Πανεπιστήμιο Πειραιώς

Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών

Κατεύθυνση: Δικτυοκεντρικά Συστήματα

Διπλωματική Εργασία

ΜΕΛΕΤΗ ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΕΝΟΣ VPN IPsec ΔΙΚΤΥΟΥ ΜΕ ΧΡΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ OPENSWAN

Σουβλίδης Βασίλης

Αθήνα 2010

Αφιερώνεται στους γονείς μου

Περίληψη

Η αυξανόμενη χρήση του διαδικτύου τόσο στην εργασία όσο και στα οικογενειακά περιβάλλοντα, έχει αυξήσει τις ανάγκες των ίδιων των εταιριών, που προσπαθούν να επεκτείνουν τις επαγγελματικές τους δραστηριότητες και να προωθήσουν τις υπηρεσίες τους ή τα υλικά αγαθά τους, όλο ένα και περισσότερο , μέσα από το διαδίκτυο. Η τεχνολογία των VPNs (Virtual Private Networks) ,έρχεται να δώσει σε πολλές από αυτές τις εταιρίες αλλά και στους αυτόνομους χρήστες την προσβασιμότητα και την επεκτασιμότητα μεταξύ αυτών με μηδαμινό κόστος υλοποίησης αλλά κυρίως με την ασφάλεια των δεδομένων που προσφέρει η τεχνολογία αυτή με βάση το πρωτόκολλο IPSec. Η πλήρης κατανόηση των VPNs, του τι μπορούν να πετύχουν, του τρόπου επέκτασης τους, οι διαφορές μεταξύ των συνδεσμολογιών τους, αλλά και η κατάλληλη διαμόρφωση τους μπορούν να κάνουν τη διαφορά.

Στην εργασία αυτή γίνεται μια προσπάθεια προσέγγισης στο να καταλάβουμε αρχικά τι είναι τα ιδεατά δίκτυα και γιατί να τα χρησιμοποιήσουμε , ποιες είναι οι αρχιτεκτονικές τους και ποια είναι τα πρωτόκολλα που χρησιμοποιούν. Παρουσιάζονται επίσης παραδείγματα εφαρμογής που δείχνουν τη χρήση των ιδεατών αυτών δικτύων σε διαφορετικές συνδεσμολογίες και διαφορετικά σενάρια, επεξηγώντας τον τρόπο τον όποιο πρέπει να εγκατασταθούν και να διαμορφωθούν πάνω από το διαδίκτυο σε πραγματικό περιβάλλον.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον καθηγητή Δρ. Χρήστο Ξενάκη για την επίβλεψη και τη βοήθεια που μου παρείχε για την ολοκλήρωση της διπλωματικής μου εργασίας.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1 Αντικείμενο και σκοπός της πτυχιακής εργασίας

Τα VPN μας επιτρέπουν να δημιουργήσουμε ένα ασφαλές ιδιωτικό δίκτυο πάνω από ένα δημόσιο δίκτυο, όπως το διαδίκτυο (Internet). Μπορεί να δημιουργηθεί χρησιμοποιώντας το κατάλληλο λογισμικό ή υλικό ή έναν συνδυασμό και των δύο που δημιουργεί έναν ασφαλές σύνδεσμο μεταξύ των μελών πάνω σε ένα δημόσιο δίκτυο. Αυτό επιτυγχάνεται μέσω της κρυπτογράφησης (encryption), της επικύρωσης/πιστοποίησης (authentication), δίοδο πακέτων (packet tunneling) και των αντιπυρικών ζωνών (firewalls). Κατά τη διάρκεια των ετών πολλοί προμηθευτές εργάστηκαν αρκετά για να εφεύρουν μία μέθοδο που να κρύβει τα πακέτα IP σε ένα πρωτόκολλο ασφαλείας. Οι μελετητές άρχισαν να αναρωτιούνται γιατί το πρωτόκολλο TCP/IP δεν αναβαθμίστηκε για να υποστηρίζει επιβεβαίωση γνησιότητας και κρυπτογράφηση. Το ίδιο το δίκτυο είναι ασφαλές και όλα αυτά που χτίζονται επάνω σε αυτό πρέπει να είναι επίσης ασφαλής. Το IPSec είναι η απάντηση σε αυτήν την ερώτηση. Το αντικείμενο της παρούσας εργασίας είναι η μελέτη της τεχνολογίας και της αρχιτεκτονικής των ιδεατών ιδιωτικών δικτύων (Virtual Private Networks). Αν και γίνεται αναφορά και στις τρεις βασικές αρχιτεκτονικές (Intranet, Extranet, Remote Access) αλλά και στα κύρια πρωτόκολλα πάνω στα οποία στηρίζονται (IPSec ,L2TP, PPTP, L2F) το ενδιαφέρον μας εστιάζεται στην ανάλυση των Intranet VPN χρησιμοποιώντας ως πρωτόκολλο ανάπτυξης τους το Internet Protocol Security (IPSec).

Συνοπτικά, οι στόχοι της εργασίας είναι:

• η θεωρητική προσέγγιση των επιμέρους τεχνολογιών των VPN ώστε ο αναγνώστης να αποκομίσει μία σφαιρική άποψη για αυτές, να κατανοήσει τις διαφορές τους έτσι ώστε να είναι σε θέση να κρίνει ποια εξ αυτών είναι και η πιο συμφέρουσα λύση στο πρόβλημά του.

• η ανάπτυξη του τρόπου λειτουργίας του πρωτοκόλλου ασφάλειας IPSec, δίνοντας έτσι στον αναγνώστη τη δυνατότητα να αντιληφθεί τα ιδιαίτερα χαρακτηριστικά του, το πώς αυτό συμπεριφέρεται και το ποσοστό ασφαλείας που παρέχει.

• η υλοποίηση ενός Intranet VPN σε Linux (Centos 5.3) χρησιμοποιώντας ως λογισμικό το Openswan (*Openswan* is an implementation of IPsec for Linux) και εκτελώντας βήμα προς βήμα τις ανάλογες ρυθμίσεις (configuration) που απαιτούνται για να διαμορφωθεί το πρωτόκολλο IPSec.

1.2 Διάρθρωση της πτυχιακής εργασίας

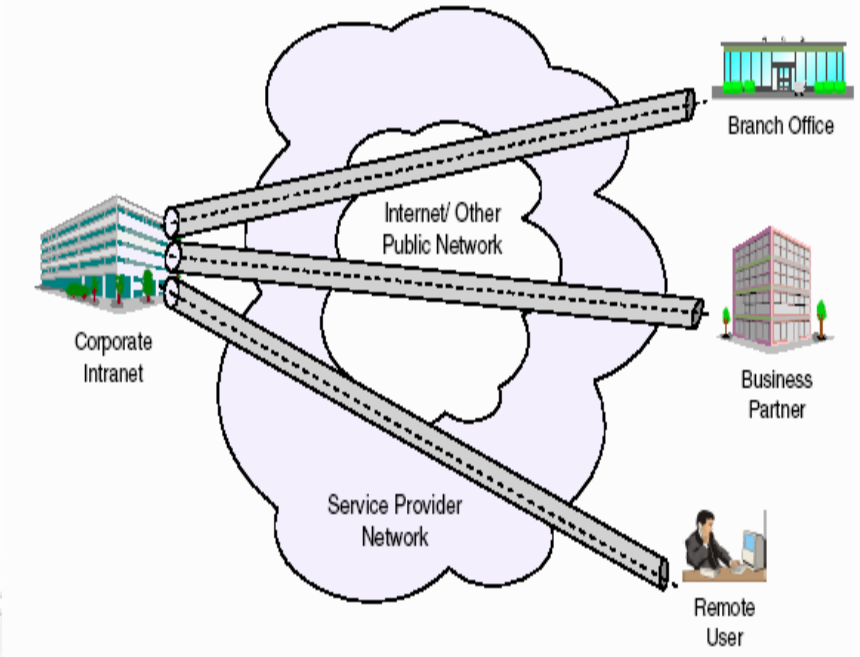
Στο κεφάλαιο 2 σκιαγραφούνται τα γνωστικά πεδία που αποτελούν το επιστημονικό και τεχνολογικό υπόβαθρο πάνω στο οποίο στηρίζεται η εργασία ενώ στο 3ο οι επιμέρους τεχνολογίες αλλά και αρχιτεκτονικές των βασικότερων ειδών VPN. Αναλύονται δηλαδή τα κυριότερα χαρακτηριστικά των Intranet, Extranet και Remote Access VPN κάνοντας παράλληλα και μια σύγκριση μεταξύ τους, εντοπίζοντας έτσι τα πλεονεκτήματα αλλά και μειονεκτήματά τους. Στο 4ο κεφάλαιο γίνεται προσέγγιση των βασικότερων πρωτοκόλλων παρουσιάζοντας τα ιδιαίτερα χαρακτηριστικά τους, κάνοντας εκτενή ανάλυση του πρωτοκόλλου IPSec. Έπειτα στο κεφάλαιο που ακολουθεί θα δούμε όλα τα σενάρια υλοποίησης ενός VPN IPSec δικτύου με εκτενή αναφορά στην παραμετροποίηση των επιμέρους αρχείων του πρωτοκόλλου IPSec. Στο κεφάλαιο 6 θα δούμε κάποια συμπεράσματα και παρατηρήσεις σχετικά με την εργασία μας που προέκυψαν συνοψίζοντας όλα τα προηγούμενα κεφάλαια. Τέλος η εργασία κλείνει με αναφορές στη σχετική βιβλιογραφία και το παράρτημα Α το οποίο μας δείχνει την εγκατάσταση ενός λειτουργικού συστήματος Linux Centos 5.3 καθώς και την εγκατάσταση του λογισμικού OpenSwan.

ΚΕΦΑΛΑΙΟ 2

2. Επιστημονικό και τεχνολογικό υπόβαθρο

2.1 Τι είναι ένα VPN;

Ένα ιδεατό ιδιωτικό δίκτυο (Virtual Private Network) είναι μια επέκταση του ιδιωτικού δικτύου μιας επιχείρησης μέσω ενός δημόσιου δικτύου όπως το Διαδίκτυο, δημιουργώντας μια ιδιωτική ασφαλή σύνδεση, ουσιαστικά μέσω μιας ιδιωτικής σήραγγας. Τα VPNs μπορούν να κάνουν ασφαλή μεταβίβαση πληροφοριών σε ολόκληρο το Διαδίκτυο συνδέοντας τους μακρινούς χρήστες, επιμέρους υποκαταστήματα, και επιχειρησιακούς συνεργάτες σε ένα εκτεταμένο εταιρικό δίκτυο, όπως φαίνεται στην Εικόνα 1.



Εικόνα 1. Εκτεταμένο εταιρικό δίκτυο

Είναι εικονικό:

Αυτό σημαίνει ότι η φυσική υποδομή του δικτύου πρέπει να είναι διαφανής σε οποιαδήποτε σύνδεση VPN. Στις περισσότερες περιπτώσεις επίσης σημαίνει ότι το φυσικό δίκτυο δεν είναι το ιδιωτικό δίκτυο του χρήστη ενός VPN αλλά είναι ένα δημόσιο δίκτυο, μοιραζόμενο με πολλούς άλλους χρήστες. Για να διευκολυνθεί η απαραίτητη διαφάνεια προς τα ανώτερα στρώματα, χρησιμοποιούνται πρωτόκολλα που υποστηρίζουν τεχνική σήραγγας. Για να ξεπεραστούν οι επιπτώσεις της μη ιδιοκτησίας του φυσικού δικτύου, γίνονται συμφωνίες παροχής υπηρεσιών με τους προμηθευτές δικτύων (network providers) για να παρέχουν, με τον καλύτερο δυνατό τρόπο, τις απαιτήσεις απόδοσης και διαθεσιμότητας που είναι αναγκαίες σε ένα VPN.

Είναι ιδιωτικό:

Ο όρος "ιδιωτικός" στο πλαίσιο ενός VPN αναφέρεται στη μυστικότητα της ροής δεδομένων πάνω από το VPN. Όπως αναφέραμε, τα δεδομένα σε ένα VPN συχνά περνούν πάνω από δημόσια δίκτυα και επομένως, πρέπει να υπάρχει πρόνοια ώστε να τηρηθούν συγκεκριμένες απαιτήσεις ασφάλειας:

- Κρυπτογράφηση στοιχείων
- Πιστοποίηση προέλευσης στοιχείων
- Ασφαλή παραγωγή και έγκαιρη ανανέωση των κλειδιών κρυπτογράφησης που απαιτούνται για κρυπτογράφηση και πιστοποίηση
- Προστασία ενάντια στην επανάληψη των πακέτων και των ψεύτικων διευθύνσεων

Είναι ένα δίκτυο

Ακόμη κι αν όχι φυσικά υπαρκτό, ένα VPN πρέπει να γίνει αντιληπτό και να αντιμετωπίζεται ως επέκταση της υποδομής δικτύων μιας επιχείρησης. Αυτό σημαίνει ότι πρέπει είναι διαθέσιμο και στο υπόλοιπο του δικτύου, σε όλο η σε ένα υποσύνολο των

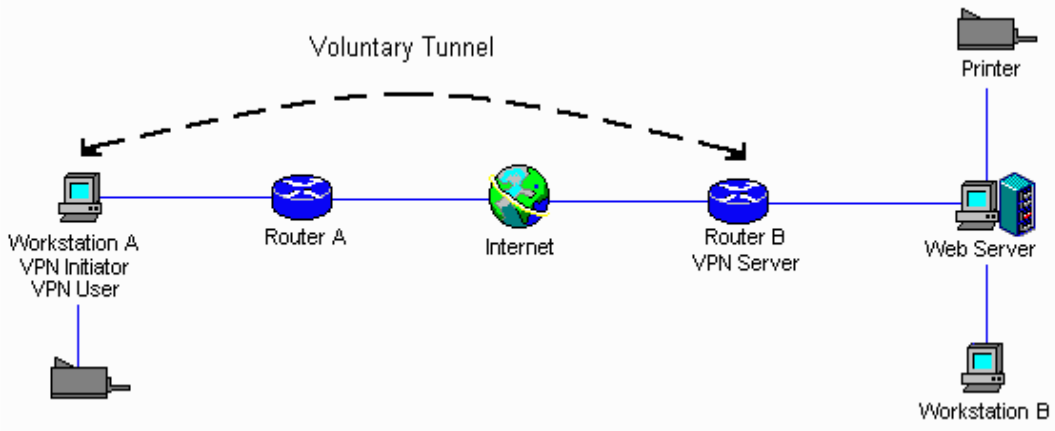
συσκευών και των εφαρμογών, επηρεάζοντας την διευθυνσιοδότηση και την δρομολόγηση. Λέγοντας όλα αυτά, ο όρος "ασφαλείς συνδέσεις σήραγγας" (secure tunneled connections) ίσως να είναι πιο κατάλληλος για να περιγράψει τεχνικά τι είναι ένα VPN, αλλά ο όρος VPN είναι αυτός που έχει επικρατήσει.

2.2 VPN Tunnel Type

Η φράση «VPN τούνελ» συσχετίζεται με τρεις πλευρές : χρήστη (user) VPN, αρχικοποιητής (initiator) VPN και εξυπηρετητή (server) VPN. Έτσι μπορούμε να έχουμε δυο διαφορετικά είδη VPN τούνελ : εθελοντικό (voluntary) και υποχρεωτικό (compulsory).

2.2.1 Εθελοντικά τούνελ (Voluntary Tunnels)

Ένα εθελοντικό τούνελ απαιτεί από το πελάτη (client) να έχει την δυνατότητα να διαχειρίζεται το δικό του VPN τούνελ , όπως φαίνεται στην Εικόνα 2.



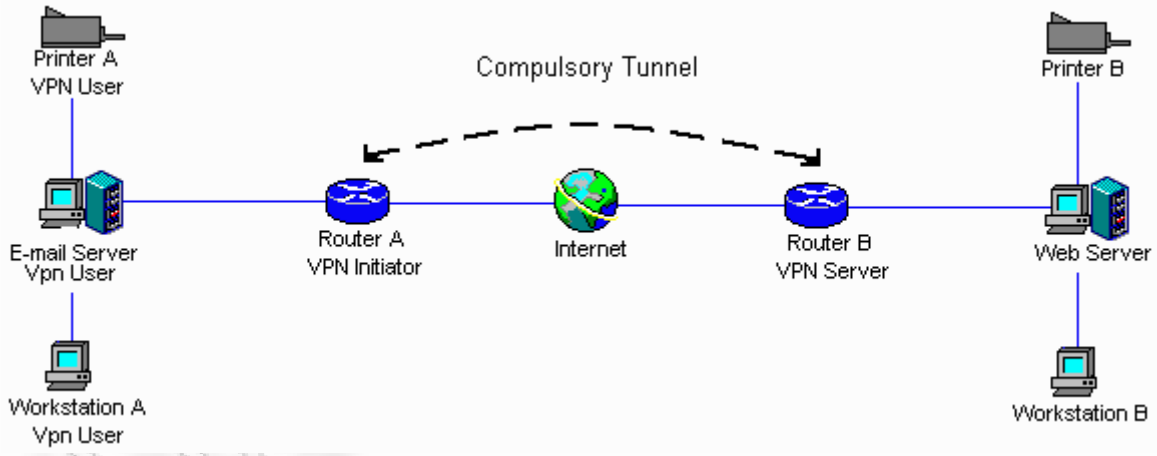
Εικόνα 2. Εθελοντικό τούνελ

Σε αυτό το σενάριο, όταν τα δεδομένα προορίζονται για το εταιρικό δίκτυο, τότε στέλνονται μέσω του τούνελ που εγκαθίσταται από τον πελάτη. Το θετικό σε αυτή την περίπτωση είναι ότι ο χρήστης VPN είναι επίσης και VPN initiator. Κατά συνέπεια αυτό επιτρέπει στο χρήστη VPN να εγκαταστήσει ένα VPN για όσο χρόνο είναι συνδεδεμένος στο Internet. Το σενάριο αυτό είναι ιδιαίτερα επωφελές όταν χρησιμοποιείται από κινητούς χρήστες. Πλεονέκτημα επίσης είναι το ότι ο VPN server δεν χρειάζεται απαραίτητα να είναι

ένας δρομολογητής (router). Το ρόλο του VPN server μπορεί εύκολα να παίξει ο Web Server B η ο Workstation B. Άλλο ένα πλεονέκτημα είναι το ότι η ανάπτυξη τους μπορεί να γίνει αρκετά γρήγορα. Και αυτό όχι επειδή η εγκατάσταση τον απαιτούμενων στοιχείων γίνεται πιο γρήγορα, αλλά επειδή μειώνεται ο αριθμός τον ανθρώπων που χρειάζεται να εμπλακούν. Το μειονέκτημα σε ένα εθελοντικό τούνελ είναι το ότι ο χρήστης του υπολογιστή πρέπει να εγκαταστήσει ειδικό λογισμικό για να μπορεί να διαχειριστεί το δικό του VPN. Αυτό μπορεί να κάνει την ανάπτυξη δύσχρηστη καθώς ένα VPN client εγκαθίσταται «βαθιά» στο λειτουργικό σύστημα και μπορεί να παρουσιαστεί πρόβλημα σε σχέση με τα προϋπάρχοντα προγράμματα. Τα εθελοντικά τούνελ συνήθως χρησιμοποιούνται στα Remote Access VPNs από τους κινητούς χρήστες επειδή σε αυτή την περίπτωση δεν γνωρίζουμε την πηγή τις δικτυακής σύνδεσης. Επίσης θα μπορούσε να είναι η καλύτερη λύση για βραχυπρόθεσμα έργα σε Extranet VPNs .

2.2.2 Υποχρεωτικά τούνελ (Compulsory Tunnels)

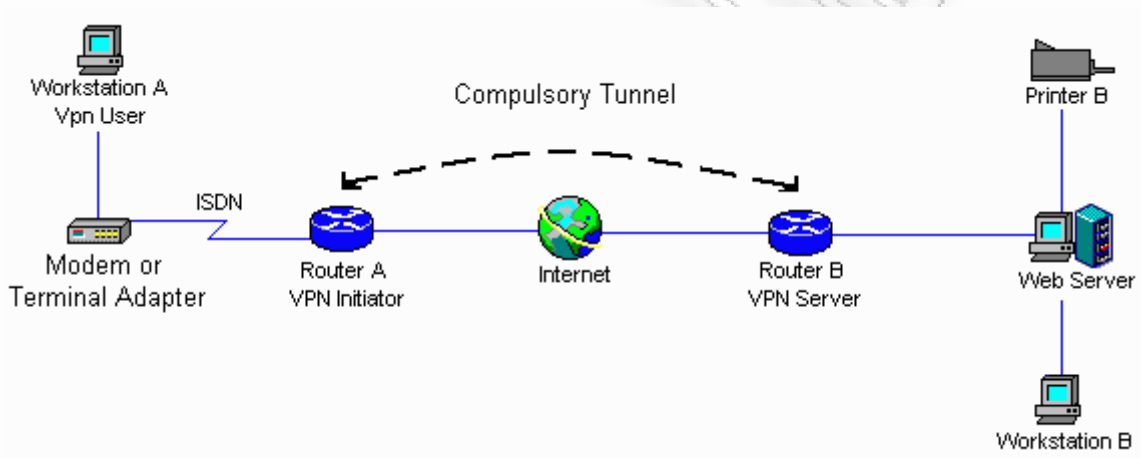
Ένα υποχρεωτικό τούνελ είναι εντελώς διαφανές στον τελικό χρήστη. Η εικόνα 1-5 δείχνει ένα παράδειγμα ενός VPN που χρησιμοποιεί ένα υποχρεωτικό τούνελ.



Εικόνα 3. Υποχρεωτικό τούνελ

Σε αυτό το παράδειγμα τα μέρη που είναι συνδεδεμένα στο δρομολογητή A χρειάζεται να χρησιμοποιήσουν το τούνελ εάν θέλουν να έχουν πρόσβαση στους πόρους η τις συσκευές που είναι συνδεδεμένα στο δρομολογητή B. Αυτού του είδους τούνελ

χρειάζονται μια συντονισμένη προσπάθεια μεταξύ των διαχειριστών των δρομολογητών A και B . Το πλεονέκτημα σε αυτή την περίπτωση είναι το ότι καμία από τις συσκευές, και στα δυο δίκτυα, δεν χρειάζεται επαναδιαμόρφωση ή κάποιο ειδικό λογισμικό. Αυτό είναι αρκετά σημαντικό για εκείνες τις συσκευές στις οποίες το λογισμικό VPN δεν μπορεί να είναι διαθέσιμο, όπως σε εκτυπωτές η κάποιο παλιό λειτουργικό σύστημα. Το μειονέκτημα σε αυτό το σενάριο είναι το ότι χρειάζεται περισσότερος χρόνος για να αναπτυχθούν νέα τούνελ, επειδή κάθε νέο τούνελ πρέπει πρώτα να διαμορφωθεί, σε αντίθεση με ένα εθελοντικό τούνελ. Αυτός είναι και ο λόγος που χρησιμοποιούνται σε όλα τα είδη VPN, με εξαίρεση τα Remote Access VPNs η αρχιτεκτονική είναι λίγο διαφορετική όπως φαίνεται και στην Εικόνα 4.



Εικονα 4. Υποχρεωτικο τουνελ

2.3 Τα οφέλη ενός VPN

Με την εκρηκτική αύξηση του Διαδικτύου, οι επιχειρήσεις απαιτείται να απαντήσουν στο ερώτημα του πώς μπορούν να εκμεταλλευτούν το Διαδίκτυο με το καλύτερο δυνατόν τρόπο για την επιχείρηση. Αρχικά, οι επιχειρήσεις χρησιμοποιούσαν το Διαδίκτυο για να προωθήσουν την εικόνα τους, τα προϊόντα, και τις υπηρεσίες μέσω των ιστοσελίδων. Ωστόσο, σήμερα, οι δυνατότητες του Διαδικτύου είναι απεριόριστες και η εστίαση έχει μετατοπιστεί στο ηλεκτρονικό εμπόριο, χρησιμοποιώντας τη σφαιρική προσιτότητα του Διαδικτύου για την εύκολη πρόσβαση σε επιχειρησιακές εφαρμογές και δεδομένα. Οι επιχειρήσεις ψάχνουν την καλύτερη λύση που θα προσφέρει ασφαλής και επικερδής επέκταση της προσιτότητας των εφαρμογών και των δεδομένων τους ανά τον

κόσμο. Ενώ οι web εφαρμογές μπορούν να χρησιμοποιηθούν για να επιτύχουν αυτό το σκοπό, το ιδεατό ιδιωτικό δίκτυο προσφέρει πιο πλήρεις και ασφαλείς λύσεις.

Τα VPNs μεταφέρουν με ασφάλεια τις πληροφορίες στο Διαδίκτυο συνδέοντας τους μακρινούς χρήστες, επιμέρους υποκαταστήματα και επιχειρησιακούς συνεργάτες σε ένα εκτεταμένο εταιρικό δίκτυο, όπως παρουσιάζεται στην Εικόνα 1. Οι φορείς παροχής υπηρεσιών Διαδίκτυου (ISPs) προσφέρουν οικονομική και αποδοτική πρόσβαση στο Διαδίκτυο, επιτρέποντας στις επιχειρήσεις να απομακρύνουν τις ακριβές, μισθωμένες γραμμές τους. Σύμφωνα με έκθεση της Infonetics Research, Inc., μπορεί να υπάρξει μείωση του κόστους σε ποσοστό από 20% έως 47% με την αντικατάσταση των μισθωμένων γραμμών για μακρινές περιοχές με VPNs. Ενώ, για τα remote access VPNs, το κέρδος μπορεί να είναι από 60% έως 80% των εταιρικών δαπανών για τα remote access dial-up.

Επιπλέον, η πρόσβαση μέσω Διαδικτύου είναι διαθέσιμη παγκοσμίως ενώ άλλες λύσεις ή τεχνολογίες μπορεί να μην είναι διαθέσιμες. Μια κατάλληλη λύση VPN πρέπει να καθορίζεται σύμφωνα με τις ανάγκες της επιχείρησης λαμβάνοντας υπόψη τα ακόλουθα ζητήματα:

- Επιχειρησιακές ανάγκες
- Ασφάλεια
- Απόδοση
- Διαλειτουργικότητα της λύσης με τα τρέχοντα συστήματά

Το κλειδί για τη μεγιστοποίηση της αξίας ενός VPN είναι η δυνατότητα των επιχειρήσεων να εξελίσσουν τα VPNs όσο οι επιχειρησιακές ανάγκες τους αλλάζουν και να τα αναβαθμίσουν εύκολα στις καινούριες τεχνολογίες. Οι προμηθευτές που υποστηρίζουν μια ευρεία σειρά υλικού και λογισμικού προϊόντων VPN παρέχουν την ευελιξία να καλύψουν αυτές τις απαιτήσεις. Ίσως εξίσου κρίσιμο στοιχείο είναι η δυνατότητα της επιχείρησης να συνεργαστεί με έναν προμηθευτή που καταλαβαίνει τα ζητήματα της ανάπτυξης ενός VPN. Έτσι, η εφαρμογή ενός επιτυχούς VPN δεν περιλαμβάνει μόνο την τεχνολογία. Η εμπειρία σε θέματα δικτύωσης του προμηθευτή ή της ομάδας που θα σχεδιάσει και υλοποιήσει το VPN παίζει σημαντικό ρόλο σε αυτήν την εξίσωση.

2.4 Βασικές αρχές σχεδιασμού ενός VPN

Παρακάτω παρουσιάζονται συνοπτικά κάποια ερωτήματα που πρέπει μια επιχείρηση να απαντήσει πριν προχωρήσει στην ανάπτυξη ενός VPN.

Ποια σενάρια VPN πρόκειται να εφαρμοστούν;

- Intranet VPN
- Extranet VPN
- Remote Access VPN
- Συνδυασμός των παραπάνω

Ποιες είναι οι εφαρμογές που τρέχουν στο δίκτυο;

Οι εφαρμογές είναι ο βασικότερος παράγοντας και αποτελούν οδηγό για οποιοδήποτε δίκτυο, ως εκ τούτου το ίδιο ισχύει και για τα VPNs. Αυτό σημαίνει ότι πρέπει να αξιολογηθούν τα οφέλη μιας λύσης VPN μέσα από τις απαιτήσεις των εφαρμογών που θέλουμε να υποστηρίξουμε και να παρέχουμε πάνω από το VPN.

Ποια είναι τα απαραίτητα επίπεδα προστασίας;

Αυτό οδηγεί στην εφαρμογή μιας πολιτικής ασφάλειας που καλύπτει τα παρακάτω:

- Πιστοποίηση
- Κρυπτογράφηση

• Ανταλλαγή κλειδιού

• Εκ των προτέρων προστασία μυστικότητας (PFS)

• Από άκρη σε άκρη προστασία

• Απόδοση

• Καταγραφή γεγονότων

• Νομικά ζητήματα

Θα υπάρξει στο μέλλον επέκταση της τοπολογίας VPN;

Η επεκτασιμότητα είναι συχνά ένα σημαντικό κριτήριο για ένα δίκτυο. Σε ένα VPN περιλαμβάνονται ζητήματα όπως τα εξής:

• Δυναμικά (IKE) ή χειροκίνητα τούνελ

• Προμοιραζόμενα κλειδιά ή πιστοποιητικά

• Δημόσια υποδομή κλειδιού (PKI)

• Γεωγραφική έκταση

• Κόστος της εφαρμογής

Πως θα είναι η υποδομή του VPN και ποιος θα το υποστηρίξει;

Αυτό περιλαμβάνει θέματα όπως τα εξής:

• Εύρος ζώνης ISP, γεωγραφική παρουσία και σχέδια πρόσβασης

• Υποστήριξη τεχνολογίας VPN από ISPs (layer-2 tunneling, IPSec,PKI, LDAP)

• Μετάβαση δικτύων

- Τοποθέτηση πυλών (gateway) VPN
- Ποιότητα των υπηρεσιών (QoS) και επιπέδων υπηρεσιών (SLAs)
- Δημόσια υποδομή κλειδιού (PKI)
- Κόστος της εφαρμογής και της υπηρεσίας

Πώς θα διαχειρίζεται το VPN;

Αυτό περιλαμβάνει, μεταξύ των άλλων, τα ακόλουθα ζητήματα:

- Πολιτικές και καθορισμός διαμόρφωσης
- Υποδομή καταλόγου (π.χ. LDAP)
- Δημόσια υποδομή κλειδιού (PKI)
- Έλεγχος, συναγερμός και καταγραφή
- Πιστοποίηση (π.χ, RADIUS)
- Δρομολόγηση και εφεδρικές γραμμές
- Εξισορρόπηση φορτίων της κυκλοφορίας και των συσκευών
- Ανίχνευση ιών
- Κόστος της εφαρμογής

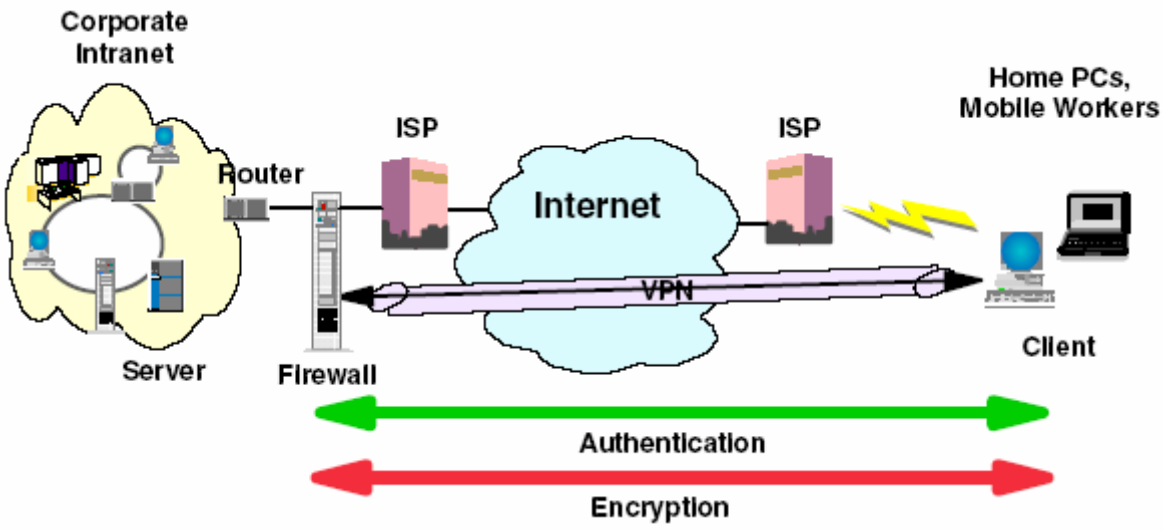
Όπως μπορούμε να δούμε, η λήψη όλων αυτών των αποφάσεων δεν είναι εύκολη και απαιτεί χρόνο, επίσης κανείς δεν μπορεί να μας εγγυηθεί ότι όλα θα γίνουν με το σωστό τρόπο.

ΚΕΦΑΛΑΙΟ 3

3. Αρχιτεκτονικές VPN

3.1 Remote Access VPNs

Ένας απομακρυσμένος χρήστης, είτε στο σπίτι είτε εκτός αυτού, θέλει να είναι σε θέση να επικοινωνήσει με ασφάλεια και χωρίς μεγάλο κόστος με το εταιρικό του δίκτυό. Αυτό το κόστος μπορεί να ελαχιστοποιείται πολύ με την εκμετάλλευση του Διαδικτύου. Παραδείγματος χάρη, ένας χρήστης ο οποίος είναι στο σπίτι ή στο δρόμο αλλά χρειάζεται ένα εμπιστευτικό αρχείο που βρίσκεται σε έναν κεντρικό υπολογιστή μέσα στο εταιρικό δίκτυό. Αποκτώντας πρόσβαση στο Διαδίκτυο μέσω μιας dial-up σύνδεσης σε ένα ISP, μπορεί να επικοινωνήσει με τον κεντρικό υπολογιστή στο εταιρικό δίκτυό και να έχει πρόσβαση στο απαραίτητο αρχείο. Ένας τρόπος να εφαρμοστεί αυτό το σενάριο είναι να χρησιμοποιηθεί ένα πρωτόκολλο εξ' αποστάσεως πρόσβασης όπως L2TP, PPTP ή L2F. Ένας άλλος τρόπος είναι να χρησιμοποιηθεί IPSec πελάτης και μια αντιπυρική ζώνη (firewall), όπως φαίνεται στην Εικόνα 5. Ιδανικά, μπορούν να συνδυαστούν και οι δύο λύσεις που θα παράσχουν την καλύτερη προστασία και τον οικονομικώς πιο αποδοτικό τρόπο για την εξ' αποστάσεως πρόσβαση. Ο πελάτης αποκτά πρόσβαση στο Διαδίκτυο μέσω της dial-up στο ISP, και έπειτα καθιερώνει μια πιστοποιημένη και κρυπτογραφημένη σήραγγα μεταξύ του και της αντιπυρικής ζώνης στο όριο του εταιρικού δικτύου.

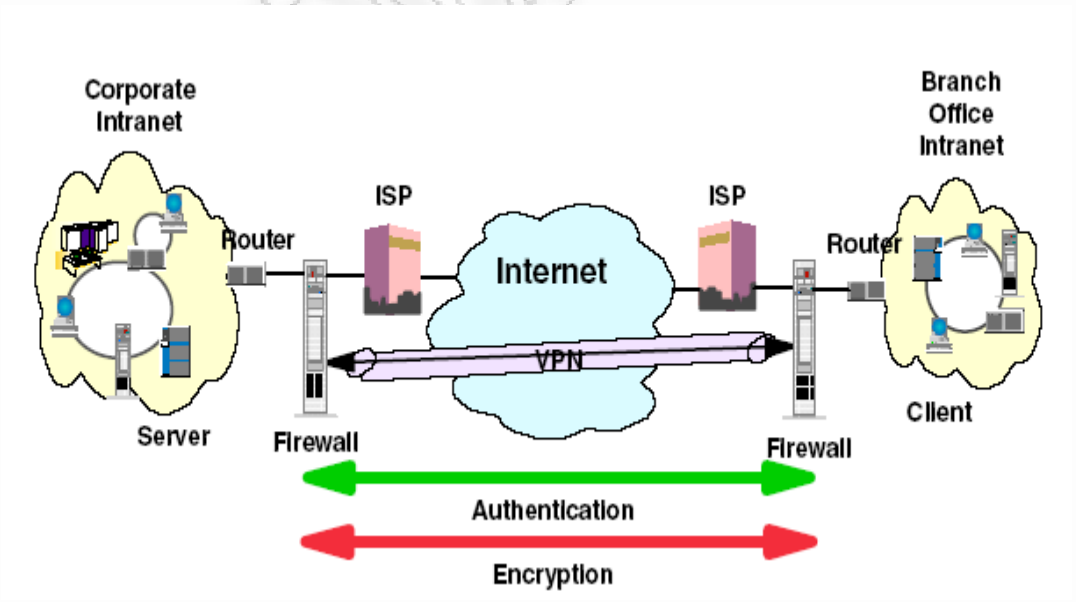


Εικόνα 5. Remote Access VPN

Με την εφαρμογή της πιστοποίησης IPSec μεταξύ του μακρινού πελάτη και της αντιπυρικής ζώνης, μπορούμε να προστατεύσουμε το δίκτυό μας από τα ανεπιθύμητα και ενδεχομένως κακόβουλα πακέτα IP. Επίσης με την κρυπτογράφηση της ροής δεδομένων μεταξύ του μακρινού χρήστη και της αντιπυρικής ζώνης, μπορούμε να αποτρέψουμε τους ξένους από να «κρυφακούν» τις πληροφορίες μας.

3.2 Intranet VPNs (Branch office interconnections)

Η αρχιτεκτονική αυτή εφαρμόζεται για να συνδεθούν με ασφάλεια δύο intranets . Η εστίαση ασφάλειάς δρομολογείται στο να προστατεύσει τα intranets της επιχείρησής ενάντια στους εξωτερικούς εισβολείς και η εξασφάλιση των δεδομένων της ενώ κυκλοφορούν στο δημόσιο Διαδίκτυο. Παραδείγματος χάρη, ας υποθέσουμε ότι η έδρα της εταιρίας θέλει να ελαχιστοποιήσει τις δαπάνες που προέρχονται από την επικοινωνία με και μεταξύ τον παραρτημάτων της . Έτσι, η επιχείρηση μπορεί ήδη να χρησιμοποιεί frame relay ή/και μισθωμένες γραμμές αλλά θέλει να εξερευνήσει άλλες επιλογές, για να μεταφέρει τα εσωτερικά εμπιστευτικά στοιχεία της, που θα είναι λιγότερο ακριβές, πιο ασφαλείς, και συνολικά προσιτές. Με την εκμετάλλευση του διαδικτύου, η σύνδεση μέσω VPN μπορεί να καθιερωθεί εύκολα και να ικανοποιήσει τις ανάγκες της επιχείρησης.



Εικόνα 6. Intranet VPN

Όπως φαίνεται στην Εικόνα 6 , ένας τρόπος να εφαρμοστεί αυτή η σύνδεση VPN μεταξύ της έδρας της εταιρίας και ενός από τα απομακρυσμένα γραφεία είναι να αγοράσει η επιχείρηση πρόσβαση στο Διαδίκτυο από ένα ISP. Αντιπυρικές ζώνες ή δρομολογητές με ενσωματωμένη λειτουργία αντιπυρικών ζωνών, ή σε μερικές περιπτώσεις ένας κεντρικός υπολογιστής με την ικανότητα IPSec, θα τοποθετούνταν στο όριο του καθενός από τα intranets για να προστατεύσει την εταιρική κίνηση από τους hackers του Διαδίκτυου.

Με αυτό το σενάριο, οι πελάτες και οι κεντρικοί υπολογιστές δεν χρειάζονται τεχνολογία υποστήριξης IPSec, δεδομένου ότι οι IPSec - αντιπυρικές ζώνες (ή δρομολογητές) παρέχουν την απαραίτητη πιστοποίηση και κρυπτογράφηση των πακέτων. Με αυτήν τη προσέγγιση, οποιεσδήποτε εμπιστευτικές πληροφορίες θα κρύβονταν από μη εμπιστευόμενους χρήστες, μέσω της αντιπυρικής ζώνης που αρνείται την πρόσβαση στους πιθανούς επιτιθέμενους.

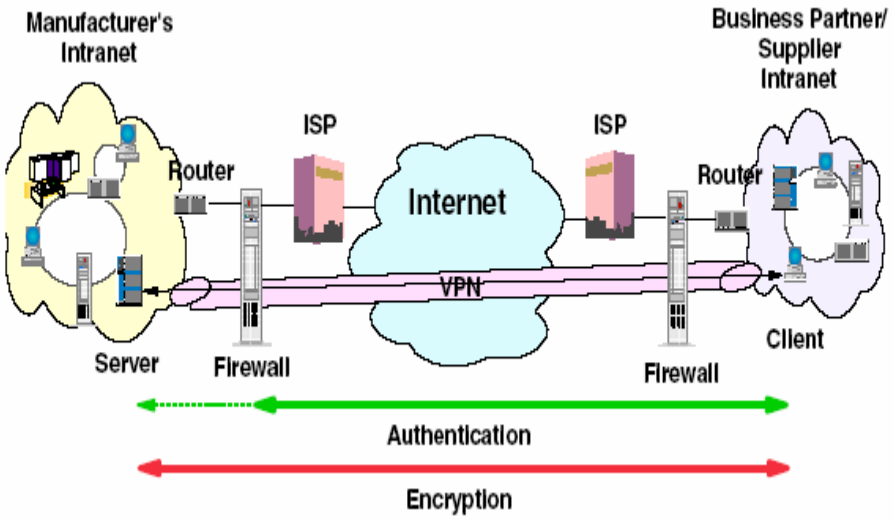
Με την καθιέρωση της σύνδεσης VPNs, η έδρα της επιχείρησης θα είναι σε θέση να επικοινωνήσει ασφαλώς και επικερδώς με τα παραρτήματα, είτε είναι τοποθετημένα τοπικά είτε απομακρυσμένα. Μέσω της τεχνολογίας VPN, κάθε κλάδος μπορεί επίσης να επεκτείνει την προσιτότητα του υπάρχοντος ενδοδικτύου του για να ενσωματώσει άλλα intranets, χτίζοντας έτσι ένα εκτεταμένο εταιρικό δίκτυο. Με τη σειρά τους αυτές οι επιχειρήσεις μπορούν εύκολα να επεκτείνουν αυτό το πρόσφατα δημιουργημένο περιβάλλον για να περιλαμβάνουν τους επιχειρησιακούς συνεργάτες, προμηθευτές, και μακρινούς χρήστες, μέσω της χρήσης IPSec τεχνολογίας.

3.3 Extranet VPNs (Business partner/supplier networks)

Οι επιχειρήσεις θέλουν να μπορούν να επικοινωνήσουν ανέξοδα και με ασφάλεια με τους επιχειρησιακούς συνεργάτες, τα υποκαταστήματα, και τους προμηθευτές τους. Πολλές επιχειρήσεις έχουν επιλέξει να εφαρμόσουν frame relay ή/και μισθωμένες γραμμές για να επιτύχουν αυτήν την αλληλεπίδραση. Αλλά αυτό είναι συχνά ακριβό και η γεωγραφική προσιτότητα μπορεί να είναι περιορισμένη. Η τεχνολογία VPN προσφέρει μια εναλλακτική λύση για τις επιχειρήσεις για να χτίσουν έναν ιδιωτικό και οικονομικώς αποδοτικό εκτεταμένο εταιρικό δίκτυο με παγκόσμια κάλυψη, κάνοντας εκμετάλλευση του Διαδικτύου ή άλλου δημόσιου δικτύου. Ας πάρουμε για παράδειγμα ένα σημαντικό προμηθευτή μιας επιχείρησης. Δεδομένου ότι είναι κρίσιμο να παρέχει συγκεκριμένα υλικά και ποσότητες στον ακριβή χρόνο που απαιτείται από την επιχείρηση, θα πρέπει πάντα να γνωρίζει τον κατάλογο και το πρόγραμμα παραγωγής. Εάν έως τώρα χειρίζεται αυτήν την αλληλεπίδραση χειροκίνητα, στοιχείο που είναι χρονοβόρο, έχει μεγάλο κόστος και ίσως

είναι ακόμα και ανακριβής. Έτσι θα επιθυμούσε να βρει έναν ευκολότερο, γρηγορότερο, και αποτελεσματικότερο τρόπο για την επικοινωνία. Εντούτοις, λαμβάνοντας υπόψη την εμπιστευτικότητα και την εξαρτώμενη από τον χρόνο φύση που έχουν αυτές οι πληροφορίες, η επιχείρηση δεν θέλει να δημοσιευθούν αυτά τα στοιχεία στην εταιρική ιστοσελίδα ή να τα διανέμει χρησιμοποιώντας κάποια εξωτερική έκθεση. Για να λύσουν αυτά τα προβλήματα, ο προμηθευτής και η επιχείρηση μπορούν να εφαρμόσουν το VPN, όπως φαίνεται στην Εικόνα 7.

Ένα VPN μπορεί να χτιστεί μεταξύ ενός υπολογιστή πελάτη, που βρίσκεται στο ενδοδίκτυο του προμηθευτή, και του εξυπηρετητή που βρίσκεται στο ενδοδίκτυο της επιχείρησης. Οι πελάτες μπορούν να πιστοποιηθούν μέσω αντιπυρικής ζώνης ή μέσω του δρομολογητή που προστατεύει το ενδοδίκτυο της επιχείρησης. Κατόπιν θα μπορούσε να καθιερωθεί μια σήραγγα, κρυπτογραφώντας όλα τα πακέτα που φεύγουν από τον πελάτη, μέσω του Διαδικτύου, προς τον εξυπηρετητή.



Εικόνα 7. Extranet VPN

Με την καθιέρωση αυτού του τύπου VPN, ο προμηθευτής μπορεί να έχει πάντα σφαιρική και on-line πρόσβαση στα κατάλογο και το προγράμματα παραγωγής, κατά τη διάρκεια της ημέρας ή της νύχτας. Γεγονός που ελαχιστοποιεί τα χειρωνακτικά λάθη και που εξαλείφει την ανάγκη για πρόσθετους πόρους, στην περίπτωση της ανακοίνωσης. Επιπλέον, η επιχείρηση μπορεί να είναι σίγουρη ότι τα δεδομένα είναι ασφαλή και εύκολα διαθέσιμα μόνο στα προοριζόμενα μέρη.

Ένας τρόπος να εφαρμοστεί αυτό το σενάριο από τις επιχειρήσεις, είναι να αγοραστεί πρόσβαση στο Διαδίκτυο από έναν ISP. Έπειτα, λαμβάνοντας υπόψη την έλλειψη ασφάλειας στο Διαδίκτυο, για να προστατεύσει τα intranets από τους εισβολείς μπορεί να αναπτύξει είτε μια αντιπυρική ζώνη, είτε IPSec δρομολογητή, είτε έναν εξυπηρετητή με IPSec. Εάν επιδιώκεται από άκρη σε άκρη προστασία, τότε το IPSec πρέπει να είναι ενεργοποιηθεί και στον πελάτη και στον εξυπηρετητή. Μέσω της εφαρμογής αυτής της τεχνολογίας VPN, η επιχείρηση θα είναι ικανή να επεκτείνει εύκολα την προσιτότητα του υπάρχοντος εταιρικού δικτύου ώστε να συμπεριλάβει έναν ή περισσότερους προμηθευτές, απολαμβάνοντας ταυτόχρονα τα οικονομικά οφέλη από τη χρησιμοποίηση του Διαδίκτυου ως backbone. Έτσι, με την ευελιξία της ανοικτής IPSec τεχνολογίας, η δυνατότητα για την επιχείρηση να ενσωματώσει περισσότερους εξωτερικούς προμηθευτές είναι απεριόριστη.

ΚΕΦΑΛΑΙΟ 4

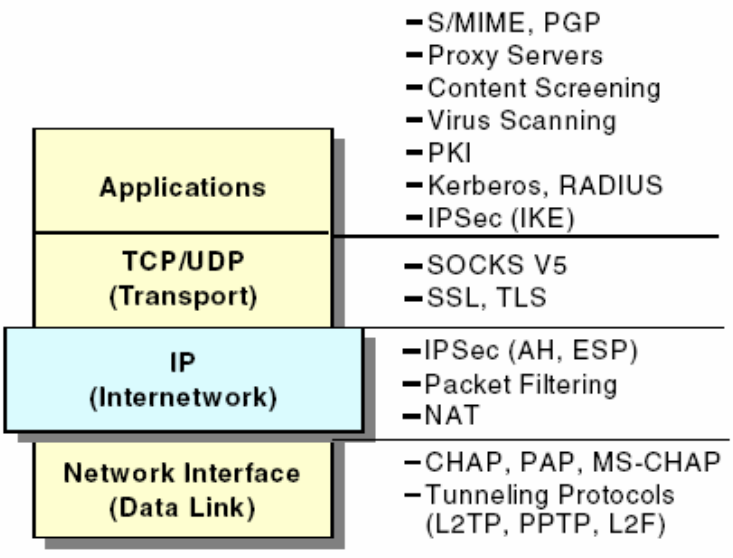
4. Πρωτόκολλα VPN

4.1 Εισαγωγή

Ένας σημαντικός παράγοντας που διαφοροποιεί τα VPN είναι τα πρωτόκολλα όπως και το στρώμα πρωτοκόλλου στο οποίο το VPN πραγματοποιείται. Σε αυτό το πλαίσιο, υπάρχουν οι ακόλουθες διαφορετικές προσεγγίσεις ενός VPN:

- Βασισμένα στο επίπεδο συνδέσμου δεδομένων (layer 2-based)
- Βασισμένα στο επίπεδο δικτύου (IPSec-based)

Υπάρχουν άλλες μέθοδοι που λειτουργούν στα ανώτερα στρώματα που συμπληρώνουν μια VPN λύση, όπως τα SOCKS, Secure Sockets Layer (SSL) και Secure Multipurpose Internet Mail Extension (S-MIME). Μερικές λύσεις προμηθευτών χρησιμοποιούν μόνο τα πρωτόκολλα ανωτέρου στρώματος για να κατασκευάσουν ένα VPN, συνήθως ένας συνδυασμός SOCKS V5 και SSL. Στην παρακάτω εικόνα παρουσιάζεται το μοντέλο διαστρωμάτωσης TCP/IP (TCP/IP layered protocol stack) και τα σχετιζόμενα με το κάθε επίπεδο VPN πρωτόκολλα.



Εικόνα 8. Πρωτόκολλα VPN

4.2 Layer 2 πρωτόκολλα (L2TP, PPTP, L2F)

Μερικά από τα σημαντικότερα layer 2 πρωτόκολλα σήραγγας (tunnel) που χρησιμοποιούνται από τους προμηθευτές των VPN είναι :

Το σημείο-προς-σημείο πρωτόκολλο σήραγγας (PPTP - Point-to-Point Tunnel) το Layer 2 Forwarding (L2F - Στρώμα προς Αποστολή), και το πρωτόκολλο 2ου στρώματος σήραγγας (L2TP - Layer 2 Tunneling Protocol).

Τα πρωτόκολλα σήραγγας δίνουν τη ν δυνατότητα να προσαρμόζονται τετραγωνικοί γόμφοι μέσα σε στρογγυλές τρύπες. Είναι σαν να έχουμε έναν στρογγυλό σωλήνα και να θέλουμε να στείλουμε έναν κύβο μέσα από αυτόν. Ο κύβος πρόκειται να κολλήσει, ή δεν πρόκειται να χωρέσει καθόλου. Ο τρόπος για να χωρέσει είναι να ενθυλακωθεί ο κύβος μέσα σε μια σφαίρα και κατόπιν να σταλεί μέσω του σωλήνα. Με άλλες λέξεις, παίρνουμε κάτι όπου το μέσο μεταφοράς που έχουμε δεν μπορεί να συνεργαστεί μαζί του και το πακετάρουμε μέσα σε κάτι που μπορεί. Όλη η δικτύωση υπολογιστών λειτουργεί με κάποια μέθοδο με τον τρόπο αυτόν. Όλα αυτά τα πρωτόκολλα σήραγγας λειτουργούν με τη σηραγγώδη μορφή του Layer 2 του προτύπου αναφοράς του OSI για πρωτόκολλα επικοινωνιών. Επίσης γνωστό ως Data Link Layer, πάνω από την IP είναι αυτό το στρώμα, όπου πρωτοκόλλα όπως το PPP λειτουργούν. Το PPP χρησιμοποιείται συνήθως για να μεταφέρει την IP και άλλα πρωτόκολλα πέρα από τις τμηματικές και ψηφιακές συνδέσεις. Χαρακτηριστικά οι συνδέσεις PPP γίνονται μεταξύ ενός πελάτη (client) και ενός μακρινού οικοδεσπότη (host), όπως ένας εξ' αποστάσεως πρόσβασης εξυπηρετητή. Επιπλέον, το PPTP, το L2F, και το L2TP χρησιμοποιούνται όλα για να ανοίξουν συνδέσεις PPP μέσω του Διαδικτύου έτσι ώστε να μπορούν να τερματιστούν σε έναν μακρινό οικοδεσπότη. Σε αυτήν την περίπτωση, η σήραγγα ενεργεί ουσιαστικά αντί της γραμμής. Επειδή χρησιμοποιούν την υπάρχουσα υποδομή PPP, αυτά τα πρωτόκολλα αποκομίζουν και τα πλεονεκτήματα του πρωτοκόλλου PPP. Σε αυτά συμπεριλαμβάνεται η δυναμική ανάθεση διευθύνσεων από μια εγκατάσταση ή από το DHCP, η βασισμένη στο χρήστη επιβεβαίωση γνησιότητας και η συμπίεση.

Διαφορές μεταξύ PPTP, L2F και L2TP

Το Σημείο-προς-Σημείο Πρωτόκολλο Σήραγγας αναπτύχθηκε από κοινού από τους μηχανικούς της Ascend Communications, της U.S. Robotics, της 3Com Corporation, της Microsoft Corporation, και της ECI Telematics για να παρέχει ένα ιδεατό ιδιωτικό δίκτυο μεταξύ των χρηστών εξ' αποστάσεως πρόσβασης και των εξυπηρετητών των δικτύων. Συγχρόνως με αυτή την αγορά η Cisco ανέπτυσσε ανεξάρτητα το πρωτόκολλο Layer 2 Farwarding. Δουλεύοντας με την Internet Engineering Task Force (IETF). Η αγορά του PPTP και η Cisco έγιναν ένα για να δημιουργήσουν την προδιαγραφή σχεδίων Διαδικτύου για το πρωτόκολλο 2ου επιπέδου σήραγγας (Level 2 Tunneling Protocol), ένα νέο πρωτόκολλο πυρήνων που συνδυάζει τα καλύτερα χαρακτηριστικά γνωρίσματα του PPTP και του L2F, διατηρώντας συμβατότητα με τα προηγούμενα. Το πρωτόκολλο αυτό ονομάστηκε L2TP. Τόσο το PPTP όσο και το L2F επιτρέπουν σε μας να χρησιμοποιήσουμε οποιαδήποτε μέθοδο επιβεβαίωση γνησιότητας που θα χρησιμοποιούσαμε κανονικά με το PPP, συμπεριλαμβανομένου του PAP και του CHAP, με οποία πρωτόκολλα επιβεβαίωσης γνησιότητας υποστηρίζουν ο πελάτης και ο εξυπηρετητής. Για την κρυπτογράφηση, το PPTP χρησιμοποιεί κρυπτογράφηση RC4 με 40-bit ή με 128-bit κλειδιά . Το L2F, από την άλλη μεριά, υποστηρίζει κρυπτογράφηση DES των 40 ή των 56-bit με τις εκδόσεις 11.2 του IOS της Cisco. Από την έκδοση 11.3(3)T κι έπειτα και υποστηρίζει IPSec, όπου μπορεί επίσης να χρησιμοποιηθεί για να κρυπτογραφήσει μια L2F σύνδεση. Το L2TP συνδυάζει τα καλύτερα χαρακτηριστικά γνωρίσματα του PPTP και του L2F και επιτρέπει είτε συνδέσεις αρχικού-πελάτη είτε απομακρυσμένες συνδέσεις αρχικού -switch L2TP. Μπορούμε να χρησιμοποιήσουμε το L2TP σε οποιαδήποτε κατάσταση όπου μπορεί να χρησιμοποιούσαμε PPTP ή L2F. Μπορεί ακόμα να χρησιμοποιήσει τα ίδια πρωτόκολλα επιβεβαίωσης γνησιότητας με άλλα, συμπεριλαμβανομένου του PAP, του CHAP και του MS-CHAP. Το IPSec είναι ο συνιστώμενος μηχανισμός κρυπτογράφησης για το L2TP. Αν και το L2TP φημιζόταν ότι «θα αντικαταστήσει» το PPTP, η Microsoft επέλεξε να συνεχίσει να παρέχει το PPTP στα Windows NT 5.0 (2000) για εκείνους που δεν επιθυμούν να διατηρήσουν τη δημόσια υποδομή κλειδιού που απαιτείται για το IPSec.

Το PPTP είναι διαθέσιμο στις εκδόσεις των Windows 2000 Server. Επίσης το Linux είναι τώρα σε θέση να υποστηρίξει PPTP. Επιπλέον υπάρχουν διάφορες συσκευές hardware που υποστηρίζουν PPTP. Αυτές οι συσκευές είναι γνωστές ποικιλοτρόπως ως access servers, remote hubs, terminal servers και remote access switches.

4.3 Layer 3 πρωτόκολλα (IPSec)

4.3.1 Εισαγωγή στο IPSec

Το 1992 η IETF (Internet Engineering Task Force) ξεκίνησε την ανάπτυξη μιας σουίτας πρωτοκόλλων, που είχε ως σκοπό την ασφάλεια του δικτύου ανεξάρτητα από τις εφαρμογές. Η ασφάλεια θα επιτυγχάνονταν με την προσθήκη πρωτοκόλλων στο επίπεδο δικτύου τα οποία θα πρόσφεραν υπηρεσίες ασφάλειας. Η σουίτα αυτή ονομάστηκε IPSec (Internet Protocol Security) και αναπτύσσεται από την ομάδα IP Security.

Οι βασικοί **στόχοι** του IPSec, είναι:

- Τα πρωτόκολλα να αναπτυχθούν στο τρίτο επίπεδο (επίπεδο δικτύου).
- Να προσφέρει μυστικότητα, ακεραιότητα και έλεγχο πρόσβασης στα ανώτερα επίπεδα.
- Να είναι ανεξάρτητο από τις εφαρμογές και η υλοποίηση του να μην απαιτεί αλλαγές στις εφαρμογές.
- Να είναι ανεξάρτητο από αλγόριθμους κρυπτογράφησης και πιστοποίησης (ένα κοινό σύνολο από αλγόριθμους θα πρέπει να υλοποιείται σε κάθε σύστημα για να εξασφαλίζεται η διαλειτουργικότητα).
- Να είναι συμβατό με τα υπάρχοντα πρωτόκολλα.

Οι υπηρεσίες ασφάλειας που προσφέρει το IPSec είναι:

- Περιορισμός πρόσβασης

Ο περιορισμός πρόσβασης είναι μια υπηρεσία ασφάλειας, που αποτρέπει την μη εξουσιοδοτημένη χρήση ενός πόρου. Για ένα σταθμό (host) οι πόροι αυτοί μπορεί να είναι,

τα δεδομένα του και η επεξεργαστική του ισχύς. Για μία ασφαλή πύλη αυτοί οι πόροι μπορεί να είναι, το δίκτυο πίσω από αυτή και οι το εύρος ζώνης της διασύνδεσης του με τα υπόλοιπα δίκτυα.

• Πιστοποίηση

Λέγοντας πιστοποίηση για το IPSec, εννοούμε την πιστοποίηση της προέλευσης των δεδομένων. Δηλαδή την διαβεβαίωση ότι τα δεδομένα ήρθαν από τον αρχικό παραλήπτη, χωρίς παραποίηση.

• Εμπιστευτικότητα

Η εμπιστευτικότητα είναι μια υπηρεσία ασφάλειας, που προστατεύει τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση. Το IPSec προστατεύει όλα τα δεδομένα των ανώτερων επιπέδων κρυπτογραφώντας τα. Τα μόνα δεδομένα τα οποία δεν μπορεί να κρυπτογραφήσει, είναι κάποια δεδομένα τα οποία χρησιμοποιούνται για την δρομολόγηση.

• Ακεραιότητα

Το IPSec υποστηρίζει δυο μορφές ακεραιότητας: μία που αφορά την ακεραιότητα του κάθε πακέτου και μία που προστατεύει από την πολλαπλή αποστολή των ίδιων πακέτων.

Τις παραπάνω υπηρεσίες τις προσφέρει το IPSec, εφαρμόζοντας τα πρωτόκολλα ασφάλειας AH (Authentication Header) και ESP (Encapsulation Security Payload).

4.3.2 Εισαγωγικές έννοιες

Συσχέτιση Ασφάλειας SA (Security Association)

Συσχέτιση ασφάλειας είναι ένα κατασκεύασμα για την επιβολή πολιτικής ασφάλειας σε ένα περιβάλλον που υλοποιεί IPSec. Ως συσχέτιση ασφάλειας θεωρούμε μία μονόδρομη λογική σύνδεση μεταξύ δύο συστημάτων που χρησιμοποιούν IPSec. Για την σύνδεση των δύο αυτών συστημάτων απαιτούνται τουλάχιστον δύο συσχετίσεις ασφάλειας, μία για κάθε κατεύθυνση.

Οι συσχετίσεις ασφάλειας μπορεί να είναι στατικές και να έχουν δημιουργηθεί από πριν για τα δυο συστήματα ή να δημιουργούνται δυναμικά όταν τα δύο συστήματα θέλουν να επικοινωνήσουν χρησιμοποιώντας ένα πρωτόκολλο δημιουργίας και διαχείρισης συσχετίσεων, όπως το IKE. Μία συσχέτιση ασφάλειας περιέχει όλες τις πληροφορίες που χρειάζεται ένα σύστημα για την δημιουργία και διαχείριση μίας (μονόδρομης) σύνδεσης. Οι πληροφορίες αυτές περιλαμβάνουν τους αλγόριθμους κρυπτογράφησης και πιστοποίησης, το πρωτόκολλο ασφάλειας που χρησιμοποιείται (AH ή ESP), το χρόνο ζωής της συσχέτισης ασφάλειας (αν δεν είναι στατική) και τον τρόπο με τον οποίο μετράτε ο χρόνος ζωής (σε sec ή KB). Μία συσχέτιση ασφάλειας μπορεί να περιέχει μόνο ένα πρωτόκολλο ασφάλειας. Για να εφαρμόσουμε παραπάνω από ένα πρωτόκολλο ασφάλειας στην επικοινωνία δύο συστημάτων χρησιμοποιούμε μια δέσμη συσχετίσεων (SA bundle).

Δέσμη Συσχετίσεων (SA bundle)

Μια δέσμη συσχετίσεων είναι ένα σύνολο από συσχετίσεις ασφάλειας οι οποίες εφαρμόζονται σε μία (μονόδρομη) σύνδεση μεταξύ δύο ή περισσότερων συστημάτων υπό την απαίτηση μίας πολιτικής ασφάλειας. Η σειρά με την οποία εφαρμόζονται οι συσχετίσεις εξαρτάται από την πολιτική ασφάλειας. Οι συσχετίσεις ασφάλειας που περιέχονται σε μια δέσμη δεν τερματίζουν απαραίτητα στο ίδιο σύστημα. Για παράδειγμα μπορούμε να έχουμε δύο συσχετίσεις σε μια δέσμη, μία από ένα φορητό σταθμό σε μία αντιπυρική ζώνη χρησιμοποιώντας το ESP (για να εξασφαλίσουμε μυστικότητα πάνω από ένα ανασφαλές δημόσιο δίκτυο) και μία δεύτερη συσχέτιση από τον φορητό σταθμό σε έναν σταθμό στο εσωτερικό δίκτυο της ασφαλής πύλης χρησιμοποιώντας το AH (για να προστατευτούμε από τυχόν spoofing επίθεση που έχει γίνει στην ασφαλή πύλη από το εσωτερικό δίκτυο).

Βάση Πολιτικής Ασφάλειας (SPD Security Policy Database)

Η βάση πολιτικής ασφάλειας ή SPD, περιέχει τις υπηρεσίες ασφάλειας που προσφέρονται στα πακέτα. Η SPD ορίζεται από τον διαχειριστή του συστήματος και αποτελεί ένα κεντρικό σημείο για επιβολή πολιτικής σε όλο το σύστημα. Συνήθως οι υλοποιήσεις έχουν μία ξεχωριστή SPD για κάθε δικτυακή διασύνδεση (network interface) που έχει ενεργοποιημένο το IPSec η οποία έχει εγγραφές για εισερχόμενη και εξερχόμενη κίνηση. Η SPD εξετάζεται για όλα τα πακέτα, εισερχόμενα και εξερχόμενα, των δικτυακών διασυνδέσεων που έχουν ενεργοποιημένο το IPSec, συμπεριλαμβανομένων και των πακέτων στα οποία δεν προσφέρει τις υπηρεσίες του το IPSec.

Τα πακέτα αυτά εξετάζονται αφού όταν γίνεται αυτή η επεξεργασία δεν μπορούμε να ξέρουμε αν θα εφαρμοστεί σε αυτά ή όχι (η διαδικασία αυτή θα το κρίνει). Για κάθε πακέτο πρέπει να υπάρχει μία εγγραφή στην SPD που θα αναφέρει πως θα επεξεργαστεί το πακέτο. Τα πακέτα ταιριάζουν στις πολιτικές της SPD με βάση τους selectors. Αν για ένα πακέτο δεν βρεθεί εγγραφή τότε το πακέτο απορρίπτεται και το γεγονός αναφέρεται στο σύστημα (π.χ. μέσω του syslog στο UNIX). Υπάρχουν τρεις περιπτώσεις επεξεργασίας των πακέτων:

- Να απορριφθεί: το πακέτο δεν στέλνεται στο δίκτυο (εξερχόμενη κίνηση), δεν προωθείται στα ανώτερα πρωτόκολλα (εισερχόμενη κίνηση) και δεν δρομολογείται στο εσωτερικό δίκτυο.
- Να μην εφαρμοστεί IPSec: το πακέτο περνάει από την στοίβα χωρίς την επιπλέον προστασία του IPSec.
- Να εφαρμοστεί IPSec: στο πακέτο προσφέρονται υπηρεσίες ασφάλειας του IPSec. Ποιες υπηρεσίες πρωτόκολλα και αλγόριθμοι θα προσφερθούν περιέχεται στο SPD.

Selectors

Οι selectors είναι πεδία στα πακέτα με βάση τα οποία γίνεται η αντιστοίχιση των πακέτων σε πολιτικές ορισμένες στην SPD. Τα πεδία και ο τρόπος αντιστοίχισης θυμίζει την επεξεργασία των πακέτων από stateless firewalls.

Τυπικοί selectors που πρέπει να υποστηρίζει η κάθε υλοποίηση:

- IP διεύθυνση προορισμού.
- IP διεύθυνση πηγής.
- Όνομα (FQDN DNS ή X500).
- Πρωτόκολλο επιπέδου μεταφοράς (TCP, UDP,…). Μπορεί να είναι κρυπτογραφημένο από το ESP.
- Αριθμός θύρας πηγής και προορισμού στα TCP και UDP. Μπορεί να είναι κρυπτογραφημένο από το ESP.

Βάση Συσχετίσεων Ασφάλειας (SAD – Security Association Database)

Η βάση συσχετίσεων ασφάλειας (SAD) περιέχει τις ενεργές συσχετίσεις ασφάλειας ενός συστήματος και τις παραμέτρους των συσχετίσεων αυτών, όπως κρυπτογραφικούς αλγόριθμους, πρωτόκολλα ασφάλειας, χρόνο ζωής κ.α..

Για την εξερχόμενη κίνηση κάθε SA στην SAD συνδέεται με μία εγγραφή στην SPD. Αν το SA στην SAD δεν υπάρχει όταν γίνεται η σύνδεση των συστημάτων τότε δημιουργείται. Για την εισερχόμενη κίνηση κάθε SA στην SAD αντιστοιχεί μοναδικά σε ένα συνδυασμό IP διεύθυνση προορισμού, IPSec πρωτόκολλο (AH ή ESP) και δείκτη παραμέτρων ασφάλειας (SPI).

4.3.3 Επεξεργασία Κίνησης

Εξερχόμενη IP Κίνηση

Κάθε εξερχόμενο πακέτο συγκρίνεται με την SPD για να καθοριστεί τι επεξεργασία θα επιβληθεί στο πακέτο. Αν το πακέτο θα απορριφθεί, αυτό θα αναφερθεί στο σύστημα (auditable event). Αν το πακέτο επιτρέπεται να περάσει, χωρίς την επιβολή του IPSec, τότε αυτό συνεχίζει την πορεία του χωρίς καμία περαιτέρω επεξεργασία από το IPSec. Αν για το πακέτο απαιτείται επιβολή υπηρεσιών του IPSec τότε αυτό αντιστοιχείται σε ένα SA ή SA bundle, ή ένα νέο SA ή SA bundle δημιουργείται για το πακέτο. Σε ένα σταθμό που υλοποιεί sockets, η SPD θα εξετάζεται κάθε φορά που δημιουργείται ένα socket για να αποφασιστεί αν θα προσφερθούν οι υπηρεσίες του IPSec στα πακέτα του socket.

Εισερχόμενη IP κίνηση

Πριν την επεξεργασία του AH ή του ESP τα τυχόν τμήματα του IP πακέτου (IP fragments) συναρμολογούνται. Τα πακέτα τα οποία θα επεξεργαστούν τα πρωτόκολλα AH και ESP αναγνωρίζονται από τον αντίστοιχο αριθμό του πρωτοκόλλου (51 και 50) στο πεδίο επόμενο πρωτόκολλο της επικεφαλίδας του IP. Κάθε πακέτο, το οποίο περιέχει AH ή ESP επικεφαλίδα, αντιστοιχίζεται σε μια συσχέτιση ασφάλειας (SA) σύμφωνα με την IP διεύθυνση προορισμού , το πρωτόκολλο ασφάλειας (AH ή ESP) και τον δείκτη παραμέτρων ασφάλειας. Αν δεν βρεθεί συσχέτιση ασφάλειας στην SAD τότε το πακέτο απορρίπτεται και το γεγονός αναφέρεται στο σύστημα. Αν βρεθεί συσχέτιση ασφάλειας τότε στο πακέτο προσφέρονται οι υπηρεσίες του IPSec τις οποίες απαιτεί η πολιτική (π.χ. κρυπτογράφηση, πιστοποίηση κ.τ.λ).

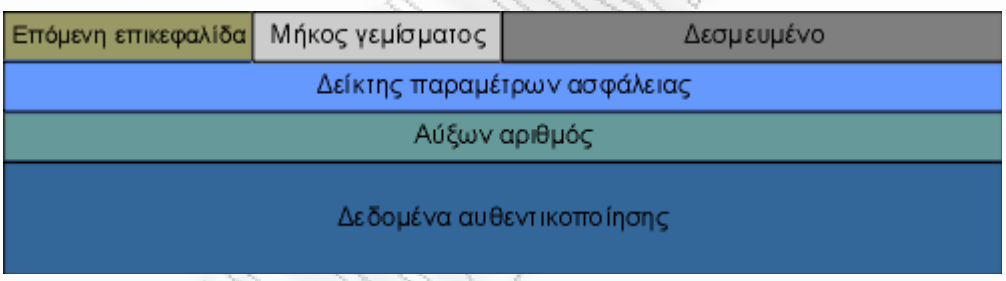
Εάν κατά την διάρκεια της επεξεργασίας προκύψει κάποιο σφάλμα τότε το πακέτο απορρίπτεται και το γεγονός αναφέρεται στο σύστημα. Αν η επεξεργασία τερματίσει με επιτυχία τότε το πακέτο προωθείται στα πρωτόκολλα επιπέδου μεταφοράς (σταθμός) ή δρομολογείται σε κάποια άλλη δικτυακή διασύνδεση (ασφαλής πύλη).

4.3.4 Η επικεφαλίδα AH

Η επικεφαλίδα αυθεντικοποίησης (AH - Authentication Header) είναι ένα πρωτόκολλο, αριθμός πρωτοκόλλου 51) του IPSec που χρησιμεύει στο να μας παρέχει πιστοποίηση της προέλευσης των δεδομένων, αξιοπιστία δεδομένων και προστασία επανάληψης. Το AH μπορεί να χρησιμοποιηθεί μόνο του ή σε συνδυασμό με το ESP. Σε σύγκριση με το ESP το AH δεν παρέχει κρυπτογράφηση των δεδομένων, αλλά προστατεύει τις επικεφαλίδες των πακέτων παρέχοντας αυθεντικοποίηση, κάτι που δεν κάνει από μόνο του το ESP, εκτός αν και αυτά τα πεδία εμπεριέχονται στη κρυπτογράφηση , όπως π.χ. στο tunnel mode.

Παρακάτω θα αναλύσουμε τις λειτουργίες και την δομή του AH.

Πεδία του Authentication Header



Εικόνα 9. Πεδία του Authentication Header

- Επόμενη επικεφαλίδα (next header)

Είναι ένα πεδίο 8-bit που περιέχει τον τύπο του επόμενου σε σειρά τμήματος του πακέτου, μετά τον AH.

- Μέγεθος πακέτου (payload length)

Το μέγεθος του AH σε 32 bit χαρακτήρες

- Δεν χρησιμοποιείται (reserved)

Είναι για μελλοντική χρήση

• Δείκτης παραμέτρων ασφαλείας (security parameters index SPI)

Ένας 32bit αριθμός που σε συνδυασμό με την διεύθυνση προορισμού και το ασφαλές πρωτόκολλο (AH) αναγνωρίζει μοναδικά μια ασφαλή διασύνδεση (SA) για το πακέτο.

• Αύξων αριθμός (sequence index)

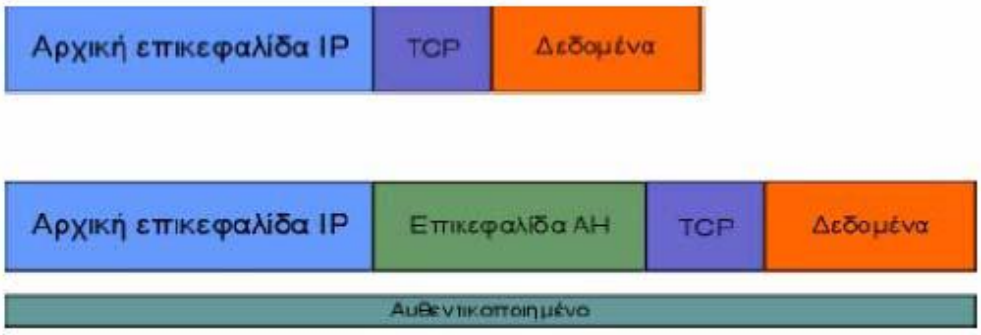
Ένας 32 bit αριθμός χρησιμοποιείται ως μετρητής για την προστασία επανάληψης

• Πληροφορίες Αυθεντικοποίησης (authentication data)

Το πεδίο αυτό περιέχει το ICV του πακέτου. Είναι μεταβλητού μήκους το οποίο πρέπει να είναι πολλαπλάσιο του μήκους 32 bit. Αναλόγως με τον αλγόριθμο που χρησιμοποιούμε το πεδίο μπορεί να γεμίσει με κενές πληροφορίες έτσι ώστε να είναι ακριβές πολλαπλάσιο των 32 bit.

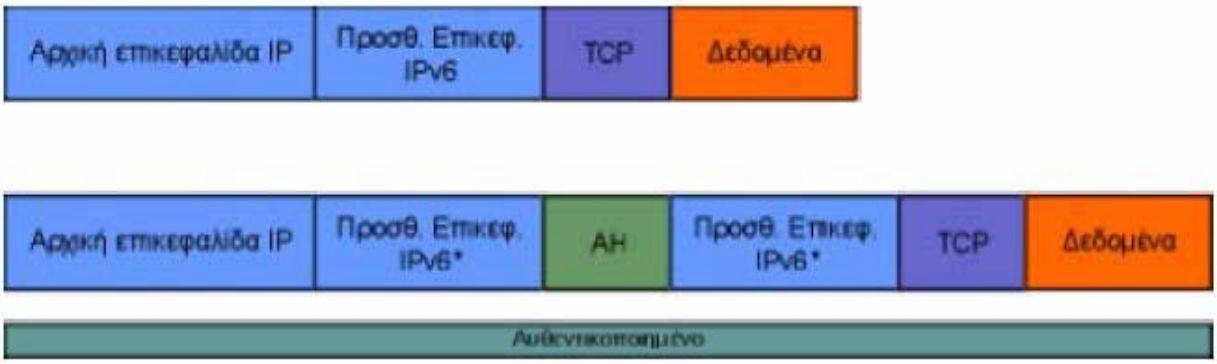
Τοποθεσία του Header

Το AH υποστηρίζει όπως και το ESP, μέθοδο μεταφοράς και μέθοδο σήραγγας. Στην μέθοδο μεταφοράς, το AH μπαίνει μετά την επικεφαλίδα IP του πακέτου και πριν από τις επικεφαλίδες των πρωτοκόλλων που βρίσκονται στο ανώτερο επίπεδο (TCP,UDP,ICMP,OSFP και αλλά). Έτσι λοιπόν, η ενθυλάκωση της επικεφαλίδας AH στο πρωτόκολλο IPv4 γίνεται όπως δείχνει η παρακάτω Εικόνα:



Εικόνα 10. Ενθυλάκωση της επικεφαλίδας AH στο πρωτόκολλο IPv4

Στην περίπτωση του πρωτοκόλλου IPv6 η ενθυλάκωση γίνεται όπως περιγράφει η εικόνα που έπεται:



Εικόνα 11. Ενθυλάκωση της επικεφαλίδας AH στο πρωτόκολλο IPv4

Στο tunnel mode έχουμε δυο διαφορετικές επικεφαλίδες IP, την εσωτερική και την εξωτερική. Το AH μπαίνει μεταξύ τους και προστατεύει όλα τα εσωτερικά πακέτα και τα δεδομένα τους. Ο εσωτερικός IP header περιέχει τις πραγματικές IP διευθύνσεις των σταθμών και ο εξωτερικός τις διευθύνσεις των σταθμών που επικοινωνούν με IPsec.

Λειτουργία πρωτοκόλλου

Ένα πακέτο υπόκειται στον AH μόνο όταν το IPsec καθορίσει ότι το πακέτο ταυτίζεται με μια ασφαλή διασύνδεση. Όταν ένα πακέτο που περιέχει έναν AH φτάσει στον προορισμό του, ο δέκτης καθορίζει ένα SA βασισμένο στη IP διεύθυνση του προορισμού, στο πρωτόκολλο ασφάλειας (AH) και το SPI. Το SA καθορίζει αν ο αύξων αριθμός του πακέτου θα μαρκαριστεί και επιλέγει τον αλγόριθμο που θα χρησιμοποιηθεί για τον υπολογισμό του ICV όπως και το κλειδί για την αναγνώριση του ICV.

Κατάτμηση

Αν χρειαστεί κατάτμηση θα γίνει μετά την ολοκλήρωση του AH στο IPSec. Για αυτό στο transport mode ο AH εφαρμόζεται μόνο σε ολόκληρα πλαίσια δεδομένων του IP και όχι σε κομμάτια.

Τιμή ελέγχου γνησιότητας (Integrity Check Value)

Ο παραλήπτης υπολογίζει την τιμή ελέγχου γνησιότητας με βάση μερικά χαρακτηριστικά του πακέτου που θα αναφέρουμε παρακάτω. Αν αυτή η τιμή είναι ίδια με αυτή που περιέχεται στην επικεφαλίδα του AH τότε το πακέτο είναι γνήσιο, αν όχι, το πακέτο απορρίπτεται και η απόρριψη επισημαίνεται. Το ICV υπολογίζεται από:

- Τα πεδία του IP header που δεν αλλάζουν ή που έχουν ένα προβλέψιμο αριθμό όταν θα φτάσει το πακέτο στον προορισμό του.

- Τον AH

- Από πληροφορίες που ανήκουν στα πιο πάνω επίπεδο και υποτίθεται ότι δεν αλλάζουν κατά τη μεταφορά.

Αν ένα πεδίο στο IP πακέτο μπορεί να αλλαχτεί τότε μηδενίζεται για τον υπολογισμό του ICV. Μηδενίζοντας τα πεδία που δεν χρησιμοποιούνται αντί να τα παραβλέπουμε προστατεύουμε το πακέτο και το μέγεθος των πεδίων του. Κάθε υλοποίηση του IPSec πρέπει να υποστηρίζει τους εξής αλγορίθμους αυθεντικοποίησης.

- HMAC-MD5-96 (RFC 2403)
- HMAC-SHA-1-96 (RFC 2404)

Αν σε ένα πακέτο το πεδίο πληροφοριών της αυθεντικοποίησης και πάλι δεν έχει μήκος 32 bit γεμίζεται με τυχαίους αριθμούς ή μηδενικά ανάλογα με την περίπτωση έτσι ώστε να πληροί τις προδιαγραφές του IPSec.

Πεδία που δεν αλλάζουν

- Έκδοση
- Μέγεθος του internet header
- Συνολικό μέγεθος
- Αναγνώριση
- Πρωτόκολλο
- Διεύθυνση αποστολέα
- Διεύθυνση προορισμού (εξαρτάται από τον τρόπο δρομολόγησης)

Πεδία που αλλάζουν αλλά είναι προβλέψιμα

- Διεύθυνση προορισμού (εξαρτάται από τον τρόπο δρομολόγησης)

Πεδία που μπορούν να αλλαχθούν (μηδενίζονται για τον υπολογισμό του ICV)

- Type of service (TOS)
- Flags
- Fragment Offset
- TTL
- Header Checksum

Τα πεδία αυτά αλλάζουν τις περισσότερες φορές για λόγους που αφορούν την δρομολόγηση των πακέτων. Αν μια επικεφαλίδα ενός πακέτου περιέχει πεδία που αλλάζουν κατά την μεταφορά τότε αυτά πρέπει να μηδενίζονται για τον υπολογισμό του ICV.

Προστασία επανάληψης

Ο μετρητής του αποστολέα μηδενίζεται όταν δημιουργείται ένα SA, και αυξάνεται κατά ένα κάθε φορά που στέλνεται ένα πακέτο. Ο αποστολέας δεν πρέπει να αφήσει τον μετρητή να γυρίσει πάλι από την αρχή, πρέπει να δημιουργήσει ένα καινούργιο SA πριν αυτό συμβεί. Η προστασία επανάληψης θεωρείται ότι είναι ενεργοποιημένη, εκτός αν το αντίθετο ειπωθεί από τον παραλήπτη. Σε μια τέτοια περίπτωση ο μετρητής δεν μηδενίζεται μέχρι να φτάσει στη μέγιστη του τιμή και να γυρίσει πάλι από την αρχή.

Από την πλευρά του παραλήπτη, εάν αυτός έχει ενεργοποιημένη την προστασία επανάληψης, τότε μηδενίζει τον μετρητή του κάθε φορά που δημιουργείται ένα καινούργιο SA. Για κάθε πακέτο που λαμβάνεται, ο αποδέκτης θα πρέπει να επιβλέπει αν ο αύξων αριθμός του πακέτου υπάρχει και σε κάποιο άλλο πακέτο που ανήκει στο ίδιο SA. Αυτό θα πρέπει να γίνεται στην αρχή του ελέγχου για να αποφεύγονται περιττοί έλεγχοι και να επιταχύνεται η όλη διαδικασία. Τα διπλά πακέτα απορρίπτονται.

4.3.5 Η επικεφαλίδα ESP

Η επικεφαλίδα ESP (Encapsulating Security Payload) είναι σχεδιασμένη για να παρέχει υπηρεσίες ασφάλειας στα πρωτόκολλα IPv4 και IPv6. Μπορεί να εφαρμοστεί αυτόνομα, αλλά και σε συνδυασμό με την AH και οι υπηρεσίες ασφάλειας που προσφέρει μπορούν να χρησιμοποιηθούν κατά την επικοινωνία δύο σταθμών, δυο αντιπυρικών ζωνών, αλλά και μεταξύ ενός σταθμού και μιας αντιπυρικής ζώνης.

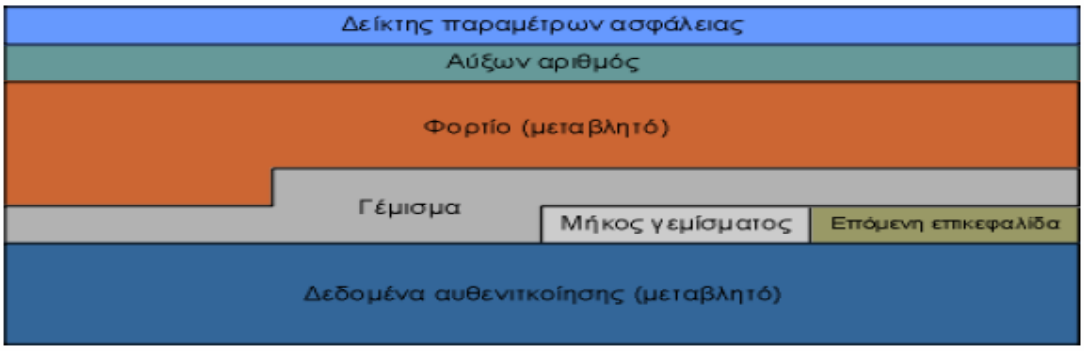
Οι υπηρεσίες ασφάλειας που προσφέρει η επικεφαλίδα ESP είναι:

- Εμπιστευτικότητα (confidentiality)
- Διασφάλιση προέλευσης (data origin authentication)
- Ακεραιότητα (connectionless integrity)
- Προστασία πολλαπλής αποστολής πακέτου (anti-reply)
- Εμπιστευτικότητα ροής κίνησης (traffic flow confidentiality)

Το ποιες από αυτές τις υπηρεσίες θα χρησιμοποιηθούν κατά την διάρκεια μιας σύνδεσης, εξαρτάται από τις παραμέτρους που θα οριστούν κατά την δημιουργία του συνδέσμου ασφάλειας (Security association) για την σύνδεση αυτή. Η εμπιστευτικότητα μπορεί να χρησιμοποιηθεί αυτόνομα. Ωστόσο κάτι τέτοιο δεν έχει νόημα, γιατί χωρίς τις υπηρεσίες διασφάλισης προέλευσης και ακεραιότητας, η σύνδεση είναι ευάλωτη σε ενεργές επιθέσεις, οι οποίες μπορούν να καταστήσουν την υπηρεσία εμπιστευτικότητας άχρηστη. Η υπηρεσία προστασίας πολλαπλής αποστολής μπορεί να εφαρμοστεί μόνο σε συνδυασμό με την διασφάλιση προέλευσης και η χρήση της αφορά μόνο τον παραλήπτη.

Τέλος η υπηρεσία εμπιστευτικότητας ροής κίνησης απαιτεί την εφαρμογή της μεθόδου σήραγγας (tunnel mode) και είναι αποτελεσματική μόνο αν εφαρμοστεί κατά την επικοινωνία μίας αντιπυρικής ζώνης και ενός σταθμού, ή μεταξύ δύο αντιπυρικών ζωνών.

Τα πεδία της επικεφαλίδας ESP



Εικόνα 12. Τα πεδία της επικεφαλίδας ESP

Η επικεφαλίδα ESP περιέχει τα παρακάτω πεδία:

- Δείκτης παραμέτρων ασφάλειας (Security parameter index)

Ο δείκτης παραμέτρων ασφάλειας είναι μία τιμή μήκους 32 bit, η οποία σε συνδυασμό με την διεύθυνση προορισμού προσδιορίζει μονοσήμαντα τον σύνδεσμο ασφάλειας, στον οποίο ανήκει το πακέτο αυτό. Την τιμή αυτή, την επιλέγει συνήθως ο παραλήπτης του πακέτου, κατά την δημιουργία του συνδέσμου ασφάλειας που διέπει την σύνδεση και η ύπαρξή της είναι υποχρεωτική. Οι τιμές από 1 έως 255 είναι δεσμευμένες

από την IANA (Internet Assigned Numbers Authority) για μελλοντική χρήση. Η τιμή 0 είναι δεσμευμένη για τοπική χρήση, ανάλογα με την εκάστοτε υλοποίηση. Μπορεί να χρησιμοποιηθεί για παράδειγμα από το λογισμικό ενός υπολογιστή κατά την δημιουργία ενός συνδέσμου ασφάλειας. Άρα λοιπόν, επικεφαλίδα με δείκτη παραμέτρων ασφάλειας 0, δεν είναι λογικό να ταξιδεύει στο διαδίκτυο .

• Αύξων αριθμός (Sequence number)

Το πεδίο αύξοντος αριθμού είναι υποχρεωτικό και χρησιμοποιείται για την υπηρεσία προστασίας πολλαπλής αποστολής. Ο αύξων αριθμός περιέχεται στο πακέτο, ακόμα και αν ο παραλήπτης δεν επιθυμεί να χρησιμοποιήσει την υπηρεσία αυτή. Κατά την δημιουργία ενός συνδέσμου ασφάλειας ο αριθμός αυτός μηδενίζεται, έτσι ώστε το πρώτο πακέτο που θα στείλει ο αποστολέας πρέπει να έχει την τιμή 1. Αν η υπηρεσία προστασίας πολλαπλής αποστολής είναι ενεργοποιημένη, ο αριθμός αυτός δεν πρέπει ποτέ να ανακυκλωθεί. Αν δηλαδή μεταδοθούν 2^32 πακέτα ο σύνδεσμος ασφάλειας πρέπει να καταστραφεί και να ξεκινήσει ένας νέος, για την συνέχεια της επικοινωνίας.

• Φορτίο (variable-length payload data)

Αυτό το πεδίο περιέχει τα δεδομένα που περιγράφει το πεδίο «Επόμενη επικεφαλίδα». Το μήκος του φορτίου δεν είναι συγκεκριμένο, παρόλα αυτά είναι ακέραιο πολλαπλάσιο του ενός byte. Αν το φορτίο είναι κρυπτογραφημένο με κάποιον αλγόριθμο, ο οποίος απαιτεί δεδομένα συγχρονισμού για την αποκρυπτογράφηση, τότε αυτά τα δεδομένα περιέχονται μέσα σε αυτό το πεδίο.

• Γέμισμα (padding)

Σε πολλές περιπτώσεις απαιτείται η χρήση αυτού του πεδίου. Για παράδειγμα, αν ο αλγόριθμος κρυπτογράφησης που έχει χρησιμοποιηθεί, απαιτεί τα δεδομένα να είναι

πολλαπλάσιο ενός αριθμού από byte, όπως δηλαδή γίνεται στην περίπτωση των αλγορίθμων που χρησιμοποιούν τμήματα (block) δεδομένων. Για αυτόν τον λόγο χρησιμοποιείται το γέμισμα, το οποίο μπορεί να είναι από 0 έως 255 bytes. Αυτό το πεδίο είναι προαιρετικό.

- Μήκος γεμίσματος (pad length)

Το πεδίο μήκος γεμίσματος είναι μία τιμή των 8bit, που δείχνει πόσα byte γεμίσματος έχουν μπει στο πακέτο. Παίρνει δηλαδή τιμές από 0 έως 255, όπου 0 σημαίνει ότι δεν υπάρχει καθόλου γέμισμα.

- Επόμενη επικεφαλίδα (next header)

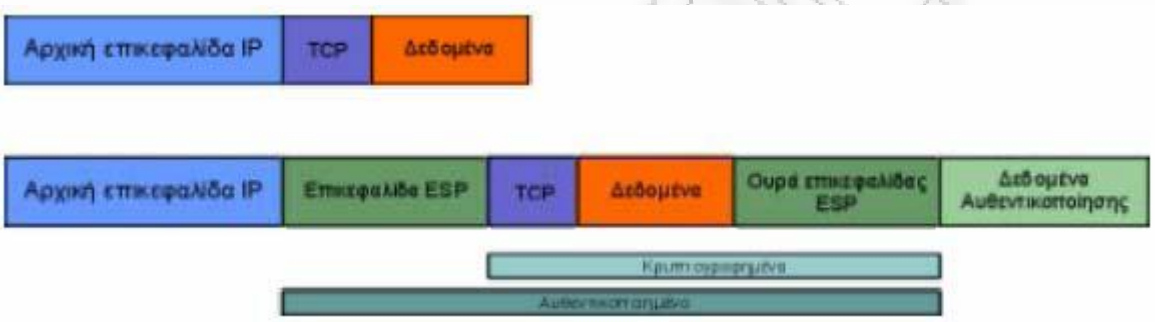
Το πεδίο αυτό έχει μήκος 8 bit και προσδιορίζει τον τύπο των δεδομένων που περιέχονται στο πεδίο φορτίου. Προσδιορίζει δηλαδή, αν το φορτίο περιέχει ένα πακέτο IP ή ένα πακέτο ανώτερου επιπέδου. Οι τιμές αυτού του πεδίου καθορίζονται από την IANA.

- Δεδομένα αυθεντικοποίησης (authentication data)

Το τελευταίο πεδίο, είναι το πεδίο πιστοποίησης, το οποίο είναι μεταβλητού μήκους. Το πεδίο αυτό περιέχει μία τιμή, η οποία υπολογίζεται από το πακέτο ESP χωρίς τα δεδομένα αυθεντικοποίησης και χρησιμοποιείται για έλεγχο ακεραιότητας από τον παραλήπτη. Το μήκος του πεδίου εξαρτάται από τον μηχανισμό ελέγχου που έχει επιλεχθεί. Το πεδίο αυτό είναι προαιρετικό και περιέχεται μόνο αν έχει επιλεχθεί από την υπηρεσία ασφάλειας.

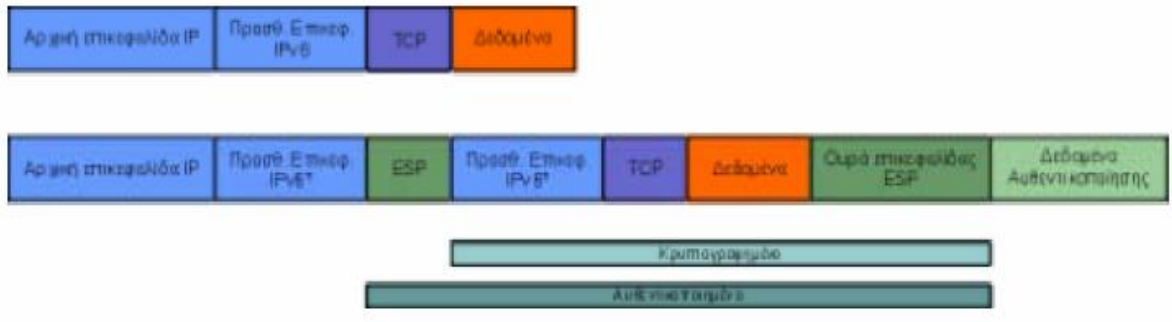
Η θέση της επικεφαλίδας ESP

Η Επικεφαλίδα ESP, όπως και η AH, μπορούν να χρησιμοποιηθούν με δύο μεθόδους. Την μέθοδο σήραγγας και την μέθοδο μεταφοράς. Η επικεφαλίδα ESP τοποθετείται μετά την επικεφαλίδα IP και πριν από την επικεφαλίδα του πρωτοκόλλου του ανώτερου επιπέδου, για παράδειγμα, πριν την επικεφαλίδα του πρωτοκόλλου TCP, που ενδεχομένως ακολουθεί. Για παράδειγμα, στην περίπτωση που θέλουμε να εισάγουμε την επικεφαλίδα ESP σε ένα πακέτο IPv4 το οποίο μεταφέρει ένα πακέτο TCP, η εισαγωγή θα γίνει όπως παρακάτω:



Εικόνα 13. Η θέση της επικεφαλίδας ESP σε IPv4

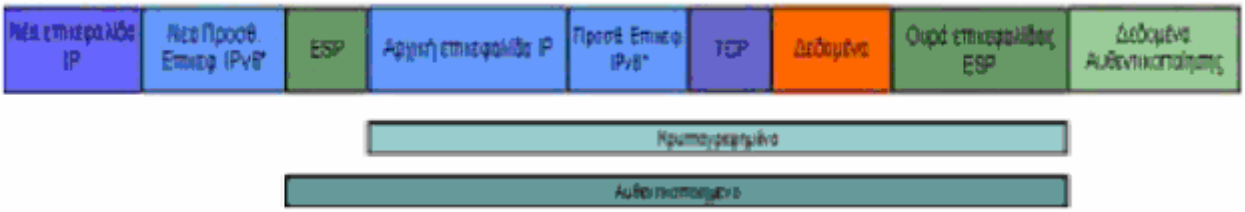
Ενώ στην περίπτωση του πρωτοκόλλου IPv6:



Εικόνα 14. Η θέση της επικεφαλίδας ESP σε IPv6

Όταν εφαρμόζεται σε μέθοδο σήραγγας το πακέτο διαμορφώνεται ως εξής:

Εικόνα 15. Η θέση της επικεφαλίδας ESP σε μέθοδο σήραγγας IPv4



Εικόνα 16. Η θέση της επικεφαλίδας ESP σε μέθοδο σήραγγας IPv6

Λειτουργία πρωτοκόλλου

Οι αλγόριθμοι που χρησιμοποιούνται από το πρωτόκολλο αυτό είναι οι παρακάτω:

- DES_CBC (RFC 2405)
- NULL (RFC 2410)
- CAST-128 (RFC 2451)
- RC5 (RFC 2451)
- IDEA (RFC 2451)
- Blowfish (RFC 2451)
- 3DES (RFC 2451)
- HMAC-MD5-96 (RFC 2403)
- HMAC-SHA-1-96 (RFC 2404)

- NULL (RFC 2410)
- DES-MAC

Κάθε υλοποίηση συμβατή με το IPSec οφείλει να υλοποιεί τουλάχιστον τους DES, HMAC, NULL.

- Διαδικασία εύρεσης σε ποιο σύνδεσμο ασφάλειας ανήκει το πακέτο

Για την διαδικασία αυτή χρησιμοποιείται το πεδίο δείκτη παραμέτρων ασφάλειας (SPI). Για κάθε σύνδεσμο ασφάλειας καθορίζεται (συνήθως από των παραλήπτη) αυτός ο αριθμός. Έστω ένας υπολογιστής λαμβάνει ένα πακέτο, με τιμή Α σε αυτό το πεδίο. Τότε αναζητά ποιος σύνδεσμος ασφάλειας από αυτούς που έχει αποκαταστήσει, έχει ως δείκτη παραμέτρων ασφάλειας αυτήν την τιμή.

Αν δεν βρεθεί κανένας σύνδεσμος ασφάλειας με αυτήν την τιμή, τότε το πακέτο απορρίπτεται. Αν βρεθεί τότε συνεχίζεται η επεξεργασία του πακέτου.

- Προστασία πολλαπλής παραλαβής πακέτου

Κάθε φορά που ο αποστολέας στέλνει ένα πακέτο, αυξάνει την τιμή που είχε πριν ο μετρητής του αύξοντος αριθμού για αυτό τον σύνδεσμο ασφάλειας. Ο παραλήπτης, όταν παραλαμβάνει ένα πακέτο περιμένει ο αύξων αριθμός του να είναι κατά ένα μεγαλύτερος από τον αντίστοιχο αριθμό του προηγούμενου πακέτου. Αν αυτό δεν ισχύει, τότε το πακέτο απορρίπτεται. Επίσης θεωρείται δεδομένο, ότι η αρίθμηση αυτή αρχίζει από το 1 και ότι το πρώτο πακέτο ενός συνδέσμου ασφάλειας έχει αύξων αριθμό 1. Αυτός ο μηχανισμός ασφάλειας, είναι στο χέρι του παραλήπτη να τον χρησιμοποιήσει, ωστόσο ο αποστολέας οφείλει να τον αυξάνει, εκτός και αν ο παραλήπτης του πει να μην κάνει κάτι τέτοιο κατά την δημιουργία του συνδέσμου ασφάλειας.

• Σύγκριση Τιμής ελέγχου ακεραιότητας

Ο αποστολέας υπολογίζει μία τιμή, με την χρήση της συνάρτησης κατακερματισμού (hash function) που έχει αποφασιστεί κατά την δημιουργία του συνδέσμου ασφάλειας. Ως είσοδος σε αυτήν την συνάρτηση μπαίνουν όλα τα πεδία του πακέτου, εκτός του πεδίου αυθεντικοποίησης. Αυτός ο υπολογισμός, γίνεται πάντα μετά την κρυπτογράφηση. Ο παραλήπτης, αφού αφαιρέσει το πεδίο αυθεντικοποίησης, χρησιμοποιεί και αυτός την ίδια συνάρτηση. Αν η τιμή που θα υπολογίσει ο παραλήπτης, είναι ίση με την τιμή που έχει βάλει ο αποστολέας στο πεδίο αυθεντικοποίησης, τότε και μόνο το πακέτο γίνεται δεκτό, στην αντίθετη περίπτωση απορρίπτεται.

• Τεμαχισμός

Αν κριθεί απαραίτητο να τεμαχιστεί κάποιο πακέτο, τότε αυτό γίνεται αφού εισάγουμε την επικεφαλίδα ESP. Με άλλα λόγια ως φορτίο για την επικεφαλίδα ESP δεν πρέπει ποτέ να μπαίνει ένα τεμάχιο ενός πακέτου. Για αυτό και αν κάποιος παραλάβει ένα πακέτο ESP, το οποίο περιέχει ως φορτίο ένα πακέτο με μη μηδενικό πεδίο μετατόπισης, ή με την σημαία «περισσότερα τεμάχια» ενεργή, τότε το πακέτο ESP θεωρείται άκυρο και απορρίπτεται.

• Κρυπτογράφηση και αποκρυπτογράφηση

Ο αποστολέας τοποθετεί στο πεδίο φορτίου τα δεδομένα, τα οποία στην περίπτωση της μεθόδου μεταφοράς είναι το πακέτο του ανώτερου επιπέδου και στην περίπτωση σήραγγας όλο το αρχικό IP πακέτο. Στην συνέχεια προσθέτει όσα byte γεμίσματος είναι απαραίτητα. Τέλος κρυπτογραφεί με τον αλγόριθμο που υπαγορεύει ο σύνδεσμος ασφάλειας τα πεδία φορτίου, γεμίσματος, μήκος γεμίσματος και επόμενο πεδίο. Ο παραλήπτης όταν παραλάβει το πακέτο αποκρυπτογραφεί με την σειρά του τα πεδία αυτά και υποβάλει το πακέτο σε περαιτέρω επεξεργασία.

4.3.6 Διαχείριση κλειδιών και συσχετίσεων ασφάλειας

Η διαχείριση των κλειδιών και των συσχετίσεων ασφάλειας μπορεί να είναι είτε χειροκίνητη είτε αυτόματη. Κάθε σταθμός πρέπει να υποστηρίζει και τους δύο τρόπους διαχείρισης για λόγους διαλειτουργικότητας σύμφωνα με το RFC 2401.

4.3.6.1 Χειροκίνητη διαχείριση κλειδιών

Στην χειροκίνητη διαχείριση κλειδιών και συσχετίσεων, οι συσχετίσεις ασφάλειας ορίζονται στατικά για κάθε ζευγάρι συνομιλούντων σταθμών. Η χειροκίνητη διαχείριση δεν είναι καλή αφού:

- Είναι επιρρεπής σε λάθη αφού απαιτεί εκτενείς ρυθμίσεις για πολλά ζευγάρια σταθμών.

- Τα κλειδιά για την επικοινωνία δύο υπολογιστών είναι στατικά και άρα υπάρχει μεγαλύτερη πιθανότητα να τα ανακαλύψει κάποιος εισβολέας.

- Τα κλειδιά συνήθως δεν είναι ισχυρά αφού η διαδικασία των ρυθμίσεων είναι κουραστική και πολλές φορές δεν χρησιμοποιούνται σωστές μέθοδοι για την δημιουργία τους.

- Δεν εφαρμόζεται σε ευρεία κλίμακα αφού απαιτούνται στατικές ρυθμίσεις για όλα τα ζευγάρια σταθμών. Από τα παραπάνω καταλαβαίνουμε ότι η διαχείριση των κλειδιών χρειάζεται αυτοματοποίηση.

4.3.6.2 Αυτόματη διαχείριση κλειδιών

Για την αυτόματη διαχείριση των συσχετίσεων χρησιμοποιούνται συγκεκριμένα πρωτόκολλα. Μερικά από τα πρωτόκολλα διαχείρισης είναι τα: Skip, Oakley, Photuris και IKE. Από αυτά κάθε σταθμός πρέπει να υποστηρίζει τουλάχιστον τον IKE. Από τα παραπάνω πρωτόκολλα εμείς θα αναφερθούμε μόνο στο Skip και στο IKE.

Skip (in band keying)

Το πρωτόκολλο SKIP (Simple Key-Management for Internet Protocols) αναπτύχθηκε από την SUN το 1995 και σταμάτησε να προωθείτε το 1998. Το SKIP είναι πλέον «νεκρό» και δεν χρησιμοποιείται. Αναφερόμαστε σε αυτό επειδή είναι το μοναδικό πρωτόκολλο που διαφέρει υπερβολικά από τα υπόλοιπα. Η διαφορά του οφείλεται στο γεγονός ότι το κλειδί με το οποίο κρυπτογραφούνται τα δεδομένα περιλαμβάνεται μέσα στο πακέτο σε μία ξεχωριστή επικεφαλίδα του SKIP.

Το SKIP είναι σχεδιασμένο για πρωτόκολλα πακέτων (datagram oriented) όπως το IP. Κάθε σταθμός έχει ένα ζευγάρι κλειδιών Diffie Hellman. Το δημόσιο κλειδί του αυθεντικοποιείται μέσω X509 πιστοποιητικά, PGP πιστοποιητικά ή χειροκίνητα. Ένα κοινό αυθεντικοποιημένο κλειδί, έστω S, υπολογίζεται από το δημόσιο του κάθε σταθμού. Όταν ένας σταθμός στέλνει δεδομένα υπολογίζει ένα τυχαίο συμμετρικό κλειδί, έστω R, Κρυπτογραφεί ή / και πιστοποιεί τα δεδομένα με το κλειδί R χρησιμοποιώντας ένα από τα AH και ESP.

Κρυπτογραφεί το κλειδί R με το κλειδί S και στέλνει τα κρυπτογραφημένα ή/και πιστοποιημένα δεδομένα το κρυπτογραφημένο R στον παραλήπτη. Ο παραλήπτης αποκρυπτογραφεί το R με το S και έπειτα περνάει τα δεδομένα και το κλειδί R στο τμήμα του IPSec για επεξεργασία όπως παρατηρούμε και στην παρακάτω εικόνα.

Εικόνα 17

Πλεονεκτήματα:

- Δεν γίνεται σύνδεση μεταξύ των δύο υπολογιστών για την ανταλλαγή κλειδιών
- Υποστηρίζει συνδέσεις μία κατεύθυνσης (π.χ. broadcast πάνω από δορυφόρους)
- Υποστηρίζει multicast
- Αντιπυρικές ζώνες που χρησιμοποιούν το SKIP μπορούν να ρυθμιστούν ώστε να κάνουν άμεση ανάκαμψη από σφάλματα

Μειονεκτήματα:

- Ακόμα μεγαλύτερα πακέτα (περιέχουν και το κρυπτογραφημένο κλειδί του πακέτου)
- Επιπλέον επεξεργασία ανά πακέτο
- Δεν διαπραγματεύονται ρυθμίσεις για τις συσχετίσεις ασφαλείας

IKE

Το IKE (Internet Key Exchange) είναι το πρότυπο πρωτόκολλο για την αυτόματη διαχείριση κλειδιών και συσχετίσεων ασφάλειας. Είναι ένα πρωτόκολλο επιπέδου εφαρμογής που χρησιμοποιεί το UDP ως πρωτόκολλο μεταφοράς και την θύρα 500. Βασίζεται στο ISAKMP (RFC 2408, RFC 2409). Το ISAKMP είναι ένα πρωτόκολλο που αποτελεί έναν σκελετό για την ανάπτυξη πρωτοκόλλων ασφαλείας. Το IKE έχει αρχιτεκτονική initiator-responder, ο initiator προτείνει κάποιες παραμέτρους επικοινωνίας και ο responder επιστρέφει ποιες από αυτές δέχεται χωρίς να μπορεί να προτείνει αυτός κάποιες παραμέτρους. Το IKE είναι πρωτόκολλο δύο φάσεων. Η πρώτη φάση χρησιμοποιεί το ISAKMP για να δημιουργήσει ένα ISAKMP SA. Η δεύτερη φάση χρησιμοποιεί το ISAKMP SA για να δημιουργήσει τουλάχιστον δύο IPSec SA (ένα για κάθε κατεύθυνση). Η πρώτη φάση έχει δύο modes, το main και το aggressive.

Στο main mode έχουμε τρία ζευγάρια μηνυμάτων:

1. Διαπραγματεύονται οι κρυπτογραφικοί αλγόριθμοι.

2. Γίνεται μια Difflie Hellman συναλλαγή και παράγεται ένα κοινό μυστικό.

3. Το κάθε σύστημα αποδεικνύει την ταυτότητά του και ότι γνωρίζει το κοινό μυστικό.

Στο aggressive mode έχουμε μόνο τρία μηνύματα:

1. Στα πρώτα δυο μηνύματα γίνεται μια συναλλαγή Diffie-Hellman και παράγεται ένα κοινό μυστικό.

2. Στα μηνύματα δυο και τρία, κάθε σύστημα αποδεικνύει ότι γνωρίζει το κοινό μυστικό.

Στο main mode τα δύο τελευταία μηνύματα είναι κρυπτογραφημένα, ώστε να έχουμε μη αποκάλυψη της ταυτότητας των συνομιλούντων, ενώ στο aggressive mode έχουμε λιγότερα μηνύματα. Στη δεύτερη φάση έχουμε δύο modes, το informational και το quick. Το informational mode χρησιμοποιείται για ανακοίνωση σφαλμάτων. Το quick mode χρησιμοποιείται για την δημιουργία IPSec SA και στο rekeying. Κατά την διάρκεια του quick mode έχουμε διαπραγμάτευση των παραμέτρων ασφάλειας και την δημιουργία κλειδιών και συσχετίσεων ασφάλειας.

PFS – Perfect Forward Secrecy

Το Perfect Forward Secrecy (PFS) είναι μία παράμετρος στην λειτουργία του IKE και σε άλλα πρωτόκολλα διαχείρισης κλειδιών. Ο διαχειριστής του κάθε σταθμού αποφασίζει αν θα χρησιμοποιήσει ή όχι PFS. Αν ένας σταθμός το έχει ενεργοποιημένο και ο άλλος όχι τότε δεν υπάρχει διαλειτουργικότητα και οι δυο σταθμοί δεν μπορούν να επικοινωνήσουν

χρησιμοποιώντας IPSec. Με την ενεργοποίηση του PFS ενισχύεται η ασφάλεια αφού οι σταθμοί εμπιστεύονται λιγότερο τις συναλλαγές του IKE. PFS έχουμε για τα κλειδιά και τις ταυτότητες των συνομιλούντων. PFS για τις ταυτότητες σημαίνει ότι η συσχέτιση ασφάλειας ISAKMP SA της πρώτης φάσης του IKE διαγράφεται μετά από την δημιουργία μίας IPSec SA. Όταν οι δύο σταθμοί ξαναδημιουργούν της συσχετίσεις ασφάλειας IPSec SA (rekeying) τότε κάνουν και τις δύο φάσεις του IKE. Για τα κλειδιά το PFS είναι εγγύηση ότι ένα κλειδί έχει δημιουργηθεί από μία μοναδική Diffie Hellman συναλλαγή και ότι δεν υπάρχει σχέση μεταξύ των κλειδιών που χρησιμοποιούνται από τους σταθμούς.

Με αυτόν τον τρόπο εξασφαλίζουμε ότι όταν κάποιο κλειδί αποκαλυφθεί σε έναν εισβολέα, αυτός θα έχει πρόσβαση μόνο στα δεδομένα που κρυπτογραφήθηκαν με αυτό το κλειδί. Το PFS προσφέρεται με μία επιπλέον Diffie Hellman συναλλαγή κατά την διάρκεια της δεύτερης φάσης του IKE όταν δημιουργείται ένα καινούργιο IPSec SA. Για την δημιουργία του IPSec SA χρησιμοποιείται το κοινό μυστικό από την επιπλέον Diffie Hellman συναλλαγή και όχι αυτό από την ISAKMP SA της πρώτης φάσης.

IPSra και οι road warriors

Ο IKE αρχικά είχε σχεδιαστεί με δεδομένο ότι οι σταθμοί θα έχουν σταθερές IP διευθύνσεις και ότι οι IP διευθύνσεις θα χρησιμοποιούνταν ως selectors στην SPD. Υπάρχουν όμως χρήστες η οποίοι δεν έχουν σταθερή IP διεύθυνση. Οι χρήστες αυτοί δεν έχουν σταθερή IP διεύθυνση είτε γιατί έχουν πρόσβαση στο διαδίκτυο με dial up, είτε γιατί ταξιδεύουν και θέλουν να έχουν πρόσβαση σε ένα δίκτυο (συνήθως μιας εταιρίας) από διάφορα δίκτυα στον κόσμο. Η τελευταία ομάδα χρηστών λέγεται road warriors.

Για τους road warriors λοιπόν, έχει δημιουργηθεί μία ομάδα στην IETF η IPSra (IP Security Remote Access). Η ομάδα αυτή έχει ως στόχο να κάνει την πρόσβαση των road warriors πιο εύκολη και πιο ασφαλής.

Η ομάδα IPsra σχεδιάζει:

- Να μην εισάγει αλλαγές στον IKE

- Να χρησιμοποιήσει για πιστοποίηση ταυτότητας δημοφιλή (σε εταιρικά περιβάλλοντα) συστήματα αυθεντικοποίησης όπως το Radius και το SecureID
- Να αξιοποιήσει πλήρως την τεχνολογία του PKI

4.3.7 Συγκεντρωτικοί πίνακες IPSec

Βασικά χαρακτηριστικά του IPSec

Αυθεντικοποίηση Ναι

Αριθμός πρωτοκόλλου (IP Protocol Number)

50 - ESP , 51 - AH

UDP Port Number 500 - IKE

Εμπιστευτικότητα (confidentiality) Ναι

Ακεραιότητα (integrity) Ναι

Διασφάλιση προέλευσης (data origin authentication) Ναι

Προστασία πολλαπλής αποστολής πακέτου (anti-reply) Ναι

Ισχύς κρυπτογράφηση Δυνατή

Υποστήριξη IOS για το IPSec . Από την έκδοση 11.3T και έπειτα

Υποστήριξη πολλών πρωτοκόλλων Όχι

RFC τα οποία είναι σχετικά με το IPSec

RFC Όνομα

2401 Security Architecture for the Internet Protocol

2402 IP Authentication Header

2403 The Use of HMAC-MD5-96 within ESP and AH

2404 The Use of HMAC-SHA-1-96 within ESP and AH

2405 The ESP DES-CBC Cipher Algorithm with Explicit IV

2406 IP Encapsulating Security Payload

2407 The Internet IP Security Domain of Interpretation of ISAKMP

2408 Internet Security Association and Key Management Protocol

2409 The Internet Key Exhange

2410 The NULL Encryption Algorithm and Its Use with IPSec

2411 IP Security Document Roadmap

2412 The OAKLEY Key Determination

2207 RSVP Extensions for IPSec Data Flows

2709 Security Model with Tunnel-mode IPSec for NAT Domains

1828 IP Authentication using Keyed MD5

2857 The use of HMAC-RIPEMD-160-96 within ESP and AH

1851 The ESP Triple DES Transform

2631 Diffie-Hellman Keu Agreement Method

ΚΕΦΑΛΑΙΟ 5

5. Σενάρια Υλοποίησης VPN

5.1 Εισαγωγή

Σκοπός της εργασίας μας είναι η υλοποίηση ενός VPN (Virtual Private Network) με το πρωτόκολλο IPSec σε λειτουργικό σύστημα Linux Centos 5.3 , με όλα τα πιθανά σενάρια που υπάρχουν για την υλοποίηση του. Θα δούμε δύο βασικές διαφορετικές συνδεσμολογίες. Η πρώτη συνδεσμολογία θα είναι η (Network-To-Network) και η δεύτερη συνδεσμολογία μας θα είναι η (Road Warrior). Στην Network-to-Network συνδεσμολογία θα δούμε την υλοποίηση ενός VPN μεταξύ δύο δρομολογητών ενώ στην Road Warrior συνδεσμολογία θα δούμε την υλοποίηση ενός VPN μεταξύ ενός δρομολογητή και ενός Laptop. Προκειμένου να πραγματοποιηθούν οι παραπάνω υλοποιήσεις, έχουμε φτιάξει τέσσερα εικονικά μηχανήματα με τη βοήθεια του λογισμικού VMware και σε κάθε ένα από αυτά έχουμε εγκαταστήσει το λογισμικό Open Swan. Παρακάτω θα δούμε όλα τα εικονικά μηχανήματα (Virtual Machines) και την παραμετροποίηση που απαιτείται προκειμένου να πετύχουμε τις παραπάνω συνδεσμολογίες. Οι ονομασίες που έχουμε δώσει σε αυτά τα εικονικά μηχανήματα είναι οι εξής:

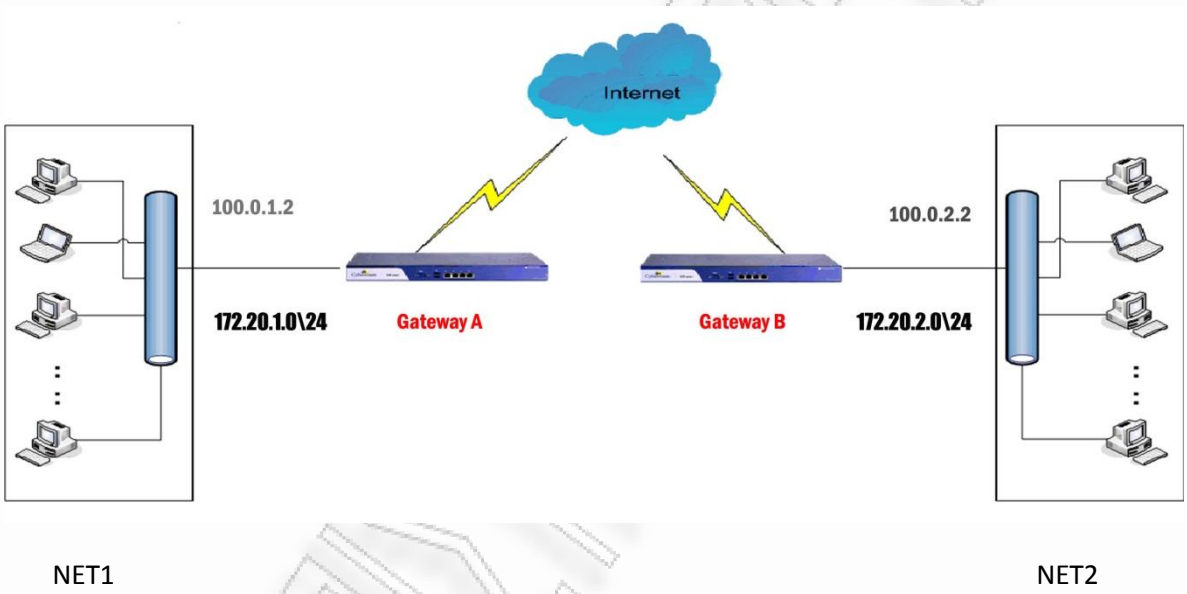
- Net 1
- Net 2
- Router
- Client1

Τα εικονικά μηχανήματα Net 1 και Net2 έχουν το ρόλο των δρομολογητών. Είναι στην ουσία δυο διαφορετικά δίκτυα μεταξύ τους με ενσωματωμένα υποδίκτυα (subnets). Το εικονικό μηχάνημα Client 1, είναι ένας υπολογιστής μέσα στο υποδίκτυο (subnet) του δρομολογητή (Net 1). Τέλος ο Router είναι ένα εικονικό μηχάνημα το οποίο το χρησιμοποιούμε στην προκειμένη περίπτωση για να προσομοιάσουμε το διαδίκτυο (Ιντερνέτ) άλλα και για την δρομολόγηση των πακέτων μας.

5.2 Υλοποίηση Net-to-Net VPN IPSec

Προκειμένου να πραγματοποιήσουμε με επιτυχία την net-to-net συνδεσμολογία χρειαζόμαστε τα εξής:

- Δύο δρομολογητές (Gateways) με λειτουργικό σύστημα Linux
- Εγκατεστημένο το λογισμικό OpenSwan και στους δύο δρομολογητές
- Ένα υποδίκτυο (Subnet) πίσω από κάθε δρομολογητή.



Εικόνα 18. Σχεδιάγραμμα υλοποίησης network-to-network VPN IPSec

5.2.1 Παραμετροποίηση των εικονικών μηχανημάτων (virtual machines)

Στην παραμετροποίηση θα δούμε το configuration στις κάρτες δικτύου που χρησιμοποιούν τα εικονικά μηχανήματα.

5.2.1.1 Παραμετροποίηση του εικονικού μηχανήματος (virtual machine) NET 1

Στο virtual machine NET 1 που στην ουσία είναι ο δρομολογητής Α στην υλοποίηση μας , περιέχει δύο κάρτες δικτύου. Η μια κάρτα δικτύου (Ethernet 0) χρησιμοποιείτε για την Public Ip του δικτύου μας σε αντίθεση με την (Ethernet 1) που χρησιμοποιείτε για την Private Ip του δικτύου. Δηλαδή το subnet του δικτύου.

Η παραμετροποίηση της κάρτας δικτύου **Ethernet 0** του δρομολογητή Α έχει ως εξής:

Ethernet 0 (Public Ip):

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
HWADDR=00:0c:29:3c:1a:a6          # Η διεύθυνση υλικού της κάρτας δικτύου
DEVICE=eth0                       # Ethernet eth0
BOOTPROTO=static                  #Δηλώνουμε ότι είναι στατική
ONBOOT=yes                        # Να ξεκινάει στο Boot του μηχανήματος
DHCP_HOSTNAME=net1.unipi.gr       #Hostname
IPADDR=100.0.1.2                  #Η Public Ip του NET 1
NETMASK=255.255.255.0             #Το netmask
NETWORK=100.0.1.0                 #Το network
BROADCAST=100.0.1.255
USERCTL=no
IPV6INIT=no
TYPE=Ethernet
```

Η παραμετροποίηση της κάρτας δικτύου **Ethernet 1** του δρομολογητή Α έχει ως εξής:

Ethernet 1 (Private Ip):

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
HWADDR=00:0c:29:3c:1a:b0          # Η διεύθυνση υλικού της κάρτας δικτύου
DEVICE=eth1                       # Ethernet  eth0
BOOTPROTO=static
ONBOOT=yes
DHCP_HOSTNAME=net1.unipi.gr
IPADDR=172.20.1.1                 #Η Private IP  του NET1
NETMASK=255.255.255.0
NETWORK=172.20.1.0
BROADCAST=172.20.1.255
USERCTL=no
IPV6INIT=no
TYPE=Ethernet
```

5.2.1.2 Παραμετροποίηση του εικονικού μηχανήματος (virtual machine) NET 2

Στο virtual machine NET 2 που στην ουσία είναι ο δρομολογητής Β στην υλοποίηση μας , περιέχει και αυτός δύο κάρτες δικτύου. Η μια κάρτα δικτύου (Ethernet 0) χρησιμοποιείτε για την Public Ip του δικτύου μας σε αντίθεση με την (Ethernet 1) που χρησιμοποιείτε για την Private Ip του δικτύου. Δηλαδή το subnet του δικτύου.

Η παραμετροποίηση της κάρτας δικτύου **Ethernet 0** του δρομολογητή Β έχει ως εξής:

Ethernet_0 (Public Ip):

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
HWADDR=00:0c:29:6c:98:4f          # Η διεύθυνση υλικού της κάρτας δικτύου
DEVICE=eth0                       # Ethernet  eth0
BOOTPROTO=static
ONBOOT=yes
DHCP_HOSTNAME=net2.unipi.gr
IPADDR=100.0.2.2                  #Η Public Ip του NET 2
NETMASK=255.255.255.0
NETWORK=100.0.2.0
BROADCAST=100.0.2.255
USERCTL=no
IPV6INIT=no
TYPE=Ethernet
```

Η παραμετροποίηση της κάρτας δικτύου **Ethernet_1** του δρομολογητή Β έχει ως εξής:

Ethernet 1 (Private Ip):

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
HWADDR=00:0c:29:6c:98:59
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
DHCP_HOSTNAME=net2.unipi.gr
IPADDR=172.20.2.1                 #Η Private IP  του NET 2
NETMASK=255.255.255.0
```

NETWORK=172.20.2.0

BROADCAST=172.20.2.255

USERCTL=no

IPV6INIT=no

TYPE=Ethernet

5.2.1.3 Παραμετροποίηση του εικονικού μηχανήματος (virtual machine) Router

Το virtual machine Router είναι στην ουσία ο δρομολογητής του δικτύου μας. Έχει τρείς κάρτες δικτύου, την (Ethernet 0) που είναι στο VmNet0 δηλαδή bridged με το κανονικό μου δίκτυο και default gateway, την (Ethernet 1) και την (Ethernet 2). Ο λόγος που η (Ethernet 0) είναι bridged με το κανονικό μου δίκτυο είναι για να μην μπορούν να πάνε τα πακέτα από την private του ενός gateway στον άλλο gateway παρά μόνο με την χρήση tunnel. Έτσι ναι μεν μπορούμε να κάνουμε ping από την public ip του ενός ,την public ip του άλλου gateway αλλά δεν υπάρχει η παραμικρή πρόσβαση στις private ip addresses του κάθε gateway από τον άλλο αλλά ούτε από τον ενδιάμεσο.

Η παραμετροποίηση της κάρτας δικτύου **Ethernet 0** του Router έχει ως εξής:

Ethernet 0 :

Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]

HWADDR=00:0c:29:29:b7:49 # Η διεύθυνση υλικού της κάρτας δικτύου

DEVICE=eth0 # Ethernet eth0

BOOTPROTO=none

ONBOOT=yes

DHCP_HOSTNAME=router.unipi.gr

IPADDR=192.168.1.155

NETMASK=255.255.255.0

NETWORK=192.168.1.0

BROADCAST=192.168.1.255

IPV6INIT=no

USERCTL=no

TYPE=Ethernet

Η παραμετροποίηση της κάρτας δικτύου **Ethernet_1** του Router έχει ως εξής:

Ethernet_1 :

Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]

HWADDR=00:0c:29:29:b7:53

DEVICE=eth1

BOOTPROTO=static

ONBOOT=yes

IPADDR=100.0.1.1

NETMASK=255.255.255.0

NETWORK=100.0.1.0

Η παραμετροποίηση της κάρτας δικτύου **Ethernet_2** του Router έχει ως εξής:

Ethernet_2:

Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]

HWADDR=00:0c:29:29:b7:5d

DEVICE=eth2

BOOTPROTO=none

ONBOOT=yes

IPADDR=100.0.2.1

NETMASK=255.255.255.0

NETWORK=100.0.2.0

5.2.1.4 Παραμετροποίηση του εικονικού μηχανήματος (virtual machine) Client

Τέλος το virtual machine **Client** είναι στην ουσία ένας σταθμός εργασίας του NET 1. Έχει μια κάρτα δικτύου (Ethernet 0) που είναι μέσα στο subnet του Net 1. Ο λόγος που χρειαζόμαστε τον Client είναι γιατί πολύ απλά δεν μπορούμε να σηκώσουμε VPN από gateway τύπου δίκτυο σε δίκτυο παρά μόνο από κάποιο σταθμό που πρέπει να ανήκει στο υποδίκτυο ενός από αυτούς και να προσπαθήσει να επικοινωνήσει με το άλλο άκρο.

Η παραμετροποίηση της κάρτας δικτύου **Ethernet 0** του Client έχει ως εξής:

Ethernet 0 (Public Ip):

Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]

HWADDR=00:0c:29:29:b7:5d

DEVICE=eth0

BOOTPROTO=static

BROADCAST=172.20.1.255

ONBOOT=yes

IPADDR=172.20.1.2

NETMASK=255.255.255.0

NETWORK=172.20.1.0

5.2.2 Παραμετροποίηση του αρχείου IPSec.secrets

Η αυθεντικοποίηση μεταξύ των δύο δρομολογητών μπορεί να γίνει με τρείς διαφορετικούς τρόπους:

- PSK Key (Preshared –key)
- RSA Key
- X.509 certificates

5.2.2.1 IPSec. secrets –PSK Key

Η διαμόρφωση του **IPSec.secrets** με ένα **pre-shared key** έχει ως εξής:

100.0.2.2 100.0.1.2 : PSK “secret”

Στο συγκεκριμένο παράδειγμα βάλαμε σαν κρυφή λέξη την λέξη “secret”. Η λέξη αυτή μπορεί να είναι οποιαδήποτε λέξη ή σειρά από χαρακτήρες θέλουμε.

5.2.2.2 IPSec. secrets –RSA Key

Προκειμένου να δημιουργήσουμε ένα RSA κλειδί πληκτρολογούμε στο command του Linux την εξής εντολή:

ipsec rsasigkey --verbose 2048 > keys.tmp

Η εντολή αυτή μας δημιουργεί ένα RSA κλειδί όπως βλέπουμε παρακάτω και το σώζουμε σε ένα αρχείο με την ονομασία keys.tmp. Προσοχή το RSA κλειδί θα πρέπει να είναι διαφορετικό στον δρομολογητή Net 1 και διαφορετικό στον δρομολογητή Net 2. Επομένως εφαρμόζουμε την πιο πάνω εντολή και στους δύο δρομολογητές.

Το αρχείο IPSec.secrets θα έχει την εξής δομή:

100.0.1.2 100.0.2.2: RSA {

RSA 2048 bits net1.unipi.gr Sun Sep 20 03:32:21 2009

for signatures only, UNSAFE FOR ENCRYPTION

#pubkey=0sAQOiofegylvYHwYssjcczBcDjgrtvDVZimvbQHhlRppS/EaA5SYM7VUoeyRySyUoGuHWq2xwPsaxL21cDtJSjAKAJxa7z7SJz5ZH0oBs4m8QUGNEFEYVeH6zxY1QS7bMXZRuxsWIxBbOMaOydj7z4EuO9MqTpKeRDnIJi/hsqYMov+cs+ISGQkGcH096dirkXXQ4R7KAINXx0GSL4G61KFp8InvNqNmJFhV+vHHwamjkP4PE0nmYuezfpvgxym3ki4E+gbNdBzyOb54E5iVUbW8FQCyOzbakFFpLEstIQSAhrjixwFs+5PKvbEGNJrNNQekOOFGyc2CHN++WX009SEzT

Modulus:
0xa2a1f7a0ca5bd81f062cb2371ccc17038e0aedbc35598a6bdb407865469a52fc4680e5260ced55287b24724b25281ae1d6ab6c703ec6b12f6d5c0ed2528c02802716bbcfb489cf9647d2806ce26f10506344144615787eb3c58d504bb6cc5d946ec6c588c416ce31a3b2763ef3e04b8ef4ca93a4a7910e72098bf86ca98328bfe72cf8848642419c1f4f7a762ae45d743847b28020d5f1d0648be06eb5285a7c227bcda8d98916157ebc71f06a68e43f83c4d27998b9ecdfa6f831ca6de48b813e81b35d073c8e6f9e04e625546d6f05402c8ecdb6a4145a4b12cb48412021ae38b1c05b3ee4f2af6c418d26b34d41e90e3851b273608737ef965f4d3d484cd3

PublicExponent: 0x03

everything after this point is secret

PrivateExponent:
0x1b1afe9acc64a4052bb21db3da2203d5ed01d24a08e441bca48abebb8bc4632a0bc0263102278e3169db6861db86af25a3c73cbd5fcbc832923a0278631755c00683c9f7f36c4d43b6a315677b1282b8108b58b658e96a734b978d61f3ccba4367cbcb96cb59225d9b48690a7dfab7427e21c3461bed826856eca9677195dc1fb6f83c1ce63ca78d3976a51665010d9bd9da653ad0634b0ac9d4102c51521d7f86e369da78aca3b73a849e6b84fda5bc85091edfc344cd0437d87bd7998b6aec6daf0ff7e02c68824d8bcf0b0605abe6bc78babb5bedfb61a108164f9bae85bdda30e2c7b72ddd8337ab5810bdd1b7159c8ebafbd70cd0f024db1b8abee2d06b

Prime1:
0xef934179554c82642202b871cc31fcb106a42fcbd18ae61bba9335067c59dd7c82ac74d1af05f3dc191c2d25cf5edb91925c2e160aa28681115e4adf2727069eaabedcb1f4630f134fc7d1c81496668d5ea3eac87f7f015db255e8bd84e70af678e78fb610e7181ee80e5a093a635da15026ce93362e24896ac705f7ba029313

Prime2:
0xadc84e5dcb89d1e8a484e37e00ac0f1c168523536cf74973ef004a5e50e1cc02767addb856774bee06848e457d182642d331eb24fa7a98454686ffddad79035801a876dbd1cf0c4e7cf63a1b1bb5010f76b443a10f912eb2d28c5cad1621f444a2a4dff6e2eaa97d362f22b905ff99c612b9213832e57d0da7acb41509f4d741

Exponent1:
0x9fb780fb8e33019816ac7af688215320af181fdd365c9967d1b778aefd913e5301c84de11f594d3d6612c8c3df9492610c3d740eb1c1af00b63edc94c4c4af1471d493214d975f62352fe1300db999b3946d473054ff563e76e3f07e589a074efb450a79609a10149ab43c0626ece916356f3462241ec306472f594fd1570cb7

Exponent2:
0x73dadee9325be145c30342540072b4bd6458c2379dfa30f7f4aadc3ee0968801a451e9258efa329eaf030983a8bac42c8ccbf218a6fc65838459ffe91e50ace556704f3d368a0834534ed16767ce00b4f9cd826b5

fb61f21e1b2e8736416a2d86c6deaa497471ba8ceca172603ffbbd961d0c0d021ee535e6fc8780e06a33a2b

Coefficient:
0x99dd9600c6c09e3ccb75ebdcb6d45ac486cacf5fdc7f5b40c2902cb9eeebec30f516de3ba1c6f48d13caa1f5f148c1657ef4b2bbc12341830cba4d2756dbef8d231d842a9dd2d946da4e3cdee3e9102f67b9af955fb3f8689625aa077c2f449805fc1772cff1f84f339ee2792db2d2caf9a6f0d96b587d946c305defa0814fa8

}

5.2.2.3 IPSec. secrets –X.509 Certificate

Το X.509 είναι ITU-T (ITU Τομέα Τυποποίησης Τηλεπικοινωνιών) πρότυπο για PKI (Public Key Infrastructure) στην κρυπτογράφηση, το οποίο, μεταξύ πολλών άλλων, ορίζει ειδικά φόρμα για PKC (Public Key Πιστοποιητικά) και ο αλγόριθμος που ελέγχει ένα συγκεκριμένο πιστοποιητικό διαδρομή είναι έγκυρη βάσει δώσει PKI (που ονομάζεται διαδρομή πιστοποίησης επικύρωση αλγόριθμο).

X.509 Ιστορία

Το X.509 ξεκίνησε σε συνεργασία με το X.500 πρότυπο το 1988 (έκδοση 1) και θα αναλάβει ένα ιεραρχικό σύστημα των αρχών πιστοποίησης για την έκδοση των πιστοποιητικών, εντελώς αντίθετο με τις τότε υπάρχουσες web εμπιστοσύνης μοντέλα - όπως το PGP - κάθε όπου μπορεί κανείς να υπογράψει έτσι που να βεβαιώνει την εγκυρότητα των άλλων ιδιωτικών ή δημόσιων βασικών πιστοποιητικών. Το 1993, μια βελτιωμένη έκδοση του X.509 - έκδοση 2 - εισήχθη με την προσθήκη δύο ακόμα τομείς, υποστήριξη και υπηρεσίες ελέγχου πρόσβασης. Το X.509-version 3, προστίθεται η συμβατότητα με άλλες τοπολογίες όπως τα μάτια και γέφυρες, και τη δυνατότητα να το χρησιμοποιήσουν σε ένα peer-to-peer, OpenPGP-παρόμοιες web περιβάλλον εμπιστοσύνης, παρόλο που είναι πολύ δύσκολο τρόπο που χρησιμοποιείται ως του 2006.

Αυτές τις μέρες το όνομα X.509 ευρέως αναφέρεται στην IETF του PKI Certificate και KEA Προφίλ του X.509 έκδοση πιστοποιητικού 3 πρότυπα, όπως αναφέρεται σύμφωνα με το RFC 3280 προδιαγραφές.

Μέσα Πιστοποιητικό

Σε ένα σύστημα X.509, η Αρχή Πιστοποίησης εκδώσει πιστοποιητικό δεσμευτική ένα δημόσιο κλειδί για μια δεδομένη αλλά μοναδικό όνομα στο X.500 παράδοση, ή για μια εναλλακτική μία όπως ένα DNS θέση ή διεύθυνση ηλεκτρονικού ταχυδρομείου. Η αυθεντικότητα του πιστοποιητικού και της αρχής πιστοποίησης, με τη σειρά του εξαρτάται

από το πιστοποιητικό ρίζας, η οποία αποτελεί αναπόσπαστο στοιχείο της αλυσίδας πρότυπο X.509 πιστοποίησης.

Πιστοποιητικό Δομή

Μια X.509 έκδοση 3 ψηφιακό πιστοποιητικό έχει τρεις βασικές μεταβλητές - το πιστοποιητικό, το πιστοποιητικό αλγόριθμος υπογραφής και το πιστοποιητικό υπογραφής. Το πιστοποιητικό που περιγράφεται από τα χαρακτηριστικά, όπως η έκδοση, αλγόριθμος ID, αύξοντα αριθμό, εκδότης, θέμα, διάρκεια ισχύος, υπό δημόσιο κλειδί πληροφορίες, επεκτάσεις και διάφορα άλλα μέσα, όπως είναι προαιρετικό και υπόκειται εκδότη μοναδικό αναγνωριστικό. Το θέμα του δημόσιου κλειδιού info χαρακτηριστικό περαιτέρω λεπτομερή από το δημόσιο κλειδί αλγόριθμο και αντικείμενο δημόσιου κλειδιού, ενώ η ισχύς προέρχεται χαρακτηριστικό έχει περαιτέρω επιλογές για μια ημερομηνία, άνω και κάτω όριο, το οποίο τελικά αποφασίσει η ζωή του πιστοποιητικού.

Υποστήριξη των πρωτοκόλλων Πιστοποιητικά X.509

- Transport Layer Security (SSL / TLS)
- IPSec
- Secure Multipurpose Internet Mail Extensions (S / MIME)
- Καρτών
- SSH
- HTTPS
- LDAPv3
- EAP

Προκειμένου λοιπόν να γίνει η πιστοποίηση των X.509 Certificates χρειαζόμαστε έναν τρίτο φορέα –οργανισμό. Υπάρχουν πολλές δημόσιες αρχές πιστοποίησης, όπως η VeriSign, Thawte και ούτω καθεξής.

5.2.3 Παραμετροποίηση του αρχείου IPSec.conf

5.2.3.1 IPSec.conf με PSK

Η δομή του IPSec.conf με PSK κλειδί έχει ως εξής:

```
config setup
        nat_traversal =yes
        klipsdebug =all
        plutodebug =all
conn net-to-net
        left=100.0.1.2                  # H Public Ip του NET 1
        leftsubnet=172.20.1.0/24        # To subnet του NET 1
        right=100.0.2.2                 # H Public Ip του NET 2
        rigthsubnet=172.20.2.0/24       # To subnet του NET 2
        type=tunnel
        authby=secret
        keyingtries=5
        auto=add
        disablearrivalcheck=no
        pfs=no
conn block
        auto=ignore
conn private
        auto=ignore
conn private-or-clear
        auto=ignore
conn clear-or-private
        auto=ignore
conn clear
        auto=ignore
conn packetdefault
        auto=ignore
```

5.2.3.2 Παραμετροποίηση του αρχείου IPSec.conf με RSA κλειδιά

Η δομή του IPSec.conf με RSA κλειδιά έχει ως εξής:

```
config setup
        nat_traversal=yes
        klipsdebug=all
        plutodebug=all
        oe=no
conn net-to-net
        left=100.0.1.2
        leftsubnet=172.20.1.0/24
        leftrsasigkey=0sAQOiofegylvYHwYssjcczBcDjgrtvDVZimvbQHhlRppS/EaA5SYM7VUoeyRySyUo
GuHWq2xwPsaxL21cDtJSjAKAJxa7z7SJz5ZH0oBs4m8QUGNEFEYVeH6zxY1QS7bMXZRuxsWIxBbOMaOy
dj7z4EuO9MqTpKeRDnlJi/hsqYMov+cs+ISGQkGcH096dirkXXQ4R7KAINXx0GSL4G61KFp8InvNqNmJFhV
+vHHwamjkP4PE0nmYuezfpvgxym3ki4E+gbNdBzyOb54E5iVUbW8FQCyOzbakFFpLEstIQSAhrjixwFs+5P
KvbEGNJrNNQekOOFGyc2CHN++WX009SEzT
        right=100.0.2.2
        rightsubnet=172.20.2.0/24
        rightrsasigkey=0sAQPC+zNYmPoch9BjxsoBuxqhIkMzMToiQh8BRveXkzvyPaVUvT1MHe+rHGkz
LY15zJCM0taktXqOLg3Y8tiDYGeAEnWKw1F/Mzrgi/9eAIqRZmdO/3u1Z+/pcLFaXeg2L9XsG9cBkgZo6X/x
Rg1Szq0u7EAXS4XrA2sH76J3jWdQUWZp1zhurQAFmlvd8bOfGLpdblLJ8yh93+wvoNtshjoPl3rGMw/272
o5IeP/o2ooHi5pusJ7xh7Vc4ZDdbZi829Irm9BXNpT5zSxyZRYZVWJhUOivqzArtPtYSAQ9PY11zaw9nWCPg
PIDBwz/jMzg+9slWENqD4xm4ymkAxgvsgZ
        type=tunnel
        keyingtries=5
        auto=add
        disablearrivalcheck=no
        pfs=no

conn block
        auto=ignore

conn private
        auto=ignore

conn private-or-clear
        auto=ignore

conn clear-or-private
        auto=ignore

conn clear
        auto=ignore

conn packetdefault
        auto=ignore
```

5.2.4 Έλεγχος IPSec VPN μεταξύ των δύο δρομολογητών με PSK κλειδί

Αρχικά ξεκινάμε το tunnel μεταξύ των δύο δρομολογητών ,NET 1 και NET 2. Δίνουμε στην γραμμή εντολών την εξής εντολή:

[root@net2~]# Ipsec auto –up net-to-net

```
[root@net2 ~]# ipsec auto --up net-to-net
104 "net-to-net" #1: STATE_MAIN_I1: initiate
003 "net-to-net" #1: received Vendor ID payload [Openswan (this version) 2.6.14
]
003 "net-to-net" #1: received Vendor ID payload [Dead Peer Detection]
003 "net-to-net" #1: received Vendor ID payload [RFC 3947] method set to=109
106 "net-to-net" #1: STATE_MAIN_I2: sent MI2, expecting MR2
003 "net-to-net" #1: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): no NA
T detected
108 "net-to-net" #1: STATE_MAIN_I3: sent MI3, expecting MR3
003 "net-to-net" #1: received Vendor ID payload [CAN-IKEv2]
004 "net-to-net" #1: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_PRESHARED
_KEY cipher=aes_128 prf=oakley_sha group=modp2048}
117 "net-to-net" #2: STATE_QUICK_I1: initiate
004 "net-to-net" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode
{ESP=>0xd174c1ac <0x262d72f4 xfrm=AES_128-HMAC_SHA1 NATOA=none NATD=none DPD=non
e}
[root@net2 ~]# _
```

Εικόνα 19. IPSec PSK established

Παρατηρούμε ότι το tunnel μας έχει εγκαθίδρυση της σύνδεσης (ISAKMP SA established).

Προκειμένου να επιβεβαιώσουμε ότι η μεταφορά των δεδομένων γίνετε σε κρυπτογραφημένη μορφή τρέχουμε την εντολή tcpdump –i (interface) σε όλα τα ενδιάμεσα κομμάτια του δικτύου. Αρχικά κάνουμε ping από τον client 1 ο οποίος βρίσκετε στο υποδίκτυο του δρομολογητή Α.

[root@client1 ~] ping 172.20.2.1

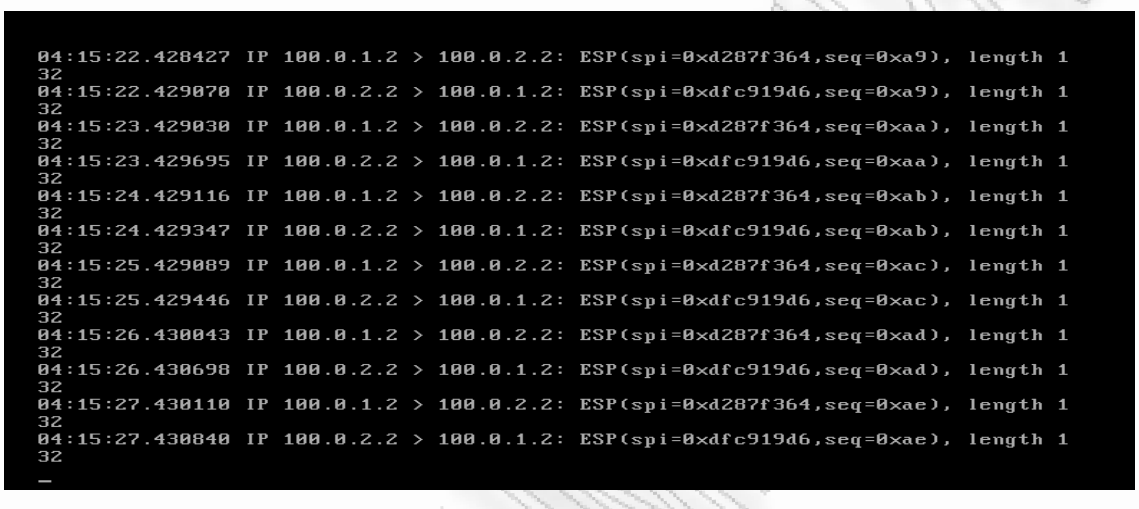
```
[root@client1 ~]# ping 172.20.2.1
PING 172.20.2.1 (172.20.2.1) 56(84) bytes of data.
64 bytes from 172.20.2.1: icmp_seq=1 ttl=63 time=1.36 ms
64 bytes from 172.20.2.1: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 172.20.2.1: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 172.20.2.1: icmp_seq=4 ttl=63 time=1.95 ms
64 bytes from 172.20.2.1: icmp_seq=5 ttl=63 time=1.26 ms
64 bytes from 172.20.2.1: icmp_seq=6 ttl=63 time=1.29 ms
64 bytes from 172.20.2.1: icmp_seq=7 ttl=63 time=0.967 ms
64 bytes from 172.20.2.1: icmp_seq=8 ttl=63 time=1.70 ms
64 bytes from 172.20.2.1: icmp_seq=9 ttl=63 time=1.33 ms
64 bytes from 172.20.2.1: icmp_seq=10 ttl=63 time=1.93 ms
64 bytes from 172.20.2.1: icmp_seq=11 ttl=63 time=1.09 ms
64 bytes from 172.20.2.1: icmp_seq=12 ttl=63 time=2.18 ms
64 bytes from 172.20.2.1: icmp_seq=13 ttl=63 time=0.979 ms
```

Εικόνα 20. Ping από τον Client 1 στο subnet του NET 2

Στην συνέχεια εκτελούμε την εντολή tcpdump στην κάρτα δικτύου (Ethernet 1) του εικονικού μηχανήματος Router.

[root@router ~]# tcpdump –I eth1

Όπως βλέπουμε στην παρακάτω εικόνα ,παρατηρούμε ότι τα πακέτα δρομολογούνται από την δημόσια(Public) Ip του δρομολογητή (Net 1) προς την δημόσια (Public) Ip του δρομολογητή (Net 2) και τα είναι κρυπτογραφημένα.



Εικόνα 21. IPSec PSK tcpdump στην κάρτα δικτύου 1 του Router

Τέλος είναι σκόπιμο να εκτελέσουμε την εντολή tcpdump και στην Ethernet 0 του δρομολογητή NET 2 προκειμένου να επιβεβαιώσουμε ότι τα πακέτα που διακινούνται είναι κρυπτογραφημένα.

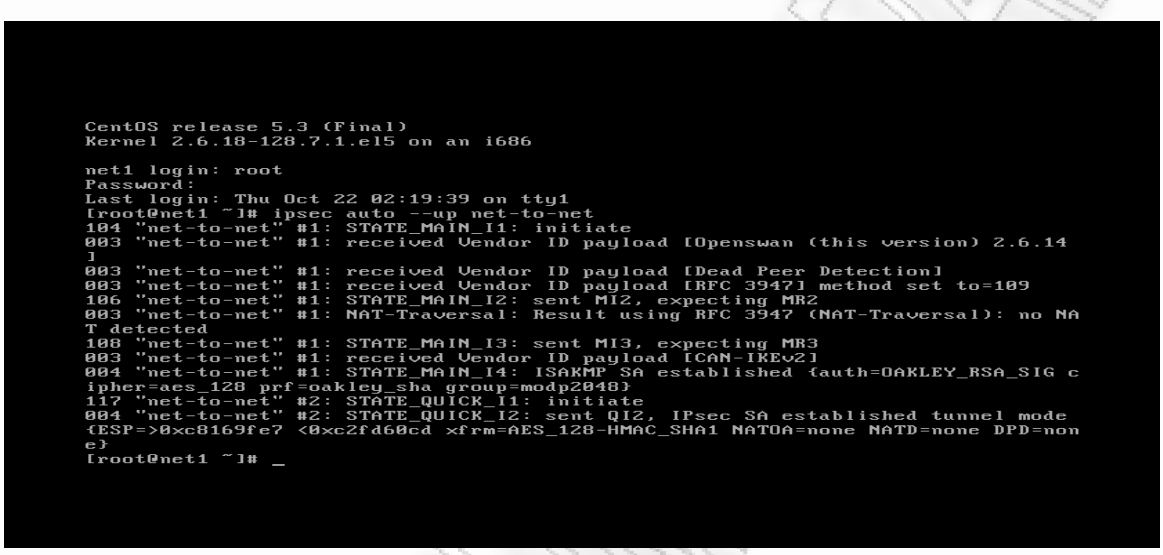
[root@net2 ~]# tcpdump –I eth0

Εικόνα 22. IPSec PSK tcpdump στην κάρτα δικτύου 0 του NET 2

5.2.5 Έλεγχος IPSec VPN μεταξύ των δύο δρομολογητών με RSA κλειδιά

Με ανάλογο τρόπο ξεκινάμε και εδώ το tunnel μεταξύ των δύο δρομολογητών NET 1 και NET 2. Δίνουμε στο command την εξής εντολή:

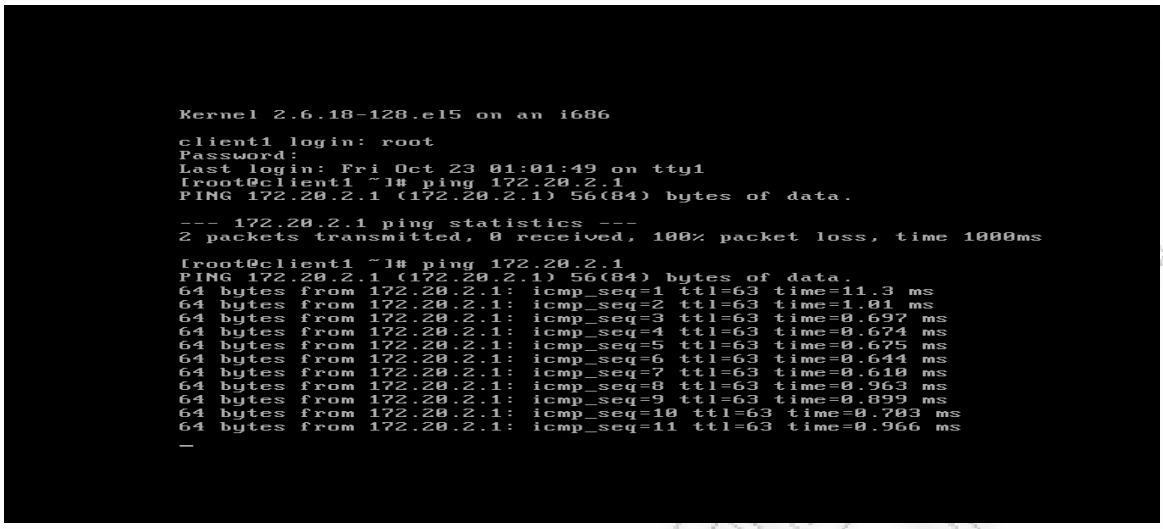
[root@net2~]# Ipsec auto –up net-to-net



Εικόνα 23. IPSec RSA established

Όπως παρατηρούμε και στην παραπάνω εικόνα, το tunnel μας έχει σηκωθεί με κλειδιά κρυπτογράφησης RSA.

Προκειμένου και σε αυτήν την περίπτωση να επιβεβαιώσουμε ότι τα πακέτα που δρομολογούνται μεταξύ των δύο δρομολογητών είναι κρυπτογραφημένα, είναι σκόπιμο να εκτελέσουμε την εντολή tcpdump σε διάφορα κομμάτια του δικτύου μας. Αρχικά εκτελούμε την εντολή ping από το εικονικό μηχάνημα Client 1 στο υποδίκτυο (subnet) του δρομολογητή NET2. Σε αντίθετη περίπτωση και χωρίς την χρήση tunnel αυτό δεν θα μπορούσε να συμβεί. Παρατηρούμε ότι το Ping εκτελείται κανονικά και παίρνουμε απάντηση από το δρομολογητή net2.

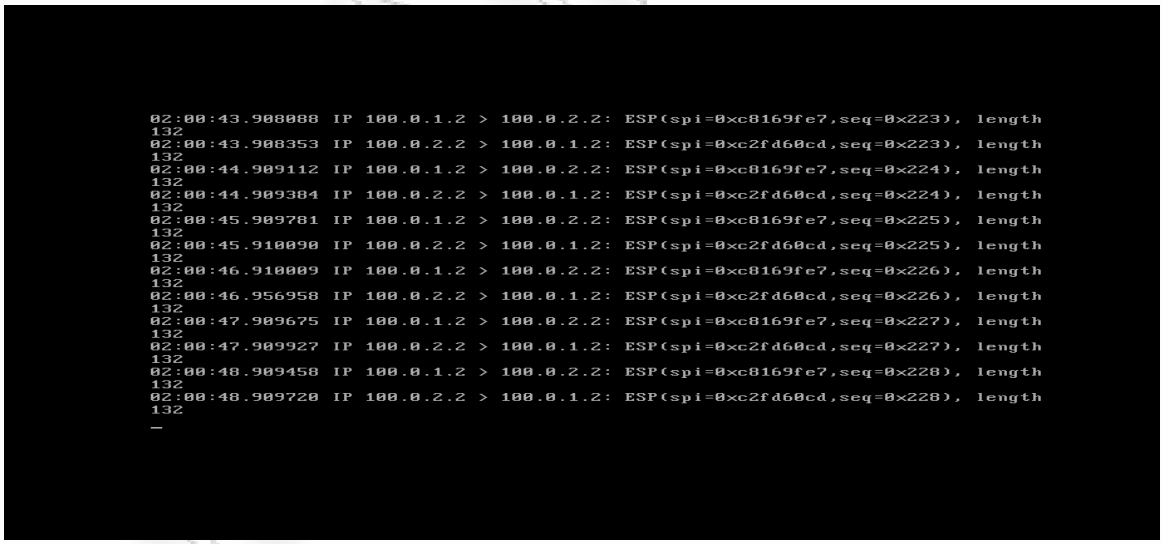


Εικόνα 24. Εκτέλεση της εντολής Ping στο subnet του δρομολογητή NET 2

Στην συνέχεια εκτελούμαι την εντολή tcpdump στα διάφορα κομμάτια του δικτύου μας, προκειμένου να επιβεβαιώσουμε ότι τα πακέτα που δρομολογούνται είναι κρυπτογραφημένα.

Αρχικά ξεκινάμε εκτελώντας την παρακάτω εντολή στο εικονικό μηχάνημα Router.

[root@router ~]# tcpdump –I eth1



Εικόνα 25. IPSec RSA tcpdump στην κάρτα δικτύου 1 του Router

Παρατηρούμε ότι τα πακέτα που διέρχονται από την δημόσια Ip του δρομολογητή Net1 προς την δημόσια Ip του δρομολογητή Net2 είναι κρυπτογραφημένα.

Στην συνέχεια εκτελούμε την εντολή tcpdump στην κάρτα δικτύου (Ethernet 2) του δρομολογητή Net2.

[root@net2 ~]# tcpdump –I eth2

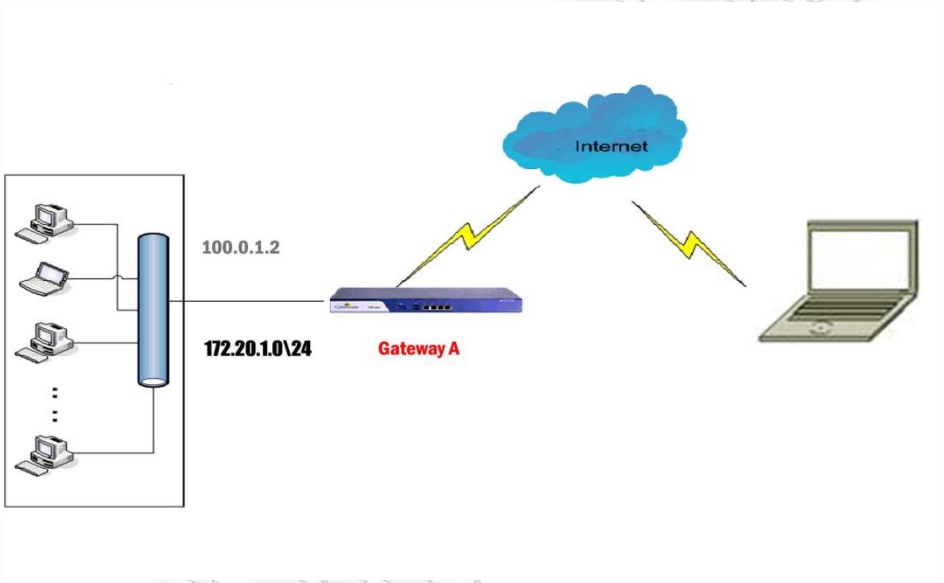
Εικόνα 26. IPSec RSA tcpdump στην κάρτα δικτύου 2 του Net2

Και σε αυτήν την εικόνα παρατηρούμε ότι τα πακέτα μας που διέρχονται προς το υποδίκτυο του δρομολογητή Net 2 είναι κρυπτογραφημένα.

5.3 Υλοποίηση Road warrior VPN

Προκειμένου να πραγματοποιήσουμε την συνδεσμολογία Road warrior χρειαζόμαστε τα εξής:

- Ένα δρομολογητή με ένα υποδίκτυο.
- Ένα Laptop με δυναμική Ip.
- Εγκατεστημένο το λογισμικό OpenSwan και στους δύο.



Εικόνα 27. Σχεδιάγραμμα υλοποίησης Road Warrior Vpn IPSec

5.3.1 Παραμετροποίηση του αρχείου IPSec.secrets

Η αυθεντικοποίηση μεταξύ του δρομολογητή Α και του Laptop μπορεί να γίνει με δύο διαφορετικούς τρόπους:

- PSK Key (Preshared –key)
- RSA Key

5.3.1.1 IPSec. secrets –PSK Key

Η διαμόρφωση του **IPSec.secrets** με ένα **pre-shared key** έχει ως εξής:

%any 100.0.1.2 : PSK “secret”

Στο συγκεκριμένο παράδειγμα βάλαμε σαν κρυφή λέξη την λέξη “secret”. Η λέξη αυτή μπορεί να είναι οποιαδήποτε λέξη ή σειρά από χαρακτήρες θέλουμε.

Σε περίπτωση που η αυθεντικοποίηση μεταξύ των δύο γίνει με PSK κλειδιά τότε πρέπει το αρχείο IPSec.secrets να είναι ίδιο και στις δύο πλευρές.

5.3.1.2 Παραμετροποίηση του αρχείου Ipsec.secrets με RSA κλειδιά στο Laptop

Προκειμένου να δημιουργήσουμε ένα RSA κλειδί στο laptop μας, πληκτρολογούμε στο command του Linux την εξής εντολή:

ipsec rsasigkey --verbose 2048 > keys.tmp

Η εντολή αυτή μας δημιουργεί ένα RSA κλειδί όπως βλέπουμε παρακάτω και το σώζουμε σε ένα αρχείο με την ονομασία keys.tmp. Προσοχή το RSA κλειδί θα πρέπει να είναι διαφορετικό στο laptop μας και διαφορετικό στον δρομολογητή Net 1. Επομένως εφαρμόζουμε την πιο πάνω εντολή και στους δύο.

Το αρχείο IPSec.secrets θα έχει την εξής δομή:

%any 100.0.1.2: RSA {

RSA 2048 bits laptop.unipi.gr Sun Sep 20 03:32:21 2009

for signatures only, UNSAFE FOR ENCRYPTION

#pubkey=0sAQOiofegylvYHwYssjcczBcDjgrtvDVZimvbQHhlRppS/EaA5SYM7VUoeyRySyUoGuH
Wq2xwPsaxL21cDtJSjAKAJxa7z7SJz5ZH0oBs4m8QUGNEFEYVeH6zxY1QS7bMXZRuxsWIxBbOMaOydj7z
4EuO9MqTpKeRDnIJi/hsqYMov+cs+ISGQkGcH096dirkXXQ4R7KAINXx0GSL4G61KFp8InvNqNmJFhV+vH
HwamjkP4PE0nmYuezfpvgxym3ki4E+gbNdBzyOb54E5iVUbW8FQCyOzbakFFpLEstIQSAhrjixwFs+5PKvb
EGNJrNNQekOOFGyc2CHN++WX009SEzT

Modulus:
0xa2a1f7a0ca5bd81f062cb2371ccc17038e0aedbc35598a6bdb407865469a52fc4680e5260ced55287b2

4724b25281ae1d6ab6c703ec6b12f6d5c0ed2528c02802716bbcfb489cf9647d2806ce26f105063441446
15787eb3c58d504bb6cc5d946ec6c588c416ce31a3b2763ef3e04b8ef4ca93a4a7910e72098bf86ca9832
8bfe72cf8848642419c1f4f7a762ae45d743847b28020d5f1d0648be06eb5285a7c227bcda8d98916157e
bc71f06a68e43f83c4d27998b9ecdfa6f831ca6de48b813e81b35d073c8e6f9e04e625546d6f05402c8ecd
b6a4145a4b12cb48412021ae38b1c05b3ee4f2af6c418d26b34d41e90e3851b273608737ef965f4d3d48
4cd3

PublicExponent: 0x03

everything after this point is secret

PrivateExponent:
0x1b1afe9acc64a4052bb21db3da2203d5ed01d24a08e441bca48abebb8bc4632a0bc0263102278e316
9db6861db86af25a3c73cbd5fcbc832923a0278631755c00683c9f7f36c4d43b6a315677b1282b8108b58
b658e96a734b978d61f3ccba4367cbcb96cb59225d9b48690a7dfab7427e21c3461bed826856eca96771
95dc1fb6f83c1ce63ca78d3976a51665010d9bd9da653ad0634b0ac9d4102c51521d7f86e369da78aca3
b73a849e6b84fda5bc85091edfc344cd0437d87bd7998b6aec6daf0ff7e02c68824d8bcf0b0605abe6bc7
8babb5bedfb61a108164f9bae85bdda30e2c7b72ddd8337ab5810bdd1b7159c8ebafbd70cd0f024db1b8
abee2d06b

Prime1:
0xef934179554c82642202b871cc31fcb106a42fcbd18ae61bba9335067c59dd7c82ac74d1af05f3dc191c
2d25cf5edb91925c2e160aa28681115e4adf2727069eaabedcb1f4630f134fc7d1c81496668d5ea3eac87f
7f015db255e8bd84e70af678e78fb610e7181ee80e5a093a635da15026ce93362e24896ac705f7ba0293
13

Prime2:
0xadc84e5dcb89d1e8a484e37e00ac0f1c168523536cf74973ef004a5e50e1cc02767addb856774bee068
48e457d182642d331eb24fa7a98454686ffddad79035801a876dbd1cf0c4e7cf63a1b1bb5010f76b443a1
0f912eb2d28c5cad1621f444a2a4dff6e2eaa97d362f22b905ff99c612b9213832e57d0da7acb41509f4d7
41

Exponent1:
0x9fb780fb8e33019816ac7af688215320af181fdd365c9967d1b778aefd913e5301c84de11f594d3d661
2c8c3df9492610c3d740eb1c1af00b63edc94c4c4af1471d493214d975f62352fe1300db999b3946d4730
54ff563e76e3f07e589a074efb450a79609a10149ab43c0626ece916356f3462241ec306472f594fd1570c
b7

Exponent2:
0x73dadee9325be145c30342540072b4bd6458c2379dfa30f7f4aadc3ee0968801a451e9258efa329eaf0
30983a8bac42c8ccbf218a6fc65838459ffe91e50ace556704f3d368a0834534ed16767ce00b4f9cd826b5
fb61f21e1b2e8736416a2d86c6deaa497471ba8ceca172603ffbbd961d0c0d021ee535e6fc8780e06a33a
2b

Coefficient:
0x99dd9600c6c09e3ccb75ebdcb6d45ac486cacf5fdc7f5b40c2902cb9eeebec30f516de3ba1c6f48d13ca
a1f5f148c1657ef4b2bbc12341830cba4d2756dbef8d231d842a9dd2d946da4e3cdee3e9102f67b9af955
fb3f8689625aa077c2f449805fc1772cff1f84f339ee2792db2d2caf9a6f0d96b587d946c305defa0814fa8

}

5.3.1.3 Παραμετροποιήση του αρχείου Ipsec.secrets με RSA κλειδιά στο δρομολογητή Α.

Προκειμένου να δημιουργήσουμε ένα RSA κλειδί στον δρομολογητή Α ,πληκτρολογούμε στο command του Linux την εξής εντολή:

ipsec rsasigkey --verbose 2048 > keys.tmp

Το αρχείο IPSec.secrets θα έχει την εξής δομή:

100.0.1.2 %any: RSA {

RSA 2048 bits net1.unipi.gr Sun Sep 20 03:32:21 2009

for signatures only, UNSAFE FOR ENCRYPTION

#pubkey=0sAQOiofegylvYHwYssjcczBcDjgrtvDVZimvbQHhlRppS/EaA5SYM7VUoeyRySyUoGuH
Wq2xwPsaxL21cDtJSjAKAJxa7z7SJz5ZH0oBs4m8QUGNEFEYVeH6zxY1QS7bMXZRuxsWIxBbOMaOydj7z
4EuO9MqTpKeRDnIJi/hsqYMov+cs+ISGQkGcH096dirkXXQ4R7KAINXx0GSL4G61KFp8InvNqNmJFhV+vH
HwamjkP4PE0nmYuezfpvgxym3ki4E+gbNdBzyOb54E5iVUbW8FQCyOzbakFFpLEstIQSAhrjixwFs+5PKvb
EGNJrNNQekOOFGyc2CHN++WX009SEzT

Modulus:
0xa2a1f7a0ca5bd81f062cb2371ccc17038e0aedbc35598a6bdb407865469a52fc4680e5260ced55287b2
4724b25281ae1d6ab6c703ec6b12f6d5c0ed2528c02802716bbcfb489cf9647d2806ce26f105063441446
15787eb3c58d504bb6cc5d946ec6c588c416ce31a3b2763ef3e04b8ef4ca93a4a7910e72098bf86ca9832
8bfe72cf8848642419c1f4f7a762ae45d743847b28020d5f1d0648be06eb5285a7c227bcda8d98916157e
bc71f06a68e43f83c4d27998b9ecdfa6f831ca6de48b813e81b35d073c8e6f9e04e625546d6f05402c8ecd
b6a4145a4b12cb48412021ae38b1c05b3ee4f2af6c418d26b34d41e90e3851b273608737ef965f4d3d48
4cd3

PublicExponent: 0x03

everything after this point is secret

PrivateExponent:
0x1b1afe9acc64a4052bb21db3da2203d5ed01d24a08e441bca48abebb8bc4632a0bc0263102278e316
9db6861db86af25a3c73cbd5fcbc832923a0278631755c00683c9f7f36c4d43b6a315677b1282b8108b58
b658e96a734b978d61f3ccba4367cbcb96cb59225d9b48690a7dfab7427e21c3461bed826856eca96771
95dc1fb6f83c1ce63ca78d3976a51665010d9bd9da653ad0634b0ac9d4102c51521d7f86e369da78aca3
b73a849e6b84fda5bc85091edfc344cd0437d87bd7998b6aec6daf0ff7e02c68824d8bcf0b0605abe6bc7
8babb5bedfb61a108164f9bae85bdda30e2c7b72ddd8337ab5810bdd1b7159c8ebafbd70cd0f024db1b8
abee2d06b

Prime1:
0xef934179554c82642202b871cc31fcb106a42fcbd18ae61bba9335067c59dd7c82ac74d1af05f3dc191c2d25cf5edb91925c2e160aa28681115e4adf2727069eaabedcb1f4630f134fc7d1c81496668d5ea3eac87f7f015db255e8bd84e70af678e78fb610e7181ee80e5a093a635da15026ce93362e24896ac705f7ba029313

Prime2:
0xadc84e5dcb89d1e8a484e37e00ac0f1c168523536cf74973ef004a5e50e1cc02767addb856774bee06848e457d182642d331eb24fa7a98454686ffddad79035801a876dbd1cf0c4e7cf63a1b1bb5010f76b443a10f912eb2d28c5cad1621f444a2a4dff6e2eaa97d362f22b905ff99c612b9213832e57d0da7acb41509f4d741

Exponent1:
0x9fb780fb8e33019816ac7af688215320af181fdd365c9967d1b778aefd913e5301c84de11f594d3d6612c8c3df9492610c3d740eb1c1af00b63edc94c4c4af1471d493214d975f62352fe1300db999b3946d473054ff563e76e3f07e589a074efb450a79609a10149ab43c0626ece916356f3462241ec306472f594fd1570cb7

Exponent2:
0x73dadee9325be145c30342540072b4bd6458c2379dfa30f7f4aadc3ee0968801a451e9258efa329eaf030983a8bac42c8ccbf218a6fc65838459ffe91e50ace556704f3d368a0834534ed16767ce00b4f9cd826b5fb61f21e1b2e8736416a2d86c6deaa497471ba8ceca172603ffbbd961d0c0d021ee535e6fc8780e06a33a2b

Coefficient:
0x99dd9600c6c09e3ccb75ebdcb6d45ac486cacf5fdc7f5b40c2902cb9eeebec30f516de3ba1c6f48d13caa1f5f148c1657ef4b2bbc12341830cba4d2756dbef8d231d842a9dd2d946da4e3cdee3e9102f67b9af955fb3f8689625aa077c2f449805fc1772cff1f84f339ee2792db2d2caf9a6f0d96b587d946c305defa0814fa8

}

5.3.2 Παραμετροποίηση του αρχείου Ipsec.conf

5.3.2.1 Παραμετροποίηση του αρχείου Ipsec.conf με RSA κλειδιά στο Laptop

Η δομή του IPSec.conf με RSA κλειδιά έχει ως εξής:

conn road

left=%defaultroute # Το σύστημα παίρνει την δυναμική IP

leftnexthop=%defaultroute #

leftid=@ laptop.unipi.gr #

leftrsasigkey=0sAQOiofegylvYHwYssjcczBcDjgrtvDVZimvbQHhlRppS/EaA5SYM7VUoeyRySyUoGuHWq2xwPsaxL21cDtJSjAKAJxa7z7SJz5ZH0oBs4m8QUGNEFEYVeH6zxY1QS7bMXZRuxsWIxBbOMaOydj7z4Eu

O9MqTpKeRDnIJi/hsqYMov+cs+ISGQkGcH096dirkXXQ4R7KAINXx0GSL4G61KFp8InvNqNmJFhV+vHHwa
mjkP4PE0nmYuezfpvgxym3ki4E+gbNdBzyOb54E5iVUbW8FQCyOzbakFFpLEstIQSAhrjixwFs+5PKvbEGNJ
rNNQekOOFGyc2CHN++WX009SEzT

right=100.0.1.2 # H Public Ip του δρομολογητή A

rightsubnet=172.20.1.0/24 # Το υποδίκτυο του δρομολογητή A

rightid=@net1.unipi.gr #

rightrsasigkey=0sAQPC+zNYmPoch9BjxsoBuxqhIkMzMToiQh8BRveXkzvyPaVUvT1MHe+rHGkzLY15zJC
M0taktXqOLg3Y8tiDYGeAEnWKw1F/Mzrgi/9eAIqRZmdO/3u1Z+/pcLFaXeg2L9XsG9cBkgZo6X/xRg1Szq0
u7EAXS4XrA2sH76J3jWdQUWZp1zhurQAFmlvd8bOfGLpdbILJ8yh93+wvoNtshjoPl3rGMw/272o5IeP/o2
ooHi5pusJ7xh7Vc4ZDdbZi829Irm9BXNpT5zSxyZRYZVWJhUOivqzArtPtYSAQ9PY11zaw9nWCPgPIDBwz/j
Mzg+9slWENqD4xm4ymkAxgvsgZ

auto=add

5.3.2.2 Παραμετροποιήση του αρχείου Ipsec.conf με RSA κλειδιά στον δρομολογητή A

conn road

left=100.0.1.2 # IP Δρομολογητή

leftid=@net1.unipi.gr #

leftsubnet=172.20.1.0/24 #

leftrsasigkey=0sAQPC+zNYmPoch9BjxsoBuxqhIkMzMToiQh8BRveXkzvyPaVUvT1MHe+rHGkzLY15zJC
M0taktXqOLg3Y8tiDYGeAEnWKw1F/Mzrgi/9eAIqRZmdO/3u1Z+/pcLFaXeg2L9XsG9cBkgZo6X/xRg1Szq0
u7EAXS4XrA2sH76J3jWdQUWZp1zhurQAFmlvd8bOfGLpdbILJ8yh93+wvoNtshjoPl3rGMw/272o5IeP/o2
ooHi5pusJ7xh7Vc4ZDdbZi829Irm9BXNpT5zSxyZRYZVWJhUOivqzArtPtYSAQ9PY11zaw9nWCPgPIDBwz/j
Mzg+9slWENqD4xm4ymkAxgvsgZ

rightnexthop=%defaultroute #

right=%any #

rightid=@laptop.unipi.gr #

rightrsasigkey=0sAQOiofegylvYHwYssjcczBcDjgrtvDVZimvbQHhlRppS/EaA5SYM7VUoeyRySyUoGuHWq
2xwPsaxL21cDtJSjAKAJxa7z7SJz5ZH0oBs4m8QUGNEFEYVeH6zxY1QS7bMXZRuxsWIxBbOMaOydj7z4Eu
O9MqTpKeRDnIJi/hsqYMov+cs+ISGQkGcH096dirkXXQ4R7KAINXx0GSL4G61KFp8InvNqNmJFhV+vHHwa
mjkP4PE0nmYuezfpvgxym3ki4E+gbNdBzyOb54E5iVUbW8FQCyOzbakFFpLEstIQSAhrjixwFs+5PKvbEGNJ
rNNQekOOFGyc2CHN++WX009SEzT

auto=add

ΚΕΦΑΛΑΙΟ 6

6. Παρατηρήσεις – Συμπεράσματα

Συνοψίζοντας τα VPN δεν κάνουν τίποτα άλλο από το να εκμεταλλεύονται επιτυχώς το διαδίκτυο ώστε να μεταφέρουν με ασφάλεια τα δεδομένα και να συνδέουν τους απομακρυσμένους χρήστες, τα επιμέρους υποκαταστήματα και τους επιχειρησιακούς συνεργάτες σ' ένα εκτεταμένο εταιρικό δίκτυο. Έτσι επιτυγχάνεται μείωση του κόστους που απαιτείται να καταβάλλει μια εταιρεία ώστε να επιτευχθεί η επικοινωνία μεταξύ των εμπλεκομένων μελών. Ποια τεχνολογία και αρχιτεκτονική θα χρησιμοποιήσει κάθε φορά εξαρτάται από τις ανάγκες της και μόνο. Η υλοποίηση επιτυγχάνεται σχετικά εύκολα αρκεί πρώτα να έχει γίνει σωστός σχεδιασμός και να μην αντιμετωπίζεται σαν ένα ξεχωριστό κομμάτι του δικτύου αλλά ως συνέχειά του.

Τα Intranet VPN καταφέρνουν με τη βοήθεια του πρωτοκόλλου IP Security να εκμεταλλευτούν κάθε δυνατότητα του VPN προσφέροντας επεκτασιμότητα, ευελιξία, σταθερότητα και κυρίως ασφάλεια. Έτσι το IPSec έχει ως στόχο να μετατρέψει το διαδίκτυο σε ένα πιο ασφαλές περιβάλλον. Για να το πετύχει αυτό προσφέρει υπηρεσίες ασφάλειας με πρωτόκολλα στο επίπεδο δικτύου. Σε καμία περίπτωση όμως η εφαρμογή του IPSec, παρά τις πλούσιες υπηρεσίες ασφάλειας που παρέχει, δεν πρέπει να δώσει την ψευδαίσθηση στον υπεύθυνο ασφαλείας ότι το σύστημά του δεν είναι αναγκαίο να παρακολουθείται και να βελτιώνεται συνεχώς.

ΚΕΦΑΛΑΙΟ 7

7. Βιβλιογραφία –Αναφορές

Oleg Kolesnikov ,Brian Hatch :Building Linux Virtual Private Networks (VPNs): New Riders Publishing, 2002

Fowler, Dennis : *Virtual Private Networks Making The Right Connection.*San Francisco: Morgan Kaufmann, 1999

Paul Wouters ,Ken Bantoft :Building and Intergrating Virtual Private Networks With Openswan , 2006

Openswan implementation of IPsec for Linux

http://www.openswan.org/

Ipsec practical configurations for Linux Freeswan

http://jixen.tripod.com/

How to configure Openswan – Openswan to Openswan connections (using RSASIG or PSK)

http://techgurulive.com/2008/11/12/how-to-configure-openswan-openswan-to-openswan-connections-using-rsasig-or-psk/

Current IPSec Internet Drafts

http://www.ietf.org/ids.by.wg/ipsec.html

IPsec and IKE Administration Guide

http://docsun.cites.uiuc.edu/sun_docs/C/solaris_9/SUNWaadm/IPSECIKEADMIN/toc.html

Red Hat Enterprise Linux 4: System Administration Guide

http://www.centos.org/docs/4/html/rhel-sag-en-4/s1-network-config-ipsec.html

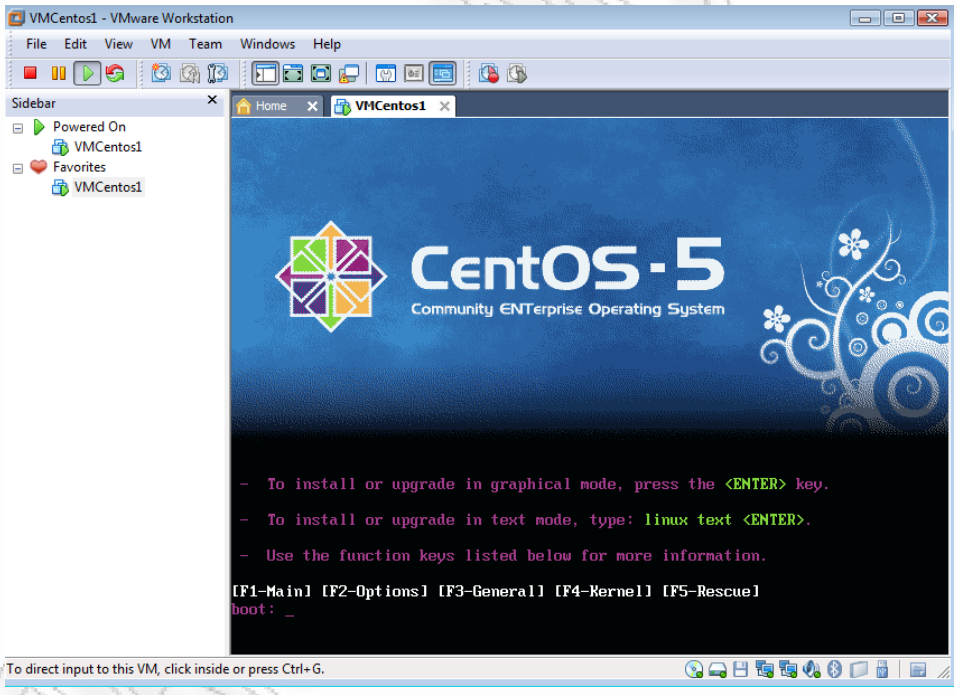
Introduction to FreeS/WAN

http://www.bec.at/support/ipsec/openswan/doc/HowTo.txt

ΠΑΡΑΡΤΗΜΑ Α

Εγκατάσταση Linux Centos 5.3 και Openswan

Στο παράρτημα Α θα δούμε αναλυτικά την εγκατάσταση και παραμετροποίηση ενός λειτουργικού συστήματος Centos 5.3 όπως και την εγκατάσταση του Openswan. Ξεκινάμε την διαδικασία εγκατάστασης από ένα iso αρχείο το οποίο κατεβάζουμε από την ιστοσελίδα του Centos (http://isoredirect.centos.org/centos/5/isos/i386/). Στην συνέχεια εκτελώντας τον συγκεκριμένο αρχείο μας ζητάει να επιλέξουμε αν η εγκατάσταση θα είναι σε γραφικό περιβάλλον ή όχι. Για λόγους απλότητας και για να γίνει πιο κατανοητό επιλέξαμε την εγκατάσταση σε γραφικό περιβάλλον όπως διακρίνουμε και στην εικόνα 1. Πατάμε λοιπόν enter για να ξεκινήσει η εγκατάσταση σε γραφικό περιβάλλον.

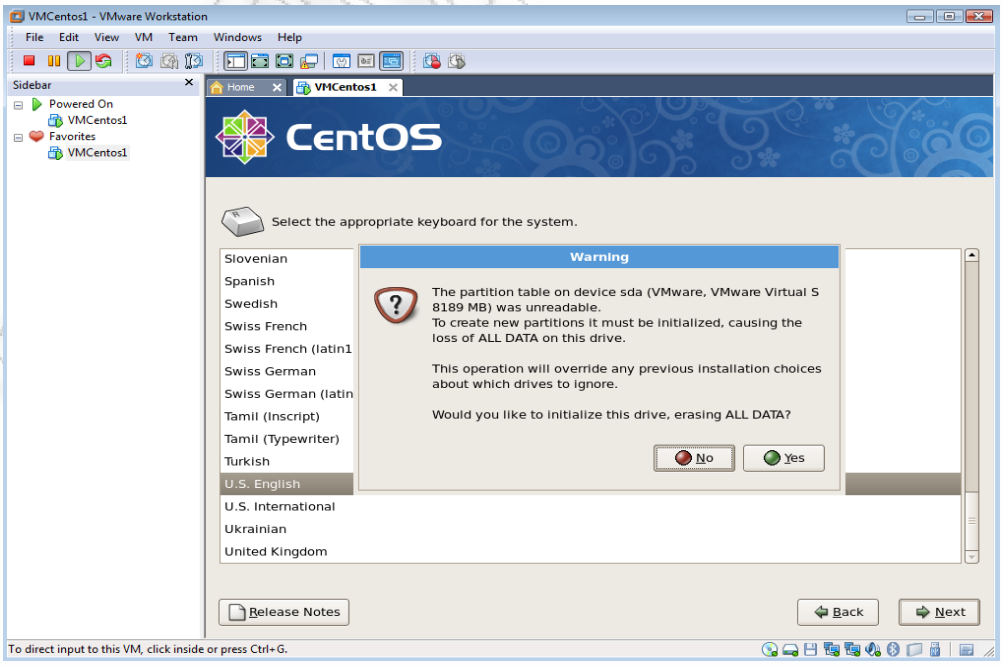


Εικόνα 1. Εγκατάσταση Linux Centos 5.3

Στην επόμενη εικόνα (Εικόνα 2), πατάμε next ώστε να συνεχιστεί η διαδικασία της εγκατάστασης.

Εικόνα 2. Εγκατάσταση Linux Centos 5.3

Στην συνέχεια (Εικόνα 3), επιλέγουμε την γλώσσα εγκατάστασης, όπου στην παρούσα εγκατάσταση θα είναι αγγλικά και δημιουργούμε ένα virtual δίσκο και κάνουμε initialize.

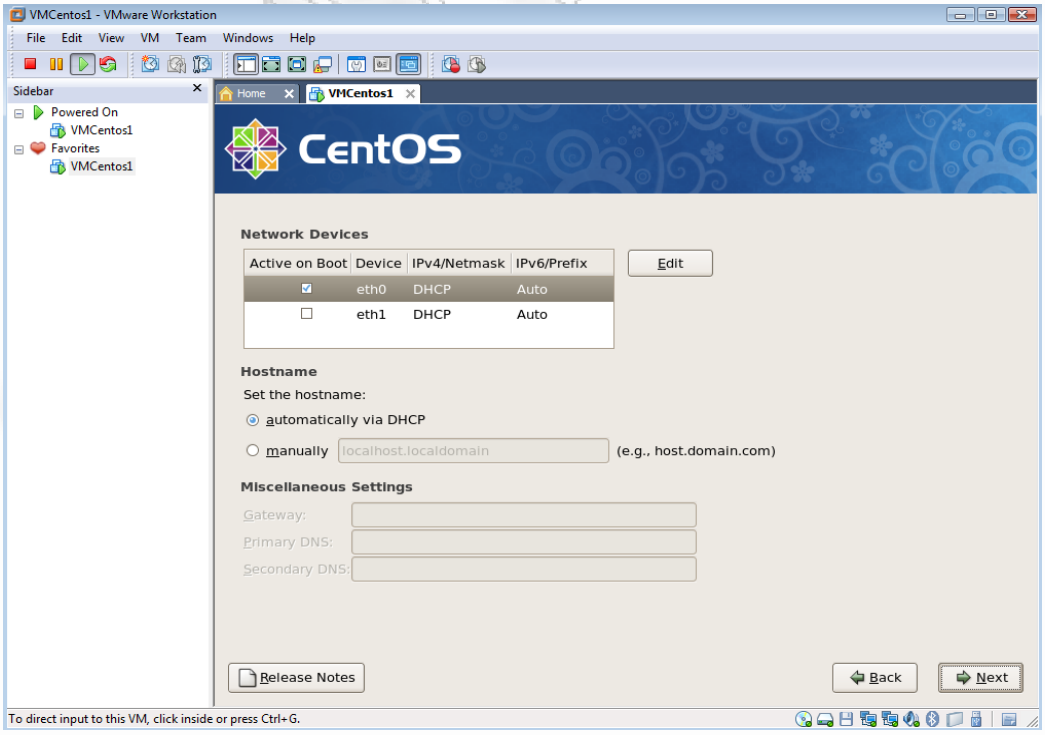


Εικόνα 3. Εγκατάσταση Linux Centos 5.3

Το επόμενο βήμα είναι να επιλέξουμε ή να επεξεργαστούμε τη διάταξη διαχωρισμού. Πατάμε το κουμπί next και συνεχίζει η εγκατάσταση (Εικόνα 4).

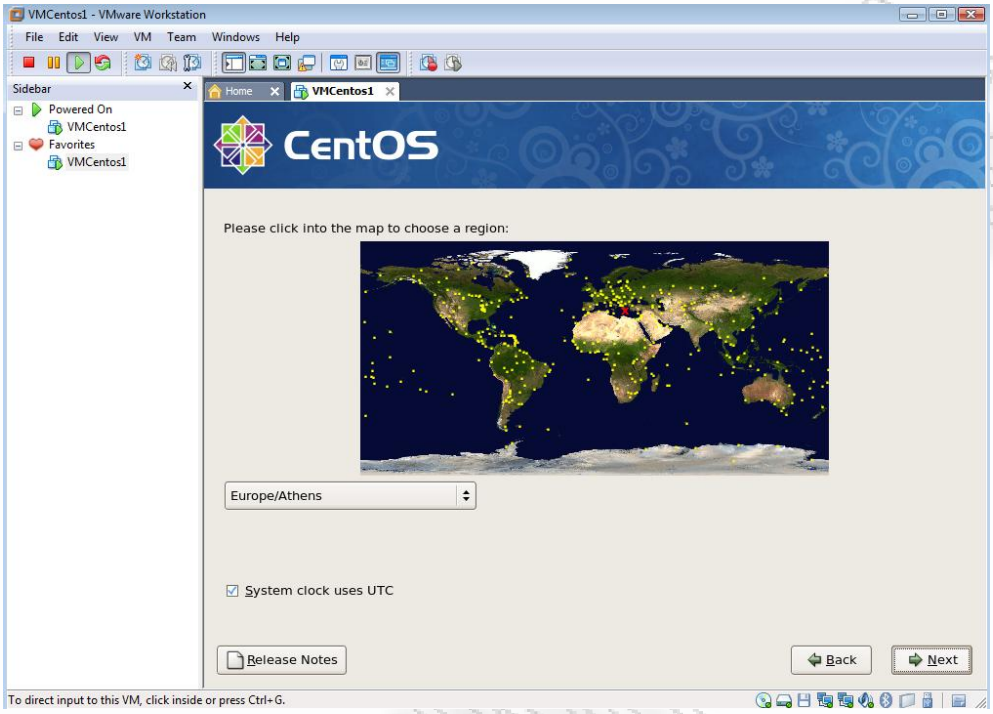
Εικόνα 4. Εγκατάσταση Linux Centos 5.3

Στο επόμενο βήμα κάνουμε τις απαραίτητες ρυθμίσεις δικτύου όπου απαιτούνται (Εικόνα 5) Πατάμε next και συνεχίζει η εγκατάσταση.



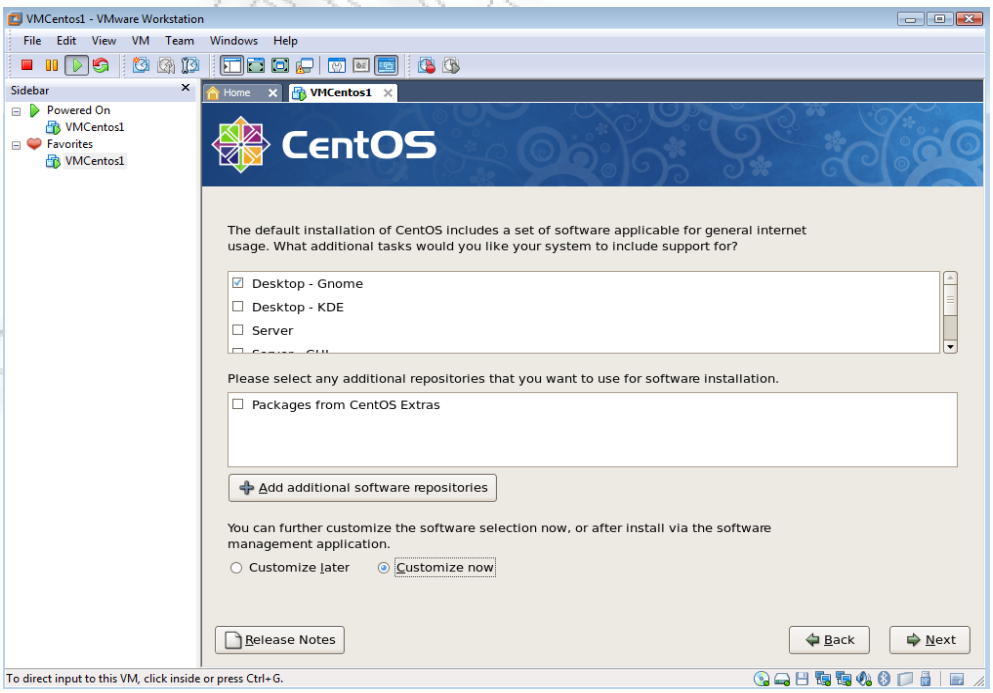
Εικόνα 5. Εγκατάσταση Linux Centos 5.3

Στην συνέχεια (Εικόνα 6), επιλέγουμε την τοποθεσία κοντά στην δική μας περιοχή και κάνουμε τις απαραίτητες ρυθμίσεις για το ρολόι.



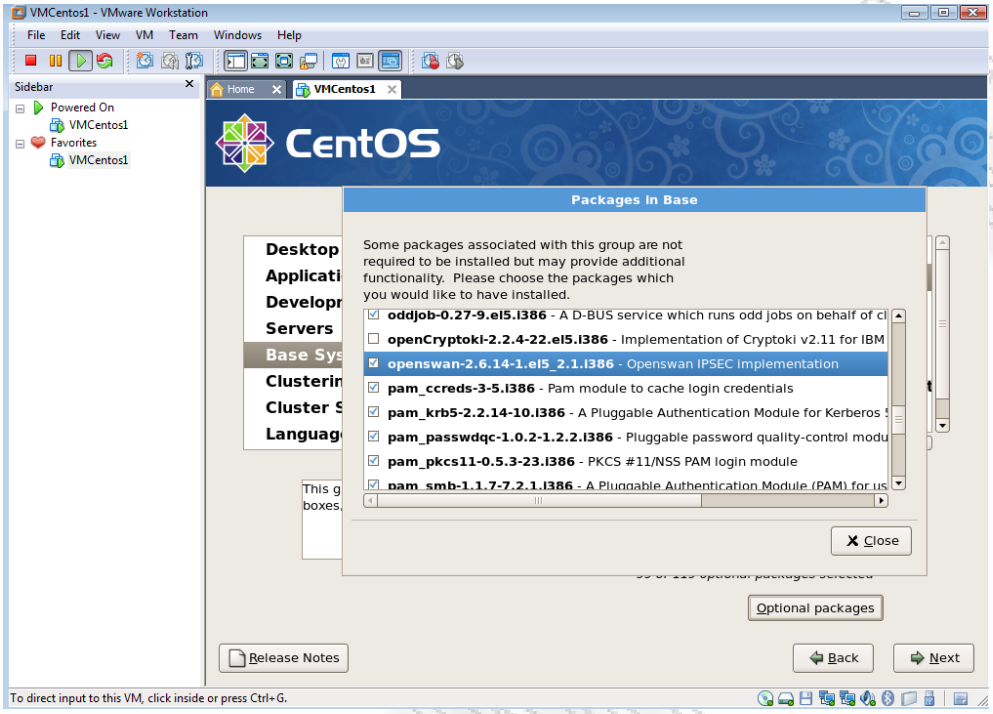
Εικόνα 6. Εγκατάσταση Linux Centos 5.3

Στο επόμενο βήμα (Εικόνα 7), μπορούμε να επιλέξουμε τις προκαθορισμένες συλλογές λογισμικού για εγκατάσταση. Μπορούμε επίσης να κάνουμε μια επιλογή αυτών που θέλουμε να εγκαταστήσουμε επιλέγοντας το αντίστοιχο κουμπί (Customize now).



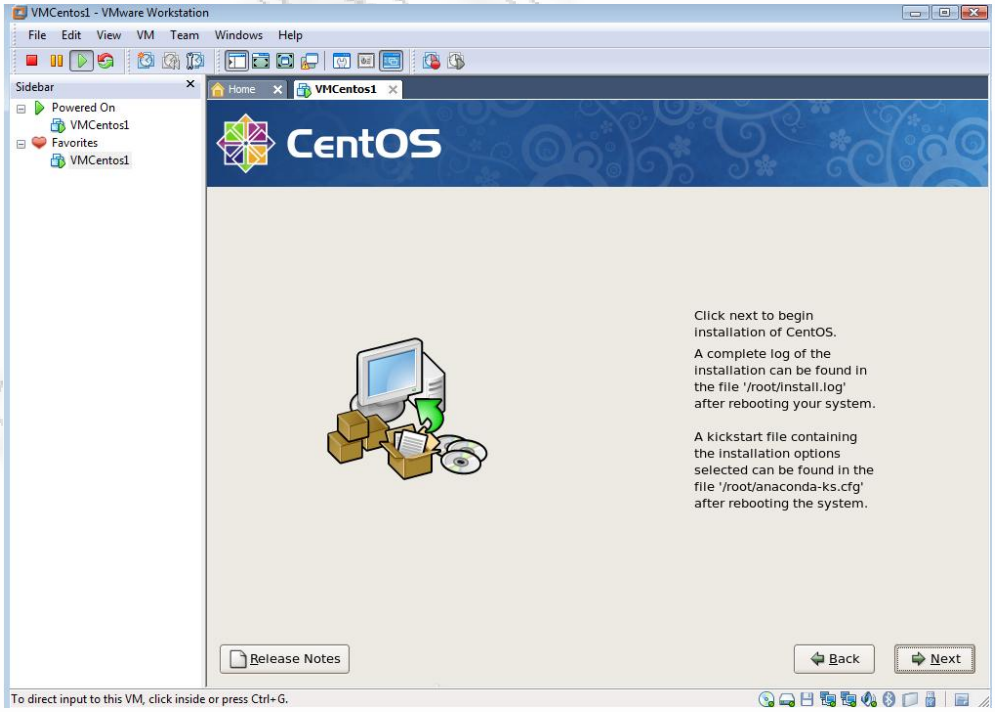
Εικόνα 7. Εγκατάσταση Linux Centos 5.3

Στην συνέχεια (Εικόνα 8), επιλέγουμε σαν επιπρόσθετο λογισμικό για εγκατάσταση το Openswan (Openswan IPSec implementation) και πατάμε next.



Εικόνα 8. Εγκατάσταση Linux Centos 5.3

Το σύστημα πλέον είναι έτοιμο προς εγκατάσταση (Εικόνα 9). Πατάμε next ώστε να ξεκινήσει.



Εικόνα 9. Εγκατάσταση Linux Centos 5.3

Το διαμέρισμα / δίσκος βρίσκεται στο στάδιο της μορφοποίησης (Εικόνα 10).

Εικόνα 10. Εγκατάσταση Linux Centos 5.3

Υπολειπόμενος χρόνος εγκατάστασης 4 λεπτά (Εικόνα 11).

Εικόνα 11. Εγκατάσταση Linux Centos 5.3

Η εγκατάσταση έχει ολοκληρωθεί. Πατώντας reboot κάνουμε επανεκκίνηση του συστήματος (Εικόνα 12).

Εικόνα 12. Ολοκλήρωση εγκατάστασης Linux Centos 5.3