes.com
  organizationName      = Tei Mesologgiou
  organizationalUnitName = IT Department
```

export OPENSSL_CONF=~/myCA/clientalice.cnf

openssl req -newkey rsa:1024 -keyout tempkey.pem -keyform PEM -out tempreq.pem -outform PEM

Σε αυτό το σημείο ο χρήστης πρέπει να εισάγει έναν κωδικό πρόσβασης. Το μήνυμα που εμφανίστηκε στην περίπτωση μας ήταν το παρακάτω:

```
Generating a 1024 bit RSA private key
.....++++++
....++++++
writing new private key to 'tempkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

openssl rsa < tempkey.pem > alice _key.pem
export OPENSSL_CONF=~/myCA/caconfig.cnf

openssl ca -in tempreq.pem -out alice_crt.pem

Ο χρήστης πρέπει να εισάγει τον κωδικό πρόσβασης της Αρχής Πιστοποίησης που δημιουργήθηκε προηγουμένως και τέλος να επιβεβαιώσει την υπογραφή του πιστοποιητικού. Στην περίπτωση μας, εμφανίστηκε το παρακάτω μήνυμα:

```
Using configuration from /home/dimitris/myCA/caconfig.cnf
Enter pass phrase for /home/dimitris/myCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'GR'
stateOrProvinceName   :PRINTABLE:'Attica'
organizationName      :PRINTABLE:'Tei Mesologgiou'
organizationalUnitName:PRINTABLE:'IT Department'
commonName            :PRINTABLE:'alice'
emailAddress          :IA5STRING:'alice@teimes.com'
Certificate is to be certified until Sep 16 12:48:25 2014 GMT (1825 days)
Sign the certificate? [y/n]:
```

rm -f tempkey.pem && rm -f tempreq.pem

Με την ολοκλήρωση και του τελευταίου βήματος, έχουμε εκδώσει το αυθυπόγραφο πιστοποιητικό για το client Alice μαζί με το αντίστοιχο ζεύγος κλειδιών, τα όποια βρίσκονται μέσα στα αρχεία **alice_crt.pem**, **alice_key.pem**

Το αρχείο **alice_key.pem** περιέχει το ιδιωτικό κλειδί:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDdGxkYxjcxKGpyn8zp4NWP/+z86wYpa8MrvlGVsDzH+S+Y+40NvaETc3Bkr
E6u4pTEgKz5jHAokXeI4hEDHqN4+3bbyNYKnIlLnirrwWKQnzCcCzB+5McefKQ9s/Xs28xOl0z1
Mh4+tC0HCm/7E3hDl2AlmH/CNnYFZzoRmEmG0wIDAQABAoGAVsUGoVFQYYtB0v/hU7s3NE
60O0EkZubybd0/eSXzhGrHAhtd7JGJf++ioO955WnoBgGVYE17yn/j0CUflgDVF6+FpFfwMi204UO
vECs6786gHWOQYeU4naxXwH5nU4yxuy4YFfxFZgmotfgdP3du74kN7On3EVLLocBp6zA6DukC
QQD2fi4E3q4sc7BefgijGBsI8ZrH9ppd9QUA3sw86hqvdVm0MrRih1K5P9Kyc+Ne0W9Q3YtNezI2h
RajTRyS84ZFAkEA5aJAeksXOHZd8CbXfUxUi3yl80UlUcWtp7Z26H2aQMCB1/i8+F28Ct1xA2+Co
b7bmfpBvujHXSDf1ZOtFXLWNwJBAKiP90ZrRW6umpCz3ZIyvOIr3q4aLMxN72L9+Ws6qI8OUA
7TkdnDMsXuKFbSu00vKdGB/2437kmsT6PS6tRvZoUCQFl5nyYHnESj2nZ4q/5mf4raRs9DYgc6vy
9aKXrtde1FFVLR2M/ttheFsUNlb8EWXPriSDva99ORu6W8pPR2ioECQEDigdzU55IIbTccfpkhYKfh
Xhqto8n2KuMlADBoZlWS YDpqs5C/Viv3y+ekit5WWebNNX4WVpimS6vbh8SkNts=
-----END RSA PRIVATE KEY-----
```

Το αρχείο **alice_crt.pem** περιέχει το πιστοποιητικό:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=Gr, ST=Attica, O=Tei Mesologgiou, OU=IT Department, CN=midi
    Validity
      Not Before: Sep 17 12:48:252009 GMT
      Not After : Sep 16 12:48:25 2014 GMT
    Subject: CN=alice, ST=Attica, C=GR/emailAddress=alice@teimes.com, O=T$
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    89:18:79:e9:9f:e9:81:9b:e7:b3:9f:67:80:82:be:
                    f8:e4:6b:00:db:99:06:2f:f9:43:c8:ab:14:65:97:
                    57:02:b8: fc: 29:23:fa:b2:88:aa:76:f3:a7:74:f3:
                    8f:02:92:4c:b3:1a:72:ca:43:2f:57:ce:f7:33:d5:
                    cb:56:25:60:e8:0a:e2:c2:71:2d:a4:e3:69:91:dc:
                    f8:c1:f5:4d:59:81:21:d2:25:73:52:d5:38:11:4d:
                    c3:95:94:8f:21:b2:be:74:7f:5d:ae:3e:a9:41:ce:
                    e3:48:d1:c1:40:24:eb:ad:b1:a1:ca:95:2f:c5:4d:
                    5a:5d:9e:fe:a9:a5:57:4a:99:ad:ee:5d:e3:0b:6a:
                    ea:8f:8a:03:24:a8:ca:43:2f:
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:198.168.211.77
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
    Signature Algorithm: md5WithRSAEncryption
        21:6a:ff:c4:06:4e:de:d2:82:67:41:24:d3:68:b8:97:c4:ad:
        0f:dd:7d:c4:1f:3f:dd:f3:94:41:04:7d:77:d2:30:49:e9:8f:
        3c:97:af:1e:63:71:8d:45:e7:17:56:f3:db:99:9b:92:e1:68:
        7a:ac:f8:fe:1d:04:89:57:f2:e1:9b:b0:cb:a7:38:6f:0b:3a:
        ad:21:c8:41:71:94:6b:2e:47:5e:10:4c:ad:0e:f0:16:d0:ce:
        07:34:15:db:38:61:93:42:7c:1a:35:59:52:e7:62:01:e4:c0:
        b1:f4:f7:1b:f1:90:e9:c4:8a:5f:f6:a6:1e:b4:d9:66:c0:ae:
        00:57:00:57:ad:19:2b:c8:27:63:ea:6c:c4:6b:c6:4a:57:7e:
        c6:4a:57:7e:e6:7e:5d:65:dc:63:cd:34:c9:71:2f:15:4a:96:
        74:0a:28:9f:c2:9f:89:e3:b8:d9:d7:d6:e1:42:05:84:cb:65:
        e0:7e:d6:c8:62:0a:76:bb:cc:5b:5f:8c:1d:d4:ab:aa:04:1b:
        51:80:af:3c:4f:df:09:75:6c:fc:4a:2e:c7:e3:2d:b5:3d:34:
        04:7a:6e:5f:a5:d2:83:4e:45:c5:18:48:0b:5a:41:1b:bf:70:
        af:57:ba:2e:87:ac:4d:7c:96:1b:9a:de:a7:f7:25: 56:f3:db
        99:9b:92
```

```
-----BEGIN CERTIFICATE-----
MIID0DCCAzmgAwIBAgIBBzANBgkqhkiG9w0BAQQFADBpMQswCQYDVQQGEwJDSDEVMB
MGA1UECBYMV2ludGVydGh1cggIMRMwEQYDVQQHEwpXaW50ZXJ0aHVyMQ0wCwYDVQ
QKEwRUZWNoMR8wHQYJKoZIhvcNAQkBFhBlNXVlbmFsQHpod2luLmNoMB4XDTk5MTAxM
TEzNTQwM1oXDTAwMTAMDEzNTQwM1owgYIxCzAJBgNVBAYTAkNIMRMwEQYDVQQIE
wpTb21lLVN0YXRlMQ0wCwYDVQQKEwRUZWNoMS0wKwYDVQQDFCRrc3kwMDguemh3W
4uY2ggSVBzZWMgY2VydGlmaWNhdGUgIzExIDAeBgkqhkiG9w0BCQEWEWU1Z2FlcnRuQHpo
d2luLmNoMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDdGxkYxjcxKGpyn8zp4NWP/
+z86wYpa8MrvlGVsDzH+S+Y+40NvaETc3BkrE6u4pTEgKz5jHAokXeI4hEDHqN4+3bbyNYKnIlL
nirrwWKQnzCcCzB+5McefKQ9s/Xs28xOl0z1Mh4+tC0HCm/7E3hDl2AlmH/CNnYFZzoRmEmG0w
IDAQABo4IBbDCCAWgwCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCBkAwCwYDR0P
BAQDAgXgMDQGCWCGSAGG+EIBDQQnFiVJUHNlYyBjZXJ0aWZpY2FtZSBmb3Iga3N5MDA4
Lnpod2luLmNoMB0GA1UdDgQWBBSJGHnpn+mBm+ezn2eAgr745GsA2zCBkwYDVR0jBIGLMI
GIgBRaXZ7+qaVXSpmt7l3jC2rqj4oDJKFtpGswaTELMAkGA1UEBhMCQ0gxFTATBgNVBAgWD
FdpbnRlcnRodXIICDETMBEGA1UEBxMKV2ludGVydGh1cjENMAsGA1UEChMEVGVjaDEfMB
0GCSqGSIb3DQEJARYQZTV1ZW5hbEB6aHdpbi5jaIIBADAzBgNVHREELDAqgRFlNWdhoesTX
yWG5repBBSJGHpsfT3G/GQ6cSKX/amHrTZZsCuAFc=
-----END CERTIFICATE-----
```

Gateway Koyto

Δημιουργία Αρχής Πιστοποίησης (CA)

Εκτελούμε τα ιδία ακριβώς βήματα για την δημιουργία Αρχής Πιστοποίησης και για την εκδώσει αυθυπόγραφων πιστοποιητικών όπως ακριβώς και στο gateway Midi.

1. ~$ cd && mkdir -p myCA/signedcerts && mkdir myCA/private && cd myCA

2. echo '01' > serial && touch index.txt

3. nano ~/myCA/caconfig.cnf
Η εντολή αυτή δημιουργεί ένα νέο αρχείο με την ονομασία **caconfig.cnf**. Σε αυτό το αρχείο εισάγουμε το παρακάτω κείμενο:

```
# My sample caconfig.cnf file.
#
# Default configuration to use when one is not provided on the command line.
#
[ ca ]
default_ca      = local_ca
#
#
# Default location of directories and files needed to generate certificates.
#
[ local_ca ]
 dir             = /home/mix/myCA
 certificate     = $dir/cacert.pem
 database        = $dir/index.txt
 new_certs_dir   = $dir/signedcerts
 private_key     = $dir/private/cakey.pem
 serial          = $dir/serial
#
#
# Default expiration and encryption policies for certificates.
#
 default_crl_days    = 3650
 default_days        = 1825
 default_md          = md5
#
policy              = local_ca_policy
x509_extensions     = local_ca_extensions
#
#
# Default policy to use when generating server certificates.  The following
# fields must be defined in the server certificate.
[ local_ca_policy ]
```

```
commonName              = supplied
stateOrProvinceName     = supplied
countryName             = supplied
emailAddress            = supplied
organizationName        = supplied
organizationalUnitName  = supplied
#
#
# x509 extensions to use when generating server certificates.
#
[ local_ca_extensions ]
subjectAltName     = IP:198.168.210.80
basicConstraints   = CA:false
nsCertType         = server
#
#
# The default root certificate generation policy.
#
[ req ]
default_bits        = 2048
default_keyfile     = /home/mix/myCA/private/cakey.pem
mixdefault_md       = md5
#
prompt                  = no
distinguished_name      = root_ca_distinguished_name
x509_extensions         = root_ca_extensions
#
#
#
[ root_ca_distinguished_name ]
commonName              = koyto
stateOrProvinceName     = Peiraias
countryName             = GR
emailAddress            = koyto@teimes.com
organizationName        = Tei Mesologgiou
organizationalUnitName  = IT Department
#
[ root_ca_extensions ]
basicConstraints        = CA:true
```

4. export OPENSSL_CONF=~/myCA/caconfig.cnf

5. openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM -days 1825

Δημιουργία αυθυπόγραφων πιστοποιητικών (self-signed) για το Gateway και Client

Έκδοση πιστοποιητικού για το gateway Koyto

nano ~/myCA/gatewaykoyto.cnf
Η εντολή αυτή δημιουργεί ένα νέο αρχείο με την ονομασία **gatewaykoyto.cnf**. Σε αυτό το αρχείο εισάγουμε το παρακάτω κείμενο:

```
#
# gatewaykoyto.cnf
#
[ req ]
prompt                 = no
distinguished_name     = server_distinguished_name
[ server_distinguished_name ]
  commonName           = koyto
  stateOrProvinceName  = Peiraias
  countryName          = GR
  emailAddress         = koyto@teimes.com
  organizationName     = Tei Mesologgiou
  organizationalUnitName = IT Department
```

export OPENSSL_CONF=~/myCA/gatewaykoyto.cnf

openssl req -newkey rsa:1024 -keyout tempkey.pem -keyform PEM -out tempreq.pem -outform PEM

openssl rsa < tempkey.pem > koyto_key.pem

export OPENSSL_CONF=~/myCA/caconfig.cnf

openssl ca -in tempreq.pem -out koyto_crt.pem

Ο χρήστης πρέπει να εισάγει τον κωδικό πρόσβασης της Αρχής Πιστοποίησης που δημιουργήθηκε προηγουμένως και τέλος να επιβεβαιώσει την υπογραφή του πιστοποιητικού. Στην περίπτωση μας, εμφανίστηκε το παρακάτω μήνυμα:

```
Using configuration from /home/mix/myCA/caconfig.cnf
Enter pass phrase for /home/mix/myCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'GR'
stateOrProvinceName       :PRINTABLE:' Peiraias'
organizationName          :PRINTABLE:'Tei Mesologgiou'
organizationalUnitName    :PRINTABLE:'IT Department'
commonName                :PRINTABLE:'koyto'
emailAddress              :IA5STRING:'koyto@teimes.com'
Certificate is to be certified until Sep 16 20:18:07 2014 GMT (1825 days)
```

Sign the certificate? [y/n]:

12. rm -f tempkey.pem && rm -f tempreq.pem

Με την ολοκλήρωση και του τελευταίου βήματος, έχουμε εκδώσει το αυθυπόγραφο πιστοποιητικό για εφαρμογές του server μαζί με το αντίστοιχο ζεύγος κλειδιών, τα οποία βρίσκονται μέσα στα αρχεία **koyto_crt.pem**, **koyto_key.pem**

Το αρχείο **koyto_key.pem** περιέχει το ιδιωτικό κλειδί:

-----BEGIN RSA PRIVATE KEY-----
0sAQN6TloFPIiDVo61Ji6ENKJbk5mScdlHctBzVNElfU7srrxkKB8VmUrsMlaYrLVJ3E2+VCQ6Qdx
Kr/P4S8BY1l/+qlh3UDRk0aR5zHpRzlStRxUvzhHVZ9aIwDtVjzhZPOC4jW85CeMZGv1LwgVylDP
I8y6a5jiszJLjp4BPJ++7kS4xMhGCUF8D+mzLKCE9HDC9DG2PHXPdUChtAT0CNpVTHFFYTM0
dIvxEEeAXCHCT1vExfizf1xCk2zt+YdmwH1y6xsr/3FGqWLkqSdDl7H/uPIT937/lz5pFjLYBrYDjM
SywXWo2Exb17dPHc5Jh4ZJGfJiLVw4UR77jlE9lD6KvF6Ukf78Dgk5j9tkPAVoKvtjnxwizYSMfAk
EAxL2G6Zb1Zw3ec7tet9gldLuGSVvN9c+nlmosxTwiUtiEyb8Xeo0EAZiOpBG0OF1JDKnFQGK66q
O25IYjWNjTCQJAQWRW5Qc2JOQOqNOaTGlMWO7vJslqayaZcWQLzQdbvTpfRFOlvwjFK2T/t+
0hnx7j9RQOD025s5WFFfOrYecGOQJAMYL06eJlvfeajQuRabjmrDrpL5r/+SWaKltsCvL4PFsrB86k
bP4CDRjEhPvDnA+1647qCisOmTA8PcSYLqraaQJBAKRM5h9DJ4S7nhD31kQw0vkL4/i1FtW3MF
xmz0/hoIQ2E07ZyD/zymvZ6PnHOOhEINwBKSUQSjsqHhdQSSyQumg=lmosxTwiUtiEyb8Xeo0EA
ZiOpB7tet9gldLuFfOrYecGSVYL06eJIvfeajQuRa9aIwDtVjzhZPOC4bjmEAxL2G6Zb1Zw
-----END RSA PRIVATE KEY-----

Το αρχείο **koyto_crt.pem** περιέχει το πιστοποιητικό:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=Gr, ST=Peiraias, O=Tei Mesologgiou, OU=IT Department, CN=koyto
    Validity
      Not Before: Sep 17 20:18:07 2009 GMT
      Not After : Sep 16 20:18:07 2014 GMT
    Subject: CN=koyto, ST=Peiraias, C=GR/emailAddress=koyto@teimes.com, O=T$
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:ba:13:87:b5:36:08:99:e4:8d:28:aa:4e:67:30:
          8b:52:cf:62:c3:99:06:2f:f9:43:c8:ab:14:65:97:
          57:02:b8:fc:29:23:fa:b2:88:aa:76:f3:a7:74:f3:
          8f:02:92:4c:b3:1a:72:ca:43:2f:57:ce:f7:33:d5:
          cb:56:25:60:e8:0a:e2:c2:71:2d:a4:e3:69:91:dc:
          f8:c1:f5:4d:59:81:21:d2:25:73:52:d5:38:11:4d:
          c3:95:94:8f:21:b2:be:74:7f:5d:ae:3e:a9:41:ce:
          e3:48:d1:c1:40:24:eb:ad:b1:a1:ca:95:2f:c5:4d:
          6e:e2:19:f0:6c:a8:84:c9:17
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        IP Address: 198.168.210.80
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Cert Type:
        SSL Server
```

```
Signature Algorithm: md5WithRSAEncryption
    12:b0:92:3d:ec:42:f0:cc:92:78:fa:79:10:fd:d8:25:30:93:
    75:9c:a2:ac:7e:5a:02:04:10:f4:35:09:d2:0b:06:11:75:1b:
    f2:73:29:29:c7:93:91:d8:93:59:fa:1c:23:ce:d1:ba:b5:d8:
    10:33:96:50:e8:6b:20:c7:f4:cc:81:72:b2:1f:e3:c3:72:71:
    40:2a:91:b0:10:28:28:68:b9:d7:e1:e6:d4:56:fb:0e:5c:4c:
    b5:28:b0:2b:67:47:5a:9b:29:87:04:c5:fc:15:24:fc:31:8e:
    c2:17:5f:68:1b:ca:4d:d0:00:68:e6:50:db:65:1f:12:95:7d:
    39:e5:b2:2e:f4:eb:02:8d:ad:19:2b:c8:27:63:ea:6c:c4:6b:
    c6:4a:57:7e:e6:7e:5d:65:dc:63:cd:34:c9:71:2f:15:4a:96:
    74:0a:28:9f:c2:9f:89:e3:b8:d9:d7:d6:e1:42:05:84:cb:65:
    e0:7e:d6:c8:62:0a:76:bb:cc:5b:5f:8c:1d:d4:ab:aa:04:1b:
    04:7a:6e:5f:a5:d2:83:4e:45:c5:18:48:0b:5a:41:1b:bf:70:
    af:57:ba:2e:87:ac:4d:7c:96:1b:9a:de:a7:f7:25:6f:f8:3c:
    51:80:af:3c:4f:df:09:75:6c:fc:4a:2e:c7:e3:2d:b5:3d:34:
    c9:34:17:95

-----BEGIN CERTIFICATE-----
MIIDMDCCAhigAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgzELMAkGA1UEBhMCR3IxDzA
NBgNVBAgTBkF0dGljYTEYMBYGA1UEChMPVGVpIE1lc29sb2dnaW91MRYwFAYDVQQLEw
1JVCBEZXBhcnRtZW50MREwDwYDVQQDEwhkaW1pdHJpczEeMBwGCSqGSIb3DQEJARYPGl
taUB0ZWltZXMuY29tMB4XDTA5MDkxNzExMjUxN1oXDTE0MDkxNjExMjUxN1owgYMxETA
PBgNVBAMTCGRpbWl0cmlzMQ8wDQYDVQQIEwZBdHRpY2ExCzAJBgNVBAYTAkdSMR4w
HAYJKoZIhvcNAQkBFg9kaW1pQHRlaW1lcy5jb20xGDAWBgNVBAoTD1RlaSBNZXNvbG9nZ2l
vdTEWMBQGA1UECxMNSVQgRGVwYXJ0bWVudDCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAuhOHtTYImeSNKKpOZzCLUs9iw5kGL/lDyKsUZZdXArj8KSP6soiqdvOndPOPApJMs
xpyykMvV873M9XLViVg6AriwnEtpONpkdz4wfVNWYEh0iVzUtU4EU3DlZSPIbK+dH9drj6pQc7j
SNHBQCTrrbGhypUvxU1u4hnwbKiEyRcCAwEAAaMxMC8wDwYDVR0RBAgwBocExqjTTTAJB
gNVHRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQQFAAOCAQEA
ErCSPexC8MySePp5EP3YJTCTdZyirH5aAgQQ9DUJ0gsGEXUb8nMpKceTkdiTWfocI87RurXYED
OWUOhrIMf0zIFysh/jw3JxQCqRsBAoKGi51+Hm1Fb7DlxMtSiwK2dHWpsphwTF/BUk/DGOwhdf
aBvKTdAAaOZQ22UfEpV9OeWyLvTrAo2tGSvlJ2PqbMRrxkpXfuZ+XWXcY800yXEvFUqWdAoo
n8KfieO42dfW4UIFhMtl4H7WyGIKdrvMW1+MHdSrqgQbBHpuX6XSg05FxRhIC1pBG79wr1e6Lo
esTXyWG5rep/clb/g8UYCvPE/fCXVs/Eoux+MttT00
yTQXlQ==
-----END CERTIFICATE-----
```

Έκδοση πιστοποιητικού για το Client Bob

nano ~/myCA/clientbob.cnf

Η εντολή αυτή δημιουργεί ένα νέο αρχείο με την ονομασία **clientbob.cnf**. Σε αυτό το αρχείο εισάγουμε το παρακάτω κείμενο:

```
#
# clientbob
#
[ req ]
prompt                  = no
distinguished_name      = client_distinguished_name
[ client_distinguished_name ]
 commonName             = bob
 stateOrProvinceName    = Peiraias
 countryName            = GR
 emailAddress           = bob@teimes.com
```

```
organizationName          = Tei Mesologgiou
organizationalUnitName    = IT Department
```

export OPENSSL_CONF=~/myCA/clientbob.cnf

openssl req -newkey rsa:1024 -keyout tempkey.pem -keyform PEM -out tempreq.pem -outform PEM

Σε αυτό το σημείο ο χρήστης πρέπει να εισάγει έναν κωδικό πρόσβασης. Το μήνυμα που εμφανίστηκε στην περίπτωση μας ήταν το παρακάτω:

```
Generating a 1024 bit RSA private key
.....++++++
....++++++
writing new private key to 'tempkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

openssl rsa < tempkey.pem > bob_key.pem

export OPENSSL_CONF=~/myCA/caconfig.cnf

openssl ca -in tempreq.pem -out bob_crt.pem

Ο χρήστης πρέπει να εισάγει τον κωδικό πρόσβασης της Αρχής Πιστοποίησης που δημιουργήθηκε προηγουμένως και τέλος να επιβεβαιώσει την υπογραφή του πιστοποιητικού. Στην περίπτωση μας, εμφανίστηκε το παρακάτω μήνυμα:

```
Using configuration from /home/mix/myCA/caconfig.cnf
Enter pass phrase for /home/mix/myCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'GR'
stateOrProvinceName   :PRINTABLE:'Peiraias'
organizationName      :PRINTABLE:'Tei Mesologgiou'
organizationalUnitName:PRINTABLE:'IT Department'
commonName            :PRINTABLE:'bob'
emailAddress          :IA5STRING:'bob@teimes.com'
Certificate is to be certified until Sep 16 21:57:38 2014 GMT (1825 days)
Sign the certificate? [y/n]:
```

rm -f tempkey.pem && rm -f tempreq.pem

Με την ολοκλήρωση και του τελευταίου βήματος, έχουμε εκδώσει το αυθυπόγραφο πιστοποιητικό για το client Bob μαζί με το αντίστοιχο ζεύγος κλειδιών, τα όποια βρίσκονται μέσα στα αρχεία **bob_crt.pem**, **bob_key.pem**

Το αρχείο **bob_key.pem** περιέχει το ιδιωτικό κλειδί:

-----BEGIN RSA PRIVATE KEY-----
a67NAsSU9UYfqQw39tKk52rSKoRw2hFprCywIFCGx5dKFkSxtww3/wxaxE4dUm69DB0LQlnHa2
hreB8LFSOjuydOdrX68O8G0TF0PW+gx2BnaZhGhHi8/TTexFKew8oxVOL/o6+q0YaslU/IAYIKwY
ExFUZXN0YmVkIFN0dXR0Z2FydDEUMBIGA1UEAxMLQWtvZ3JpbW8gQ0ExLjAsBgkqhkiG9w
0BCQEWH0RhdmlkLkx1dHpAcnVzLnVuaS1zdHV0dGdhcnQuZGWCCQD8rty8iEhJUzAdBgNVH
BS0XBX+S1oKll9/dbotk4uT79OTTTCBtwYDVR0jBIGvMIGsgBT/z8crhIwq6ewIpIADdTekr3NzIq
GBiKSBhTCBgjELMAkGA1UEBhMCREUxETAPBgNVBAoTCEFrb2dyaW1vMRowGAYDVQQL
REEFjAUgRJmcmFua0Bha29ncmaWQuTHV0ekBydXMudW5pLXN0dXR0Z2FydC5kZTAoBglghk
gBhvhCAQQEGxYZaHR0cDovLy9wdWIvY3JsL2NhY3JsLmNybDAoBglghkgBhvhCAQMEGxYZa
HR0cDovLy9wdWIvY3JsL2NhY3JsLmNybDAqBgNVHR8EIzAhMB+gHaAbhhlodHRwOi8vL3B1
Yi9jcmwvY2FjcmwuY3JsMA0GCSqGSIb3DQEBBQUAA4ICAQCsOxM293l25IUKRS6WHAg6vU
Y3DR5sC7XC/O7JawS7ltby5vcmcwKgYDVR0SBCMwIYEfRGF2jd+2/i8HBuPjs8PiqBJBsNRdhr1h
CFAC6IkSHI2VMGNIcOt
-----END RSA PRIVATE KEY-----

Το αρχείο **bob_crt.pem** περιέχει το πιστοποιητικό:

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=Gr, ST=Peiraias, O=Tei Mesologgiou, OU=IT Department, CN=koyto
    Validity
      Not Before: Sep 17 21:57:38 2009 GMT
      Not After : Sep 16 21:57:38 2014 GMT
    Subject: CN=bob, ST=Peiraias, C=GR/emailAddress=bob@teimes.com, O=T$
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          89:18:79:e9:9f:e9:81:9b:e7:b3:9f:67:80:82:be:
          f8:e4:ed:a4:77:69:23:d4:53:05:2b:1f:3a:65:34
          57:02:b8:fc:29:23:fa:b2:88:aa:76:f3:a7:74:f3:
          8f:02:92:4c:b3:1a:72:ca:43:2f:57:ce:f7:33:d5:
          55:32:bb:26:de:0a:48:d8:fc:c8:c0:c8:77:f6:5d:
          c3:95:94:8f:21:b2:be:74:7f:5d:ae:3e:a9:41:ce:
          e3:48:d1:c1:40:24:eb:ad:b1:a1:ca:95:2f:c5:4d:
          61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c2:6e:
          5a:5d:9e:fe:a9:a5:57:4a: a5:94:ac:8a:67:00:9a:
          d9:8f::a8:2d:96:44:c9:2f:
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        IP Address: 198.168.210.80
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Cert Type:
        SSL Server
  Signature Algorithm: md5WithRSAEncryption
    9b:9d:70:e3:4e:de: 9d:70:e3cd:34:d2:82:67:41:24:d3:68:

0f:dd:7d:c4:1f:3f:dd:f3:94:41:04:7d:77:d2:30:49:e9:8f:
3c:97:af:1e:63:71:8d:45:e7:17:56:f3:db:99:9b:92:e1:68:
7a:ac:f8:fe:1d:04:89:57:f2:e1:9b:b0:cb:a7:38:6f:0b:3a:
ad:21:c8:41:71:94:6b: f0:16:d0:ce:4c:ad:0e:ee:bc:0e:fe:
07:34:15:db:38:61:93:42:7c:1a:35:59:52:e7:62:01:e4:c0:
7b:92:f8:cb:77:3f:56:22:9d:96:8b:b9:05:c4:18:01:bc:40:
9b: c9:71:2f:15:4a:96:67:b8:97:c4:ad:d1:fc:f8:f4:d7:9c:
74:0a:28:9f:c2:9f:89:e3:b8:d9:d7:d6:e1:42:05:84:cb:65:
e0:7e:d6:c8:62:0a:76::8c:1d:d4:ab:aa:04:1b: 2e:47:5e:10
51:80:af:3c:4f:df:09:75:6c:fc:4a:2e:c7:e3:2d:b5:3d:34:
04:7a:6e:5f:a5:d2:83:4e:45:c5:18:48:0b:5a:41:1b:bf:70:
7c:8e:7b:58:b9:0e:28:4c:90: bb:cc:5b:5f ab:20:83:61:9e:
ab:78:2b:a4:

-----BEGIN CERTIFICATE-----
UEChMIQWtvZ3JpbW8xETAPBgNVBAsTCEludGVybmV0MRYwFAYDVQQDEw1GcmFuayBGa
XJlbWFuMQowCAYDVQQFEwE0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/WV
iJsu1GBxiPShQFeLD2WsJf5Zybjiv6Terp/1N5YrMxh1sQImFdyY0RFwEY4mpsnHQftJ8CvNFGAR5
1Kyr1Y8lRi3f+tKgRD+nmhIhaa+IU3SIRRtzA7FQ1atQX2+N+jQ1NTInDTfAe+P81F2GvWEIUALo
tC0HCm/7E3hDl2AlmH/CNnYFZzoRmEmG0wIDAQABo4IBbDCCAWgwCQYDVR0TBAIwADA
RBglghkgBhvhCAQEEBAMCBkAwCwYDR0PBAQDAgXgMDQGCWCGSAGGEIjAgBggrBgEFB
QcDAgYIKwYBRjcNHmwLtci5Pv05NNMIG3BgNVHSMEga8wgayAFP/PxyuEjCrp7AikgAN1N6S
vc3MioYGIpIGFMI=AgTBkF0dGljYTEYMBYGA1UEChMPVGVpIE1lc29sb2dnaW91MRYwFAY
DVQQLEw1JVCBEZXBhcnRtZW50MREwDwYDVQQyBDQTEuMCwGCSqGSIb3+DQEJAYfRG
F+2aWQuTHV0ekBydXMudW5pLXN0dXR0Z2FydC5kZYIJAPyu3LyISElTMB0GA1UdEQQMBS
B'mZyYW5rQGFrb2dyaW1vLm9yZzAqBgNVHRIEIzAhgR9EYXZpZC5MdXR6QHJ1cy51bmktc3R
1dHRnYXJ0LmRlMCgGCWCGSAGG+EIBBAQbFhlodHRwOi8vL3B1Yi9jcmwvY2FjcmwuY3JsM
CgGCWCGSAGG+EIBAwQbFhlodHRwOi8vL3B1Yi9jcmwvY2FjcmwuY3JsMCoGA1UdHwQjMC
EwH6AdoBuGsA2zCBkwYDVR0jBIGLM4nRkinXiMGUQUapxjQ2t5Xn3gO7Ywv/akqM6yKsXK3
wNMdGwbWfpRqjd1A==
-----END CERTIFICATE-----

Για την εγκατάσταση του πιστοποιητικού του client Alice, που δημιουργήθηκε πιο πάνω, θα πρέπει το πιστοποιητικό να μετατραπεί σε PKCS#12 μορφή, ώστε να είναι συμβατό με το λειτουργικό σύστημα (Windows) που διαθέτει ο υπολογιστής του client Alice. Η εντολή που επιτρέπει την μετατροπή είναι:

openssl pkcs12 -export -in ~/myCA/alice_crt.pem -inkey~/myCA/alice_key.pem -certfile ~/myCA /cacert.pem -out ~/myCA/alice_crt.pem.p12

Αντίστοιχα θα πρέπει να μετατραπεί και το πιστοποιητικό του Client Bob:

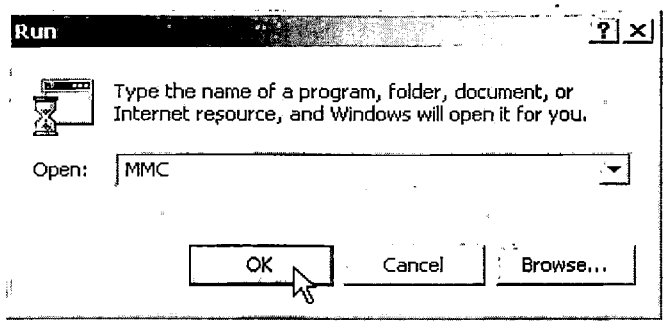
openssl pkcs12 -export -in ~/myCA/bob_crt.pem -inkey~/myCA/bob_key.pem -certfile ~/myCA /cacert.pem -out ~/myCA/bob_crt.pem.p12

Αφού ολοκληρωθούν τα παραπάνω βήματα, η ακόλουθη διαδικασία για την εγκατάσταση των πιστοποιητικών σε εικονογραφημένη μορφή, όπως αντλήθηκε από την ιστοσελίδα http://support.real-time.com/open-source/ipsec/index.html#add, είναι:

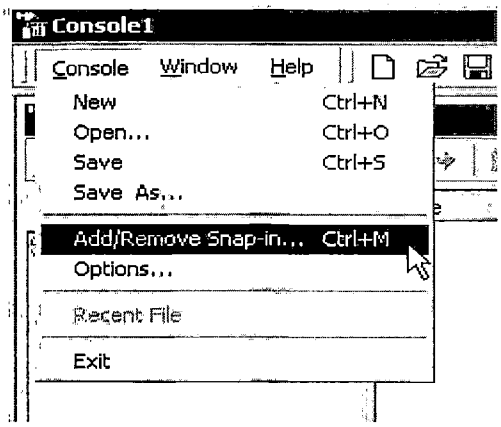
Client Alice

1. Πατάμε Start → Run

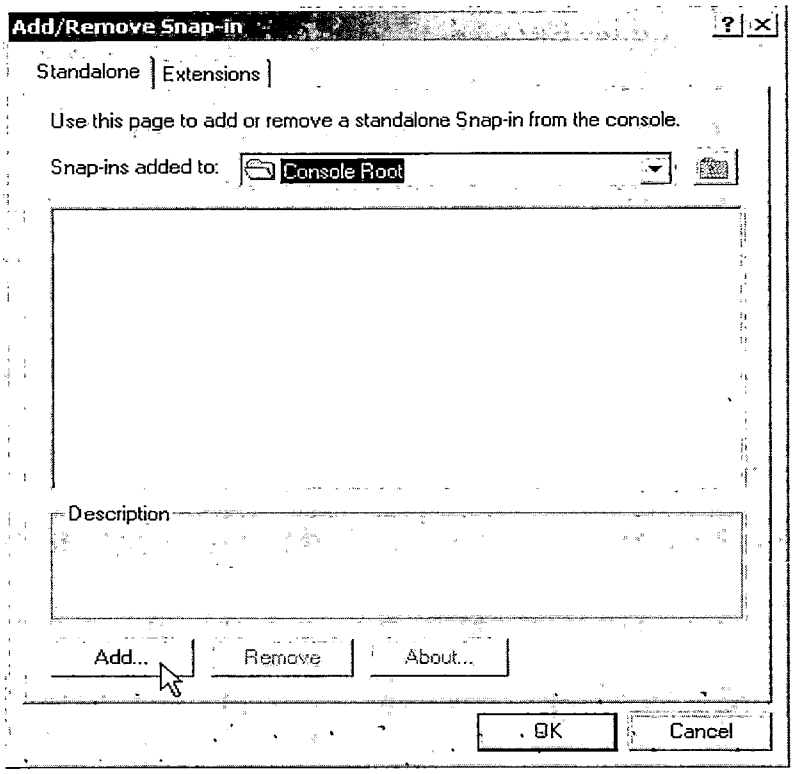
2. Πληκτρολογούμε MMC



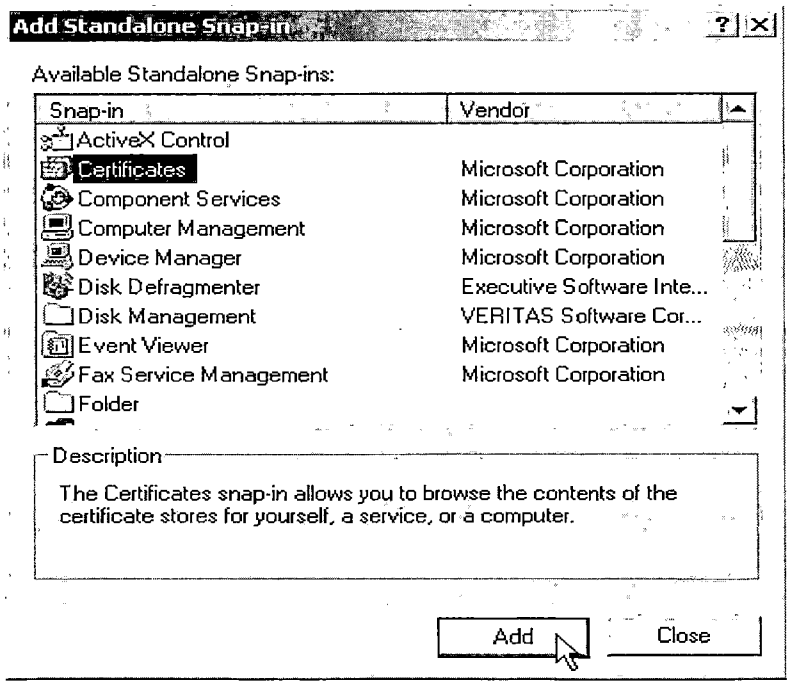
3. Επιλέγουμε από το παρακάτω παράθυρο File (ή Console) → Add/Remove Snap-in



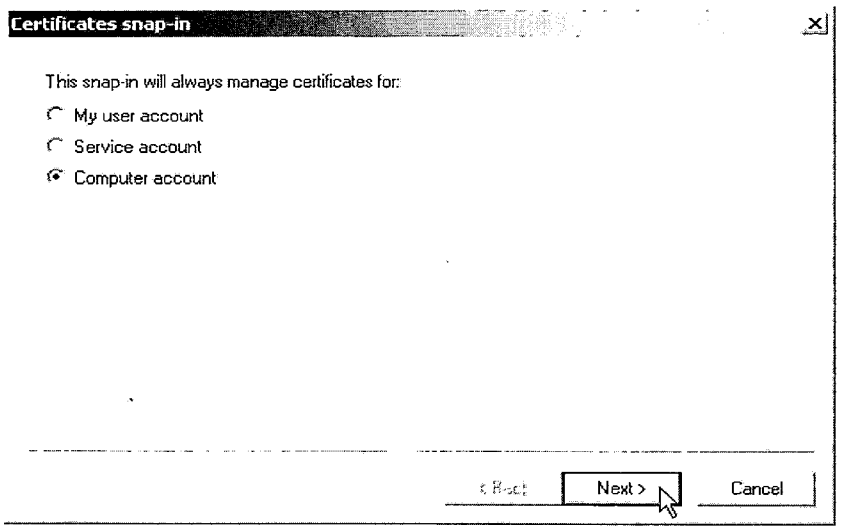
4. Επιλέγουμε Add



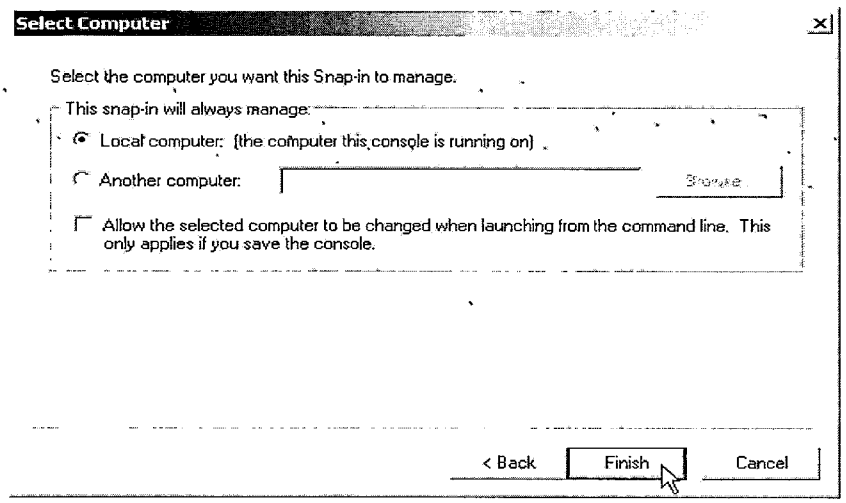
5. Κάνουμε κλικ στην επιλογή certificates →Add



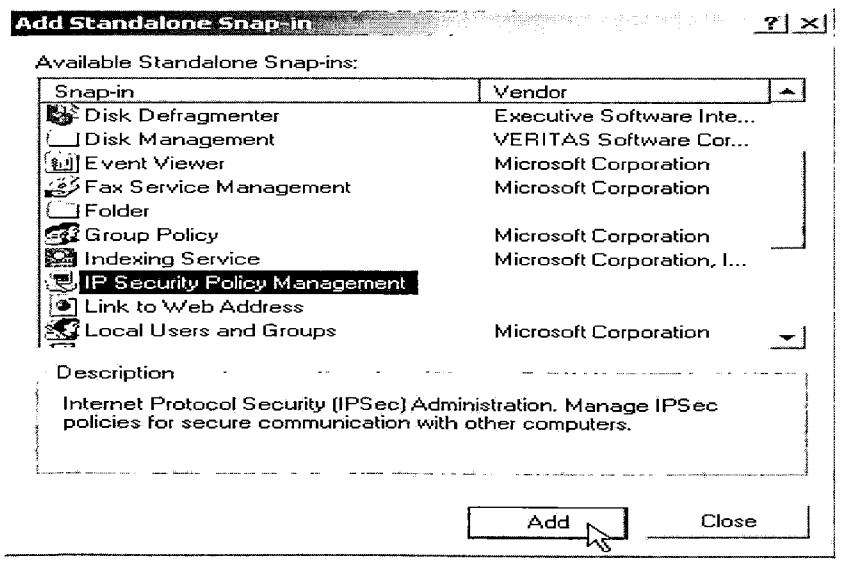
6. Επιλέγουμε το Computer Account → Next



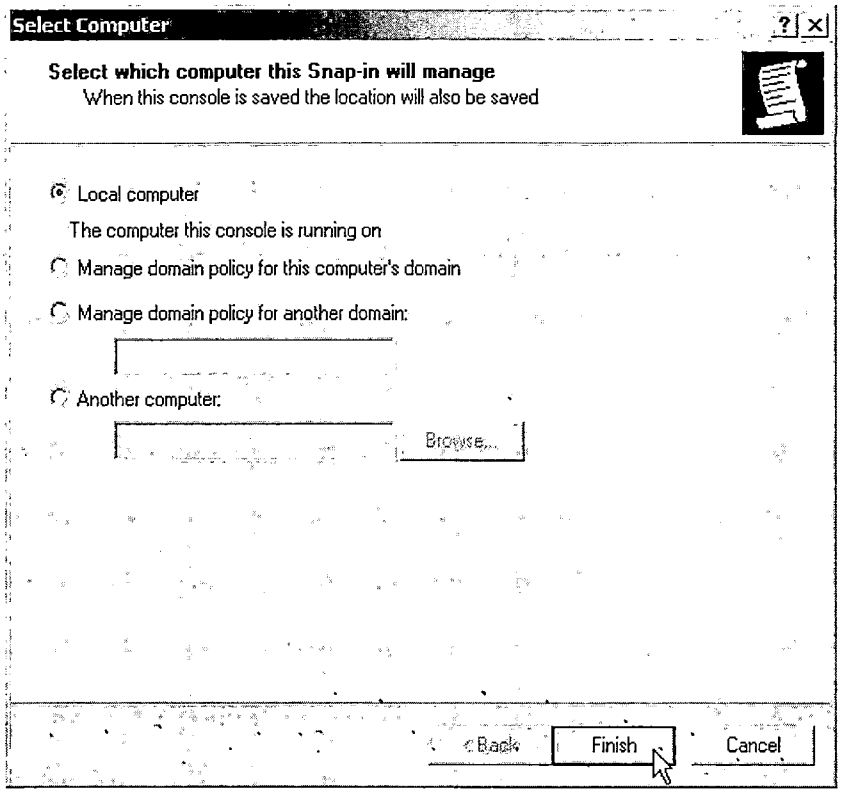
7. Επιλέγουμε Local computer → Finish



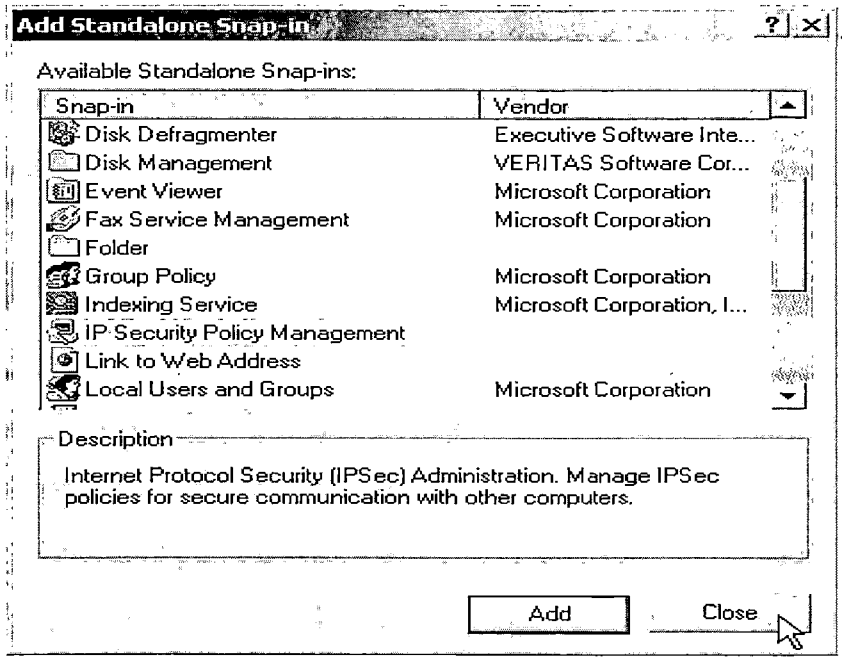
8. Σε αυτό το παράθυρο κάνουμε κλικ στο IP Security Policy Management →Add



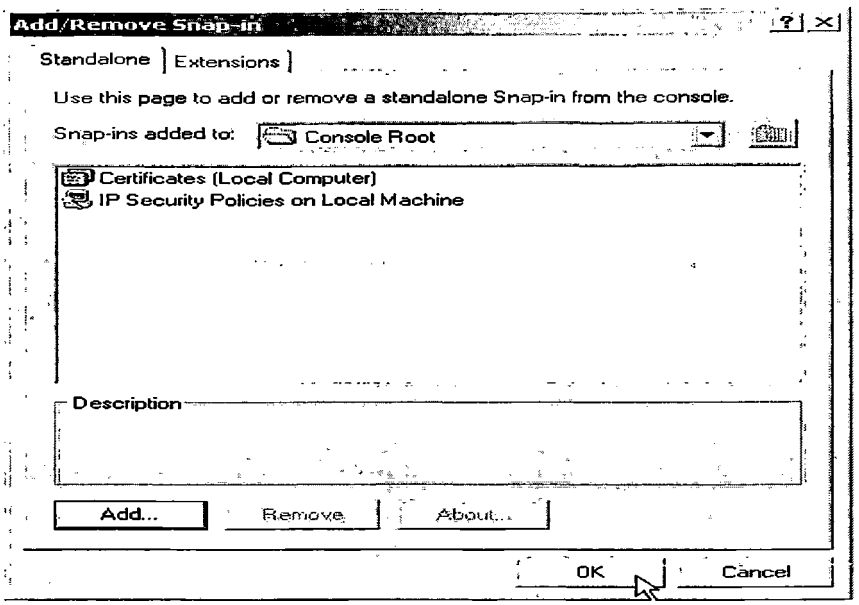
9. Επιλέγουμε Local Computer → Finish



10. Πατάμε Close

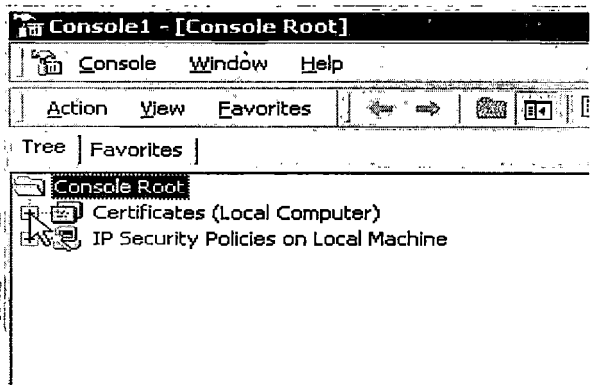


11. Κάνουμε κλικ πάνω στο OK

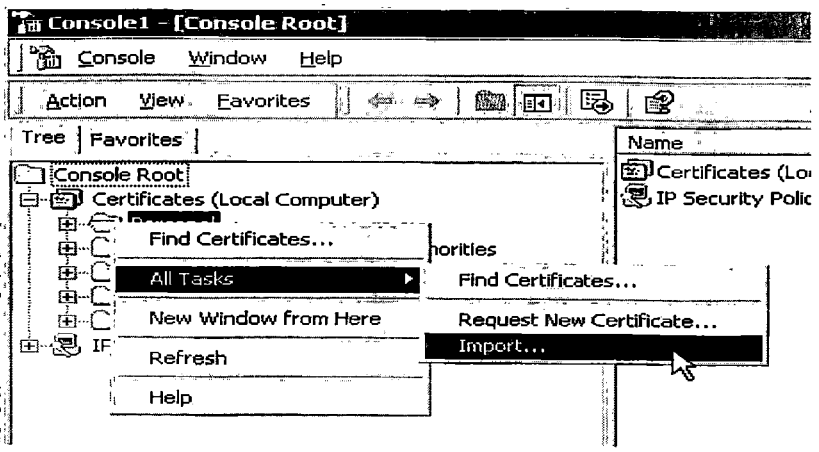


Σε αυτό το στάδιο προσθέτουμε το πιστοποιητικό που θέλουμε:

1. Κάνουμε κλικ πάνω στο σύμβολο + δίπλα από το Certificates (Local Computer)

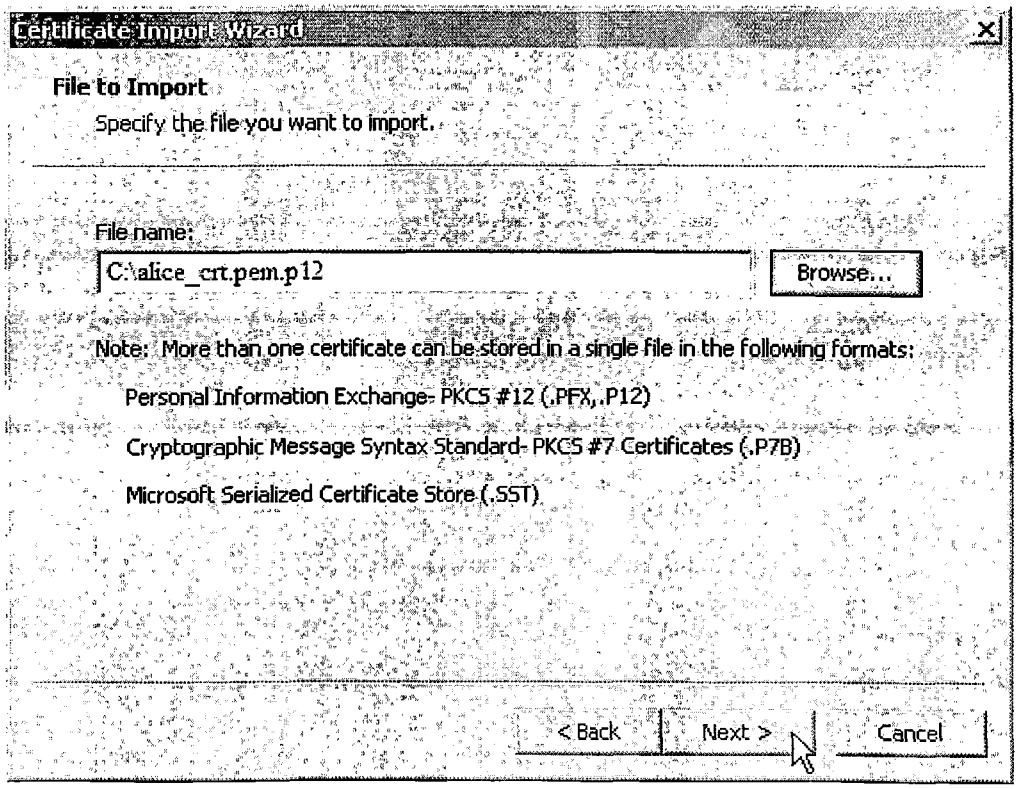


2. Κάνουμε διπλό κλικ στο Personal και έπειτα κλικ στο All Tasks → Import...

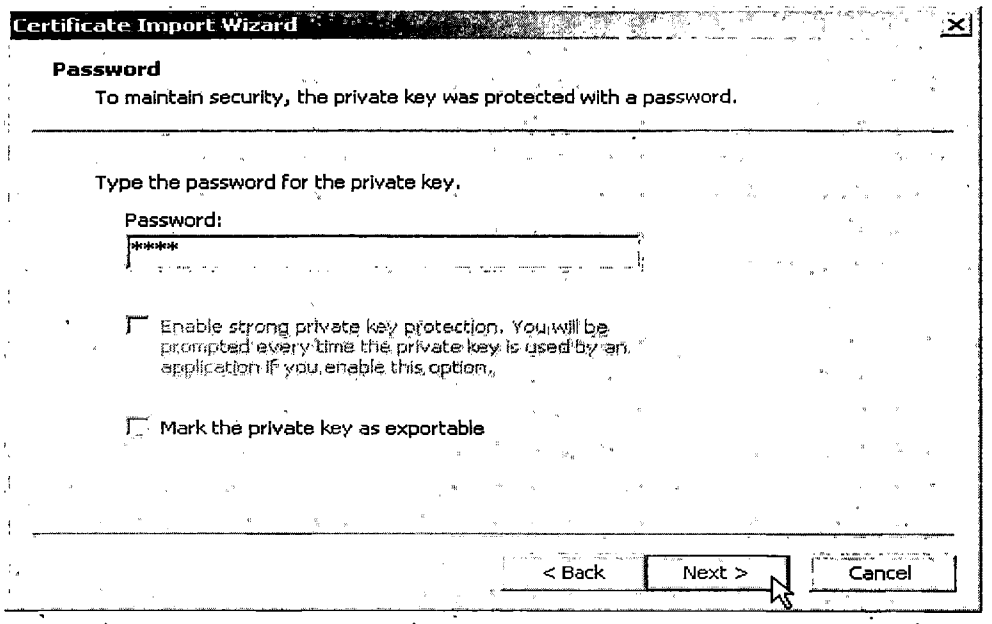


3. Επιλέγουμε Next

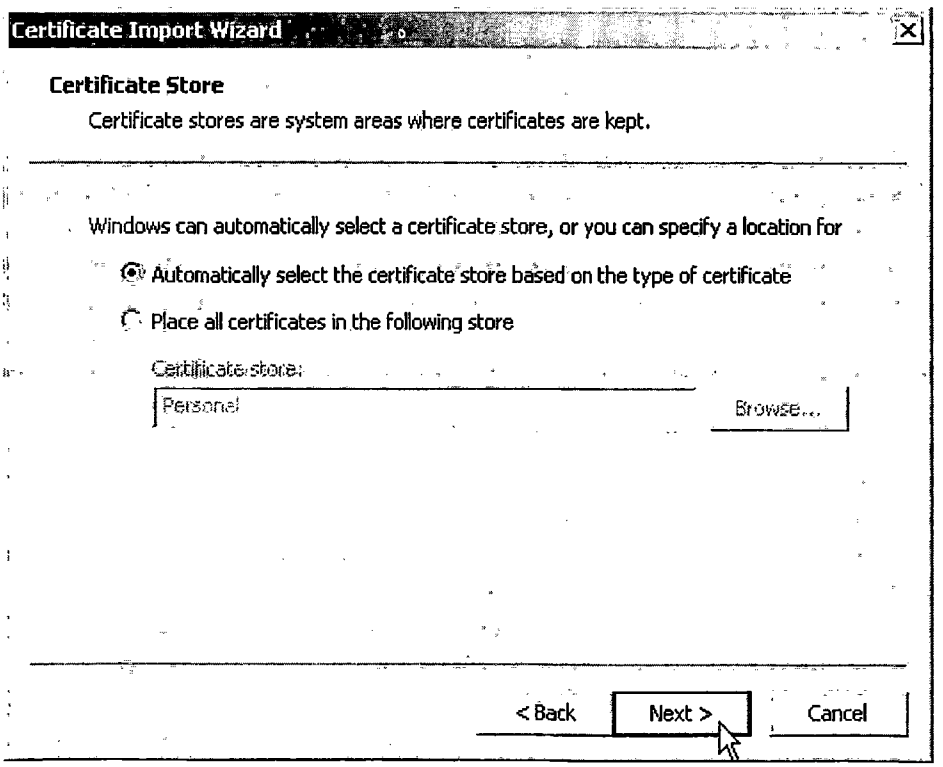
4. Εισάγουμε την διαδρομή που έχουμε αποθήκευση το πιστοποιητικό που μετατρέψαμε πριν σε μορφή .P12.



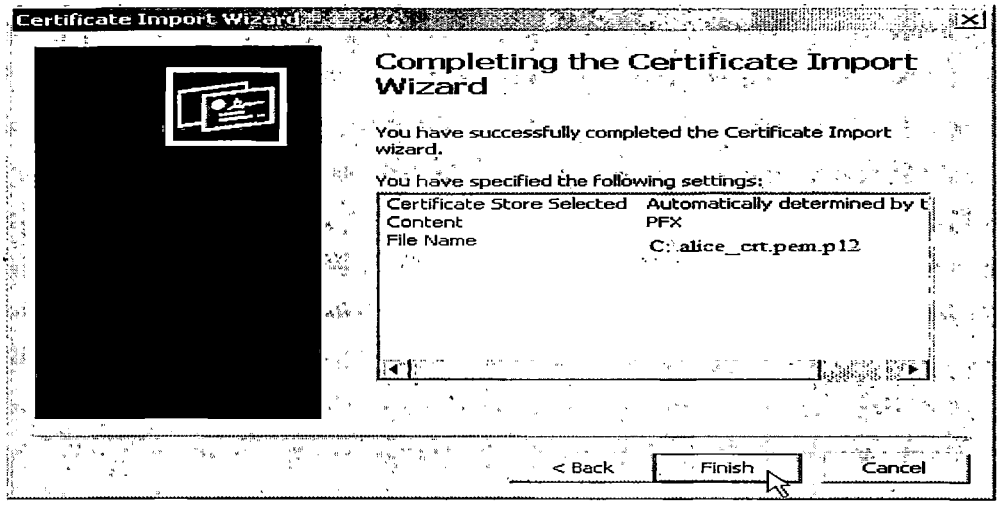
5. Εάν θέλουμε να χρησιμοποιήσουμε ένα κωδικό εξαγωγής το τοποθετούμε σε αυτό το πεδίο, ειδάλλως μπορούμε να το αφήσουμε κενό και να προχωρήσουμε στο επόμενο βήμα



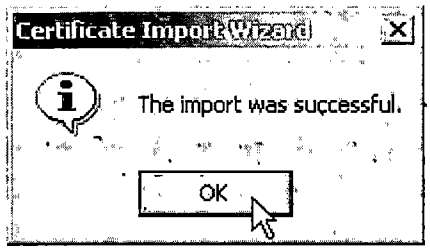
6. Επιλέγουμε Automatically select the certificate store based on the type of certificate → Next



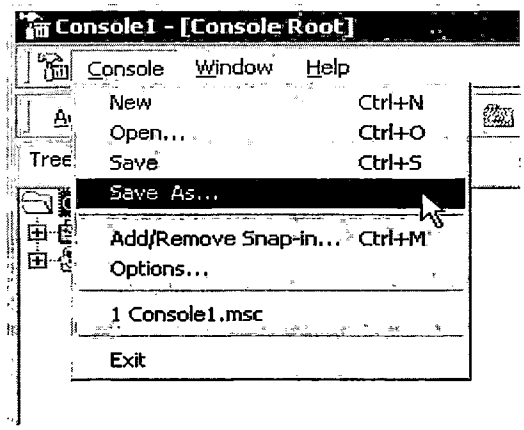
7. Επιλέγουμε Finish



8. Πατάμε OK



9. Αποθηκεύουμε τις αλλαγές που έγιναν



Με την παραπάνω λογική φορτώνουμε το πιστοποιητικό και στον υπολογιστή του client Bob

Παράρτημα Γ– StrongSwan

Gateway MIDI

```
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup                #καθορίζει γενικές παραμέτρους διαμόρφωσης
        crlcheckinterval=180
        strictcrlpolicy=no
        plutostart=no           # Δεν εκκινεί pluto daemon (IKEv1) αλλά Charon (IKEv2)

conn %default           # Περιέχει προεπιλεγμένες τιμές που εφαρμόζονται σε όλες τις συνδέσεις
        ikelifetime=60m         #Καθορίζει οτι μέχρι 60m θα είναι ο χρόνος προτού το κανάλι
                                  για την ανταλλαγή κλειδιών της σύνδεσης αρχίσει πάλι
                                  την διαπραγμάτευση
        ikeylife=20m            #Η διάρκεια ζωής ενός σετ κλειδιών κρυπτογράφησης/
                                  αυθεντικοποίησης μετά από μια επιτυχημένη διαπραγμάτευση
                                  μέχρι την λήξη της
        rekeymargin=3m          #Μέχρι 3m προτού να λήξει η σύνδεση επιτρέπετε να γίνονται
                                  προσπάθειες προτού η διαδικασία αντικατάστασης εκκινήσει
        keyingtries=1           #Επιτρέπετε μέχρι και μια προσπάθεια για την διαπραγμάτευση
                                  της σύνδεσης
        keyexchange=ikev2       #Η μέθοδος ανταλλαγής κλειδιών είναι ikev2
        leftsubnet=10.10.0.0/16 #Το υποδίκτυο που ανήκει ο client alice
        left=198.168.30.10      #Η δημόσια IP διεύθυνση του gateway midi
        leftcert=/home/dimitris/myCA/midi_crt.pem   #Το X.509 πιστοποιητικό του
                                                      gateway midi
        leftid="C=Gr, ST=Attica, O=Tei Mesologgiou, OU=IT Department, CN=midi
                emailAddress=midi@teimes.com"  #Είναι το πεδίο οπου αναγνωρίζετε
                                                 μοναδικά ο gateway midi

conn net-net    #Ονομα της σύνδεσης
        leftsubnet=10.10.0.0/16     #Το υποδίκτυο που ανήκει ο client alice
        right=198.168.30.11         #Η δημόσια IP διεύθυνση του gateway koyto
        rightsubnet=11.10.0.0/16    #Το υποδίκτυο που ανήκει ο client bob
        rightid="C=Gr, ST=Peiraias, O=Tei Mesologgiou, OU=IT Department
                CN=koyto, emailAddress=koyto@teimes.com"  #Είναι το πεδίο οπου
                                                            αναγνωρίζετε μοναδικά
                                                            ο gateway koyto
       auto=add    #Φορτώνει την σύνδεση χωρίς να την εκκινήσει κατά την έναρξη του IPsec

conn host-host    #Ονομα της σύνδεσης
        right=198.168.30.11     #Η δημόσια IP διεύθυνση του gateway koyto
        rightid="C=Gr, ST=Peiraias, O=Tei Mesologgiou, OU=IT Department,
                CN=koyto, emailAddress=koyto@teimes.com"  #Είναι το πεδίο οπου
                                                            αναγνωρίζετε μοναδικά
                                                            ο gateway koyto

        auto= add    #Φορτώνει την σύνδεση χωρίς να την εκκινήσει κατά την έναρξη του IPsec
```

```
conn nat-t      #Ονομα της σύνδεσης
        leftsubnet=10.10.0.0/16    #Το υποδίκτυο που ανήκει ο client alice
        right=%any                 #Κάθε IP διεύθυνση από το δίκτυο του client bob
        rightsubnet=11.10.0.0/16   #Το υποδίκτυο που ανήκει ο client bob
        auto= add     #Φορτώνει την σύνδεση χωρίς να την εκκινήσει κατά την έναρξη του IPsec
```

Client Alice

```
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup
        crlcheckinterval=180
        strictcrlpolicy=no
        plutostart=no

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        keyexchange=ikev2
conn nat-t
        left=%defaultroute  #Ολες οι συνδέσεις θα χρησιμοποιήσουν μια default route
        leftcert=/home/dimitris/myCA/alice_crt.pem    # Το X.509 πιστοποιητικό του
                                                        client alice
        leftid="C=Gr, ST=Attica, O=Tei Mesologgiou, OU=IT Department, CN=alice
                emailAddress=alice@teimes.com"      #Είναι το πεδίο οπου αναγνωρίζετε
                                                        μοναδικά ο gateway midi
        right=198.168.30.11
        rightid"=C=Gr, ST=Peiraias, O=Tei Mesologgiou, OU=IT Department,
                CN=koyto, emailAddress=koyto@teimes.com"
        rightsubnet=11.10.0.0/16
        auto=add
```

Gateway Koyto

```
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup
        crlcheckinterval=180
        strictcrlpolicy=no
        plutostart=no

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
```

```
        keyingtries=1
        keyexchange=ikev2
        leftsubnet=11.10.0.0/16
        left=198.168.30.11
        leftcert=/home/mix/myCA/koyto_crt.pem
        leftid=="C=Gr, ST=Peiraias, O=Tei Mesologgiou, OU=IT Department,
                CN=koyto, emailAddress=koyto@teimes.com"

conn net-net
        leftsubnet=11.10.0.0/16
        right=198.168.30.10
        rightsubnet=10.10.0.0/16
        rightid="C=Gr, ST=Attica, O=Tei Mesologgiou, OU=IT Department,
                CN=midi, emailAddress=midi@teimes.com"
        auto=add

conn host-host
        right=198.168.30.10
        rightid="C=Gr, ST=Attica, O=Tei Mesologgiou, OU=IT Department,
                CN=midi, emailAddress=midi@teimes.com"
        auto=add

conn nat-t
        leftsubnet=11.10.0.0/16
        right=%any
        rightsubnet=10.10.0.0/16
        auto=add
```

Client Bob

```
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup
        crlcheckinterval=180
        strictcrlpolicy=no
        plutostart=no
conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        keyexchange=ikev2
conn nat-t
        left=%defaultroute
        leftcert=/home/mix/myCA/bob_crt.pem
        leftid="C=Gr, ST=Peiraias, O=Tei Mesologgiou, OU=IT Department,
                CN=bob, emailAddress=bob@teimes.com"
```

```
right=198.168.30.10
rightid"=C=Gr, ST=Attica, O=Tei Mesologgiou, OU=IT Department,
        CN=midi, emailAddress=midi@teimes.com"
rightsubnet=10.10.0.0/16
auto=add
```

Για την πτυχιακή εργασία, έγιναν ορισμένες ρυθμίσεις για το Network Address Translation (NAT) με σκοπό να εξαιρεθεί η tunnelling κίνηση:

Gateway midi

```
#! /bin/bash
# Network Configuration
#Αυτό το script προωθεί τα πακέτα
echo 1 > /proc/sys/net/ipv4/ip_forward
# Βγάζει όλους τους κανόνες από παλιούς iptables rules στο "filter table"
iptables -F
# Βγάζει όλους τους παλιούς κανόνες στο nat table
iptables -t nat -F
# Αυτό το script ενεργοποιεί το Network address
# Iptables -t nat -A POSTROUTING -o eth1  -j SNAT --to 198.168.30.10
# Το NAT εξαιρεί την κίνηση στο άλλο τοπικό δίκτυο στο τέλος του IPsec tunnel
iptables -t nat -A POSTROUTING -o eth0 -d ! 10.10.0.0/16 -j SNAT --to
198.168.30.11
# Αυτη η εντολή δρομολογεί όλη την κίνηση από το δίκτυο 10.10.0.0/16 μέσω του
#gateway Midi
route add -net 10.10.0.0 netmask 255.255.0.0 gw 198.168.30.10
#service to start ipsec
service ipsec start
starting ipsec tunnel called net-to-net defined /etc/ipsec.conf
ipsec auto --up net-to-net
```

Gateway Koyto

```
#! /bin/bash
# Network Configuration
#Αυτό το script προωθεί τα πακέτα
echo 1 > /proc/sys/net/ipv4/ip_forward
# Βγάζει όλους τους κανόνες από παλιούς iptables rules στο "filter table"
iptables -F
# Βγάζει όλους τους παλιούς κανόνες στο nat table
iptables -t nat -F
# Αυτό το script ενεργοποιεί το Network address
# Iptables -t nat -A POSTROUTING -o eth1  -j SNAT --to 198.168.30.11
# Το NAT  εξαιρεί την κίνηση στο άλλο τοπικό δίκτυο στο τέλος του IPsec tunnel
iptables -t nat -A POSTROUTING -o eth0 -d ! 11.10.0.0/16 -j SNAT --to
198.168.30.10
# Αυτη η εντολή δρομολογεί όλη την κίνηση από το δίκτυο 11.10.0.0/16 μέσω του
#gateway Koyto
route add -net 11.10.0.0 netmask 255.255.0.0 gw 198.168.30.11
```

#service to start ipsec
service ipsec start
starting ipsec tunnel called net-to-net defined /etc/ipsec.conf

Ξενόγλωσση Βιβλιογραφία

[1] Naganand Doraswamy and Dan Harkins, (2003), "IPSec: the new security standard for the Internet, intranets, and virtual private networks", 2nd edition, Prentice-Hall, Inc.

[2] Ken Bantoft, Paul Wouters (2006), "Openswan: Building and Integrating Virtual Private Networks", Packt Publishing Ltd

[3] Gupta Meeta, (2003), "Building a Virtual Private Network", Premier Press.

[4] Alcatel, (2000), "Understanding the IPSec Protocol Suite"

[5] Cisco Systems Inc., (2003), "Internetworking Technologies Handbook", 4th edition, Cisco Press

[6] Kireeti Kompella, "MPLS-based Layer 2 Virtual Private Networks", White Paper, Juniper networks, 2001

[7] Karen Kent, Ryan Lewkowski, Sheila Frankel, Angela Orebaugh, Ronald Ritchey and Steven Sharma, (2005), "Guide to IPSec VPNs", Recommendations of the National Institute of Standards and Technology (NIST), special publication 800-77

[8] Shashank Khanvilkar and Ashfaq Khokhar, (2004), "Virtual Private Networks: An overview with performance evaluation", IEEE communication magazine, October 2004

[9] Christopher Negus, (2004), "Red Hat Linux Bible, Fedora and Enterprise Edition", Willey Publishing Inc.

[10] K. Kompella et al. "Layer 2 VPNs Over Tunnels", Internet draft (draftkompella-ppvpn-l2vpn-01.txt), November 2001

[11] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, (2006), "Recommendation for Key Management - Part 1: General (Revised)", National Institute of Standards and Technologies (NIST), special publication 800-57, May 2006

[12] Northcutt S., Zeltser L., Winters S., Frederick K. K. and Ritchey W. R, (2003), "Inside network perimeter security: definitive guide to firewalls, virtual private networks (VPN), routers, and intrusion detection systems", Sams Publishing

[13] Deal Richard, (2005), "The complete Cisco VPN configuration guide", Cisco Press

[14] Vijay Bollapragada, Mohamed Khalid and Scott Wainner, (2005), "IPSec VPN Design", Cisco Press

[15] Shashank Khanvilkar and Ashfaq Khokhar, (2004), "Virtual Private Networks: An overview with performance evaluation", IEEE Communication magazine, October 2004

[16] Jochen Eisinger, (2001), "Exploiting known security holes in Microsoft's PPTP Authentication Extensions (MS-CHAPv2)", University of Freiburg

[17] David Wagner and Bruce Schneier (1996), "Analysis of the SSL 3.0 protocol", Proceedings of the Second USENIX Workshop on Electronic Commerce, Oakland, California, November 1996

[18] Russell Lusignan, Oliver Steudler, Jacques Allison (2000) "Managing Cisco Network Security: Building Rock-Solid Networks"

[19] Wesley Chou (2002), "Inside SSL: The Secure Sockets Layer Protocol", IEEE July-August 2002, IT Professional, Volume 4, Issue 4

[20] Tim Dierks and Eric Rescorla (2006), "The TLS Protocol Version 1.2", Internet Draft, the Internet Society

Ελληνική Βιβλιογραφία

[1] Δρ Ελευθέριος Μπόζιος, (2004), "Σημειώσεις Εφαρμοσμένης Ασφάλειας Πληροφοριακών Συστημάτων", Τμήμα Πληροφορικής Σ.Τ.ΕΦ., Τ.Ε.Ι. Θεσσαλονίκης

[2] Πομπόρτσης Αν, Παπαδημητρίου Γ, (2004), "Ασφάλεια Δικτύων Υπολογιστών" Εκδόσεις Τζιόλα

[3] Σ. Κάτσικα, Δ. Γκρίτζαλη, Σ. Γκρίτζαλη (Επιστημονική Επιμέλεια), (2004), "Ασφάλεια Πληροφοριακών Συστημάτων", Εκδόσεις Νέων Τεχνολογιών

[4] Βενιέρης Ι. (2006) , "Τεχνολογίες Διαδικτύου", Εκδόσεις Τζιόλα

[5] Ξενάκης Χρήστος (2009), "Πρωτόκολλα Ασφάλειας Επιπέδου Internet (IPsec)", Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά

[6] Δουίτσης Θανάσης, Καλογεράς Δημήτρης, Χριστιάς Παναγιώτης, Αντρέας Πολυράκης, Δημήτρης Ματσάκης, Σπύρος Παπαγεωργίου, (2007), "Δοκιμαστική Υπηρεσία «Διαχείριση Πρόσβασης Μέσω IPSec»", Εθνικό Μετσόβιο Πολυτεχνείο Κέντρο Δικτύων - ΚΕΔ

URLs

[1] Netscape Corporation, "Using RSA Public Key Cryptography"
http://home.netscape.com/newsref/ref/rsa.html

[2] Ε.Κ.Ε.Φ.Ε ΔΗΜΟΚΡΙΤΟΣ, "VPN (Virtual Private Network)"
http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/vpn.htm

[3] Ε.Κ.Ε.Φ.Ε ΔΗΜΟΚΡΙΤΟΣ, "IPSec (IP Security)"
http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ipsec.htm

[4] Carnegie Mellon University –CERN, "Smurf IP Denial-of-Service Attacks"
http://www.cert.org/advisories/CA-1998-01.html

[5] RFC Database: http://www.rfc-editor.org/rfc.html

[6] HERVÉ SCHAUER CONSULTANTS, "IPsec: a technical overview"
http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en

[7] FreeS/WAN FAQ
http://www.freeswan.org/freeswan_trees/CURRENT-TREE/doc/faq.html

[8] StrongSwan http://www.strongswan.org/

[9] Openswan: http://www.openswan.org/

[10] NIST IPsec: Project http://csrc.nist.gov/archive/ipsec/index.html

Παρουσιάσεις

[1] Ι.Σ. Βενιέρης, (2001) "Δίκτυα Ευρείας Ζώνης"
http://icbnet.ntua.gr/icbnet/Mathimata/InternetTech/slides/3-Internet Security.ppt

[2] Kyesang Lee, (2003),"Internet Key Exchange version 2", Dept. of Information & Communications Eng., Dongeui University
http://seclab.cs.ucdavis.edu/seminars/IKEv2.ppt

[3] Αντώνης Λίτκε, (2009), "Secure Sockets Layer (SSL) protocol", Τμήμα Πληροφορικής, Πανεπιστήμιο Ιωαννίνων
www.cs.uoi.gr/~alitke/Internet_technologies_10th_presentation.ppt

[4] Κώστας Λιμνιώτης, (2009), "Κρυπτογραφία: (Αλγόριθμοι δημοσίου κλειδιού)-El Gamal, Diffie-Hellman, Τ.Ε.Ι Λαμίας
http://users.teilam.gr/~klimn/cryptography/Lab/Lec7.pdf

[5] Κώστας Λιμνιώτης, (2009), "Κρυπτογραφία: Αλγόριθμος τμήματος-Block ciphers", Τ.Ε.Ι.) Λαμίας http://users.teilam.gr/~klimn/cryptography/Lec3.pdf

[6] International Telecommunication Union (2008), "Internet Protocol Security (IP Sec)"
www.itu.int/ITU-D/arb/COE/2008/Cyber08/IP%20DOCS/Unit%205-IPsec-SSL-email%20security.ppt

RFCs

- Request for Comment (RFC) αρχεία σχετικά με το IPsec

Ονομασία	URL
RFC 1828: IP Authentication Using Keyed MD5	http://www.ietf.org/rfc/rfc1828.txt
RFC 1829: The ESP DES-CBC Transform	http://www.ietf.org/rfc/rfc1829.txt
RFC 2085: HMAC-MD5 IP Authentication with Replay Prevention	http://www.ietf.org/rfc/rfc2085.txt
RFC 2104: HMAC: Keyed-Hashing for Message Authentication	http://www.ietf.org/rfc/rfc2104.txt
RFC 2401: Security Architecture for the Internet Protocol	http://www.ietf.org/rfc/rfc2401.txt
RFC 2402: IP Authentication Header	http://www.ietf.org/rfc/rfc2402.txt
RFC 2403: The Use of HMAC-MD5-96 within ESP and AH	http://www.ietf.org/rfc/rfc2403.txt
RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH	http://www.ietf.org/rfc/rfc2404.txt
RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV	http://www.ietf.org/rfc/rfc2405.txt
RFC 2406: IP Encapsulating Security Payload (ESP)	http://www.ietf.org/rfc/rfc2406.txt
RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP	http://www.ietf.org/rfc/rfc2407.txt
RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)	http://www.ietf.org/rfc/rfc2408.txt
RFC 2409: The Internet Key Exchange (IKE)	http://www.ietf.org/rfc/rfc2409.txt
RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec	http://www.ietf.org/rfc/rfc2410.txt
RFC 2411: IP Security Document Roadmap	http://www.ietf.org/rfc/rfc2411.txt
RFC 2412: The OAKLEY Key Determination Protocol	http://www.ietf.org/rfc/rfc2412.txt
RFC 2451: The ESP CBC-Mode Cipher Algorithms	http://www.ietf.org/rfc/rfc2451.txt
RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH	http://www.ietf.org/rfc/rfc2857.txt
RFC 3173: IP Payload Compression Protocol (IPComp)	http://www.ietf.org/rfc/rfc3173.txt
RFC 3526: More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE)	http://www.ietf.org/rfc/rfc3526.txt

RFC 3554: On the Use of Stream Control Transmission Protocol (SCTP) with IPsec	http://www.ietf.org/rfc/rfc3554.txt
RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec	http://www.ietf.org/rfc/rfc3566.txt
RFC 3602: The AES-CBC Cipher Algorithm and Its Use With IPsec	http://www.ietf.org/rfc/rfc3602.txt
RFC 3664: The AES-XCBC-PRF-128 Algorithm for IKE	http://www.ietf.org/rfc/rfc3664.txt
RFC 3686: Using AES Counter Mode with IPsec ESP	http://www.ietf.org/rfc/rfc3686.txt
RFC 3706: A Traffic-Based Method of Detecting Dead IKE Peers	http://www.ietf.org/rfc/rfc3706.txt
RFC 3715: IPsec-NAT Compatibility Requirements	http://www.ietf.org/rfc/rfc3715.txt
RFC 3884: Use of IPsec Transport Mode for Dynamic Routing	http://www.ietf.org/rfc/rfc3884.txt
RFC 3947: Negotiation of NAT-Traversal in the IKE	http://www.ietf.org/rfc/rfc3947.txt
RFC 3948: UDP Encapsulation of IPsec ESP Packets	http://www.ietf.org/rfc/rfc3948.txt

- **Υπόλοιπα Request for Comment (RFC) αρχεία**

Ονομασία	URL
RFC 1334: PPP Authentication Protocols	http://www.ietf.org/rfc/rfc1334.txt
RFC 1661: The Point-to-Point Protocol (PPP)	http://www.ietf.org/rfc/rfc1661.txt
RFC 1968: The PPP Encryption Control Protocol (ECP)	http://www.ietf.org/rfc/rfc1968.txt
RFC 2003: IP Encapsulation within IP	http://www.ietf.org/rfc/rfc2003.txt
RFC 2246: The TLS Protocol Version 1.0	http://www.ietf.org/rfc/rfc2246.txt
RFC 2341: Cisco Layer Two Forwarding	http://www.ietf.org/rfc/rfc2341.txt
RFC 2637: Point-to-Point Tunneling Protocol	http://www.ietf.org/rfc/rfc2637.txt
RFC 2661: Layer Two Tunneling Protocol	http://www.ietf.org/rfc/rfc2661.txt
RFC 2784: Generic Routing Encapsulation	http://www.ietf.org/rfc/rfc2784.txt
RFC 2818: HTTP Over TLS	http://www.ietf.org/rfc/rfc2818.txt

RFC 2888: Secure Remote Access With L2TP	http://www.ietf.org/rfc/rfc2888.txt

RFC 3078: Microsoft Point-to-Point Encryption (MPPE) Protocol	http://www.ietf.org/rfc/rfc3078.txt
RFC 3193: Securing L2TP Using IPsec	http://www.ietf.org/rfc/rfc3193.txt
RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts	http://www.ietf.org/rfc/rfc3316.txt
RFC 3546: Transport Layer Security (TLS) Extensions	http://www.ietf.org/rfc/rfc3546.txt
RFC 3748: Extensible Authentication Protocol (EAP)	http://www.ietf.org/rfc/rfc3748.txt

Παράρτημα Ε– Ακρωνύμια

3DES	Triple DES

A

AES	Advanced Encryption Standard
AES-CBC	AES-Cipher Block Chaining
AH	Authentication Header

C

CA	Certification Authority
CHAP	Challenge Handshake Authentication Protocol
CRL	Certificate Revocation List

D

DES	Digital Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name System
DSL	Digital Subscriber Line
DSS	Digital Signature Standard

E

EAP	Extensible Authentication Protocol
EC2N	Elliptic Curve over $G[2^N]$
ESP	Encapsulating Security Payload

F

FTP	File Transfer Protocol

G

GRE	Generic Routing Encapsulation

H

HMAC	Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure

I

ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISA	Interconnection Security Agreement
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
IT	Information Technology
IV	Initialization Vector

L

L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 VPN
L3VPN	Layer 3 VPN

M

MAC	Message Authentication Code
MODP	Modular Exponential

N

NAT	Network Address Translation
NAT-T	Network Address Translation Traversal
NIC	Network Interface Card

O

OCSP	Online Certificate Status Protocol

P

PAP	Password Authentication Protocol
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment

S

SA	Security Association
SAD	Security Association Database
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SPD	Security Policy Database
SPI	Security Parameters Index
SSH	Secure Shell
SSL	Secure Sockets Layer

T

TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TTL	Time to Live

U

UDP	User Datagram Protocol

URL	Uniform Resource Locator

V

VoIP	Voice over IP
VPN	Virtual Private Network
VPNC	Virtual Private Network Consortium

W

WAN	Wide Area Network

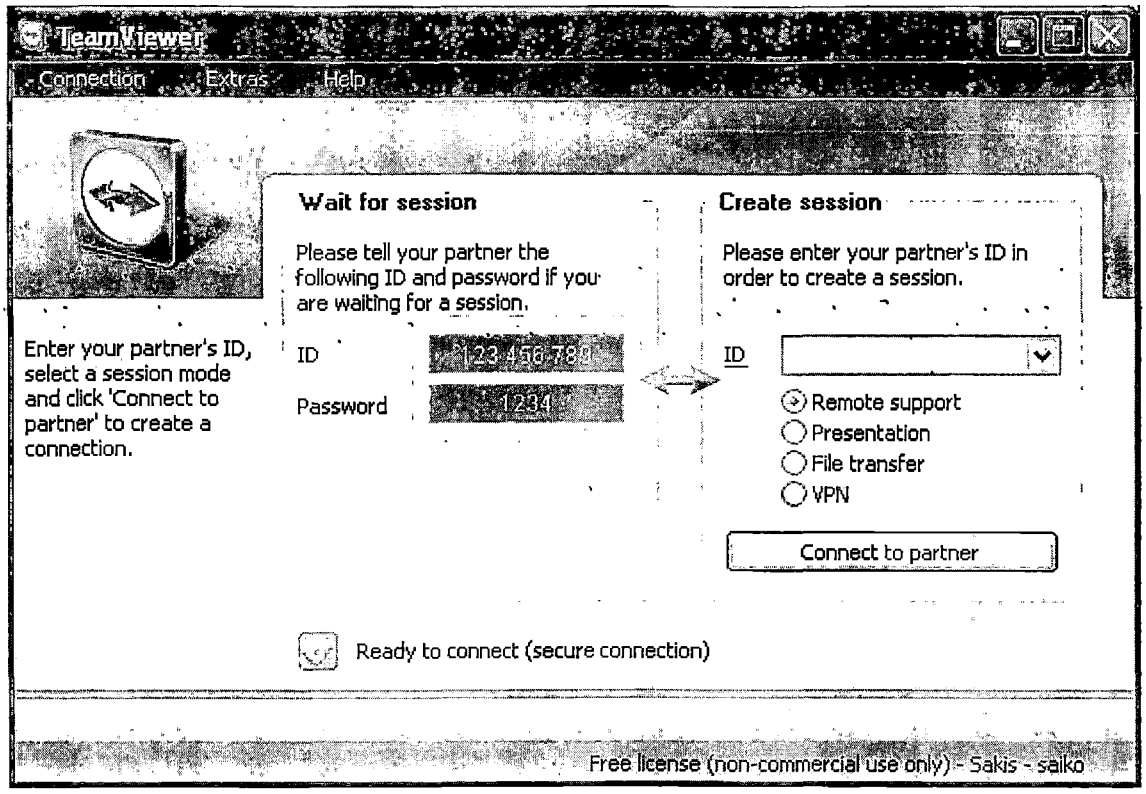
X

XOR	Exclusive OR

Β΄ ΜΕΡΟΣ

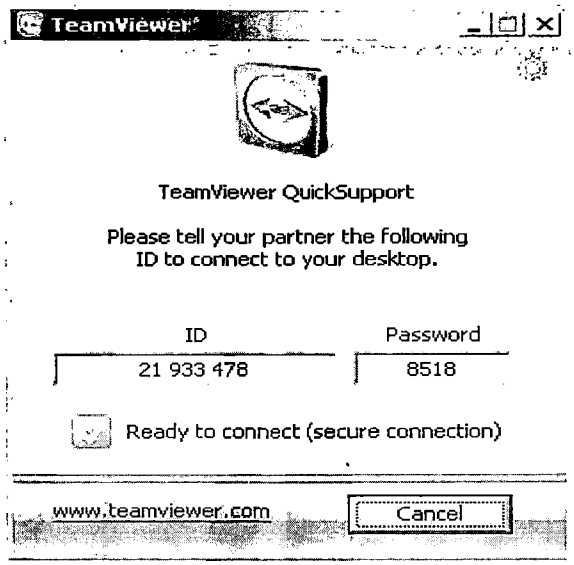
Παράρτημα Α— Εγκατάσταση του TeamViewer

Εγκαθιστούμε και κατόπιν εκτελούμε την εφαρμογή TeamViewer Full Version στον υπολογιστή του γραφείου διασύνδεσης.



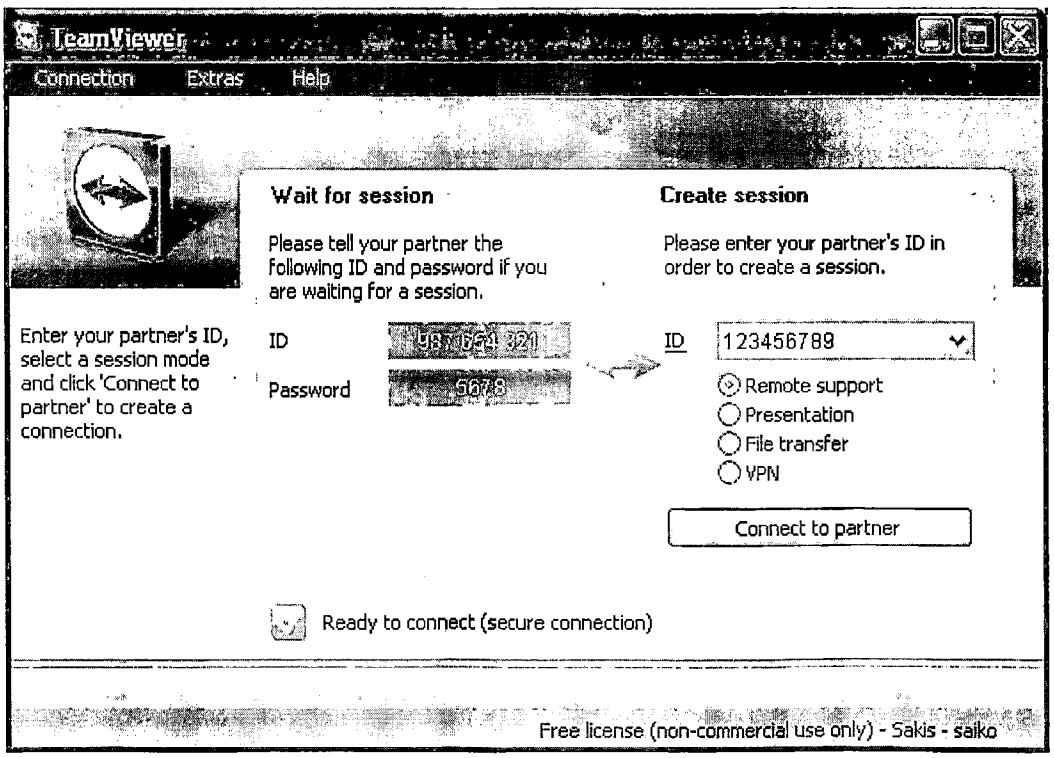
Εδώ διακρίνουμε τα πεδία "**ID**" και "**Password**". Κάθε εγκατάσταση του TeamViewer που κάνουμε, μας δίνει διαφορετικά ID και Password. Επίσης, κάθε φορά που εκτελούμε το TeamViewer στον ίδιο Η/Υ μας δίνει το ίδιο ID αλλά διαφορετικό password.

Εγκαθιστούμε την εφαρμογή TeamViewer Host στο διαδραστικό σταθμό.

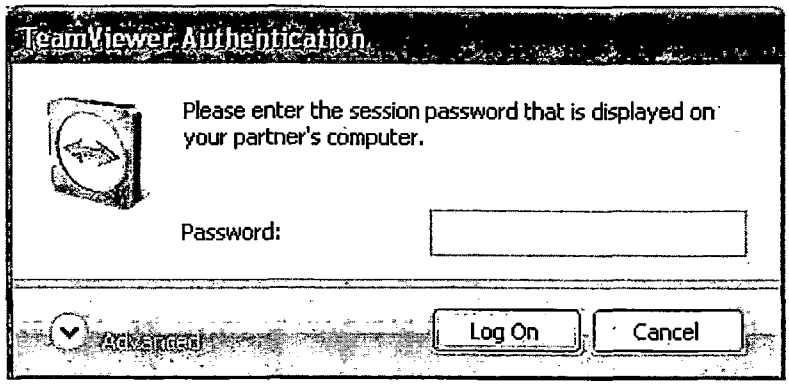


Στην παραπάνω εικόνα βλέπουμε τα στοιχεία πρόσβασης (ID και Password) του διαδραστικού σταθμού, τα οποία παράγει αυτόματα η εφαρμογή TeamViewer.

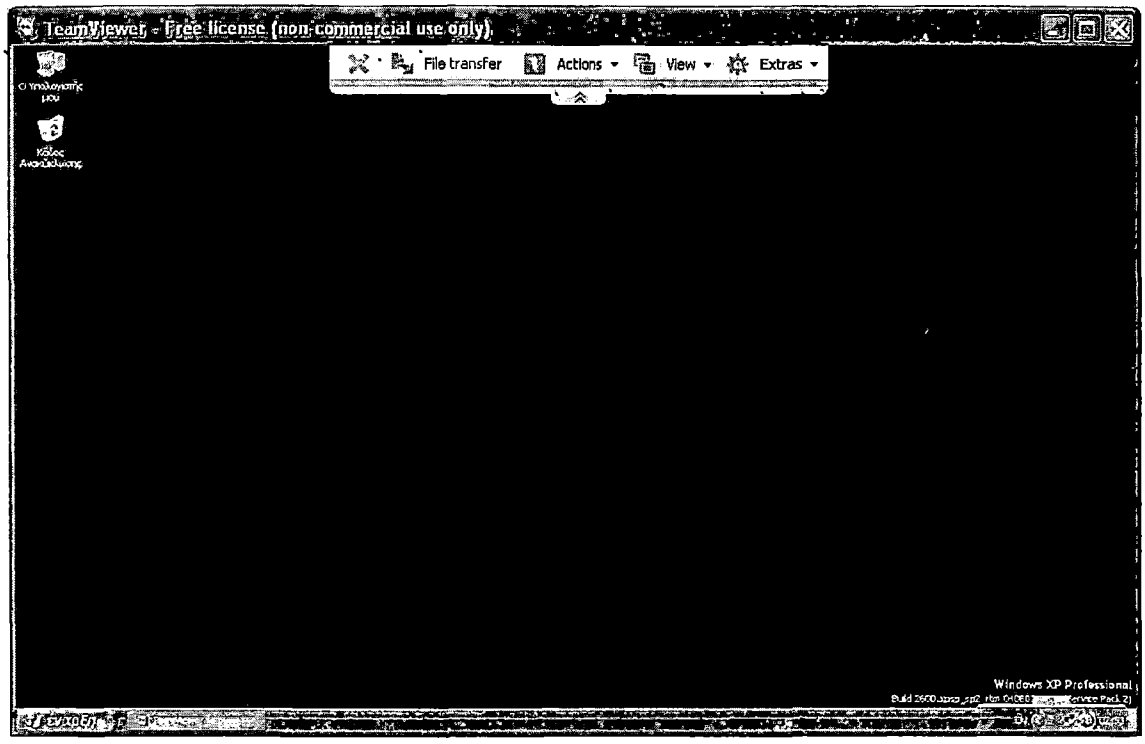
Εφόσον εμείς θέλουμε να συνδεθούμε με τον διαδραστικό σταθμό, στο παράθυρο αυτό θα πρέπει να γράψουμε το ID του TeamViewer του διαδραστικού σταθμού στη δεξιά μεριά, ενώ παράλληλα επιλέγουμε "Remote support". Έπειτα πατάμε το κουμπί "**Connect to partner**".



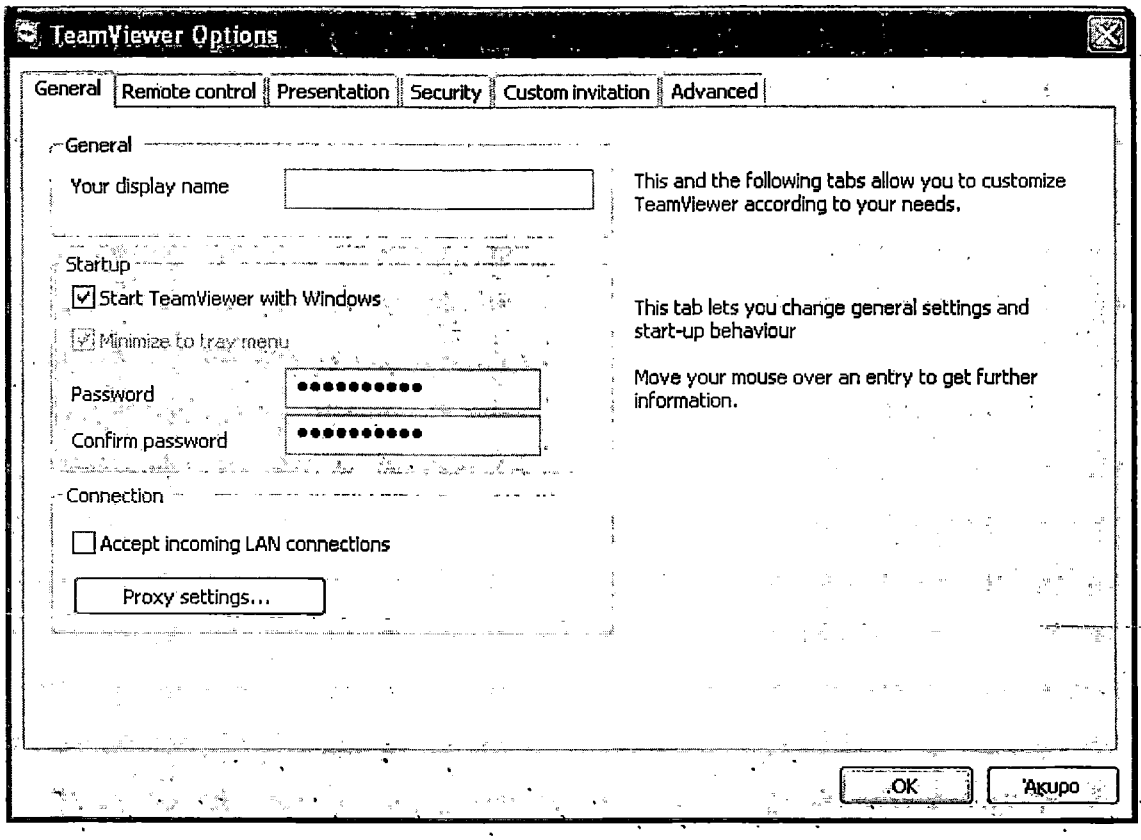
Σε λίγο μας εμφανίζει ένα άλλο μικρότερο παράθυρο στο οποίο γράφουμε το Password του διαδραστικού σταθμού. Μετά πατούμε στο κουμπί "**Log On**"



Αφού γίνει η επαλήθευση των ID και Password η σύνδεση εγκαθίσταται άμεσα, βλέπουμε την οθόνη του απομακρυσμένου υπολογιστή (διαδραστικός σταθμός) και αποκτούμε τον πλήρη έλεγχο. Όλα τα δεδομένα είναι πλήρως κρυπτογραφημένα και ασφαλή.



Υπάρχει και η δυνατότητα να ρυθμίσουμε το TeamViewer ώστε να εκτελείται και ως υπηρεσία με την εκκίνηση των Windows. Αυτό γίνεται ως εξής: Στο μενού του TeamViewer επιλέγοντας "**Extras > Options**", μας εμφανίζεται ένα παράθυρο με τις διάφορες ρυθμίσεις που μπορούμε να κάνουμε στην εφαρμογή. Στην καρτέλα "**General**" επιλέγουμε "**Start TeamViewer with Windows**", γράφουμε έναν κωδικό στα πεδία "Password" και "**Confirm Password**" και πατάμε το κουμπί "**OK**".



Έτσι, μόλις ανοίγει ο Η/Υ του διαδραστικού σταθμού, αυτόματα φορτώνει και το TeamViewer και μπορούμε να συνδεθούμε σε αυτόν απομακρυσμένα δηλώνοντας το ID του και το Password που αποθηκεύσαμε στο τελευταίο βήμα. Έτσι αν για παράδειγμα γίνει επανεκκίνηση στον Η/Υ του διαδραστικού σταθμού, δε θα χρειαζόμαστε κάποιον να εκτελέσει το TeamViewer για μας και να μας πει το νέο του password.

Παράρτημα Β– Βιβλιογραφία

[1] Σταθμοί πληροφόρησης Friendlyway
http://www.infokiosk-impress.gr/gr/downloads/fw_impress.pdf

[2] Διαδραστικός Σταθμός Πληροφόρησης (Infokiosk) στο ΤΕΙ Μεσολογγίου, (2008), http://www.epdo.teimes.gr/Lists/Announcements/Attachments/84/infokiosk.pdf

[3] Προμήθεια Infokiosk για το Γραφείο Διασύνδεσης του Τ.Ε.Ι. Μεσολογγίου, (2008), http://news.teimes.gr/news/wp-content/uploads/2008/06/prokirixi-promithias-infokiosk-gtr-diasyndesis-tei-m-f812-2186-04-06-08.doc

[4] TeamViewer
http://www.teamviewer.com/index.aspx

[5] TeamViewer Security Information, (2009),
http://www.teamviewer.com/images/pdf/TeamViewer_SecurityStatement.pdf

[6] Manual TeamViewer 4.1, (2009),
http://www.teamviewer.com/help/teamviewer_manual.pdf