Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

An analysis of VPN protocols and their usage in Cyber ranges

Ιωάννα Κωνσταντίνου

Επιβλέπων Καθηγήτρια
Αδαμαντίνη Περατικού

Μάιος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

An analysis of VPN protocols and their usage in Cyber ranges

Ιωάννα Κωνσταντίνου

Επιβλέπων Καθηγήτρια
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
Στην Ασφάλεια Υπολογιστών και Δικτύων
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2021

Περίληψη

Η συνεχής και αυξανόμενη χρήση του διαδικτύου, επέφερε ουσιαστικές αλλαγές στον τρόπο λειτουργίας των επιχειρήσεων. Η εξέλιξη αυτή, ναι μεν αύξησε την παραγωγικότητα και την κερδοφορία τους, αλλά ταυτόχρονα δημιούργησε και νέες απαιτήσεις στις επιχειρήσεις αυτές. Ένα δίκτυο το οποίο απλά συνδέει σταθερά σημεία στην επιχείρηση, δεν είναι πλέον αρκετό. Οι απομακρυσμένοι χρήστες, όπως εξωτερικοί συνεργάτες, χρειάζονταν πρόσβαση στους πόρους του δικτύου της επιχείρησης. Συνεπώς πολλές επιχειρήσεις στράφηκαν προς τα Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPNs) για να μπορέσουν να αναβαθμίσουν την υπάρχουσα WAN υποδομή τους και να μπορέσουν να επιλύσουν προβλήματα επικοινωνίας, οργάνωσης και διαχείρισης των δεδομένων τους από όπου και αν βρίσκονταν.

Στη μεταπτυχιακή αυτή διατριβή γίνεται αρχικά μια επεξήγηση για το τι είναι τα ιδεατά δίκτυα και γιατί τα χρησιμοποιούμε, καθώς και την αρχιτεκτονική και τα πρωτόκολλα που χρησιμοποιούν. Γίνεται αναφορά στο βέλτιστο τρόπο διασύνδεσης των cyber ranges με την χρήση VPN τεχνολογιών. Εστιάζει στους τύπους δικτύων VPN σε σχέση με την απομακρυσμένη σύνδεση, τη σύνδεση μέσω Intranet καθώς και τις απαιτήσεις και τις τεχνολογίες του.

Στη συνέχεια δημιουργείται ένα VPN με τη χρήση κάποιων πρωτοκόλλων και έγινε αξιολόγηση βάση ορισμένων κριτηρίων. Σκοπός είναι να αναδειχθεί η τεχνολογία που αποδίδει καλά κάτω από διάφορες συνθήκες φορτίου, αναλύοντας την ποιότητα υπηρεσίας, καθώς και την προστασία του δικτύου από πιθανή μη εξουσιοδοτημένη πρόσβαση ή καταστροφή.

Summary

The continuous and increasing use of the Internet has brought about substantial changes in the way businesses operate. This development although it increased their productivity and profitability, but at the same time created new needs for these companies. A network that simply connects fixed points to t he business is no longer enough. Remote users, such as external partners, needed access to the company's network resources. As a result, many companies have turned to Virtual Private Networks (VPNs) to upgrade their existing WAN infrastructure and be able to solve problems communicating, organizing, and managing their data from wherever they are.

This master's thesis initially explains what virtual networks are and why we use them, as well as the architecture and protocols they use. Reference is made to the best way to connect cyber ranges using VPN technologies. Focuses on VPN network types as they relate to remote connectivity, connection via Intranet, as well as its requirements and technologies.

Furthermore, a VPN is created using certain protocols and evaluated using a set of criteria. The goal is to show the technology that performs better under various load conditions, analyzing the quality of service, as well as protecting the network from possible unauthorized access or destruction.

Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή αποτελεί το επιστέγασμα μιας μεγάλης προσωπικής προσπάθειας αλλά ταυτόχρονα και μια αδιάκοπης συμπαράστασης από κάποιους ανθρώπους τους οποίους θα ήθελα να ευχαριστήσω και να εκφράσω την ευγνωμοσύνη μου για τη βοήθειά τους.

Πρώτα, θα ήθελα να ευχαριστήσω την επιβλέποντα καθηγήτρια μου Δρ. Αδαμαντίνη Περατικού, για τη στήριξη τη συμπαράσταση και την άρτια επιστημονική καθοδήγηση στην ολοκλήρωση της παρούσας διατριβής. Με διαρκή ενθάρρυνση, καθώς και τη θετική και αισιόδοξη της αύρα έφερα εις πέρας την εκπόνηση της διατριβής.

Ένα μεγάλο ευχαριστώ, το οφείλω στην οικογένειά μου, για όλη τη βοήθεια και τη στήριξη που μου έδωσαν. Στάθηκαν συμπαραστάτες στο πλευρό μου αδιαμαρτύρητα και υπέμειναν τις ατελείωτες ώρες δουλειάς και την κούραση μου με υπομονή και ενθάρρυνση.

Περιεχόμενα

Πίνακας σχημάτων – διαγραμμάτων – εικόνων

Όροι κλειδιά

VPN – Virtual Private Network

PPTP – Point to point Tunneling protocol

IPSEC – Internet protocol Security

SSL – Secure Sockets Layer

L2TP – Layer 2 Tunneling Protocol

ESP – Encapsulating Security Protocol

Security Protocols

VPN Vulnerabilities

Κεφάλαιο 1
Εισαγωγή

Όλο και περισσότεροι επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο απαιτούνται από τον κλάδο καθώς αυξάνεται ο αριθμός των απειλών στον κυβερνοχώρο. Αυτό είχε ως αποτέλεσμα την ανάγκη να εφαρμόσουν και να συνδυάσουν μέτρα ασφαλείας με τη χρήση νέων τεχνολογιών και καθιερωμένων μεθοδολογιών. Πολλά έθνη και ιδιωτικοί οργανισμοί χρησιμοποιούν ιδιωτικά περιβάλλοντα εκπαίδευσης και προσομοίωσης με βάση το cloud, τα λεγόμενα Cyber-Range. Το Cyber Range παρέχει τα μέσα για την εκπαίδευση στο Cyber Security και μπορεί να θεωρηθεί ως ένα ισχυρό εργαλείο για την παροχή ποσοτικής και ποιοτικής αξιολόγησης για εκπαιδευτικές δραστηριότητες.

1.1 Αναγκαιότητα και σπουδαιότητα της έρευνας

Η απομακρυσμένη χρήση δικτύου σε μια επιχείρηση / οργανισμό απαιτεί πρόσβαση στους πόρους της. Αυτό εξ υπακούει επέκταση του τοπικού δικτύου έτσι ώστε οι εργαζόμενοι – συνεργάτες να μπορούν να επικοινωνούν με την επιχείρηση τους από όπου και αν βρίσκονται. Συνεπώς πολλές επιχειρήσεις στρέφονται προς τα εικονικά Ιδιωτικά Δίκτυα (VPN'S). Η έρευνα αυτή συγκρίνει τον τρόπο σύνδεσης των τοπικών δικτύων και των VPN, με σκοπό να συμβάλει στην περαιτέρω γνώση της σπουδαιότητας των εικονικών δικτύων.

1.2 Σκοπός της Μεταπτυχιακής Διατριβής

Αυτή η διατριβή επικεντρώνεται στο να αναγνωρίσει ποσοτικά, το βέλτιστο τρόπο διασύνδεσης των cyber ranges με την χρήση VPN τεχνολογιών. Σκοπός είναι να δείξει την τεχνολογία που αποδίδει καλά κάτω από διάφορες συνθήκες φορτίου.

1.3 Βασικά ερευνητικά ερωτήματα

Ποιος είναι ο καλύτερος τρόπος διασύνδεσης των cyber ranges;

Μπορεί η τεχνολογία VPN να χρησιμοποιηθεί για ανάλυση αποτελεσματικότητας επικοινωνίας;

Ποια τεχνολογία αποδίδει καλύτερα κάτω από διάφορες συνθήκες φορτίου.

1.4 Οργάνωση της Διατριβής

Η παρούσα μεταπτυχιακή διατριβή θα ολοκληρωθεί μέσα από 7 κεφάλαια ως εξής:

Στο παρόν κεφάλαιο (πρώτο) γίνεται μια εισαγωγική αναφορά στους στόχους και στο αντικείμενο της έρευνας.

Στο κεφάλαιο 2, αναφέρεται η βιβλιογραφική ανασκόπηση της όλης εργασίας.

Στο κεφάλαιο 3 σημειώνονται οι ευπάθειες και τα ζητήματα ασφάλειας των εικονικών δικτύων.

Αφού ολοκληρωθεί το θεωρητικό μέρος, το κεφάλαιο 4 εμβαθύνει στη μεθοδολογία που χρειάστηκε για την δημιουργία και εγκατάσταση ενός VPN.

Ακολούθως, στο κεφάλαιο 5 γίνεται μια υλοποίηση με σκοπό τον έλεγχο του εικονικού δικτύου αναφέροντας τα αποτελέσματα.

Στο κεφάλαιο 6 γίνεται μια αναφορά στα πλεονεκτήματα και μειονεκτήματα των εικονικών δικτύων.

Η διατριβή ολοκληρώνεται με συμπεράσματα ερμηνεύοντας τα αποτελέσματα της παρούσας έρευνας.

Κεφάλαιο 2
Ανασκόπηση βιβλιογραφίας

Ένα δίκτυο το οποίο επικεντρώνεται στο να συνδέει απλά σταθερά σημεία μιας επιχείρησης /οργανισμού, δεν είναι πλέον αρκετό. Υπάρχει η ανάγκη για απομακρυσμένη χρήση του δικτύου (VPN) (1)παρέχοντας όμως σύμφωνα με τον James S. Tiller (2) το ίδιο επίπεδο ασφάλειας και την ίδια πολιτική σε όλο το μήκος του σαν να επρόκειτο για ιδιωτικό δίκτυο.

Υπάρχουν διάφορες τεχνολογίες VPN (3) που βασίζονται σε τεχνολογία Point-to-Point Tunneling Protocol (PPTP), IP Security standard Protocol (IPsec) ή SSL (Secure Sockets Layer)

Γενικά, το PPTP δεν προτιμάται λόγω ζητημάτων ασφάλειας, που προκύπτουν από την απλότητα του πρωτοκόλλου ενώ τα IPsec και SSL είναι ένα σύνολο κρυπτογραφικών πρωτοκόλλων που παρέχουν ασφαλή επικοινωνία.

Θα αναλυθούν εις βάθος τα πρωτόκολλα IPSEC (4), L2TP και Virtual tunnels (5) μέσα από ένα Cyber Range (6) αφού αυτό παρέχει τα μέσα για την εκπαίδευση στο Cyber Security και μπορεί να θεωρηθεί ως ένα ισχυρό εργαλείο για την παροχή ποσοτικής και ποιοτικής αξιολόγησης για εκπαιδευτικές δραστηριότητες. Έτσι θα διαφανεί ποια τεχνολογία αποδίδει καλύτερα (7) κάτω από διάφορες συνθήκες φορτίου αλλά και ποια τεχνολογία VPN είναι η βέλτιστη ως προς την απόδοση.

Επιπρόσθετα θα μελετηθεί κατά πόσον ένα VPN δίκτυο είναι ασφαλές και προστατευμένο από μια πιθανή μη εξουσιοδοτημένη πρόσβαση ή καταστροφή σύμφωνα με τον Nguyen, Nam (8).

2.1 Τι είναι το Virtual Private Network

Ένα εικονικό ιδιωτικό δίκτυο (VPN (9) – Virtual Private Network) είναι ένα δίκτυο ιδιωτικών δεδομένων το οποίο χρησιμοποιεί την υπάρχουσα τηλεπικοινωνιακή υποδομή, παρέχοντας όμως την διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα και ασφάλεια χρησιμοποιώντας πρωτόκολλα διόδου (tunneling protocol) και διάφορες

διαδικασίες ασφάλειας. Σύμφωνα και με τον IETF[1] τα VPNs θεωρούνται ως εξομοίωση ενός προσωπικού Wide Area Network (WAN) χρησιμοποιώντας ένα προσβάσιμο μέσο επικοινωνίας όπως είναι το Internet και τα IP δίκτυα. Κύριος σκοπός ενός VPN είναι να δώσει στην επιχείρηση τις ίδιες ακριβώς δυνατότητες με τις ιδιωτικές γραμμές, όμως με αρκετά χαμηλότερο κόστος αφού χρησιμοποιεί ένα δημόσιο τηλεπικοινωνιακό δίκτυο. Με ένα εικονικό ιδιωτικό δίκτυο έχουμε τις ίδιες δυνατότητες με το δημόσιο, με την διαφορά ότι υπάρχει ταυτόχρονη μεταφορά ψηφιακών δεδομένων και φωνής από την ίδια ταχύτητα, όμως με το ίδιο επίπεδο ασφάλειας. Ένα VPN μεταφέρει δεδομένα δημιουργώντας ένα τούνελ και προωθώντας τα μέσα από αυτό. Για τη μεταφορά αυτή, το πακέτο του χρήστη ενσωματώνεται σε ένα άλλο πακέτο με μια νέα κεφαλίδα η οποία περιέχει όλες τις πληροφορίες που χρειάζονται για να μπορεί το πακέτο να "ταξιδέψει " μέσα από το μη ασφαλές δημόσιο δίκτυο. Ο δέκτης του πακέτου το λαμβάνει, εξάγει το αρχικό πακέτο και το προωθεί καταλλήλως. Αυτό το μονοπάτι ονομάζεται τούνελ και για να μπορεί να γίνει αυτή η μεταφορά θα πρέπει και τα δύο άκρα να χρησιμοποιούν το ίδιο πρωτόκολλο.

2.2 Ιστορική αναδρομή

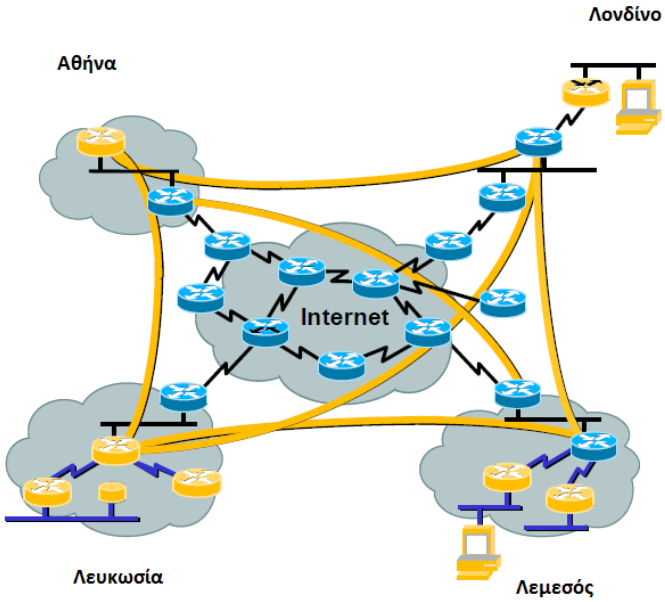
Τα Εικονικά Ιδιωτικά Δίκτυα στη σημερινή εποχή αποτελούν ένα σύγχρονο και ταυτόχρονα εξελισσόμενο πεδίο και εφαρμόζονται κυρίως σε μεγάλες εταιρείες αλλά και σε κάποιες περιπτώσεις απομακρυσμένης πρόσβασης των χρηστών με απώτερο σκοπό την κάλυψη της επικοινωνιακής τους ανάγκης. Η τεχνολογία αυτή έχει αρκετά πλεονεκτήματα, τα κυριότερα από αυτά το χαμηλότερο κόστος και η μεγάλη ευελιξία στη διαχείριση τους. Ο όρος «εικονικό δίκτυο» σημαίνει ότι οι δικτυακές συνδέσεις είναι ιδεατές, με την έννοια ότι όλα τα δεδομένα που αποστέλνονται μεταξύ δύο χρηστών μπορεί κάθε φορά να ακολουθούν διαφορετική διαδρομή μέχρι να φτάσουν στον προορισμό τους. Ο όρος «ιδιωτικό δίκτυο» σημαίνει ότι η πρόσβαση σε αυτό γίνεται μόνο από εξουσιοδοτημένους χρήστες.

[1] Η Internet Engineering Task Force είναι ένας διεθνής οργανισμός που αναπτύσσει και προωθεί διαδικτυακά πρότυπα (www.ietf.org)

2.3 Τα πρώτα ιδιωτικά δίκτυα

Τα πρώτα ιδιωτικά δίκτυα εμφανίστηκαν το 1960. Οι μισθωμένες αυτές γραμμές χρησιμοποιήθηκαν για τα εξής:

Επικοινωνία μέσω τηλεφώνου
Μετάδοση δεδομένων
Σύνδεση με δημόσια ή ιδιωτικά δίκτυα
Σύνδεση Τηλεφωνικών Κέντρων
Χρήση FAX
Σύνδεση με το διαδίκτυο



Σχήμα 1: VPN μιας επιχείρησης με πολλά παραρτήματα πάνω στο IP

Η πιο συνηθισμένη περίπτωση Εικονικών Ιδιωτικών Δικτύων είναι το IP VPN. Βασίζεται στο πρωτόκολλο IP, όπου οι πληροφορίες διαμορφώνονται σε πακέτα IP και μεταδίδονται στο δίκτυο IP (σχήμα 1). Είναι μια σύνδεση δικτύου η οποία από την πλευρά των χρηστών συμπεριφέρεται σαν να είναι μια ιδιωτική σύνδεση, παρά το ότι χρησιμοποιείται κοινή διαμοιρασμένη δικτυακή υποδομή (shared communication infrastructure). Επίσης η εφαρμογή των Εικονικών Ιδιωτικών Δικτύων μπορεί να

βασίζεται και στις τεχνολογίες ATM[2] (Asynchronous Transfer Mode), Frame Relay[3] ή MPLS[4] (Multiprotocol Label Switching). Το ATM και το Frame Relay λειτουργούν στο επίπεδο data link του μοντέλου OSI[5], ενώ το MPLS λόγω της ιδιομορφίας του λειτουργεί ανάμεσα στο data link και στο network layer.

2.4 Πρωτόκολλο IP

Το IP είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για τη διασύνδεση ηλεκτρονικών υπολογιστών οι οποίοι ανήκουν είτε στο ίδιο δίκτυο είτε σε διαφορετικό. Η μετάδοση αυτή γίνεται με την τεχνική των πακέτων (datagrams). Το κάθε πακέτο του IP θα φτάσει στον παραλήπτη του διασχίζοντας ένα ή και περισσότερα δίκτυα IP χωρίς όμως να έχει εξάρτηση από άλλα πακέτα (προηγούμενα ή επόμενα) και έτσι μπορεί να διατηρήσει την αυτονομία του μέσα στο δίκτυο. (10)
Θεωρείται πρωτόκολλο τρίτου επιπέδου το οποίο ασχολείται με τον κατακερματισμό (fragmentation) μεγάλων πακέτων και την διευθυνσιοδότηση. Παρόλα αυτά δεν θεωρείται αξιόπιστο καθώς δεν εξασφαλίζει την απ΄ άκρου εις άκρου ακεραιότητα των δεδομένων μέσω κάποιων τεχνικών επανεκπομπής, ελέγχου ροής κλπ. Όλες αυτές οι λειτουργίες θα επιτευχθούν με το πρωτόκολλο TCP το οποίο ανήκει στο αμέσως ανώτερο επίπεδο.

2.5 Τεχνολογία MPLS

Το MPLS (11) είναι ένα πρωτόκολλο το οποίο δημιουργήθηκε από την IETF [6] και έχει στόχο την αύξηση της ευελιξίας και της απόδοσης του παραδοσιακού IP, αλλά ταυτόχρονα να δώσει τη δυνατότητα για την παροχή νέων υπηρεσιών στο Διαδίκτυο.

[2]Ο ασύγχρονος τρόπος μεταφοράς ATM είναι ένας τρόπος μεταγωγής και διασύνδεσης των ευρυζωνικών δημόσιων δικτύων για τη μεταφορά πληροφοριών.
[3] Frame Relay είναι μια τεχνολογία WAN η οποία δίνει τη δυνατότητα σε οργανισμούς και εταιρείες να διασυνδέουν τα τοπικά δίκτυα τους χρησιμοποιώντας όμως ως δίκτυο κορμού το δημόσιο δίκτυο.
[4] MPLS ορίζεται μια τεχνική δικτύωσης μεταγωγής πολλαπλών πρωτοκόλλων και κατ΄επέκταση διασφάλιση αξιόπιστων συνδέσεων.
[5] Το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή μοντέλο αναφοράς OSI (αγγλ. OSI reference model) είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων η οποία καθορίστηκε από την πρωτοβουλία Ανοικτή Διασύνδεση Συστημάτων – OSI. Είναι γνωστό και ως μοντέλο των επτά επιπέδων, βλέπε https://en.wikipedia.org/wiki/OSI_model
[6] Internet Engineering Task Force: αναπτύσσει και προωθεί πρότυπα (Standards) του Internet, συνεργαζόμενη στενά με τους οργανισμούς **W3C** και **ISO/IEC** βλέπε, https://el.wikipedia.org/wiki/IETF

2.6 Αρχιτεκτονικές εικονικών ιδιωτικών δικτύων

Τα Εικονικά Ιδιωτικά Δίκτυα, κατηγοριοποιούνται με διάφορους τρόπους, σύμφωνα με την οπτική γωνία που θα μελετηθούν ως εξής:

1. Βάση της αντιστοιχίας τους με τα επίπεδα του μοντέλου αναφοράς OSI
    a) Εικονικά Ιδιωτικά Δίκτυα επιπέδου Δικτύου (3ου): στην ομάδα αυτή ανήκουν τα VPN τα οποία κτίζονται πάνω σε IP δίκτυα και χρησιμοποιούν το πρωτόκολλο IPSec, καθώς και τα VPN που κτίζονται σε MPLS δίκτυα.
    b) Εικονικά Ιδιωτικά Δίκτυα επιπέδου Ζεύξης Δεδομένων (2ου): στην ομάδα αυτή ανήκουν τα VPN στα οποία χρησιμοποιείται κάποιο από τα πρωτόκολλα L2F, PPTP και L2TP, και όσα μπορούν να αναπτυχθούν πάνω στην τεχνολογία MPLS.
    c) Εικονικά Δίκτυα επιπέδου Μεταφοράς (4ου): στην ομάδα αυτή ανήκουν τα VPN στα οποία χρησιμοποιείται το πρωτόκολλο SSL.

2. Βάση του είδους της διόδου[7] (tunnel) που αναπτύσσεται ως εξής:
    a) Εθελοντικό τούνελ (Voluntary Tunnel) : απαιτεί από τον πελάτη (client) να έχει τη δυνατότητα να διαχειρίζεται το δικό του VPN τούνελ. Σε αυτή την περίπτωση, όταν τα δεδομένα προορίζονται για το εταιρικό δίκτυο, στέλνονται μέσω του τούνελ που εγκαθίσταται από τον πελάτη.
    b) Υποχρεωτικό τούνελ (Compulsory ή Mandatory Tunnel): ένα υποχρεωτικό τούνελ είναι εντελώς διαφανές στον τελικό χρήστη.

3. Βάση του ποιοι είναι οι τελικοί χρήστες του VPN (ποια δύο μέρη συνομιλούν) ως εξής:
    a) VPN «πελάτης προς δίκτυο» (client to LAN) όπου ένας απλός χρήστης συνδέεται με τον υπολογιστή του σε ένα τοπικό δίκτυο. (μπορεί επίσης να ονομαστεί και «Εικονικό Ιδιωτικό Δίκτυο Απομακρυσμένης Πρόσβασης»)
    b) VPN «δίκτυο προς δίκτυο» (LAN to LAN), όπου τα δεδομένα μεταφέρονται μέσω της διόδου που αναπτύσσεται μεταξύ των δυο τοπικών δικτύων.

[7] Με τον όρο "Δίοδο" εννοούμε πρακτικά το νοητό κύκλωμα που σχηματίζεται, μέσω του οποίου γίνεται η μετάδοση των δεδομένων στο VPN.

Αντιστοιχώντας ένα Εικονικό Ιδιωτικό Δίκτυο με κάποιο είδος από τις τρεις πιο πάνω κατηγορίες, μπορούμε να το περιγράψουμε πλήρως. Πιο κάτω θα ακολουθήσει μια ανάλυση βασισμένη στην πρώτη κατηγοριοποίηση, δηλαδή ως προς τα επίπεδα των πρωτοκόλλων που χρησιμοποιούνται, σε σχέση με τα επίπεδα αναφοράς του OSI.

2.7 Το πρωτόκολλο IPSec (Internet Protocol Security)

Για την ύπαρξη ασφαλής μετάδοσης δεδομένων πάνω σε ένα δίκτυο IP, χρειάστηκε η δημιουργία ενός νέου πρωτοκόλλου με μηχανισμό κρυπτογράφησης. Το εν λόγω πρωτόκολλο πρέπει να είναι εφαρμόσιμο σε IP δίκτυα, αφού το TCP/IP δεν παρέχουν μηχανισμούς κρυπτογράφησης. Έτσι το IETF[8] ανάπτυξε το πρωτόκολλο IPSec με στόχο την ασφαλή ανταλλαγή και μετάδοση δεδομένων (Packets) μέσω του στρώματος IP. Σήμερα, αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των VPN.
Βασικός στόχος στην ανάπτυξη του IPSec, είναι η αντιμετώπιση των θεμάτων ασφαλείας που προκύπτουν από τη χρήση του Διαδικτύου για πραγματοποίηση ιδιωτικών επικοινωνιών, χωρίς να απαιτείται πρόσθετος εξοπλισμός, αλλά ούτε αλλαγές σε υφιστάμενες εφαρμογές.
Έτσι το πρωτόκολλο IPSec προσφέρει τις πιο κάτω υπηρεσίες:

- **Ακεραιότητα των δεδομένων (Integrity),** η οποία διασφαλίζει ότι τα πακέτα των δεδομένων, δεν έχουν αλλοιωθεί ή παραποιηθεί κατά τη διάρκεια της μεταφοράς τους από τυχών σφάλματα επικοινωνίας ή παράνομους «εισβολείς».(Η διασφάλιση αυτή γίνεται με τη χρήση των πρωτοκόλλων ασφάλειας AH (Authentication Header και ESP (Encapsulation Security Payload)

- **Εμπιστευτικότητα (Confidentiality),** η οποία προσφέρει τη δυνατότητα επεξεργασίας και αναγνώρισης των δεδομένων μόνο από εγκεκριμένους χρήστες.

[8] Internet Engineering Task Force

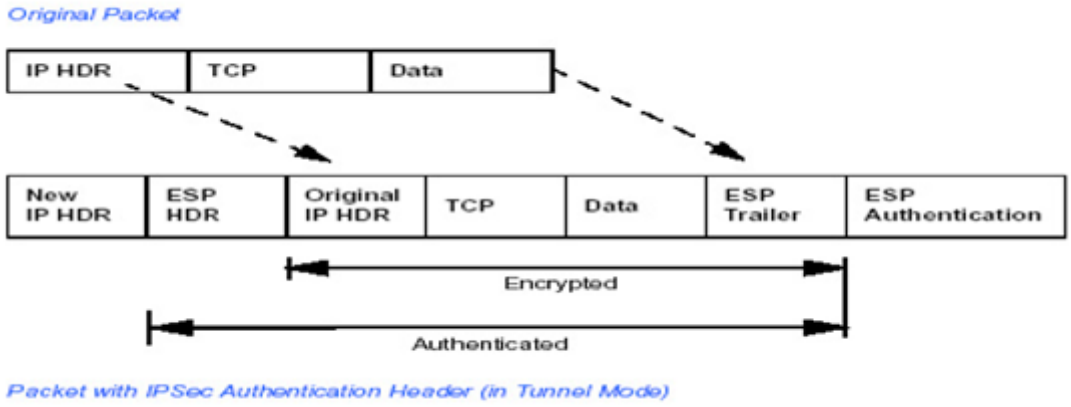
- **Εξακρίβωση της γνησιότητας της προέλευσης των δεδομένων (Authentication),** κατά την οποία επαληθεύονται ότι τα δεδομένα στάλθηκαν πράγματι από το χρήστη που ισχυρίζεται ότι τα έστειλε.

2.7.1 Τρόπος Λειτουργίας

Το IPSec πρωτόκολλο ελέγχεται από μια πολιτική ασφαλείας σε κάθε υπολογιστή και μια παραμετροποιημένη σύνδεση ασφαλείας ανάμεσα στον αποστολέα και τον παραλήπτη (Security Association – SA). Αποτελεί μια λογική σύνδεση μεταξύ δύο συσκευών που μεταφέρουν δεδομένα. Προσφέρει ασφάλεια δεδομένων για κίνηση μονής κατεύθυνσης χρησιμοποιώντας τα καθορισμένα πρωτόκολλα του IPSec. Ένα τέτοιο τούνελ τυπικά αποτελείται από δύο SAs, τα οποία μαζί παρέχουν ένα προστατευμένο κανάλι δεδομένων διπλής κατεύθυνσης. Ένα SA επιτρέπει σε μια επιχείρηση/οργανισμό να έχει πλήρως τον έλεγχο για το ποιοι πόροι επικοινωνούν με ασφάλεια σύμφωνα με την πολιτική προστασίας της εταιρείας. Όμως για να μπορεί να επιτευχθεί αυτό, θα πρέπει η επιχείρηση να δημιουργήσει (να «στήσει») πολλά SA με απώτερο σκοπό τη δημιουργία πολλών VPN αλλά και επιπλέον SAs μέσα στο VPN έτσι ώστε να μπορέσει να υποστηρίξει και άλλα τμήματα ή συνεργάτες της εταιρείας. Οι συσχετισμοί αυτοί χρησιμοποιούν δύο τρόπους λειτουργίας:

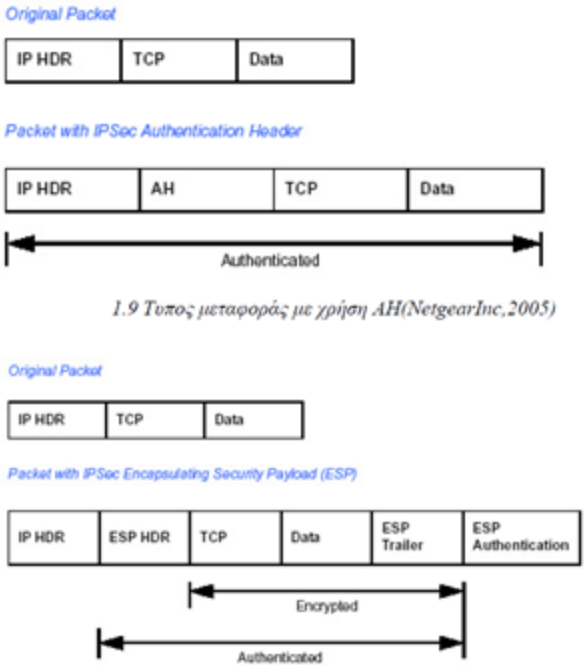
- Τούνελ (χρησιμοποιείται για gateway-to-gateway IPSec προστασία - σχήμα 2)
- Μεταφοράς (χρησιμοποιείται για host-to-host IPSec προστασία – σχήμα 3)

- Τύπος τούνελ: όλο το πακέτο ενσωματώνεται και γίνεται το φορτίο (payload) το οποίο κάνει χρήση του IPSec. Έτσι, δημιουργείται μια νέα κεφαλίδα IP η οποία περιέχει τις δύο διευθύνσεις των gateways. Οι gateways πραγματοποιούν την ενσωμάτωση /αποενσωμάτωση εκ μέρους των εξυπηρετητών. Με αυτόν τον τρόπο, αποτρέπεται η υποκλοπή και ανάλυση δεδομένων από κάποιο επιτιθέμενο, όπως επίσης δεν μπορεί να φανεί από πού και προς που πάνε τα πακέτα.



Σχήμα 2: Τύπος τούνελ με AH

- Τύπος μεταφοράς : δεν γίνεται αλλαγή των κεφαλίδων IP στον τύπο αυτό. Αυτές που μεταφέρονται είναι οι κεφαλίδες του αρχικού πακέτου και το επεξεργασμένο φορτίο του πακέτου (οι διευθύνσεις IP της πηγής και του προορισμού, δεν αλλάζουν). Όμως η κεφαλίδα δεν προστατεύεται και έτσι μπορεί ένας επιτιθέμενος να μάθει από πού προέρχεται αλλά και που πάει το πακέτο.



1.9 Τυπος μεταφοράς με χρήση AH(NetgearInc,2005)

Σχήμα 3: Τύπος μεταφοράς με χρήση ESP

Οι λειτουργίες που εκτελεί το IPSec μπορούν να κατηγοριοποιηθούν σε δύο επίπεδα. Το πρώτο επίπεδο σχετίζετε με τα δεδομένα (data plane) και το άλλο με το επίπεδο του

ελέγχου (control plane). Το πρώτο επίπεδο, υλοποιείται με τη χρήση δύο IPSec πρωτοκόλλων:

- Το πρωτόκολλο αυθεντικοποίησης επικεφαλίδας - Authentication Header (AH) και
- Το πρωτόκολλο Ασφαλούς Ενθυλάκωσης Πακέτου - encapsulating Security Payload (ESP)

Και τα δύο αυτά πρωτόκολλα εκτελούν ενέργειες σχετικά με το χειρισμό των πακέτων, όπως για παράδειγμα η κρυπτογράφηση και αποκρυπτογράφηση τους.
Το δεύτερο επίπεδο υλοποιείται με τη χρήση του πρωτοκόλλου

- Internet Key Exchange (IKE[9])

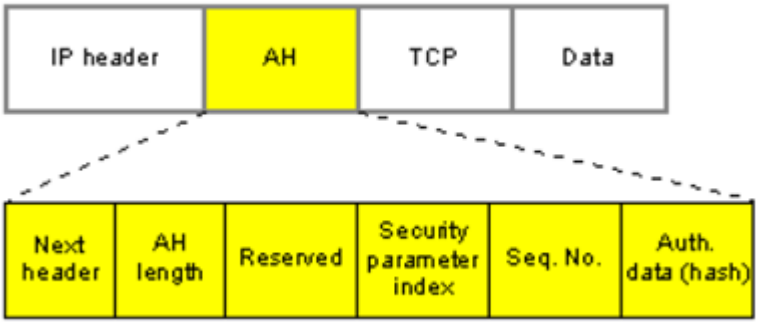
Το οποίο αφορά την ανταλλαγή των πληροφοριών πιστοποίησης και άλλων πληροφοριών μεταξύ των δύο άκρων του tunnel.

2.8 Το πρωτόκολλο Authentication Header (AH)

Το AH πρωτόκολλο (12) παρέχει προστασία στην ακεραιότητα των δεδομένων και της επικεφαλίδας των πακέτων που μεταφέρονται, καθώς επίσης και αυθεντικοποίηση του χρήστη (για αποφυγή διπλότυπων πακέτων). Δεν παρέχει ασφάλεια εμπιστευτικότητας καθώς δεν έχει οποιοδήποτε μηχανισμό κρυπτογράφησης. Προαιρετικά μπορεί να προσφέρει και προστασία από διάφορες επιθέσεις δικτύου όπως replay attack (η οποία προστατεύει από μη εξουσιοδοτημένη αναμετάδοση των πακέτων). Στην αρχική έκδοση του IPSec χρησιμοποιούταν σε συνδυασμό με το ESP πρωτόκολλο, γιατί αυτό παρείχε μεθόδους κρυπτογράφησης. Στη συνέχεια, στη δεύτερη έκδοση του IPSec προστέθηκαν δυνατότητες Encapsulating Security Payload, και το πρωτόκολλο AH άρχισε σιγά σιγά να χάνει την αξία του. Όμως παρόλα αυτά το AH έχει ακόμα αξία γιατί παρέχει αυθεντικοποίηση σε ορισμένα πεδία ενός πακέτου που το ESP δεν μπορεί.

Η μορφή της κεφαλίδας του AH πρωτοκόλλου είναι:

[9] Internet Key Exchange – το πρωτόκολλο που χρησιμοποιείται για τη δημιουργία μιας συσχέτισης ασφαλείας στη σουίτα πρωτοκόλλου IPsec. Βασίζεται στα πρωτόκολλα Oakley και ISAKMP. (Πηγή: Wikipedia)



Σχήμα 4: Μορφή AH και ενσωμάτωση σε πακέτο IP

Τα πεδία της κεφαλίδας είναι:

Next Header: Προσδιορίζει ποια θα είναι η επόμενη κεφαλίδα που είναι παρούσα στο πακέτο (π.χ. TCP, UDP)

Payload Length: το μέγεθος του φορτίου (πολλαπλάσιο των 32 bit)

Reserved: Πρέπει να τεθεί σε μηδενικά πριν την αποστολή (η τιμή αυτή είναι δεσμευμένη για μελλοντική χρήση)

Security Parameter Index (SPI): προσδιορίζει στον παραλήπτη ποια πρωτόκολλα ασφαλείας χρησιμοποιήθηκαν από τον αποστολέα

Sequence Number: ακολουθιακός αριθμός ο οποίος αυξάνεται κατά ένα για κάθε νέο πακέτο που καταφθάνει στο δέκτη από τον ίδιο αποστολέα και με το ίδιο SPI (χρησιμοποιείται για να αποφεύγεται η κατά λάθος επανεκπομπή του ίδιου πακέτου).

Authentication Data:ο υπολογισμός της τιμής των πιστοποιημένων δεδομένων. Πάντα πρέπει να είναι πολλαπλάσιο των 32bit.

Τρόπος λειτουργίας Authentication Header

Για να μπορέσουμε να εξετάσουμε συνολικά πως λειτουργεί το πρωτόκολλο AH θα χωρίσουμε την επεξεργασία που πραγματοποιείται σε δύο μέρη, την επεξεργασία των

- εξερχόμενων και
- εισερχόμενων πακέτων

Επεξεργασία εξερχόμενων: στην περίπτωση αυτή, όταν ένα πακέτο προς εκπομπή φτάσει στο στρώμα του IPSec, ελέγχεται μέσω της βάσης δεδομένων SPD[10], η πολιτική ασφαλείας που ακολουθεί ο σταθμός για την κατηγορία πακέτων στην οποία ανήκει το συγκεκριμένο πακέτο. Αν το συγκεκριμένο πακέτο πρέπει να «ασφαλιστεί», τότε εφαρμόζονται σε αυτό τα αντίστοιχα πρωτόκολλα (AH, ESP). Όταν γίνει η επιλογή του κατάλληλου συσχετισμού ασφάλειας και η εγκατάσταση του, αμέσως μετά πρέπει να μηδενιστεί η τιμή του Sequence Number. Η επιλογή του κατάλληλου συσχετισμού SA γίνεται μέσα από τη Βάση Δεδομένων Συσχετισμού Ασφάλειας (Security Association Database – SAD) που υπάρχει σε κάθε σταθμό.

Επεξεργασία εισερχόμενων: με την παραλαβή του πακέτου από το δίκτυο, ο τερματικός σταθμός διαβάζει τη διεύθυνση IP του αποστολέα, το πρωτόκολλο ασφαλείας (AH) και την τιμή SPI. Μέσα από αυτόν το συνδυασμό αποφαίνεται για το ποια SA από τη SAD πρέπει να χρησιμοποιηθεί. Τα επόμενα βήματα καθορίζονται από τη SA στην οποία καταλήγει:

1. Αν υποστηρίζεται η υπηρεσία αποφυγής επανάληψης πακέτου, ο σταθμός θα ελέγξει την τιμή του Sequence Number, η οποία αν συμπίπτει με την τιμή κάποιου προηγούμενου πακέτου, το νέο πακέτο θα απορριφθεί.
2. Επισημαίνεται ο αλγόριθμος ο οποίος θα υπολογίσει εκ νέου την τιμή ICV όπως επίσης και κάποιο πιθανό κλειδί για την κωδικοποίηση της. Έτσι ο παραλήπτης θα υπολογίσει την τιμή του ICV, θα την κωδικοποιήσει και θα τη συγκρίνει με αυτή που ήρθε στο πακέτο. Αν συμπίπτουν οι τιμές, τότε θα αποδεχτεί το πακέτο.
3. Αν το πακέτο στάλθηκε από μια λάθος διεύθυνση, θα είχε αποφανθεί για μια SA η οποία δεν θα είχε χρησιμοποιηθεί. Θα χρησιμοποιούσε άλλο αλγόριθμο υπολογισμού του ICV, το οποίο θα κατέληγε σε ένα διαφορετικό ICV από αυτό που ήρθε με το πακέτο, όπου τελικά το πακέτο θα απορριφθεί.

2.8.1 Συμπέρασμα για το πρωτόκολλο AH

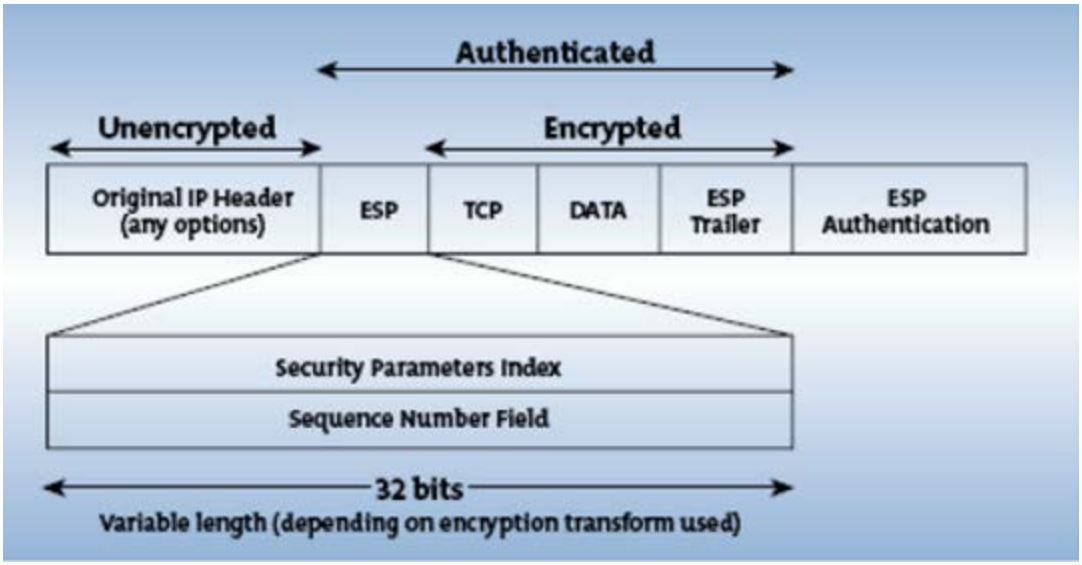
- Το πρωτόκολλο AH παρέχει προστασία ακεραιότητας των δεδομένων για όλα τα πακέτα (επικεφαλίδα και δεδομένα), με τη μόνη εξαίρεση ότι ορισμένα πεδία από την IP επικεφαλίδα, τα οποία νόμιμα αλλάζουν την τιμή τους κατά τη μετάδοση.

[10] Security Policy Database: είναι η βάση στην οποία αποθηκεύονται πληροφορίες οι οποίες κατηγοριοποιούν τη διερχόμενη κίνηση σε αυτή που απαιτεί IPSec προστασία, σε αυτή που δεν απαιτεί IPSec προστασία και σε αυτή που απορρίπτεται.

- Το AH περιέχει την IP διεύθυνση του προορισμού και της αφετηρίας στους υπολογισμούς που πρέπει να γίνουν για την προστασία ακεραιότητας δεδομένων, κάτι που δημιουργεί ασυμβατότητες με την τεχνολογία NAT.
- Επίσης το AH παρέχει μόνο αυθεντικοποίηση και όχι κρυπτογράφηση, και πλέον οι πιο πολλές υλοποιήσεις IPSec γίνονται με τη δεύτερη έκδοση του, όπου το ESP μπορεί να παρέχει προστασία ακεραιότητας. Είναι σημαντικό να αναφερθεί ότι η χρήση του AH έχει μειωθεί σημαντικά και πλέον κάποιες υλοποιήσεις IPSec δεν υποστηρίζουν καθόλου AH.

2.9 Το πρωτόκολλο Ασφαλούς Ενθυλάκωσης πακέτου (ESP -Encapsulating Security Payload)

Το πρωτόκολλο ESP είναι το δεύτερο κομμάτι της ομάδας πρωτοκόλλων του IPSec. Επιπρόσθετα των χαρακτηριστικών του AH το ESP παρέχει και το απόρρητο του πακέτου, δηλαδή ένα μηχανισμό κρυπτογράφησης των IP δεδομένων χρησιμοποιώντας έναν συμμετρικό αλγόριθμο κρυπτογράφησης. Επίσης παρέχει ταυτοποίηση και διασφάλιση ακεραιότητας δεδομένων όπως η επικεφαλίδα Ταυτοποίησης στην περίπτωση που απαιτείται εμπιστευτικότητα δεδομένων. Ο πιο κοινός αλγόριθμος που χρησιμοποιεί το ESP είναι ο DES (Data Encryption Standard). Όπως φαίνεται και στο πιο κάτω σχήμα η επικεφαλίδα ESP αποτελείται από ένα τμήμα παραμέτρων ασφαλείας και ένα σειριακό αριθμό και εισάγεται ανάμεσα στην επικεφαλίδα IP και στο υπόλοιπο πακέτο. Το τμήμα Παραμέτρων Ασφαλείας (Security Parameters Index – SPI) και ο σειριακός αριθμός έχουν τις ίδιες λειτουργίες όπως και στην περίπτωση της Επικεφαλίδας Ταυτοποίησης. Επιπρόσθετα, τα τμήματα TCP των δεδομένων είναι επίσης κρυπτογραφημένα.



Σχήμα 5: Δομή πρωτοκόλλου ESP

Στο IPSec τα IP πακέτα δεδομένων που αποστέλλονται μέσω του Internet πρώτα κρυπτογραφούνται και στη συνέχεια ενσωματώνονται σε ένα επιπλέον IP πακέτο. Τόσο οι δρομολογητές του Internet όσο και του εταιρικού δικτύου, μπορούν να δουν μόνο τα εξωτερικά IP πακέτα, ενώ τα ενθυλακωμένα είναι προστατευμένα στο τμήμα δεδομένων του εσωτερικού IP πακέτου.

Οι υπηρεσίες ασφάλειας που προσφέρει η επικεφαλίδα ESP είναι:
Εμπιστευτικότατα (confidentiality)
Διασφάλιση προέλευσης (data origin authentication)
Ακεραιότητα (connectionless integrity)
Προστασία πολλαπλής αποστολής πακέτου (anti-reply)
Εμπιστευτικότητα ροής κίνησης (traffic flow confidentiality)

Υπάρχουν δύο καταστάσεις στο ESP, όπως και στο AH:

- Κατάσταση διόδου (tunnel)
- Κατάσταση μεταγωγής (transport)

Κατάσταση διόδου: Χρησιμοποιείται αρκετά περισσότερο από ότι η κατάσταση μεταγωγής. Σε αυτή την περίπτωση το ESP δημιουργεί μια νέα επικεφαλίδα για κάθε πακέτο. Η νέα επικεφαλίδα συγκαταριθμεί τα δύο τερματικά άκρα του ESP tunnel, σαν αφετηρία και προορισμό του πακέτου. Το ESP μπορεί μόνο να κρυπτογραφεί ή/και να παρέχει προστασία ακεραιότητας και στα δεδομένα και στην αρχική IP επικεφαλίδα

κάθε πακέτου. Με την κρυπτογράφηση τα δεδομένα δεν μπορούν να διαβαστούν ή να τροποποιηθούν από κανένα άλλο.

Κατάσταση μεταγωγής (μεταφοράς): Εδώ, το ESP χρησιμοποιεί την αρχική IP επικεφαλίδα αντί να δημιουργήσει μια καινούρια. Μπορεί μόνο να κρυπτογραφεί ή και να παρέχει προστασία ακεραιότητας δεδομένων. Το αρχικό πακέτο επεξεργάζεται και ύστερα εισέρχεται η ESP επικεφαλίδα μετά την IP επικεφαλίδα. Στο τέλος του πακέτου εισέρχονται 2 νέα πεδία, το ESP trailer και τα προαιρετικά δεδομένα εξακρίβωσης γνησιότητας (ESP Authentication-optional)

2.9.1 Τρόπος λειτουργίας ESP

Όπως και στο πρωτόκολλο AH, έτσι και στο ESP, θα χωρίσουμε την επεξεργασία σε δύο μέρη την επεξεργασία των :

- Εξερχόμενων και
- Εισερχόμενων πακέτων

Σχήμα 6: Τρόπος καθορισμού ενός IPSec μετασχηματισμού (πρωτόκολλα- αλγόριθμοι – τρόποι υλοποίησης

Επεξεργασία εξερχόμενων πακέτων: το πακέτο προς αποστολή θα φτάσει στο στρώμα IPSec. Θα συμβουλευτεί την πολιτική ασφάλειας από τη βάση SPD για τον τύπο

του πακέτου, θα καταλήξει σε συγκεκριμένη SA και θα εφαρμόσει το πρωτόκολλο ESP στο πακέτο. Στο στάδιο αυτό, συγχωνεύει στα δεδομένα (Data) οτιδήποτε υπάρχει μετά την επικεφαλίδα ESP και προσθέτει ότι χρειάζεται στο padding. Στη συνέχεια κωδικοποιείται το πακέτο (κωδικοποιούνται τα data, padding, padding length και next header). Ο αλγόριθμος κωδικοποίησης ορίζεται από τον SA. Στη συνέχεια υπολογίζεται η τιμή του sequence number, ανεξάρτητα από το εάν είναι επιλεγμένη η υπηρεσία αποφυγής επαναλήψεων, και τέλος υπολογίζεται η τιμή ICV στο authentication data εάν είναι επιλεγμένη η υπηρεσία πιστοποίησης δεδομένων για το πρωτόκολλο ESP.

Επεξεργασία εισερχόμενων πακέτων: όταν φτάσει ένα πακέτο, το IPSec του παραλήπτη διαβάζει τη μεταβλητή SPI, τη διεύθυνση IP του αποστολέα και το πρωτόκολλο ESP, συμβουλεύεται την SPD και καταλήγει στην SA που έχει χρησιμοποιηθεί. Μετά, πάντα με οδηγό τη SA προχωρεί στα πιο κάτω βήματα:

1. Αν είναι επιλεγμένη η υπηρεσία πιστοποίησης του πακέτου, θα υπολογίσει ξανά την τιμή ICV σύμφωνα πάντα με τον αλγόριθμο που ορίζει ο SA και τη συγκρίνει με αυτή που περιέχεται στο πακέτο.

2. Αν είναι επιλεγμένη η υπηρεσία αποφυγής επαναλήψεων ελέγχει την τιμή του sequence number.

3. Αποκωδικοποιούνται τα κρυπτογραφημένα δεδομένα με τη βοήθεια του αλγόριθμου (που ορίζει ο SA) και τελικά παραλαμβάνεται το αυθεντικό πακέτο.

2.9.2 Συμπέρασμα για το πρωτόκολλο ESP

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

Σε κατάσταση μεταγωγής, το ESP παρέχει κρυπτογράφηση και προστασία ακεραιότητας για την «καθαρή πληροφορία» (payload) και για το αρχικό IP πακέτο, όπως επίσης

προστασία ακεραιότητας για την επικεφαλίδα ESP. Δεν είναι όμως συμβατό με την τεχνολογία NAT.

2.10 Διαχείριση Κλειδιών

Η ανταλλαγή κλειδιών στο IPSec είναι ένα θέμα ζωτικής σημασίας. Το IPSec χρησιμοποιεί το Internet Key Exchange (IKE) πρωτόκολλο για να διευκολύνει και να αυτοματοποιήσει τις Συσχετίσεις Ασφάλειας (SA) και την ανταλλαγή κλειδιών μεταξύ του αποστολέα και του παραλήπτη οι οποίοι μεταφέρουν δεδομένα. Κάνοντας χρήση των κλειδιών αυτών διασφαλίζεται ότι ο παραλήπτης και ο αποστολέας μπορούν να έχουν πρόσβαση στο μήνυμα. Αυτό που το κάνει ασφαλές, είναι ο τρόπος ανανέωσης του κλειδιού έτσι ώστε αυτοί που επικοινωνούν μεταξύ τους, να το κάνουν με ασφάλεια. Υπάρχουν δύο τρόποι ανανέωσης κλειδιών:

- Χειροκίνητη διαχείριση
- Αυτόματη διαχείριση

Χειροκίνητη διαχείριση κλειδιών: τα κλειδιά εισάγονται με το χέρι στις συσκευές που θα χρησιμοποιήσουν το πρωτόκολλο IPSec χωρίς τη χρήση κρυπτογράφησης. Ορίζονται, είτε από το διαχειριστή είτε στέλνονται με email. Αυτός ο τρόπος χρησιμοποιείται σε περιπτώσεις μικρών δικτύων. Ο τρόπος αυτός δεν συστήνεται αφού:

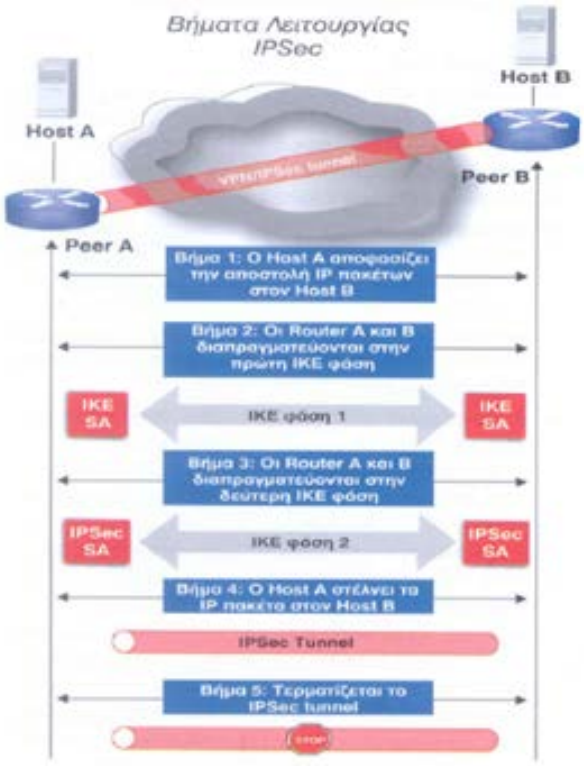
- Είναι επιρρεπής σε λάθη αφού απαιτεί εκτενείς ρυθμίσεις για πολλά ζευγάρια σταθμών.
- Τα κλειδιά για την επικοινωνία δύο υπολογιστών είναι στατικά και άρα υπάρχει μεγαλύτερη πιθανότητα να τα ανακαλύψει κάποιος εισβολέας
- Τα κλειδιά συνήθως δεν είναι ισχυρά αφού η διαδικασία των ρυθμίσεων είναι κουραστική 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.

Αυτόματη διαχείριση κλειδιών: η αυτόματη διαχείριση κλειδιών γίνεται με βάση το πρωτόκολλο IKE. Αυτός ο τρόπος διαχείρισης είναι χρήσιμος για μεγάλης έκτασης χρήσης του VPN. Κάθε μηχανή παράγει ένα ψευδοτυχαίο αριθμό τον οποίο κρυπτογραφεί με το δημόσιο κλειδί (public key) της άλλης μηχανής. Η πιστοποίηση

επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια συνάρτηση κατακερματισμού του τυχαίου αριθμού, αποκρυπτογραφώντας με τα ιδιωτικά κλειδιά (private keys) ότι λαμβάνουν από το συνομιλητή τους. υποστηρίζεται μόνο ο αλγόριθμος δημοσίων κλειδιών RSA.

Ο ακριβής ρόλος του IKE για τη διεκπεραίωση μιας IPSec επικοινωνίας μεταξύ δύο ή περισσότερων συσκευών αντικατοπτρίζεται στην ακόλουθη διαδοχή βημάτων (σχήμα 7):

- **Ενεργοποίηση μιας IPSec συνόδου**: σε αυτό το βήμα καθορίζεται το σύνολο των IP πακέτων που πρόκειται να προστατευθούν μέσω του IPSec.
- **IKE – 1η φάση**: δημιουργία και λειτουργία της IKE συσχέτισης ασφαλείας.
- **IKE – 2η φάση**: δημιουργία και λειτουργία της AH/ESP συσχέτισης ασφαλείας.
- **Μεταφορά δεδομένων**: τα IP πακέτα που επιλέχθηκαν από το 1ο βήμα, μεταφέρονται
- **Τερματισμός της IPSec συνόδου**: όταν ολοκληρωθεί η μεταφορά των IP πακέτων και πλέον δε χρησιμοποιείται η παραπάνω σύνοδος, τότε τερματίζεται.



Σχήμα 7: Σύνολο βημάτων που πρέπει να πραγματοποιηθούν για την επιτυχή μετάδοση δεδομένων μέσω το IPSec πρωτοκόλλου

2.11 Εφαρμογές

Το IPSec είναι ένα standard πρωτόκολλο για την υλοποίηση κρυπτογραφικών μηχανισμών σε δρομολογητές, τοίχους ασφάλειας (firewalls), αλλά και σε LANs ή μεμονωμένους κόμβους (hosts) που επικοινωνούν μέσω internet. Πιο συγκεκριμένα, υποστηρίζει την ασφαλή επικοινωνία μεταξύ δύο κόμβων, όπως επίσης και μεταξύ δύο LANs, εκτός από την client/server επικοινωνία που υποστηρίζουν τα άλλα πρωτόκολλα.

Επιπλέον, το IPSec είναι χρήσιμο για τη διασφάλιση της απομακρυσμένης πρόσβασης (μέσω dial-up) διασυνδέσεων VPN με απομακρυσμένα σημεία εντός εταιρικών ιδιωτικών δικτύων.

Γενικότερα το IPSec χρησιμοποιείται για να προσφέρει τη μέγιστη δυνατή ασφάλεια σε περιπτώσεις χρηματοπιστωτικών ιδρυμάτων, χρηματιστηριακών εταιρειών και γενικά οπουδήποτε η μεταφερόμενη πληροφορία είναι ιδιαίτερα ευαίσθητη. Επιπλέον προσφέρει κρυπτογράφηση, ποιότητα στη διάδοση δεδομένων και προστασία των τοπικών δικτύων από κακόβουλες επιθέσεις.

Προβλήματα που καλείται να αντιμετωπίσει το IPSec είναι η αύξηση του μεγέθους των πακέτων (άρα μεγαλύτερος χρόνος επεξεργασίας), η μη δυνατότητα καθορισμού συγκεκριμένων καθολικών αλγορίθμων κρυπτογράφησης (λόγω νομοθετικών δυσκολιών που αντιμετωπίζουν πολλοί αλγόριθμοι σε διάφορες χώρες), καθώς και το γεγονός ότι εφαρμόζεται μόνο σε IP δίκτυα (κάτι που σημαίνει ότι σε κάποια υπάρχοντα ιδιωτικά δίκτυα δε μπορεί να εφαρμοστεί)

2.12 L2TP (Layer 2 Tunneling Protocol)

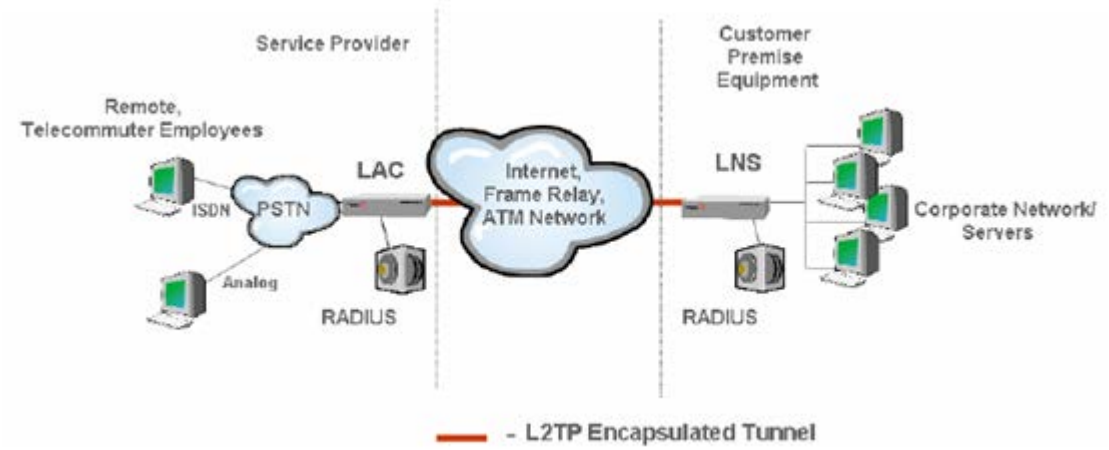
Το Layer Two Tunneling Protocol (L2TP), είναι ένα πρωτόκολλο δημιουργίας «τούνελ» και είναι το αποτέλεσμα της συγχώνευσης των πρωτοκόλλων PPTP και L2F μετά από συμφωνία των εταιριών που τα ανάπτυξαν.
Συνδυάζει πολλά χαρακτηριστικά και πλεονεκτήματα άλλων πρωτοκόλλων και επίσης την υποστήριξη μεγάλων εταιριών. Είναι ευέλικτο αφού λειτουργεί στο δεύτερο επίπεδο

του μοντέλου OSI και δίνει τη δυνατότητα χρήσης των πρωτοκόλλων IPX και NETBEUI[11] καθώς επίσης και των τεχνολογιών ATM και Frame Relay (άρα μπορεί να χρησιμοποιηθεί και σε δίκτυα που δε βασίζονται σε IP).
Λόγω έλλειψης κρυπτογράφησης το L2TP χρησιμοποιείται μαζί με το IPSec. Όταν το L2TP εκτελείται πάνω στο IPSec οι υπηρεσίες ασφάλειας παρέχονται από το IPSec, δηλαδή AH και ESP. όλοι οι έλεγχοι και τα δεδομένα του L2TP εμφανίζονται ως ομογενοποιημένα IP πακέτα δεδομένων στο IPSec σύστημα.
Το L2TP χρησιμοποιεί δύο servers για τη σύνοδο:

- Τον LAC (L2TP Access Concentrator) - Βρίσκεται στον ISP και χρησιμοποιείται για την εγκαθίδρυση μιας διόδου σε ένα δημόσιο δίκτυο π.χ. PSTN, ISDN, η οποία τερματίζεται στον LNS του κόμβου προορισμού
- Τον LNS (L2TP Network Server) – Βρίσκεται στον προορισμό και χρησιμοποιείται για τον τερματισμό του tunnel. Αναλαμβάνει την αυθεντικοποίηση του χρήση. Όταν ο LNS λάβει αίτηση για σύνδεση (δημιουργία διόδου) από ένα LAC, αυθεντικοποιεί τον αιτούντα και δημιουργεί το tunnel.

Στη δίοδο που δημιουργείται μεταξύ του Access Concentrator και του Network Server μπορούν να υπάρχουν ταυτόχρονα πολλές σύνοδοι (επικοινωνίες) όπου κάθε σύνοδος έχει ένα δικό της μοναδικό αριθμό Call ID, που υπάρχει στην επικεφαλίδα κάθε L2TP πακέτου. Μπορούν επίσης να υπάρχουν ταυτόχρονα πολλές διαφορετικές δίοδοι μεταξύ του ίδιου Access Concentrator και του Network Server.
Η αρχική σύνδεση του χρήστη με τον LAC, γίνεται με τη χρήση του PPP, μέσω του οποίου ενθυλακώνονται διαφόρων ειδών πακέτα (Apple, Talk, IP, IPX, NETBEUI) και γίνεται μια πρώτη αυθεντικοποίηση του χρήστη. Μια δεύτερη πιστοποίηση της ταυτότητας του χρήστη συμβαίνει αμέσως μετά με τη χρήση του RADIUS[12]. Τέλος, ένα VPN που υλοποιείται με βάση το L2TP μπορεί να υποστηρίξει αυθόρμητες (voluntary) όσο και αναγκαστικές (compulsory) διόδους. Σχηματικό διάγραμμα ενός L2TP VPN φαίνεται στο σχήμα 8.

[11] Το NetBIOS Extended User Interface (NetBEUI) είναι ένα πρωτόκολλο δικτύου που χρησιμοποιείται συνήθως σε μικρά τοπικά δίκτυα (LAN) με 1 εως 200 υπολογιστές. Στις πιο πολλές περιπτώσεις έχει αντικατασταθεί από το TSP/IP.
[12] RADIUS: Remote Authentication Dial-In User Service Server



Σχήμα 8: Δίοδος που αναπτύσσεται σε L2TP VPN

Τα στάδια δημιουργίας μιας L2TP διόδου είναι :

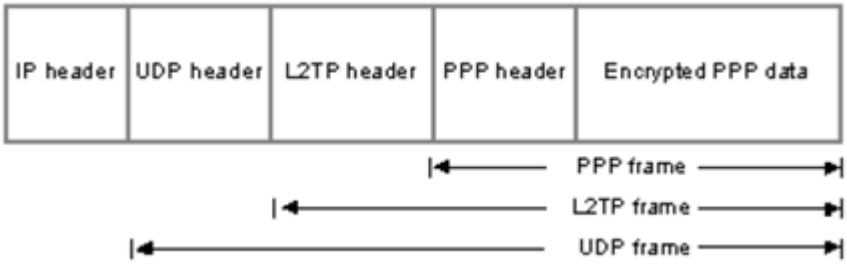
Στάδιο 1: Ο απομακρυσμένος χρήστης συνδέεται με τον LAC του ISP με τη χρήση του PPP.oLAC αυθεντικοποιεί τον χρήση, με βάση το User name και Password του. Στη συνέχεια, ο LAC προσδιορίζει την IP διεύθυνση του LNS που ανήκει στο LAN για το οποίο απαιτεί τη σύνδεση ο χρήστης. Μεταξύ LAC και LNS, η επικοινωνία L2TP ξεκινά.

Στάδιο 2: μετά την εκκίνηση της L2TP συνόδου, ξεκινά η αυθεντικοποίηση του χρήση στον LNS. Μπορεί να χρησιμοποιηθεί οποιοσδήποτε τυποποιημένος αλγόριθμος αυθεντικοποίησης (δεν υπάρχει περιορισμός για αλγόριθμο αυθεντικοποίησης).

Στάδιο 3: Μετά και από την επιτυχή αυθεντικοποίηση, μπορεί να δημιουργηθεί ένα προστατευμένο tunnel μεταξύ LAC και LNS. Το L2TP δεν προορίζει ρητά μεθόδους για την κρυπτογράφηση (η οποία παρέχει την ασφάλεια), ωστόσο για διόδους πάνω σε IP δίκτυα, μπορεί να χρησιμοποιηθεί το πρωτόκολλο IPSec. Τότε το L2TP ενθυλακώνεται σε UDP πακέτα που μεταφέρονται μεταξύ LAC και LNS μέσω IPSec tunnel. Για αυτό χρησιμοποιείται σαν βασική η UDP port 1701, αλλά μπορεί να χρησιμοποιηθεί και οποιαδήποτε άλλη.

Η κεφαλίδα ενός L2TP πρωτοκόλλου έχει την ακόλουθη μορφή[13]

[13] https://tools.ietf.org/html



Σχήμα 9: Μορφή κεφαλίδας ενός L2TP πρωτοκόλλου

Θα πρέπει να σημειωθεί ότι το L2TP πρωτόκολλο μπορεί να χρησιμοποιηθεί και για σύνδεση δίκτυο προς δίκτυο (LAN to LAN tunneling).

Κεφάλαιο 3

Ευπάθειες και ζητήματα ασφαλείας

Σύμφωνα με τον οργανισμό ENISA[14], τα VPN αποτελούν από τους πιο ασφαλείς τρόπους για να περιηγηθεί κάποιος στο διαδίκτυο, και όπως αναφέραμε πιο πάνω περιέχουν πολλά πρωτόκολλα που τα κάνουν ασφαλές παρέχοντας αυθεντικοποίηση, ακεραιότητα των δεδομένων και κρυπτογράφηση. Όμως ότι διακινείται μέσω του δικτύου είτε ιδιωτικού είτε δημοσίου, αποτελεί στόχο για επίδοξους «χάκερ» οι οποίοι έχουν σκοπό να κλέψουν τα πακέτα που διακινούνται και να τα πουλήσουν ή να τα εκθέσουν στο διαδίκτυο (WikiLeaks). Βασισμένοι όμως στις επιθέσεις, οι οργανισμοί και οι εταιρίες που αναπτύσσουν πρωτόκολλα και δίκτυα, τα ενισχύουν και τα ενημερώνουν κατάλληλα για ασφαλέστερη σύνδεση στο διαδίκτυο.

3.1 Ευπάθειες (13) των VPN δικτύων

- **VPN Hijacking** (14): Είναι ένα είδος ευπάθειας και είναι η μη-εξουσιοδοτημένη κατάληψη και χρήση μιας VPN σύνδεσης ενός απομακρυσμένου χρήστη, και ο επιτιθέμενος παριστάνει τον εξουσιοδοτημένο χρήση στο δίκτυο αυτό.
- **Man-in-the-middle**:[15] Αυτού του τύπου οι επιθέσεις επηρεάζουν την κυκλοφορία μεταξύ των ομάδων που επικοινωνούν και περιλαμβάνει διακοπή, εισαγωγή, διαγραφή και τροποποίηση των μηνυμάτων, επιστροφή των μηνυμάτων πίσω στον αποστολέα, επανάληψη παλιών μηνυμάτων και ανακατεύθυνση τους.
- **Αυθεντικοποίηση χρήση**: Αν και όπως έχουμε αναφέρει τα VPN είναι ο ασφαλέστερος τρόπος σύνδεσης, δε διαθέτουν ισχυρούς μηχανισμούς αυθεντικοποίησης χρήστη και για αυτό πρέπει να είναι όσο το δυνατόν πιο

[14] ENISA: Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και πληροφοριών (www.enisa.europa.eu)

[15] https://owasp.org/www-community/controls/Certificate_and_Public_Key_Pinning

ισχυροί για να αποτραπεί μια τυχόν μη-εξουσιοδοτημένη πρόσβαση στους πόρους του δικτύου.

- **Ιοί και κακόβουλο λογισμικό**: Αποτελεί κίνδυνο από τη μεριά του χρήστη ο οποίος μπορεί να έχει μολυνθεί με κάποιο ιό ή λογισμικό και έχουν παραβιαστεί οι κωδικοί πρόσβασης του στο VPN. Αν το δίκτυο είναι εταιρικό, μπορεί η μόλυνση αυτή να εξαπλωθεί σε όλο το δίκτυο αν το anti-virus που υπάρχει δεν είναι σε θέση να αντιμετωπίσει τον ιό/λογισμικό.
- **Μη εξουσιοδοτημένη πρόσβαση**: Κάποιοι χρήστες ή ακόμα και δίκτυα, πιθανόν να έχουν κάποια δικαιώματα πρόσβασης που μπορεί να μην χρειάζονται.

3.2 Ευπάθειες (15) Χρήστη

- Κατά τη χρήση του VPN, παρόλο που το τούνελ υλοποιείται με τέτοιο τρόπο ώστε ο χρήστης να είναι ανώνυμος και να προστατεύονται τα στοιχεία της ταυτότητας του, δεν του παρέχεται η απόλυτη ανωνυμία σε κανένα επίπεδο.
- Σε όλες τις πρωταρχικές φάσεις της έναρξης της ζεύξης μεταξύ του διακομιστή και του χρήστη, υπάρχουν «κομμάτια» τα οποία μπορούν να «σπαστούν» από κάποιο επίδοξο ο οποίος θέλει να αποκομίσει κάποια στοιχεία.
- Κατά τη διάρκεια της αυθεντικοποίησης του χρήστη μπορούν να υποκλαπούν στοιχεία όπως κωδικοί πρόσβασης στο VPN, όπου κάποιος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες ενός ιδιωτικού δικτύου.

Οι ευπάθειες αυτές προκαλούνται είτε από ελλιπείς υλοποιήσεις των πρωτοκόλλων, είτε από τους μηχανισμούς κρυπτογράφησης που χρησιμοποιούνται από κάποιο πρόγραμμα που χρησιμοποιεί ανασφαλείς συνδέσεις για τη μεταφορά δεδομένων (π.χ. κάποιο port που δεν ανήκει στο VPN). Επιπρόσθετα, ο χρήστης είναι εκτεθειμένος σε περίπτωση που ο διακομιστής της υπηρεσίας VPN δεν έχει λάβει όλα τα απαραίτητα μέτρα ασφαλείας όπως firewall.

Μια μελέτη έδειξε ότι το 90% που χρησιμοποιούν SSL για την υλοποίηση του VPN δεν τηρούν ενημερωμένους τους μηχανισμούς κρυπτογράφησης για την ασφάλεια των χρηστών τους. Αντίστοιχα το 74% δεν χρησιμοποιούν ενημερωμένους αλγόριθμους ψηφιακής υπογραφής. Τέλος το 41% χρησιμοποιεί πιστοποιητικά τα οποία είναι μεγέθους 1024 bit τα οποία θεωρούνται ανασφαλή (John Leyden J, 2016) (16).

Φαίνεται ότι κάθε μηχανισμός με την πάροδο του χρόνου γίνεται ολοένα και πιο ευάλωτος στις επιθέσεις, λόγω της προόδου της τεχνολογίας, καθιστώντας τους χρήστες ευάλωτους σε διάφορες επιθέσεις.

3.3 Ζητήματα ασφαλείας στα VPN δίκτυα

Παρόλο που τα δίκτυα VPN υλοποιούνται έτσι ώστε να είναι ασφαλή για το χρήστη και να προστατεύσουν την ιδιωτικότητά του, πολλές φορές δεν καλύπτουν όλες τις απαραίτητες προϋποθέσεις. Ειδικά οι δωρεάν πάροχοι VPN τις περισσότερες φορές παρέχουν ελλιπή ασφάλεια για τον χρήστη, κάτι που τελικά καθιστά τη χρήση του δικτύου VPN μη ουσιαστική.

Από τα πιο σημαντικά ζητήματα ασφαλείας είναι η διαρροή της διεύθυνσης IP του χρήστη από το τούνελ VPN. Μέσα από μια μελέτη σε 14 από τους μεγαλύτερους παρόχους VPN παρατηρήθηκε ότι όταν ο χρήστης συνδέεται χρησιμοποιώντας το πρωτόκολλο IPv6 τότε η διεύθυνση του είναι ακόμα εμφανής στους κόμβους τους οποίους περνάνε τα δεδομένα του, ή ο DNS ο οποίος μπορεί να έχει πέσει θύμα επίθεσης (Vasile, 2015) (17)

Ένα ακόμα σημαντικό ζήτημα είναι οι επιθέσεις DoS (Denial of Service[16]) οι οποίες αποτελούν τις πιο κοινές επιθέσεις στους servers (εξυπηρετητές). Συνήθως μειώνουν τη διαθεσιμότητα των πόρων του δικτύου. Ο επιτιθέμενος, δημιουργεί μεγάλες υπολογιστικές διεργασίες, οι οποίες ονομάζονται πλημμύρες, με τεράστιο όγκο διπλών πακέτων με σκοπό το θύμα της επίθεσης να μην μπορεί να χρησιμοποιήσει τις υπηρεσίες δικτύου, ίσως και για πολλές μέρες. Υπάρχουν πολλών ειδών τέτοιες επιθέσεις όπως UDP, ICMP, SYN πλημμύρες κ.α. Για το λόγο αυτό, υπάρχουν διάφορα συστήματα τα οποία είναι υπεύθυνα για να αντιμετωπίζουν τις επιθέσεις αυτές.

Επιπρόσθετα, ακόμα ένα ζήτημα ασφάλειας είναι η επίθεση του ενδιάμεσου (man in the middle attack). Η επίθεση αυτή είναι όταν κάποιος συνδέεται στην πορεία μετάδοσης των δεδομένων με σκοπό να υποκλέψει. Παρόλο που μεταφέρονται ασφαλώς μέσα από το τούνελ, αν οι αλγόριθμοι κρυπτογράφησης δεν είναι σωστά υλοποιημένοι, μπορεί

[16] DOS: είναι ένας τύπος επίθεσης σε μια υπηρεσία όπου διαταράσσει την κανονική λειτουργία της και εμποδίζει την πρόσβαση άλλων χρηστών σε αυτήν.

κάποιος τρίτος να έχει πρόσβαση στα δεδομένα. Για το λόγο αυτό, πολλοί πάροχοι υπηρεσιών VPN έχουν την ασφάλεια να διακόπτουν τη σύνδεση εάν βλέπουν κάποια αλλαγή στη δρομολόγηση των πακέτων ή αλλαγή στη διεύθυνση IP του χρήστη.

Εκτός από τον χρήστη, ζητήματα ασφαλείας μπορούν να προκύψουν και στα δίκτυα τα οποία συνδέεται ο χρήστης. Τέτοια ζητήματα είναι κυρίως το ότι μέσα από το VPN ο χρήστης παίρνει δικαιώματα πρόσβασης στο δίκτυο είτε τα χρειάζεται είτε όχι. Η χρήση VPN πολλές φορές στα ιδιωτικά δίκτυα αποτελεί κενό ασφαλείας ειδικά όταν υπάρχουν συνδέσεις ταυτόχρονα σε πολλές τοποθεσίες και η κάθε μια υλοποιεί το δικό της VPN. Θα πρέπει όλες οι πολιτικές προστασίας να είναι διάφανες και ενημερωμένες σε όλες τις τοποθεσίες ταυτόχρονα. Εάν σε αυτά τα δίκτυα έχουν πρόσβαση και εξωτερικού συνεργάτες μέσω VPN θα πρέπει οι πολιτικές ασφάλειας να είναι ακόμα πιο μεγάλες και ο κατακερματισμός του δικτύου σε περιοχές πρόσβασης ανάλογα με τον VPN διακομιστή που συνδέονται ακόμα μεγαλύτερος, έτσι ώστε να μην είναι δυνατή η διαρροή ευαίσθητων πληροφοριών.

3.4 «Τοίχοι ασφαλείας» (Firewalls)

Οι τοίχοι ασφαλείας (firewalls) χρησιμοποιούνταν ανέκαθεν για να προστατεύουν τα LANs από εισβολή μη εξουσιοδοτημένων πακέτων. Στην ουσία, πραγματοποιούν φιλτράρισμα σε κάθε πακέτο, το οποίο βασίζεται σε κάποια κριτήρια όπως το είδος του πακέτου, η εφαρμογή στην οποία ανήκει ή η IP διεύθυνση.
Υπάρχουν τριών ειδών τοίχοι ασφαλείας:

- Φίλτρα πακέτων (Packet filters)
- Πύλες ασφαλείας (Security gateways – proxies)
- Έξυπνα φίλτρα (Smart filters ή stateful inspections firewalls)

Φίλτρα πακέτων: Ένα φίλτρο πακέτων εξετάζει στα εισερχόμενα πακέτα της IP διευθύνσεις πηγής και προορισμού και επιτρέπουν τη διέλευση, με βάση κάποιους κανόνες που έχει θέσει ο διαχειριστής του δικτύου. Σημαντικά πλεονεκτήματα των πακέτων φίλτρων είναι η εύκολη υλοποίηση τους, καθώς και το γεγονός ότι είναι διαφανή στο χρήστη. Φυσικά η πολυπλοκότητά τους μεγαλώνει όσο αυξάνονται οι κανόνες φιλτραρίσματος. Επιπλέον, το να επιλέγεται πρόσβαση με βάση την IP διεύθυνση δεν είναι και η καλύτερη λύση, αφού η IP από μόνη της δεν εξασφαλίσει

αυθεντικοποίηση του αποστολέα. Ακόμα μια αδυναμία των πακέτων φίλτρων, είναι το ότι δεν προστατεύουν από επιθέσεις "man-in-the-middle-attack". Τέλος πρέπει να συνυπολογιστεί και το γεγονός ότι πολλές εφαρμογές δεν έχουν σταθερές θύρες (ports) στις οποίες στέλνουν πακέτα, έτσι είναι αρκετά δύσκολο να υπάρξουν στατικοί κανόνες φιλτραρίσματος.

Πύλες ασφαλείας: Επιτρέπουν στους χρήστες να χρησιμοποιούν ένας proxy server προκειμένου να επικοινωνήσουν με ασφαλή συστήματα. Ο proxy server δέχεται μια σύνδεση από τη μια πλευρά και, αν η σύνδεση επιτρέπεται, δημιουργεί μια δεύτερη σύνδεση με τον προορισμό από την άλλη πλευρά. Ο χρήστης που ζητά τη σύνδεση δεν συνδέεται ποτέ κατευθείαν στον προορισμό. Ένας proxy server, προκειμένου να εξυπηρετήσει διάφορα είδη κίνησης, πρέπει να περιέχει πολλούς proxy agents. Οι πύλες ασφαλείας χωρίζονται σε δύο κατηγορίες ανάλογα με το είδος του proxy server:

- Circuit Proxies: ένας circuit proxy τοποθετείται ανάμεσα στον δρομολογητή δικτύου (Network router) και στο Internet. Στο Internet δεν μεταδίδονται οι πραγματικές IP διευθύνσεις, αλλά μόνο η διεύθυνση του proxy. Ένας circuit proxy δεν εξετάζει ποτέ το είδος της εφαρμογής στην οποία υπάγονται τα πακέτα που δέχεται. Μειονέκτημα τους έναντι των πακέτων φίλτρων είναι το γεγονός ότι είναι πιο αργοί από τα φίλτρα πακέτων, γιατί δομούν εκ νέου την IP διεύθυνση κάθε πακέτου. Ένα πρότυπο για circuit proxy είναι το SOCKS[17]. Είναι ειδικό firewall που επιτρέπει την πρόσβαση μόνο σε κατάλληλά SOCKS πακέτα. Άρα απαιτείται το κατάλληλο software για να μετατρέπει κάθε πακέτο στην κατάλληλη μορφή. Οι περισσότεροι browsers υποστηρίζουν το SOCKS. Επιπλέον υποστηρίζει TCP και UDP εφαρμογές.
- Application Proxies: η μόνη διαφορά τους με τους circuit proxies είναι ότι εξετάζουν ολόκληρο το πακέτο (δηλαδή δουλεύουν στο 7ο επίπεδο και όχι στο 3ο). Χρειάζεται ένας agent για κάθε IP υπηρεσία π.χ. HTTP, RTP, SMTP, για την οποία θέλουμε να ελέγχουμε την πρόσβαση. Συνεπώς, για κάθε νέα υπηρεσία, δεν μπορεί να χρησιμοποιηθεί κάποιος υφιστάμενος agent. Η πιστοποίηση ταυτότητας είναι πιο ασφαλής. Ωστόσο, είναι πιο αργοί από τους circuit proxies.

[17] Το SOCKS είναι ένα proxy πρωτόκολλο δικτύου που επιτρέπει τους χρήστες που βρίσκονται από τη μία μεριά του SOCKS εξυπηρετητή να έχουν πλήρη πρόσβαση με τους χρήστες που βρίσκονται από την άλλη μεριά χωρίς να απαιτείται από το χρήστη η απευθείας πρόσβαση με τη IP διεύθυνση.

Έξυπνα φίλτρα: τα firewalls αυτά βασίζονται στην τεχνική Stateful Multi-Layer Inspection (SMLI). Στόχος της, εκτός της μέγιστης δυνατής ασφάλειας, είναι και η βέλτιστη δυνατή απόδοση. Τα έξυπνα φίλτρα μοιάζουν με τους application proxies, υπό την έννοια ότι εξετάζουν όλο το πακέτο, δηλαδή τις κεφαλίδες όλων των επιπέδου του OSI. Χρησιμοποιούν όμως ειδικούς αλγόριθμους (traffic-screening) για να καθορίσουν ή μη, τη διέλευση των εισερχόμενων πακέτων. Ένα έξυπνο φίλτρο κλείνει όλες τις TCP θύρες και τις ανοίγει δυναμικά όταν κάποιες συνδέσεις τις χρειάζονται. Επίσης υποστηρίζει UDP πακέτα. Λόγω της μεγάλης ασφάλειας που παρέχουν χρησιμοποιούνται αρκετά στα VPN, αν και συνδυάζονται και με proxies για παροχή αυθεντικοποίησης.

Κεφάλαιο 4
Μεθοδολογία

Στην ποσοτική αυτή έρευνα, αφού μελετήθηκε η θεωρία, θα υλοποιηθεί πείραμα για να δείξει την καταλληλόλητα των διαφόρων VPN τεχνολογιών για την διασύνδεση Cyber ranges. Η υλοποίηση θα εκτελεστεί σε ένα περιβάλλον cyber range όπου θα γίνει εγκατάσταση του Open VPN (18) σε Ubuntu εικονική μηχανή, έτσι ώστε να υπάρχει σύνδεση ανάμεσα σε server και client. Από προεπιλογή δημιουργεί ένα ζεύγος CA (Certificate Authority) και ιδιωτικό/δημόσιο κλειδί το οποίο είναι μοναδικό στην εγκατάσταση του server με σκοπό την επαλήθευση της ταυτότητας.

Στη συνέχεια θα γίνει έλεγχος του δικτύου για αποστολή και λήψη πακέτων, έτσι ώστε να διαφανεί αν και κατά πόσο επηρεάζεται το δίκτυο αφού λειτουργεί μέσω ιδεατού δικτύου. Ο έλεγχος θα γίνει μέσω του δωρεάν εργαλείου Iperf και θα αναλυθούν κάποια αποτελέσματα μέσω γραφικών παραστάσεων.

Ακολούθως, θα γίνει δειγματοληπτική μελέτη για τη χρήση των VPN δικτύων, μέσω ερωτηματολογίου που θα δοθεί σε χρήστες κάποιων εταιρειών. Θα χρησιμοποιηθεί ένα μέρος δείγμα του πληθυσμού ώστε να εξοικονομηθεί κυρίως χρόνος μιας και οι μετρήσεις σε ολόκληρο τον πληθυσμό ήταν αδύνατο να γίνουν. Το ερωτηματολόγιο θα σταλεί σε συγκεκριμένες εταιρείες που η φύση της εργασίας τους, τους επιτρέπει τη χρήση των εικονικών δικτύων. Οι απαντήσεις θα αναλυθούν στατιστικά με γραφικές παραστάσεις. Για την απάντηση των ερευνητικών ερωτημάτων σχεδιάστηκε ηλεκτρονικό ερωτηματολόγιο . Στην συγκεκριμένη περίπτωση, επιλέχθηκε ένα δείγμα πέραν των 30 ατόμων το οποίο είναι αντιπροσωπευτικό και αξιόπιστο μιας και εκφράζει τις διαφοροποιήσεις του πληθυσμού βάσει του σκοπού της μελέτης αυτής.

4.1 OpenVPN

Το OpenVPN (19) είναι μια εφαρμογή που υλοποιεί VPN για τη δημιουργία συνδέσεων point-to-point, point-to-network και network-to-network. Οι συνδέσεις αυτές είναι κρυπτογραφημένες και παρέχει επίσης την υπηρεσία authentication. Το OpenVPN βασίζεται στο SSL/TLS security και υποστηρίζει ethernet bridging, TCP / UDP tunnel, δυναμικές διευθύνσεις IP και DHCP. Το σημαντικότερο πλεονέκτημα του είναι η εύκολη εγκατάσταση και ρύθμιση, αλλά και η ευελιξία του. Προσφέρει ένα αρκετά καλό συνδυασμό ασφάλειας, ταχύτητας, εμπιστευτικότητας, ακεραιότητας και συμβατότητας. Έχει τη δυνατότητα να δουλέψει τόσο με UDP όσο και με TCP. Είναι ένα λογισμικό ανοικτού κώδικα και διατίθεται δωρεάν.

4.2 Iperf

Το Iperf (20) είναι ένα εργαλείο ανοικτού κώδικα για τη μέτρηση της απόδοσης του εύρους ζώνης στα TCP και UDP πρωτόκολλα. Στην ουσία, μετράει την απόδοση ενός end-to-end δικτύου αναλύοντας τη διακίνηση μεταξύ των δύο άκρων είτε προς μια κατεύθυνση είτε αμφίδρομα. Ο χρήστης, ρυθμίζοντας διάφορες παραμέτρους και UDP χαρακτηριστικά, μπορεί να μετρήσει το μέγιστο εύρος ζώνης σε TCP. Αυτό μπορεί να γίνει με την εγκατάσταση του Iperf και στα δύο τερματικά τα οποία χρησιμοποιούνται ως server και client αντίστοιχα. Φυσικά μπορούμε να χρησιμοποιήσουμε και τρίτο τερματικό, το οποίο θα “ακούει” τα άλλα δύο τρέχοντας tcpdump, αλλά θα προκληθεί κάποια καθυστέρηση στο δίκτυο. Το Iperf παράγει μόνο του τα πακέτα που στέλνει και για αυτό δεν υπάρχουν καθυστερήσεις από το δίσκο ή άλλο περιφερειακό κατά τη μέτρηση.

Η ποιότητα ενός δικτύου μπορεί να μετρηθεί βάση των πιο κάτω παραμέτρων:

- Latency (response time ή RTT): αυτό φαίνεται από μια απλή εντολή ping
- Jitter (latency variation): μπορεί να μετρηθεί με UDP Iperf test
- Απώλεια datagrams: μπορεί να μετρηθεί με UDP Iperf test
- Bandwidth: μπορεί να μετρηθεί με TCP Iperf test

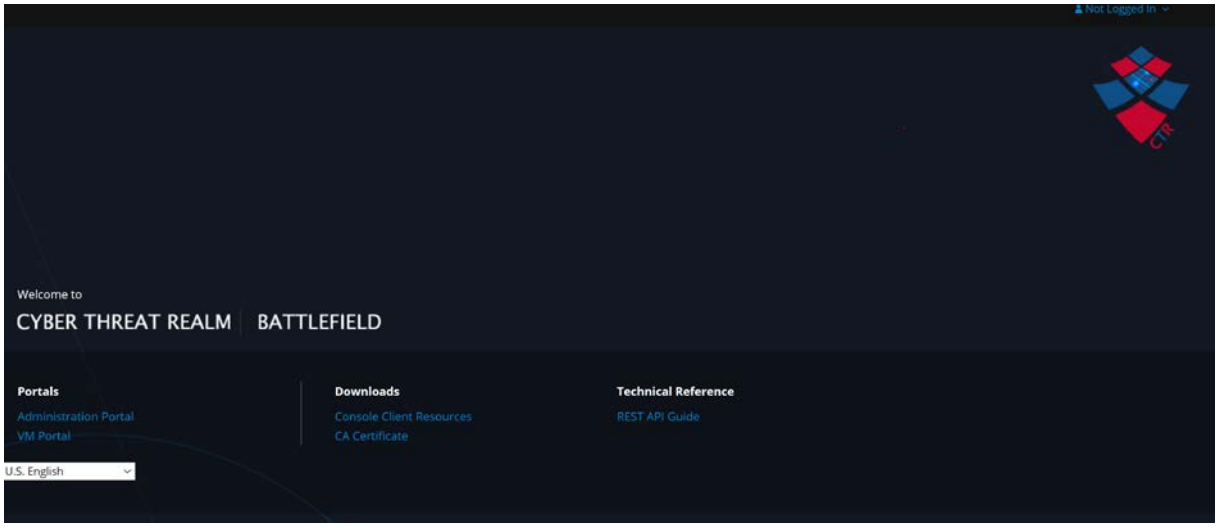
Η διαφορά (21) ανάμεσα στα πρωτόκολλα TCP και UDP είναι ότι το TCP χρησιμοποιεί διεργασίες έτσι ώστε να σιγουρεύεται ότι τα πακέτα έχουν σταλεί και παραληφθεί σωστά από τον δέκτη, ενώ το UDP δεν το ενδιαφέρει τόσο η αξιοπιστία όσο η ταχύτητα.

Όταν χρησιμοποιείται για τη δοκιμή UDP χωρητικότητας, το Iperf επιτρέπει στο χρήστη να καθορίσει το μέγεθος του datagram και δίνει αποτελέσματα για το datagram throughput και την απώλεια πακέτων (packet loss). Όταν χρησιμοποιείται για δοκιμές TCP χωρητικότητας, μετράει την απόδοση του ωφέλιμου φορτίου (payload).

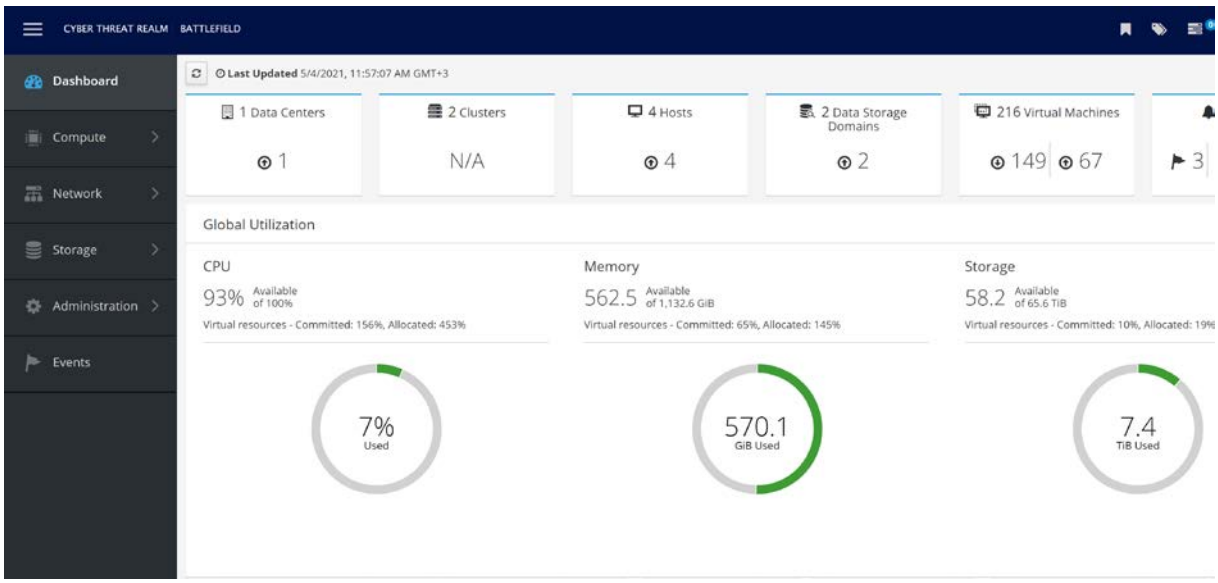
Κεφάλαιο 5
Υλοποίηση

Για την υλοποίηση όπως εξηγήσαμε στο κεφάλαιο 4 θα χρησιμοποιηθεί ένα cyber range περιβάλλον. Το περιβάλλον αυτό ανήκει στο Ανοικτό Πανεπιστήμιο Κύπρου και στην ερευνητική ομάδα Cybersecurity and telecommunications research lab.
Το cyber range είναι πειραματικό. Τα χαρακτηριστικά του είναι ως εξής:

- 4 hosts
- 1 external network provided
- 2 data storage domains
- 216 virtual machines
- Memory – 1,132.6 GB
- Storage 65.6 TB



Εικόνα 1: Cyber range portal

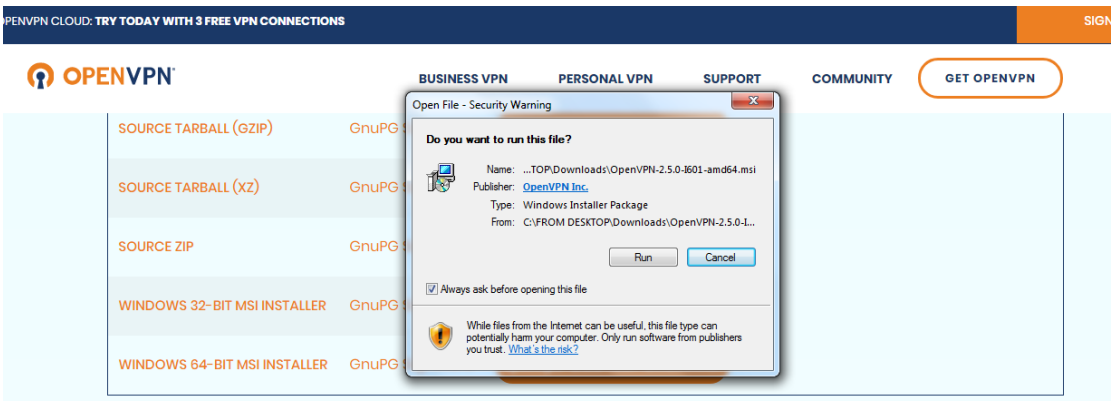


Εικόνα 2: Χαρακτηριστικά cyber range

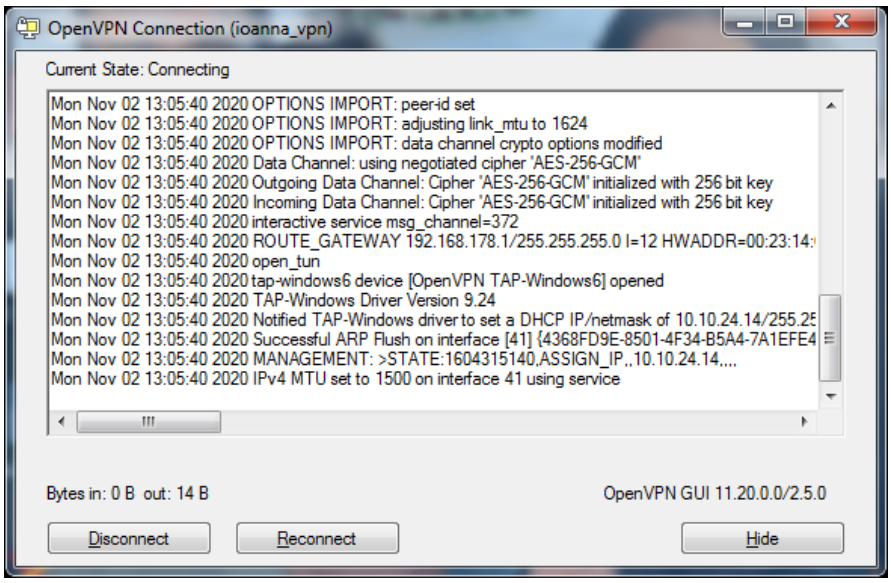
Ακολουθώντας τα πιο κάτω βήματα κάνουμε εγκατάσταση του Open VPN και EasyRSA σε μηχανή Ubuntu 18.04:

- Δημιουργία VPN Server
- Δημιουργία CA (Certificate Authority) Server
- Δημιουργία κλειδιών και αρχείων κρυπτογράφησης
- Δημιουργία πιστοποιητικού πελάτη και ζεύγους κλειδιών
- Διαμόρφωση OpenVPN
- Διαμόρφωση δικτύου Server
- Ενεργοποίηση της υπηρεσίας OpenVPN
- Δημιουργία αρχείων διαμόρφωσης πελάτη
- Εγκατάσταση του Client Configuration

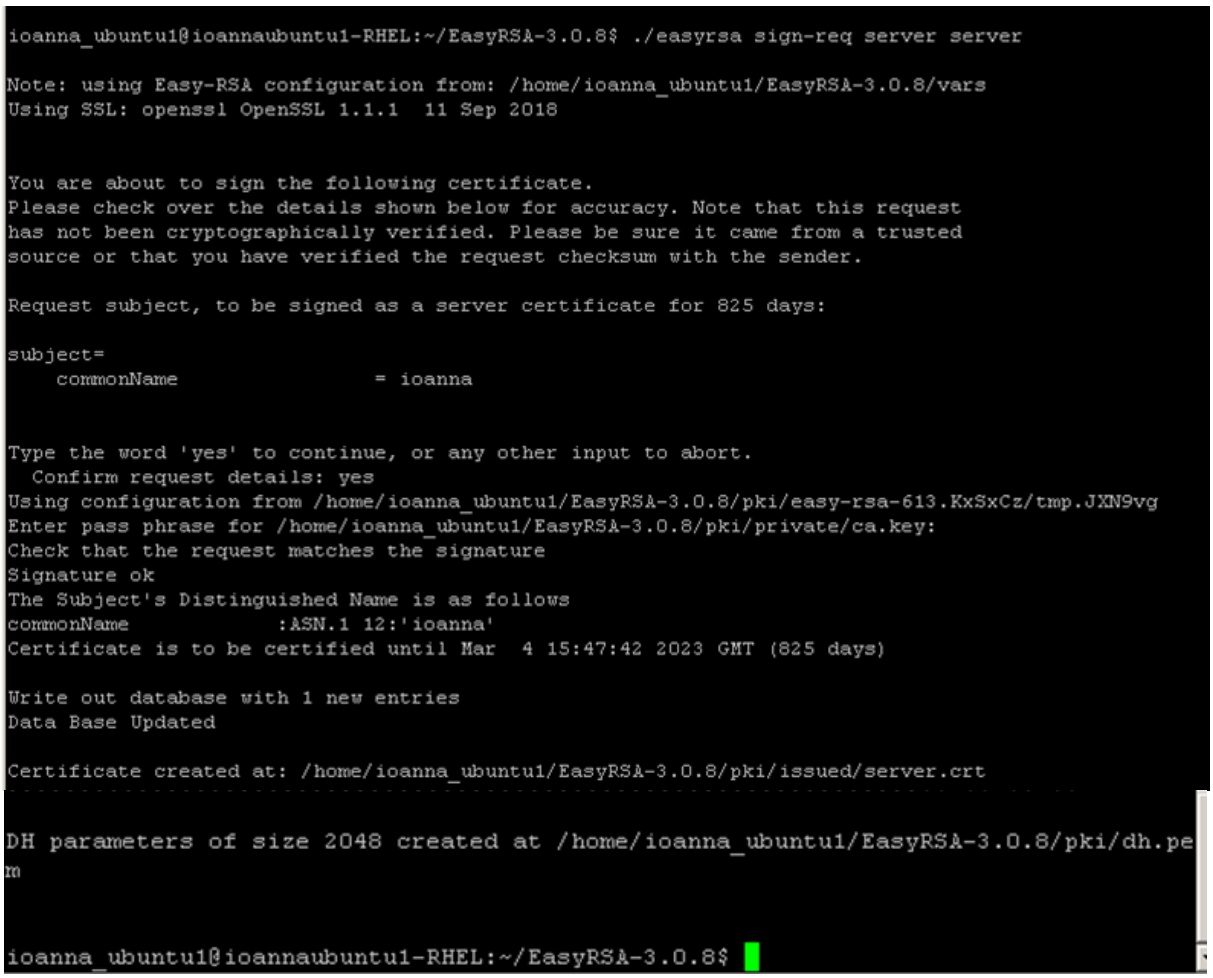
Το Open VPN είναι ένα TLS/SSL VPN. Αυτό σημαίνει ότι χρησιμοποιεί πιστοποιητικά για την κρυπτογράφηση της κίνησης μεταξύ του server και του client. Οπότε για αρχή θα κατεβάσουμε το EasyRSA το οποίο θα χρησιμοποιηθεί για την κατασκευή της υποδομής του δημόσιου κλειδιού. Το CA θα δημιουργηθεί σε ένα standalone server. Αυτό γίνεται για αποτροπή πρόσβασης μη εξουσιοδοτημένων χρηστών στο VPN μας, γιατί εάν ένας εισβολέας διεισδύσει στο server, θα μπορούσε να έχει πρόσβαση στο ιδιωτικό κλειδί και να το χρησιμοποιήσει υπογράφοντας πιστοποιητικά δίνοντας πρόσβαση στο VPN.



Εικόνα 3: Download Open VPN



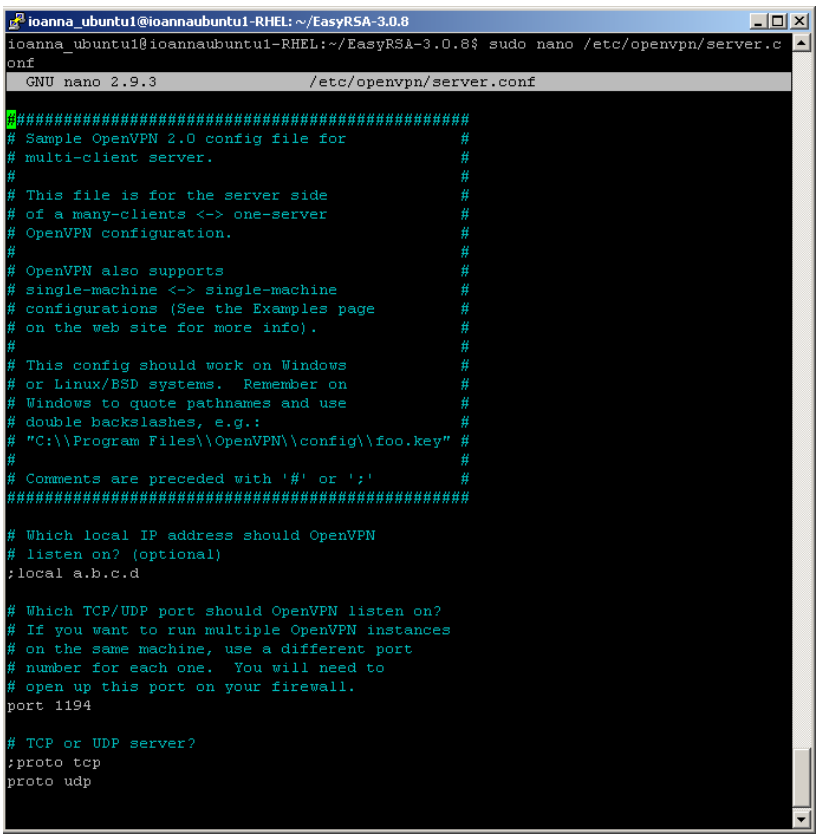
Εικόνα 4: Σύνδεση στο VPN



Εικόνα 5: Δημιουργία πιστοποιητικών server, κλειδιού και αρχείων κρυπτογράφησης

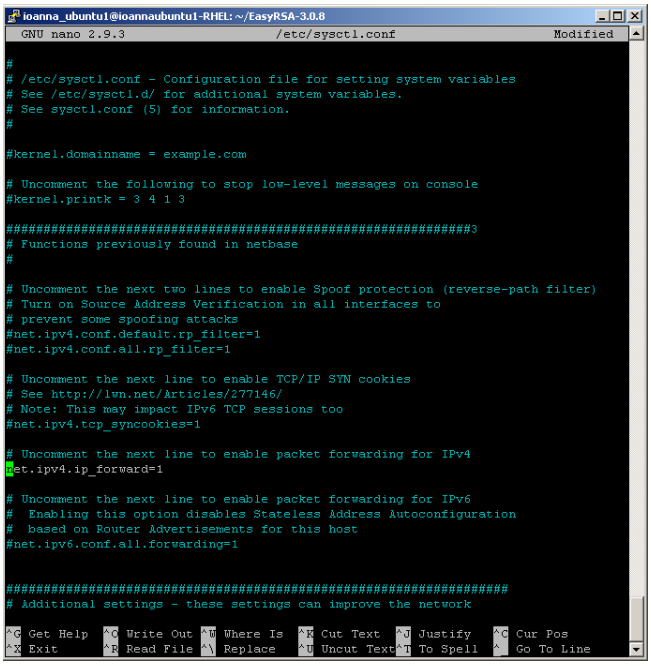
Εικόνα 6: Δημιουργία πιστοποιητικού client και key pair.

Αφού έχουν δημιουργηθεί τα πιστοποιητικά και τα κλειδιά των server και client ξεκινά η διαμόρφωση του OpenVPN.



Εικόνα 7: Διαμόρφωση OpenVPN

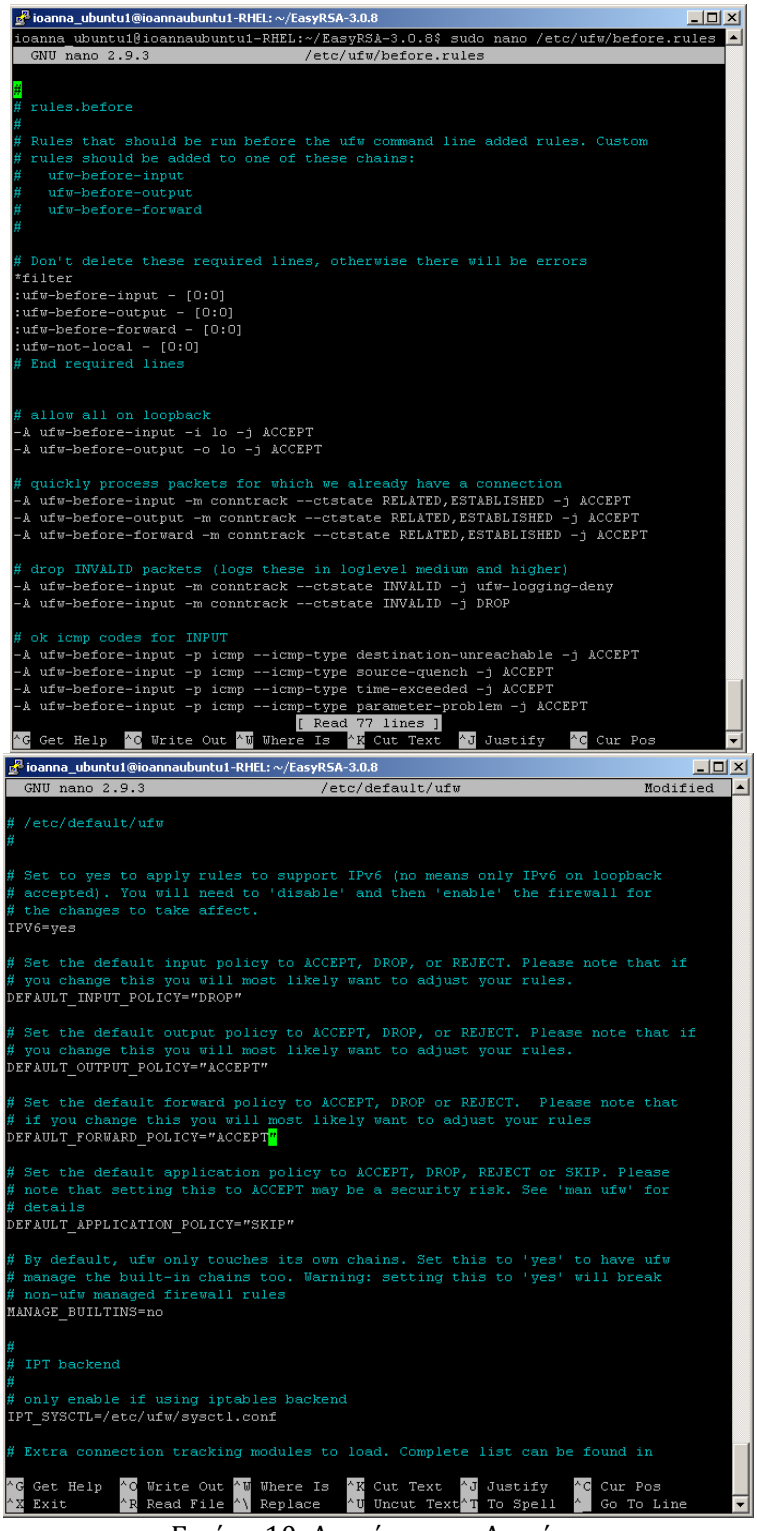
Ακολούθως γίνεται η διαμόρφωση του δικτύου έτσι ώστε να μπορεί να δρομολογεί σωστά την κίνηση μέσω του VPN.



Εικόνα 8: Διαμόρφωση Δικτύου

```
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo nano /etc/sysctl.conf
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo sysctl -p
net.ipv4.ip_forward = 1
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ ip route | grep default
default via 10.200.100.1 dev enp1s0 proto dhcp metric 100
```

Εικόνα 9: Διαμόρφωση Δικτύου



Εικόνα 10: Διαμόρφωση Δικτύου

```
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo ufw allow 443/udp
Rules updated
Rules updated (v6)
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo ufw disable
Firewall stopped and disabled on system startup
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? Y
Firewall is active and enabled on system startup
```

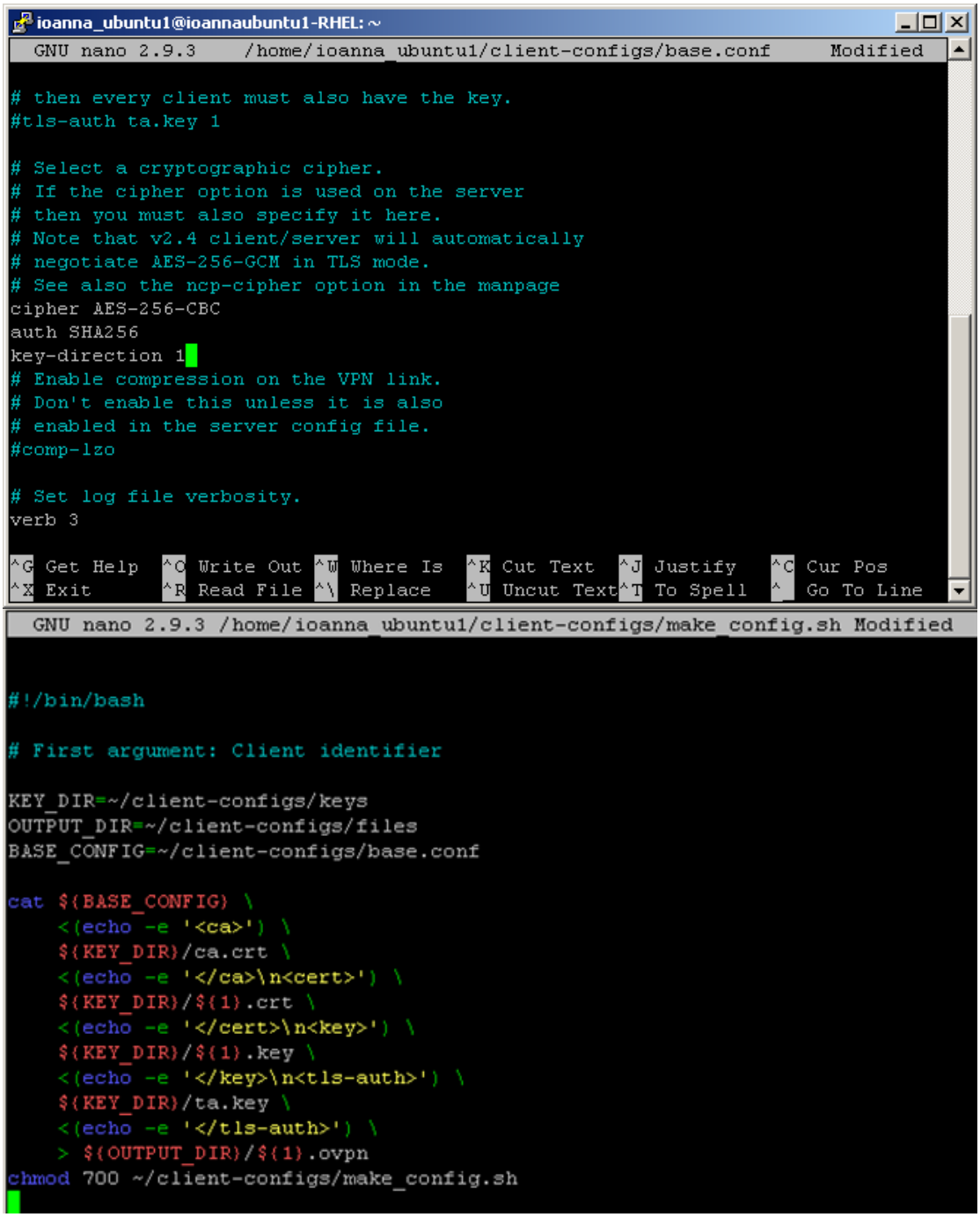
Εικόνα 11: Διαμόρφωση Δικτύου

```
ioanna_ubuntu1@ioannaubuntu1-RHEL: ~/EasyRSA-3.0.8
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo systemctl start openvpn
ioanna_ubuntu1@ioannaubuntu1-RHEL:~/EasyRSA-3.0.8$ sudo systemctl status openvpn
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset:
   Active: active (exited) since Sun 2020-11-22 12:40:35 EET; 2 weeks 5 days ago
 Main PID: 933 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 4654)
   CGroup: /system.slice/openvpn.service

Νοε 22 12:40:35 ioannaubuntu1-RHEL systemd[1]: Starting OpenVPN service...
Νοε 22 12:40:35 ioannaubuntu1-RHEL systemd[1]: Started OpenVPN service.
lines 1-9/9 (END)
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enable
   Active: active (exited) since Sun 2020-11-22 12:40:35 EET; 2 weeks 5 days ago
 Main PID: 933 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 4654)
   CGroup: /system.slice/openvpn.service

Νοε 22 12:40:35 ioannaubuntu1-RHEL systemd[1]: Starting OpenVPN service...
Νοε 22 12:40:35 ioannaubuntu1-RHEL systemd[1]: Started OpenVPN service.
~
~
~
~
~
~
~
~
```

Εικόνα 12: Διαμόρφωση Δικτύου

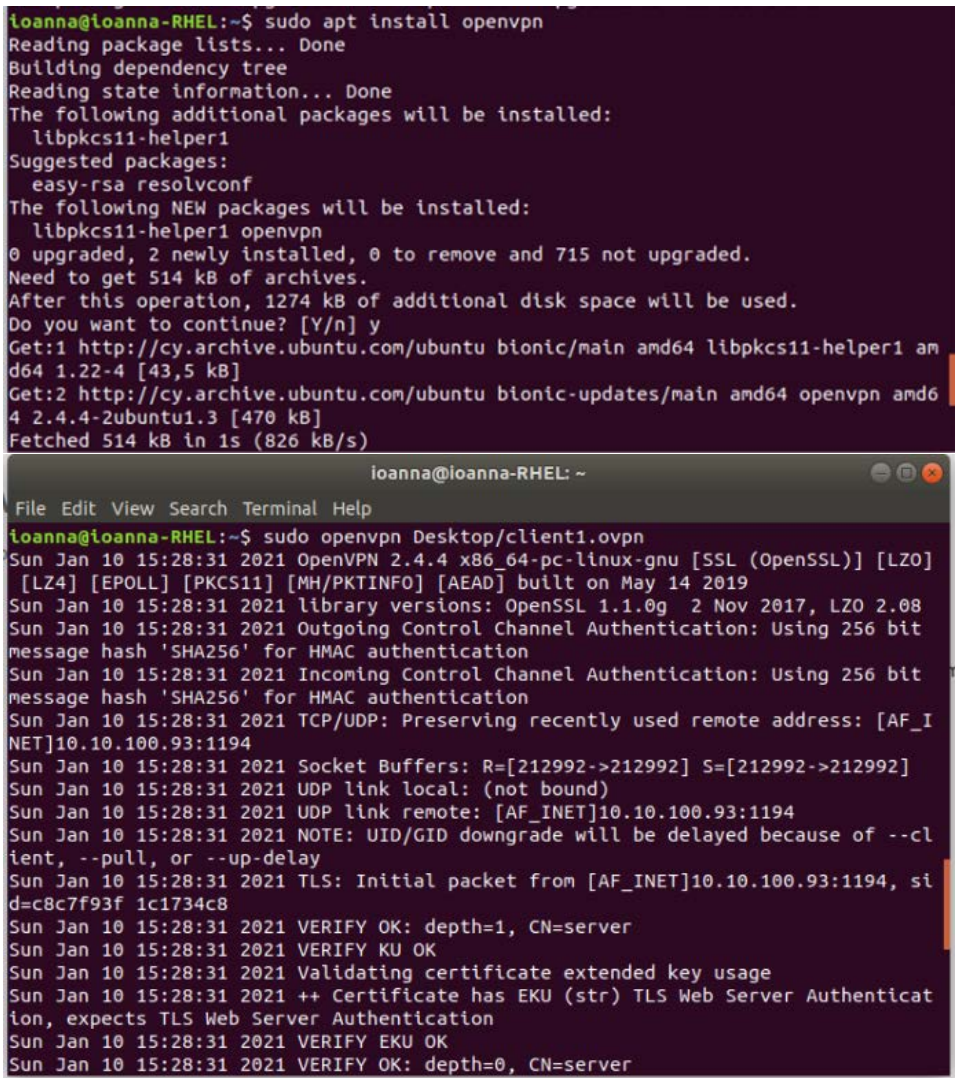
```
ioanna_ubuntu1@ioannaubuntu1-RHEL:~$ sudo nano /etc/openvpn/server.conf
ioanna_ubuntu1@ioannaubuntu1-RHEL:~$ mkdir -p ~/client-configs/files
ioanna_ubuntu1@ioannaubuntu1-RHEL:~$ cp /usr/share/doc/openvpn/examples/sampl
e-config-files/client.conf ~/client-configs/base.conf
ioanna_ubuntu1@ioannaubuntu1-RHEL:~$ nano ~/client-configs/base.conf
  GNU nano 2.9.3    /home/ioanna_ubuntu1/client-configs/base.conf

#################################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
#################################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client
```

Εικόνα 13: Δημιουργία υποδομής client



Εικόνα 14: Δημιουργία υποδομής client

Αφού έγινε η διαμόρφωση προχωράμε σε εγκατάσταση σε περιβάλλον Linux.



Εικόνα 15: Εγκατάσταση σε περιβάλλον Linux

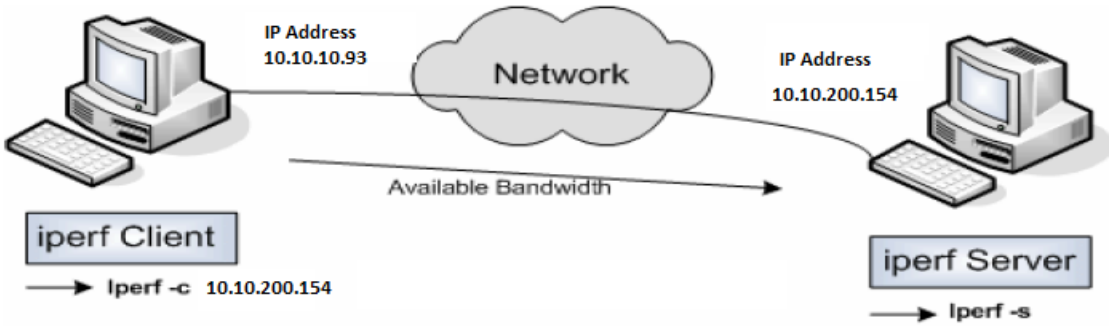
Αφού ολοκληρώθηκε η διαμόρφωση και η εγκατάσταση του εργαλείου OpenVPN, χρησιμοποιήθηκε το εργαλείο Iperf για την ανάλυση του δικτύου.

Παράμετροι που μπορούν να χρησιμοποιηθούν με το Iperf για εξαγωγή πληροφοριών:

```
Usage: iperf [-s|-c host] [options]
       iperf [-h|--help] [-v|--version]

Client/Server:
  -f, --format    [kmKM]   format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval  #        seconds between periodic bandwidth reports
  -l, --len       #[KM]    length of buffer to read or write (default 8 KB)
  -m, --print_mss          print TCP maximum segment size (MTU - TCP/IP header)
  -o, --output    <filename> output the report or error message to this specified file
  -p, --port      #        server port to listen on/connect to
  -u, --udp                use UDP rather than TCP
  -w, --window    #[KM]    TCP window size (socket buffer size)
  -B, --bind      <host>   bind to <host>, an interface or multicast address
  -C, --compatibility      for use with older versions does not sent extra msgs
  -M, --mss       #        set TCP maximum segment size (MTU - 40 bytes)
  -N, --nodelay            set TCP no delay, disabling Nagle's Algorithm
  -V, --IPv6Version        Set the domain to IPv6

Server specific:
  -s, --server             run in server mode
  -U, --single_udp         run in single threaded UDP mode
  -D, --daemon             run the server as a daemon

Client specific:
  -b, --bandwidth #[KM]    for UDP, bandwidth to send at in bits/sec
                           (default 1 Mbit/sec, implies -u)
  -c, --client    <host>   run in client mode, connecting to <host>
  -d, --dualtest           Do a bidirectional test simultaneously
  -n, --num       #[KM]    number of bytes to transmit (instead of -t)
  -r, --tradeoff           Do a bidirectional test individually
  -t, --time      #        time in seconds to transmit for (default 10 secs)
  -F, --fileinput <name>   input the data to be transmitted from a file
  -I, --stdin              input the data to be transmitted from stdin
  -L, --listenport #       port to recieve bidirectional tests back on
  -P, --parallel  #        number of parallel client threads to run
  -T, --ttl       #        time-to-live, for multicast (default 1)
  -Z, --linux-congestion <algo>  set TCP congestion control algorithm (Linux only)

Miscellaneous:
  -x, --reportexclude [CDMSV]   exclude C(connection) D(data) M(multicast) S(settings)
V(server) reports
  -y, --reportstyle C      report as a Comma-Separated Values
  -h, --help               print this message and quit
  -v, --version            print version information and quit
```

Εικόνα 16: Παράμετροι Iperf

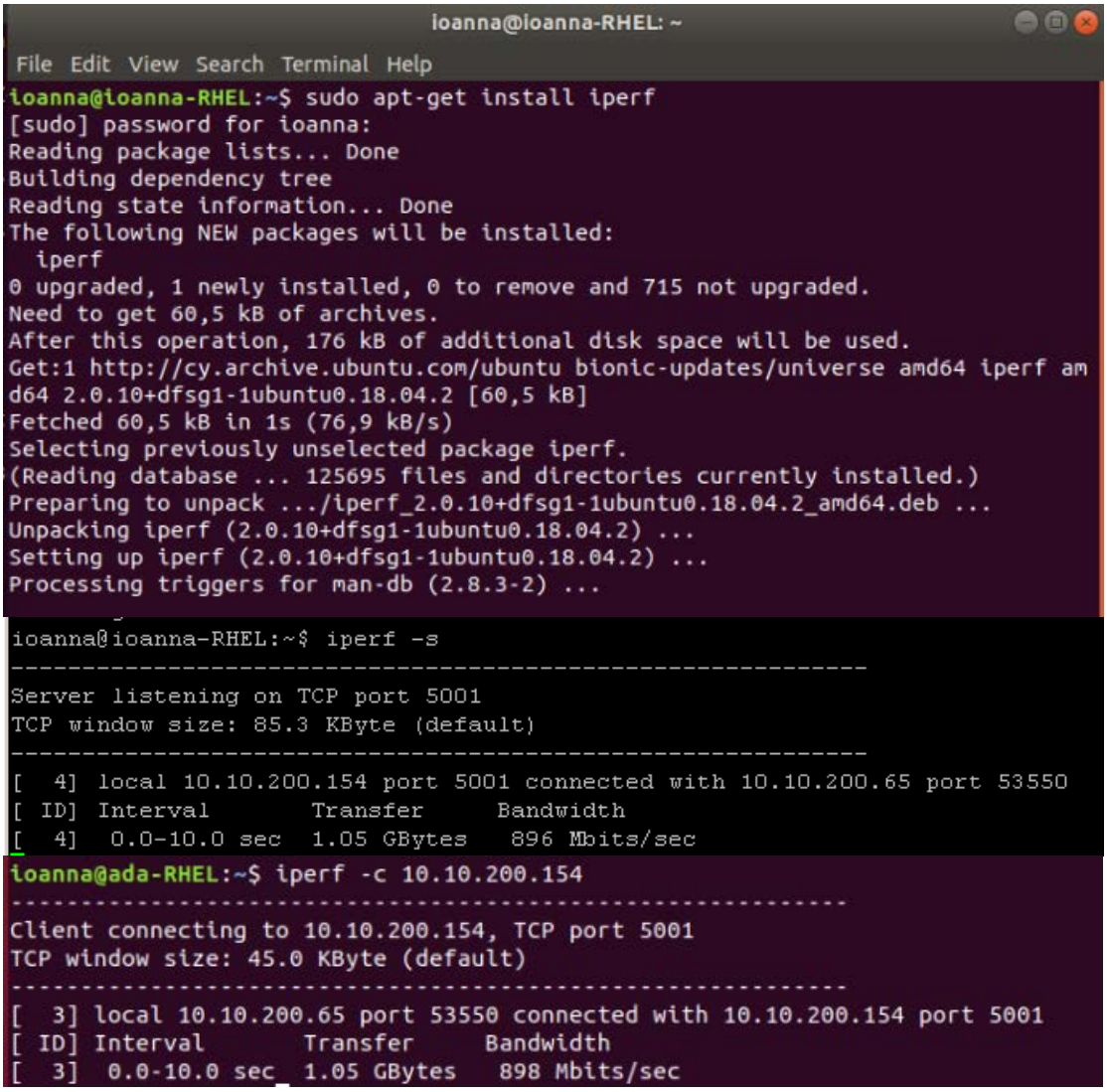
Ως προεπιλογή, ο Iperf client ενώνεται με τον Iperf server στο TCP port 5001 και το bandwidth που εμφανίζεται στο Iperf είναι αυτό από τον client στον server. Αν θέλουμε να χρησιμοποιήσουμε UDP tests, τότε θα χρησιμοποιήσουμε το -u argument.



Εικόνα 17: Δίκτυο client-server

Παραδείγματα ελέγχου δικτύου:

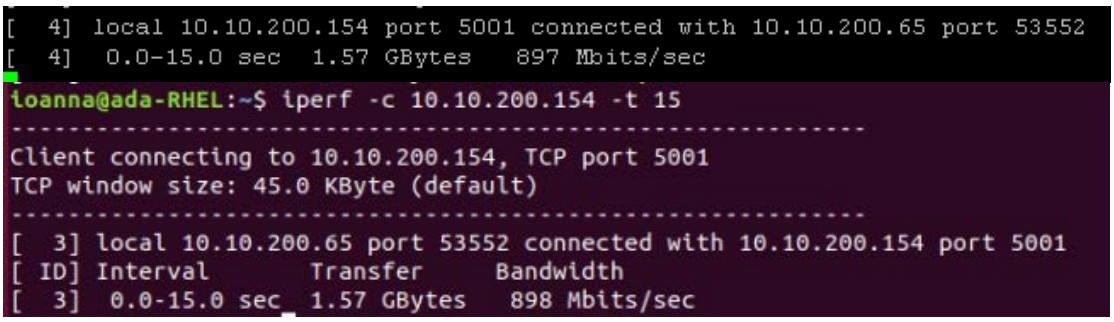
1. Για να ελέγξουμε το δίκτυο μας τρέχουμε στον server την εντολή iperf -s και στον client την εντολή iperf -c 10.10.200.154 όπου είναι η IP διεύθυνση του server (αφού κάνουμε εγκατάσταση το iperf):



Εικόνα 18: Εντολή iperf -c

2. Αν θέλουμε να στείλουμε δεδομένα σε συγκεκριμένο χρόνο (Data for N secs) πρέπει να οριστούν τα δευτερόλεπτα με -t:

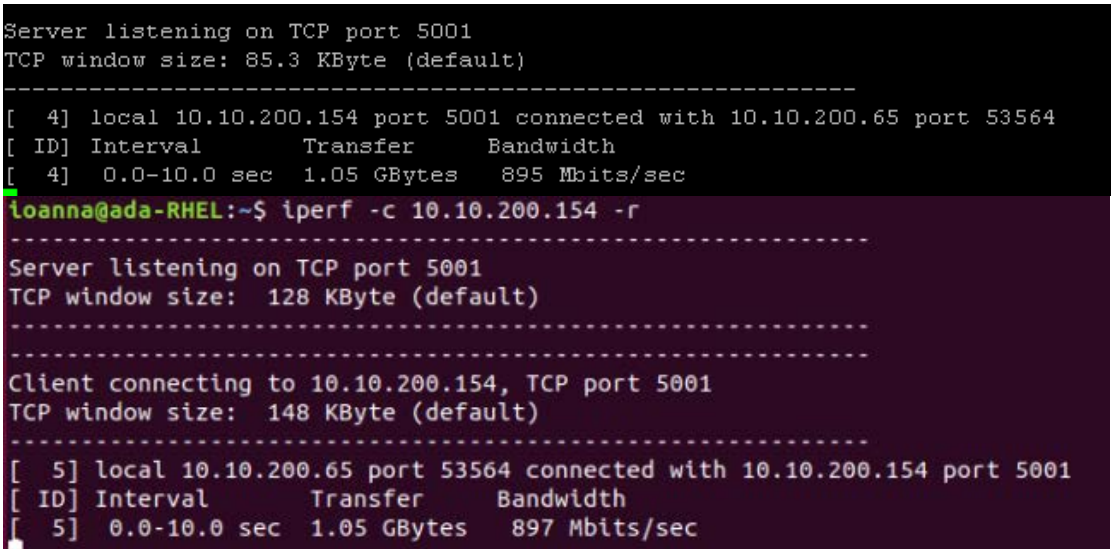
-t: time in seconds to listen for new traffic connections, receive traffic or transmit traffic



Εικόνα 19: Εντολή iperf -t

3. Μέτρηση αμφίδρομης κατεύθυνσης:

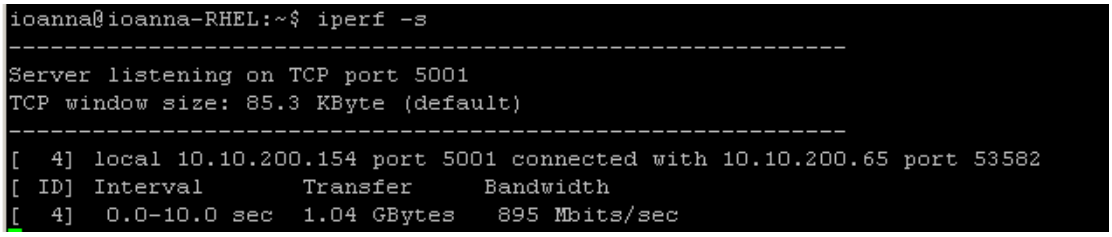
-r: Do a bidirectional test individually – client-to-server, followed by a reversed test, server-to-client



Εικόνα 20: Εντολή iperf -r

4. Μέτρηση ταυτόχρονης αμφίδρομης κατεύθυνσης:

-d: Do a bidirectional test simultaneously.



```
ioanna@ada-RHEL:~$ iperf -c 10.10.200.154 -d
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size:  128 KByte (default)
------------------------------------------------------------
------------------------------------------------------------
Client connecting to 10.10.200.154, TCP port 5001
TCP window size:  153 KByte (default)
------------------------------------------------------------
[  5] local 10.10.200.65 port 53582 connected with 10.10.200.154 port 5001
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-10.0 sec  1.04 GBytes   897 Mbits/sec
```

Εικόνα 21: Εντολή iperf -d

Υπάρχει συμφωνία στον αριθμό των Bytes ωστόσο οι τιμές του bandwidth διαφέρουν ανάμεσα σε κατευθύνσεις και τερματικά.

5. Χρησιμοποιώντας την παράμετρο -u πραγματοποιούμε test UDP port (αντί του default TCP port) το οποίο προσφέρει σημαντικές πληροφορίες αναφορικά με την καθυστέρηση το jitter και το packet loss:

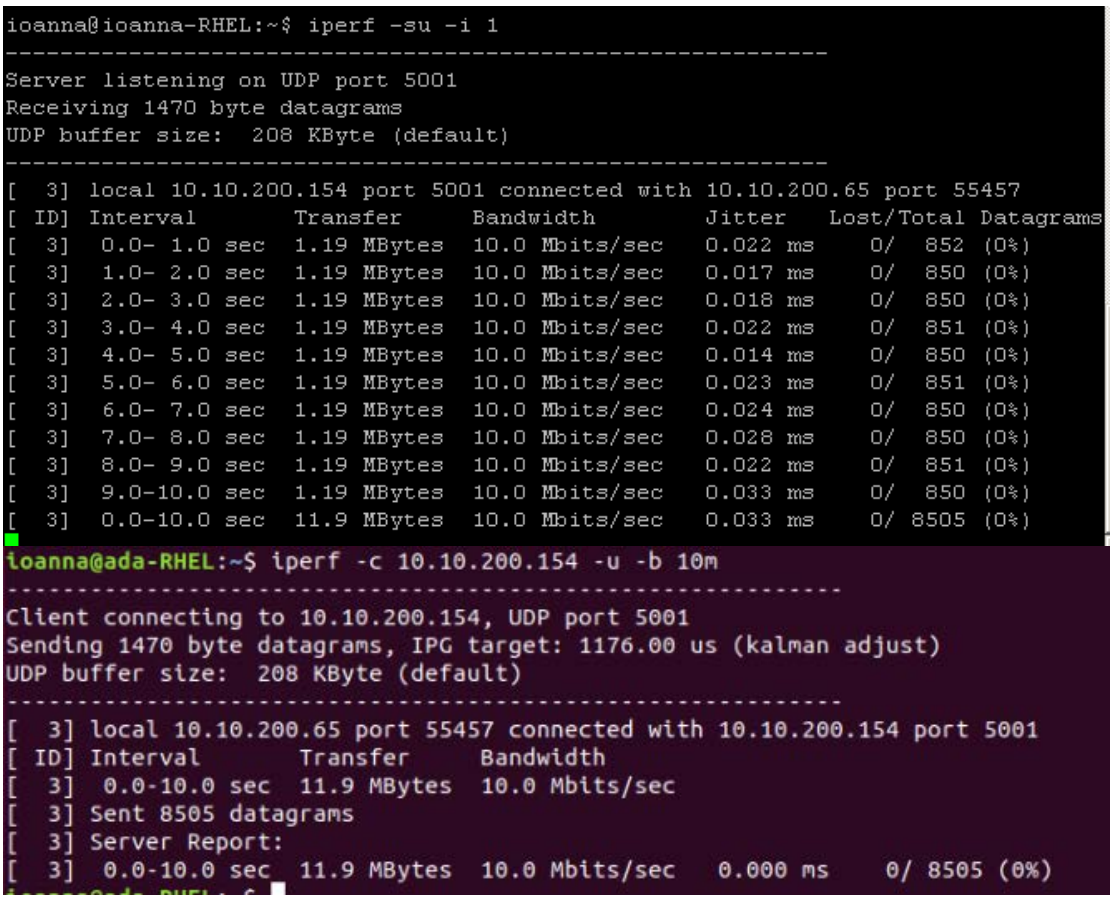
-u: use UDP rather than TCP

```
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.200.154 port 5001 connected with 10.10.200.65 port 35124
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.054 ms    0/  893 (0%)
ioanna@ada-RHEL:~$ iperf -c 10.10.200.154 -u
------------------------------------------------------------
Client connecting to 10.10.200.154, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.200.65 port 35124 connected with 10.10.200.154 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.000 ms    0/  893 (0%)
```

Εικόνα 22: Εντολή iperf -u

6. Έλεγχος για απώλεια πακέτων (packet loss) μέσω UDP: για να υπάρχει καλή ποιότητα στη σύνδεση, η απώλεια πακέτων δεν θα πρέπει να ξεπερνάει το 1%. Ένα μεγάλο ποσοστό χαμένων πακέτων θα προκαλέσει πολλές αναμεταδόσεις TCP τμημάτων κάτι που θα επηρεάσει το bandwidth. Στο πιο κάτω παράδειγμα έχει αλλαχθεί η τιμή του μέγιστου bandwidth που θα χρησιμοποιηθεί περιορίζοντας το στα 10 Mbps.

-b: set the target bandwidth



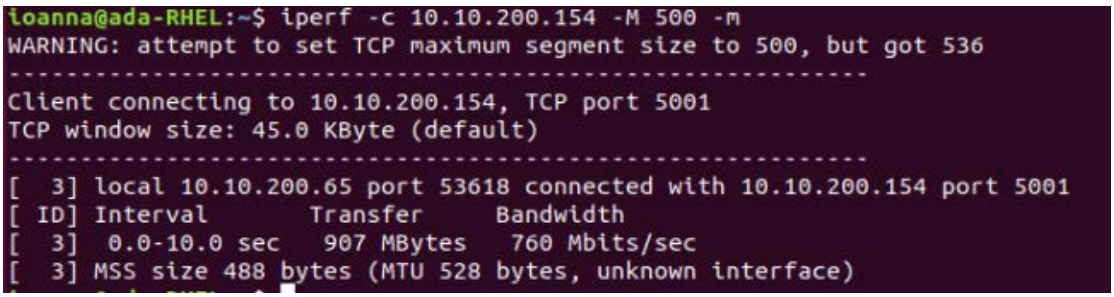
Εικόνα 23: Εντολή iperf -b

Όπως φαίνεται το bandwidth έχει περιοριστεί στα 10 Mbps, και υπάρχει μηδενική απώλεια πακέτων. Η τιμή του jitter είναι σημαντική σε δίκτυα που υποστηρίζουν VoIP, καθώς ένα υψηλό jitter μπορεί να διακόψει μια κλήση. Το Jitter είναι η διακύμανση της καθυστέρησης (latency) και δεν βασίζεται στην καθυστέρηση. (Μπορεί να έχουμε ψηλό χρόνο ανταπόκρισης και πολύ χαμηλό jitter)

7. Εδώ εξετάζουμε το bandwidth και ταυτόχρονα ζητείται να εκτυπωθεί η τιμή MSS (maximum segment size).

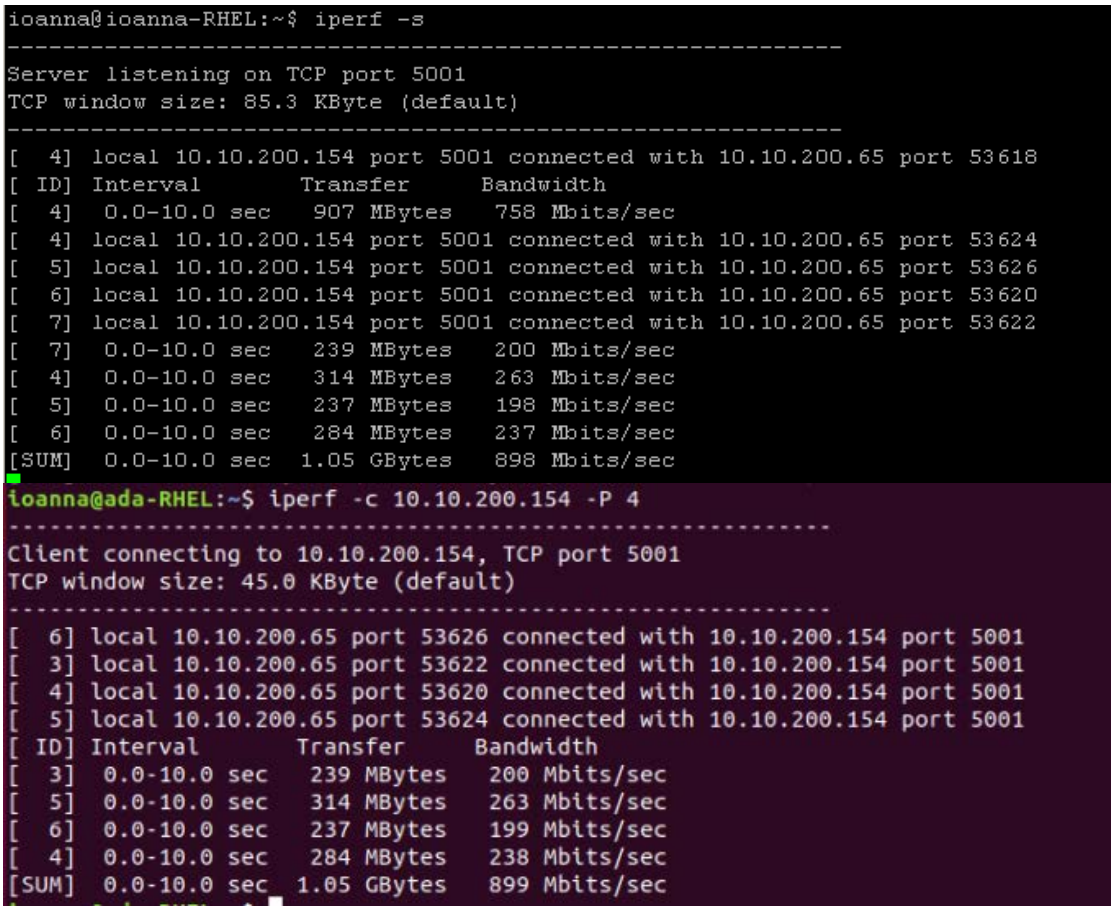
MSS=MTU -TCP&IP headers

Σημ. Υψηλό MTU και MSS αποφέρουν μεγαλύτερη αποτελεσματικότητα bandwidth



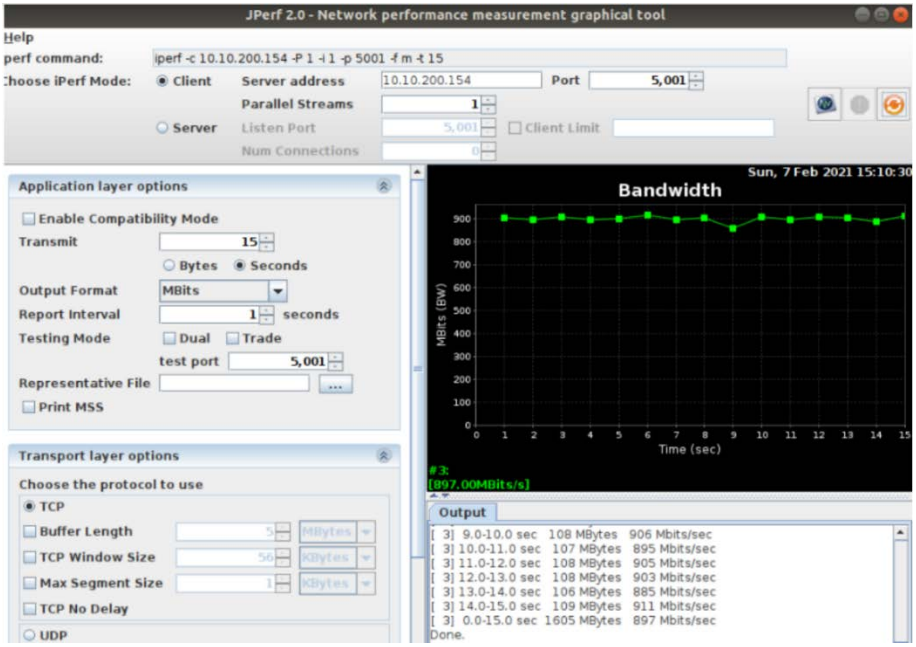
Εικόνα 24: Εντολή iperf -M

8. Με το -p πραγματοποιούμε παράλληλα τεστ σε διαφορετικές πόρτες.



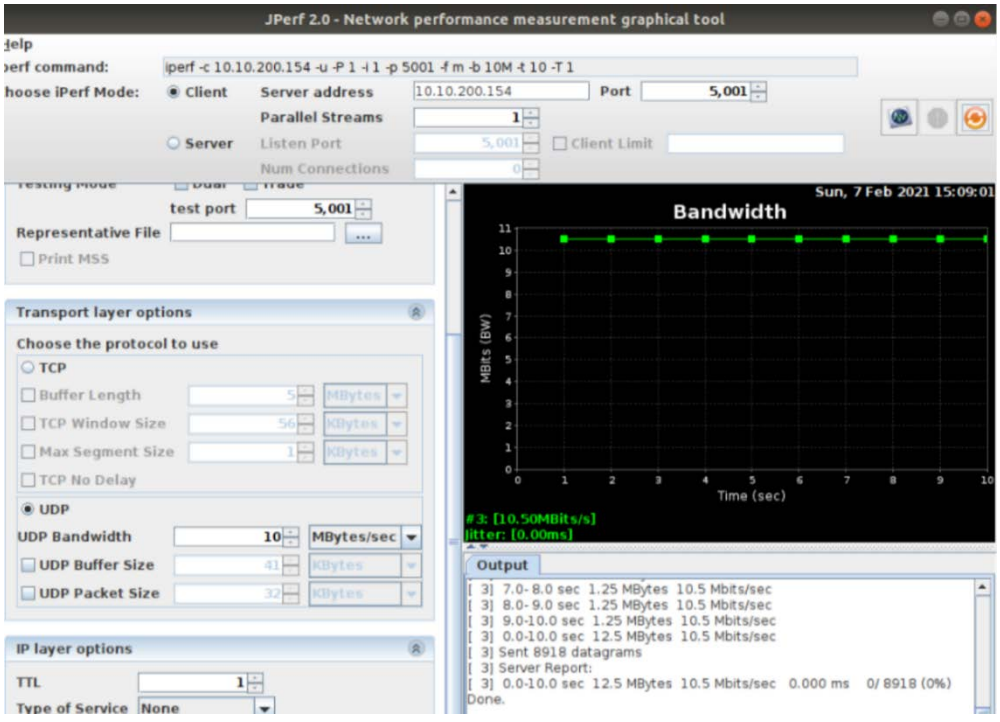
Εικόνα 25: Εντολή iperf -P

Βάζοντας τα πιο πάνω δεδομένα στο εργαλείο "JPerf – Network performance measurement graphical tool" φαίνεται ότι δεν υπάρχει απώλεια πακέτων.



Εικόνα 26: JPerf

Μηδενική απώλεια πακέτων υπάρχει και στην περίπτωση χρήσης του UDP όπως φαίνεται και στην εικόνα 27:



Εικόνα 27: JPerf - UDP

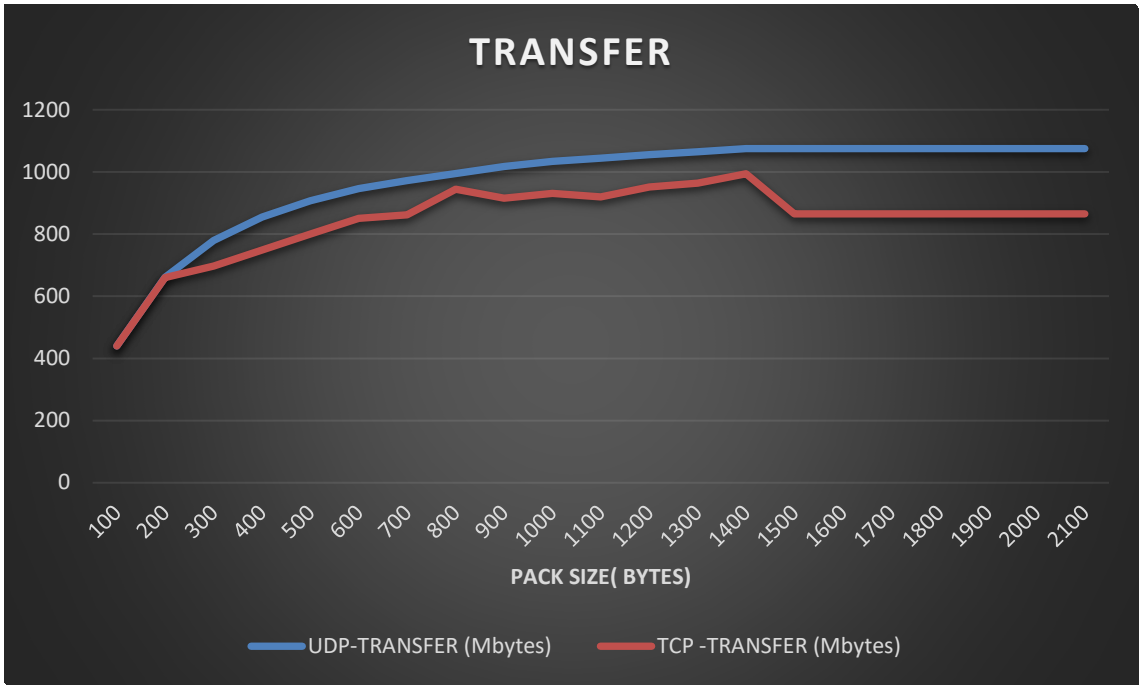
5.1 Αποτελέσματα

Προκειμένου να πάρουμε συγκρίσιμα πειραματικά αποτελέσματα, έγιναν διάφοροι έλεγχοι με το εργαλείο Iperf, τόσο με το πρωτόκολλο UDP όσο και με το TCP.

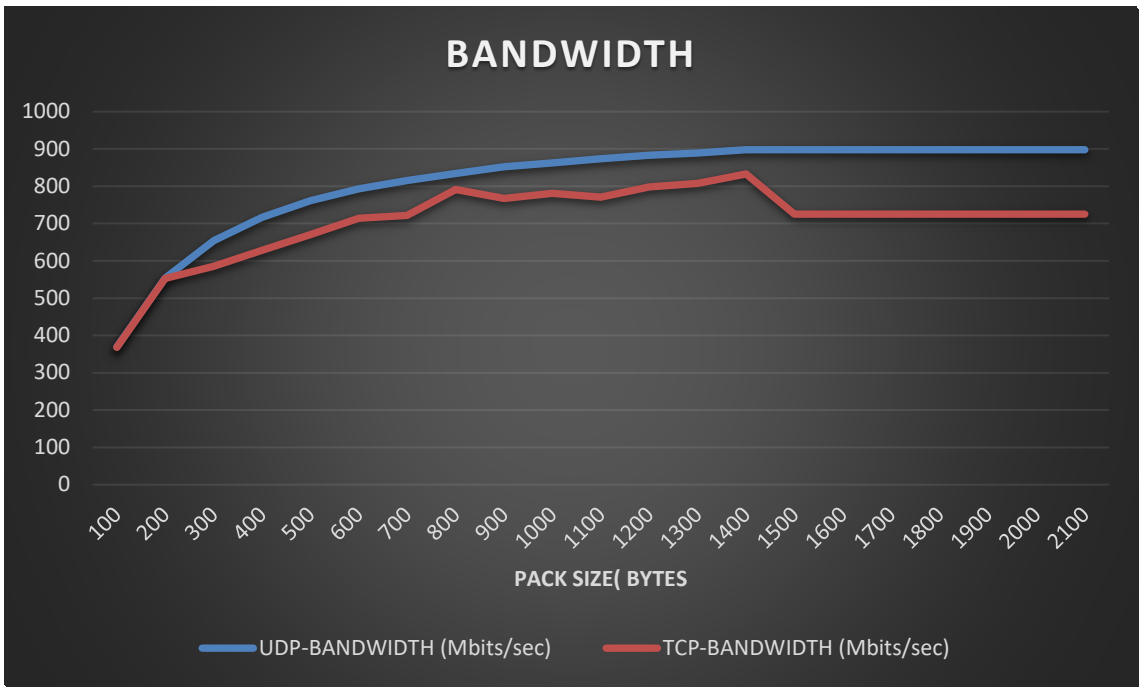
Κατά τον έλεγχο με UDP πρωτόκολλο, το Iperf επιτρέπει στον χρήστη να καθορίσει το μέγεθος του πακέτου (datagram) και δίνει αποτελέσματα για την απόδοση και απώλεια πακέτων.

Κατά τον έλεγχο με TCP πρωτόκολλο, το Iperf μετρά την απόδοση (throughput) του payload.

Στις μετρήσεις χρησιμοποιήθηκαν διάφορα μεγέθη πακέτων από 100 έως και 2100bytes, και εκτελέστηκε η ίδια εντολή και στα δύο πρωτόκολλα.



Διάγραμμα 1: Μέτρηση -Transfer



Διάγραμμα 2: Μέτρηση -Bandwidth

Εδώ φαίνεται ξεκάθαρα ότι με το UDP πρωτόκολλο από τα 1500 packet size και πάνω, το transfer και το Bandwidth δεν αυξάνονται πλέον αφού ένα "τυπικό" μέγεθος πακέτου κυμαίνεται από τα 1000 μέχρι τα 1500 bytes.
Το UDP έχει αυξημένη ταχύτητα μεταφοράς σε σύγκριση με το TCP αφού το πρωτόκολλο UDP παρέχει πιο ψηλό χρόνο μεταφοράς και ταχύτητα σε σχέση με το TCP.

Επίσης στο πιο πάνω πείραμα φαίνεται ότι η αποδοτικότητα του δικτύου μέσω UDP είναι καλύτερη σε σχέση με το TCP. Σύμφωνα με τον οργανισμό IETF , το UDP προσφέρει ταχύτητα, και το TCP αξιοπιστία αφού κάνει διόρθωση σφαλμάτων. Παρόλο που στο πιο πάνω πείραμα φαίνεται "καλύτερο" το UDP, εντούτοις οι περισσότεροι χρησιμοποιούν το TCP αφού προσφέρει εντοπισμό και διόρθωση λαθών και εγγυάται την παράδοση όλων των πακέτων όπως φαίνεται και στον πίνακα 1:

	TCP	**UDP**
Ταχύτητα	Αργή	Γρήγορη
Αξιοπιστία	Ψηλή	Χαμηλή
Εντοπισμός λαθών	Ναι	Μόνο σε κατεστραμμένα πακέτα (corrupted)
Διόρθωση λαθών	Ναι	Όχι, απορρίπτει τα κατεστραμμένα πακέτα
Έλεγχος συμφόρησης	Ναι	Όχι

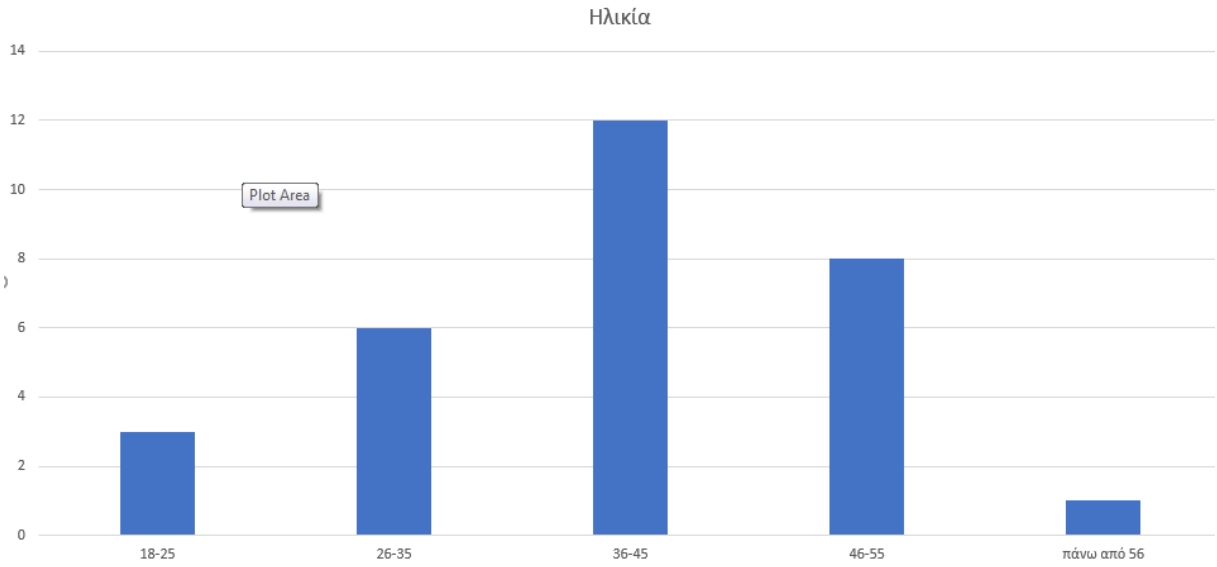
Πίνακας 1: Σύγκριση απόδοσης TCP – UDP

5.2 Ερωτηματολόγιο

Το επόμενο βήμα της διατριβής περιλαμβάνει ένα ερωτηματολόγιο το οποίο στάλθηκε σε συγκεκριμένες εταιρείες όπου κάνουν χρήση των εικονικών δικτύων, με σκοπό να προωθηθεί σε τυχαία άτομα με email. Επιλέγηκαν συγκεκριμένα 4 εταιρείες όπου τον τελευταίο χρόνο, λόγω covid-19, χρησιμοποιούν σε καθημερινή βάση συνδέσεις VPN. Οι εταιρείες αυτές ανήκουν στις κατηγορίες: πληροφορική, τηλεπικοινωνίες, εκπαίδευση, και κυβερνητική υπηρεσία εξυπηρέτησης πολιτών. Οι ερωτήσεις ήταν σχετικές με το VPN. Το ερωτηματολόγιο που στάλθηκε φαίνεται στο παράρτημα 1. Ο αριθμός του δείγματος που ανταποκρίθηκαν στις ερωτήσεις ήταν 30 άτομα.

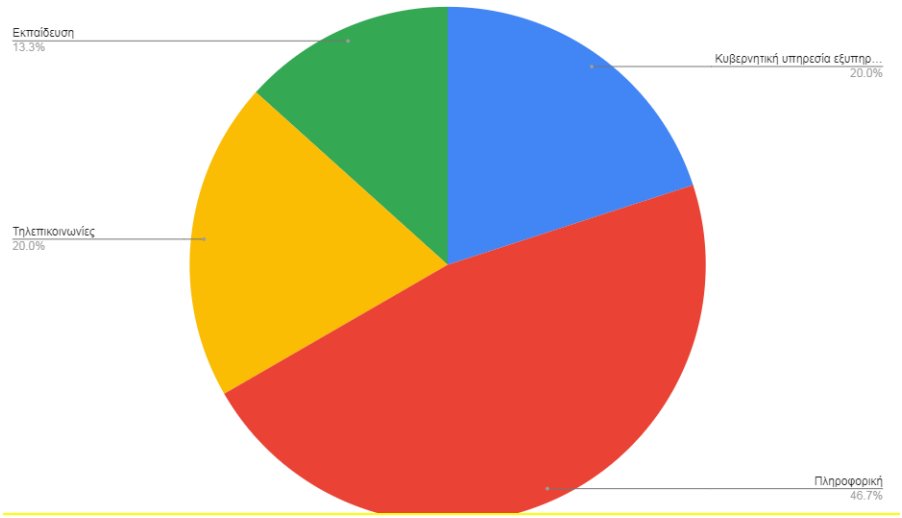
5.2.1Αποτελέσματα Ερωτηματολογίου

Στις ερωτήσεις απάντησαν 17 άντρες και 13 γυναίκες. 12 άτομα δήλωσαν ότι ανήκουν στην ηλικία 36-45, ενώ ένα άτομο ανήκει στην ηλικία πάνω από 65. 3 άτομα εμπίπτουν στην ηλικιακή ομάδα 18-25, 6 άτομα στην ομάδα 26-35 και 8 άτομα στην ομάδα 46-55.



Διάγραμμα 3: Ερώτηση 2 από το ερωτηματολόγιο

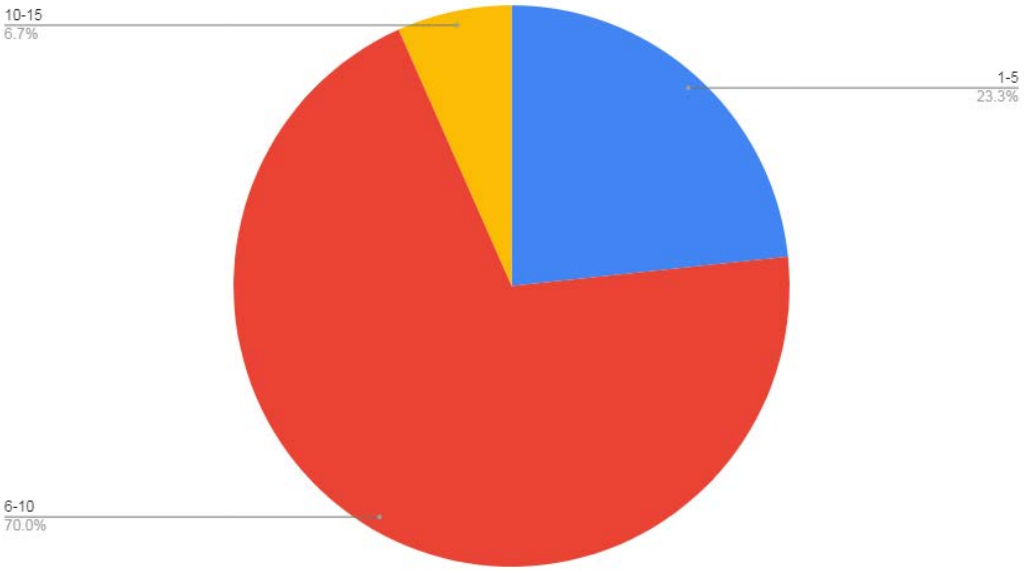
Η επόμενη ερώτηση αφορούσε τον τομέα που εργάζονται οι χρήστες. Το μεγαλύτερο ποσοστό ανήκει στον τομέα της πληροφορικής με 43,3% και το πιο μικρό στον τομέα της εκπαίδευσης με 13,3%.



Διάγραμμα 4: Ερώτηση 3 από το ερωτηματολόγιο

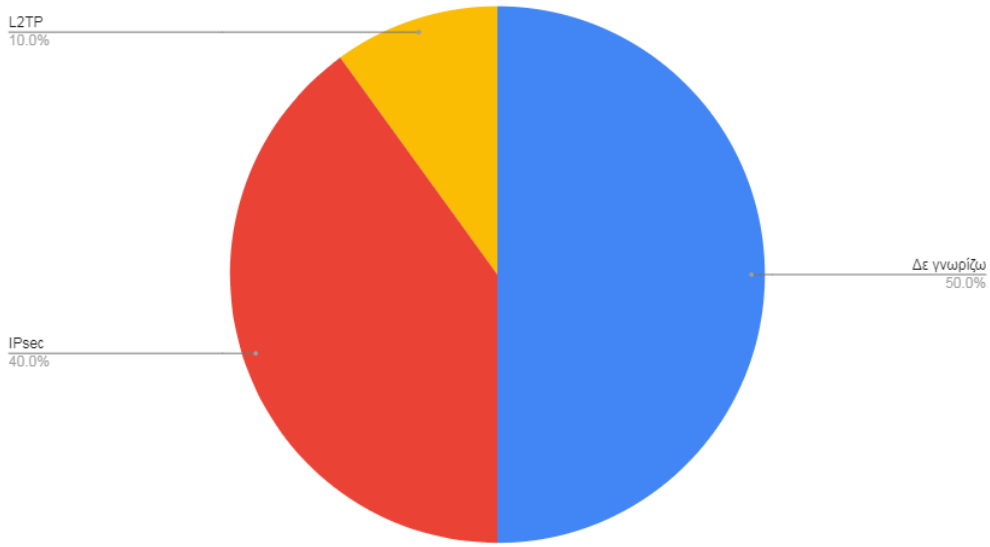
Στη συνέχεια οι χρήστες ρωτήθηκαν αν χρησιμοποιούν το VPN, και οι περισσότεροι απάντησαν θετικά με το ποσοστό να ανεβαίνει το 96,7% σε σχέση με τις αρνητικές απαντήσεις με 3,3%.

Ακολούθως οι χρήστες απάντησαν ερώτηση σχετικά με την ημερήσια χρήση του VPN. Το 70% των χρηστών συνδέονται 6-10 ώρες την ημέρα, το 23% 1-5 ώρες ενώ το 6,7% το χρησιμοποιούν 10-15 ώρες σε ημερήσια βάση.



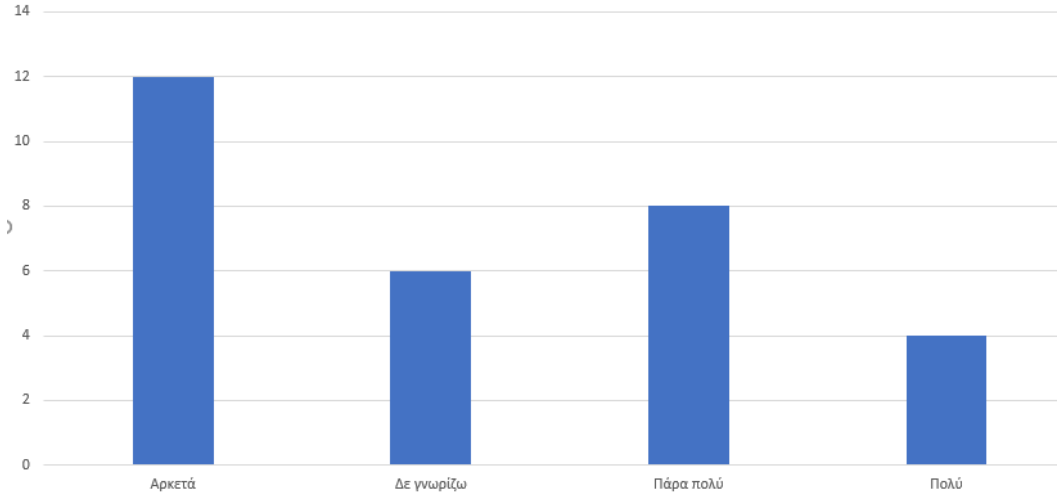
Διάγραμμα 5: Ερώτηση 5 από το ερωτηματολόγιο

Η ερώτηση 6, σχετίζεται με την τεχνολογία του VPN που χρησιμοποιούν οι χρήστες. Είναι σημαντικό να αναφερθεί ότι το 50% δε γνωρίζει τι είδους τεχνολογία χρησιμοποιεί η σύνδεση VPN που χρησιμοποιεί. Το 40% απάντησε IPSec, ενώ το 10% L2TP.



Διάγραμμα 6: Ερώτηση 6 από το ερωτηματολόγιο

Στην ερώτηση κατά πόσο οι χρήστες θεωρούν ασφαλή την VPN σύνδεση τους, 12 άτομα απάντησαν "αρκετά", ενώ 4 απάντησαν "πολύ". Αξίζει να σημειωθεί ότι, παρόλο που το 50% δεν γνώριζε την VPN τεχνολογία που χρησιμοποιούν, μόνο το 20% δε γνωρίζει πόσο ασφαλής είναι η VPN σύνδεση του (6 άτομα).

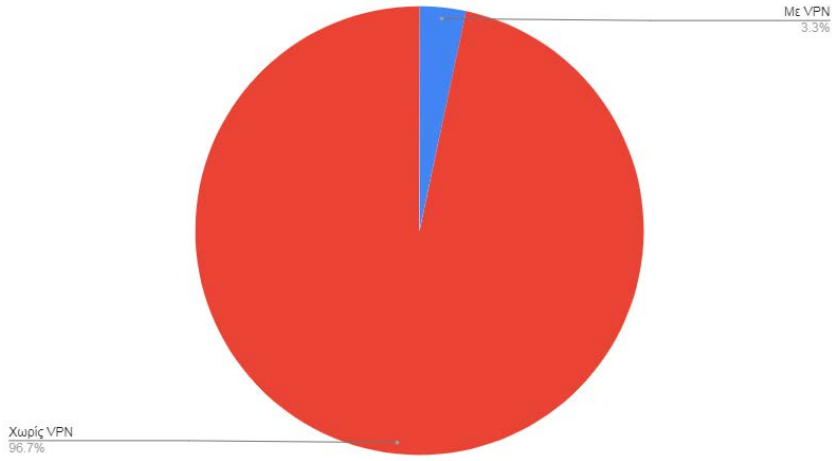


Διάγραμμα 7: Ερώτηση 7 από το ερωτηματολόγιο

Η επόμενη ερώτηση ήταν κατά πόσο οι χρήστες γνωρίζουν αν ένα VPN δίκτυο χρησιμοποιεί τεχνολογίες κρυπτογράφησης. Οι απαντήσεις μοιράστηκαν ανάμεσα στο "Ναι" και "Όχι".

Διάγραμμα 8: Ερώτηση 8 από το ερωτηματολόγιο

Το ερωτηματολόγιο ολοκληρώθηκε με ερώτηση αναφορικά με την ταχύτητα του διαδικτύου. Κατά πόσο δηλαδή η σύνδεση είναι πιο γρήγορη με ή χωρίς VPN. Οι χρήστες απάντησαν ότι η σύνδεση χωρίς VPN είναι πιο γρήγορη με ποσοστό 96,7%.



Διάγραμμα 9: Ερώτηση 9 από το ερωτηματολόγιο

Από τα πιο πάνω αποτελέσματα φαίνεται ότι παρόλο που γίνεται χρήση των εικονικών δικτύων, εντούτοις, οι περισσότεροι χρήστες δε γνωρίζουν τι τεχνολογία χρησιμοποιούν αλλά ούτε και αν η σύνδεση τους, τους παρέχει εμπιστευτικότητα κάνοντας χρήση αλγόριθμους κρυπτογράφησης. Όμως αρκετοί χρήστες θεωρούν ότι μια σύνδεση VPN είναι αρκετά ασφαλή.

Πιο κάτω θα αναλύσουμε εις βάθος τις απαντήσεις της ερώτησης 7, κατά πόσο οι χρήστες θεωρούν ασφαλή την VPN σύνδεση τους, μετατρέποντας τις επιλογές σε αριθμούς για ευκολία:

Καθόλου = 1

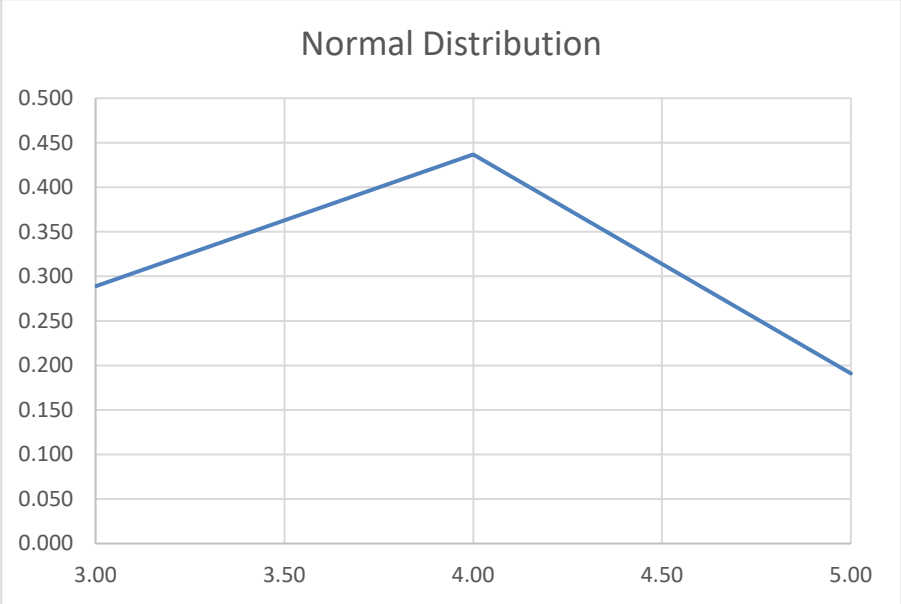
Λίγο = 2

Αρκετά = 3

Πολύ = 4

Πάρα πολύ = 5

Ενσωματώνουμε τα αποτελέσματα σε γραφική παράσταση μέσω της Microsoft Excel, και φαίνεται ότι οι χρήστες είναι αρκετά ικανοποιημένοι όσον αφορά την ασφάλεια των εικονικών δικτύων που χρησιμοποιούν.



Διάγραμμα 10: Standard deviation με τη χρήση της μέσης τιμής

Τα αποτελέσματα κυμαίνονται μεταξύ 3 και 4, κάτι το οποίο μας δείχνει ότι η μερίδα των χρηστών που χρησιμοποιούν το VPN στην καθημερινότητά τους φαίνονται ικανοποιημένοι σε αρκετά καλό βαθμό, αφού ο αριθμός 3 ισοδυναμεί με το "αρκετά" και ο αριθμός 4 με το "πολύ". Να σημειωθεί ότι δεν παραλήφθηκαν απαντήσεις με τις επιλογές 1 και 2, που αντιστοιχούν στα καθόλου και λίγο. Άρα σαν γενικό συμπέρασμα μπορούμε να πούμε ότι, παρόλο που το VPN μπήκε στη ζωή μας πιο πολύ τον τελευταίο χρόνο λόγω covit 19, και αρκετοί αναγκάστηκαν να δουλέψουν από το σπίτι, αλλά και επιπλέον αρκετοί δε γνωρίζουν τι ακριβώς είναι και τι τεχνολογίες χρησιμοποιεί,

εντούτοις οι πιο πολλοί χρήστες νοιώθουν αρκετά ικανοποιημένοι όσον αφορά την ασφάλεια των δεδομένων που διακινούν μέσω διαδικτύου.

Κεφάλαιο 6

Πλεονεκτήματα-Μειονεκτήματα VPN

6.1 Πλεονεκτήματα (22) VPN

Η χρήση VPN αποφέρει σημαντικά οφέλη σε όλα τα μέρη που συμμετέχουν, είτε αυτά αποτελούν την εταιρεία που το χρησιμοποιεί, είτε τον τελικό χρήστη του VPN, είτε τον ISP που παρέχει την υποδομή. Σε γενικές γραμμές τα οφέλη περιλαμβάνουν μείωση των δαπανών για τις τηλεπικοινωνίες, καλύτερη διαχείριση και ευκολότερη συντήρηση, πιο εύκολη κατασκευή του συστήματος.

- Άμεσα οικονομικά οφέλη, αφού επιτυγχάνεται σημαντική μείωση στο συνολικό κόστος των εταιρειών (σταματούν οι μισθωμένες γραμμές , οι κλήσεις μεγάλων αποστάσεων, αφαιρείται ο εξοπλισμός απομακρυσμένης πρόσβασης)
- Εξελιγμένος σχεδιασμός δικτύου – αποφεύγεται η πολυπλοκότητα του WAN. Δίνεται η επιλογή επέκτασης του δικτύου και η παροχή πρόσβασης σε απομακρυσμένους χρήστες (ευελιξία).
- Κεντρικοποιημένος έλεγχος, αφού το VPN είναι ένας καλός μηχανισμός ανίχνευσης βλαβών και προσφοράς μεγαλύτερης ασφάλειας. Επίσης υπάρχει καλύτερος έλεγχος κυκλοφορίας μέσα στο δίκτυο – ευελιξία στη δρομολόγηση (flexible routing).
- Ευκολίες στον τελικό χρήστη, αφού μειώνεται το κόστος σύνδεσης, αλλά παράλληλα γίνεται σύνδεση από οποιοδήποτε σημείο σε παγκόσμια βάση.
- Προσφορά στρατηγικού πλεονεκτήματος, αφού βελτιώνονται οι υπηρεσίες ενός οργανισμού σε σχέση με τους υπόλοιπους. Υπάρχει βελτίωση σε θέματα αξιοπιστίας και απόδοσης από πλευράς καθυστέρησης.

6.2 Μειονεκτήματα VPN

Εκτός από τα ελκυστικά πλεονεκτήματα των VPN υπάρχουν και κάποια μειονεκτήματα τα οποία θα πρέπει να ληφθούν υπόψη:

- Επιβάρυνση πακέτων: στην πλειονότητα των τεχνολογιών VPN το αρχικό πακέτο επιβαρύνεται με περισσότερες πληροφορίες κεφαλίδας. Αυτό οδηγεί στην αύξηση του μεγέθους αλλά συγχρόνως μπορεί να απαιτηθεί κατακερματισμός, κάτι που πιθανόν να επηρεάσει την απόδοση του δικτύου.
- Απαίτηση πόρων: η διαχείριση των εικονικών συνδέσεων αλλά και η υλοποίηση των κρυπτογραφικών τεχνικών συνήθως απαιτούν μαθηματικούς υπολογισμούς οι οποίοι δαπανούν πόρους.
- Δυσκολία υλοποίησης και διαχείρισης: η υλοποίηση ενός VPN απαιτεί εξιδεικευμένες γνώσεις και αρκετή προσοχή αφού μέσα από το δημόσιο δίκτυο διακινούνται ευαίσθητα δεδομένα.
- Διαθεσιμότητα: η διαθεσιμότητα των VPN συνδέσεων εξαρτάται απόλυτα από τη διαθεσιμότητα του δημόσιου δικτύου. Αν το δημόσιο δίκτυο δεν είναι διαθέσιμο, τότε οι εικονικές συνδέσεις ορίζονται ανενεργές.

Κεφάλαιο 7
Επίλογος

Συνοψίζοντας, μπορούμε να πούμε ότι τα VPN δεν κάνουν τίποτα άλλο από το να εκμεταλλεύονται επιτυχώς το διαδίκτυο έτσι ώστε να μεταφέρουν με ασφάλεια τα δεδομένα και να συνδέουν τους απομακρυσμένους χρήστες, τα επιμέρους υποκαταστήματα και τους επιχειρησιακούς συνεργάτες σε ένα εκτεταμένο εταιρικό δίκτυο. Έτσι επιτυγχάνεται μείωση του κόστους που απαιτείται να καταβάλλει μια εταιρεία ώστε να επιτευχθεί η επικοινωνία μεταξύ των εμπλεκόμενων μελών της. Το ποια αρχιτεκτονική και ποια τεχνολογία θα χρησιμοποιηθεί κάθε φορά, εξαρτάται από τις εκάστοτε ανάγκες. Για την χρήση VPN τεχνολογιών σε περιβάλλοντα cyber range για την διασύνδεση τους όπως φάνηκε και από την βιβλιογραφική ανασκόπηση και από την υλοποίηση, είναι μια βιώσιμη λύση για multi domain ασκήσεις μεταξύ των cyber ranges.

7.1 Συμπέρασμα

Η υλοποίηση μπορεί να επιτευχθεί σχετικά εύκολα αρκεί να γίνει ένας σωστός σχεδιασμός και να μην αντιμετωπίζεται σαν ένα ξεχωριστό κομμάτι του δικτύου αλλά ως συνέχεια του. Από το ερωτηματολόγιο που έγινε φάνηκε ότι παρόλο που οι πιο πολλοί σήμερα, ανεξαρτήτως ηλικίας, χρησιμοποιούν μια σύνδεση VPN, δε γνωρίζουν τι είδους σύνδεση είναι αλλά ούτε και αν είναι ασφαλείας. Επίσης θεωρούν τη σύνδεση με VPN αρκετά αργή. Μια μελλοντική μελέτη θα ήταν να εξευρεθούν τρόποι αντιμετώπισης της αργής σύνδεσης.

Παράλληλα όμως, όσο εξελίσσεται η τεχνολογία, τόσο εξελίσσονται και οι επιθέσεις και κατ' επέκταση γίνεται και πιο απαιτητικός ο εντοπισμός τους, θα πρέπει να γνωρίζουμε όσο γίνεται πιο λεπτομερώς τον τρόπο που θα στήσουμε το δίκτυο μας. Μελλοντικά, θα πρέπει να ερευνηθούν και τρόποι σωστής επέκτασης του εικονικού δικτύου το οποίο να υποστηρίζει νέες εγκαταστάσεις , συντήρηση τους καθώς και άμεση αντιμετώπιση και

υποστήριξη τυχών προβλημάτων. Επιπλέον μια έρευνα που θα μπορούσε να γίνει στο μέλλον, είναι να δημιουργηθεί μια εφαρμογή η οποία να εντοπίζει όλους τους τύπους επιθέσεων και να αναπτυχθεί μηχανισμός ο οποίος να μπλοκάρει τέτοιες επιθέσεις, έτσι ώστε το δίκτυο να είναι όσον το δυνατό πιο ασφαλή. Επίσης θα μπορούσε να μελετηθεί και τρόπος διασύνδεσης εικονικών δικτύων μέσω του δικτύου κινητής τηλεφωνίας.

Βιβλιογραφία

1. **Stewart, Michael.** *Network Security, Firewalls and VPNs.* Burlington : Jones & Barlett Learning. LLC, 2014. σσ. 320-345. Τόμ. 2.
2. **James S. Tiller.** *A technical guide to IPSec virtual private Networks.* London : CRC Press LLC, 2017. σσ. 11-15. Τόμ. 2.
3. **David, Balaban.** What Is A VPN Protocol And Which One Should You Use? *is Buzz news.* 17 June 2019.
4. **Michael, Solomon G.** *Security Strategies in windows platforms and applivations.* 2nd. s.l. : Jones & Bartlett Learning, 2019. σσ. 70-80.
5. **M. N. Ogbu, G. N. Onoh, K. C. Okafor.** *Cloud based virtual private networks using IP tunneling for remote site interfaces.* 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON). Nigeria : IEEE, 2017.
6. **Leonard, Barolli, Amato, Flora και Francesco, Moscato.** *Web, Artificial Intelligence and Network Applications.* Switzerland : Springer Nature Switzerland AG, 2020.
7. **Kotuliak, I., P, Rybár και P, Trúchly.** *Performance comparison of IPsec and TLS based VPN technologies.* 2011 9th International Conference on Emerging eLearning Technologies and Applications (ICETA). Slovakia : IEEE, 2011. σσ. 110-138.
8. **Nam, Nguyen.** *Essential Cyber security Handbook in Greek.* 2018.
9. *What Is A VPN Protocol And Which One Should You Use?* **Balaban, David.** s.l. : https://informationsecuritybuzz.com, 2019.
10. **Teodor Sommestad, Mathias Ekstedt,Hannes Holm,Muhammad Afzal.** Security mistakes in information system deployment projects. *Information Management & Computer Security* . 19, 2011, Τόμ. 2, 80-94.
11. **K.Karuna Jyothi, Dr.B.Indira Reddy.** *Study on Virtual Private Network (VPN), VPN's Protocols And Security.* Telangana, India : s.n., 2018.
12. **Muchamed Elezi, Bujar Raufi.** *Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption.* Tetovo : Procedia, 2015.
13. **Rama Bansode, Anup Girdhar.** *Common Vulnerabilities Exposed in VPN – A Survey.* 2020.
14. **Georgia Dede, Rossen Naydenov, Apostolos Malatras.** *Cybersecurity Challenges in the uptake of Artificial Intelligence in Autonomous Driving.* Luxembourg : ENISA, 2021.
15. *A Survey of VPN Performance Evaluation.* **Avani J.Patel, Ankita Gandhi.** s.l. : International Journal on Recent and Innovation Trends in Computing and Communication, 2017, Τόμ. 5.
16. **Leyden, John.** https://www.theregister.com/2016/02/26/ssl_vpns_survey/. *https://www.theregister.com.* [Ηλεκτρονικό] 26 02 2016.
17. *A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients.* **Vasile C. Perta, Marco V. Barbera, Gareth Tyson, Hamed Haddadi, Alessandro Me.** Rome,London : Sciendo, 2015.
18. *VPN protocols explained: how do they work?* **Mazūra, Justinas.** s.l. : https://cybernews.com, 2021.
19. *Open source system OpenVPN in a function of Virtual Private.* **A Skendzic, B Kovacic.** Croatia : s.n., 2016.
20. *Using iPerf to Troubleshoot Speed and Throughput Issues.* **Soman, Stanley.** 2016.
21. *Performance Comparison between TCP and UDP Protocols in Different Simulation Scenarios.* **Fahad Taha AL-Dhief, Naseer Sabri, N. M. Abdul Latiff,Nik Noordini, Musatafa Abbas,Omar Ibrahim Obaid.** Malaysia : s.n., 2018.
22. **Vasconcellos, Eduardo.** https://www.business.com/vpn/protocols/. *Identifying the Differences Between VPN Protocols.* [Ηλεκτρονικό] 2021.

Ιστοσελίδες

www.ietf.org
https://en.wikipedia.org/wiki/OSI_model
https://el.wikipedia.org/wiki/IETF
https://tools.ietf.org/html
www.enisa.europa.eu
https://owasp.org/www-community/controls/Certificate_and_Public_Key_Pinning
https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-18-04
https://www.computerworld.com
https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html#~types-of-vpns

Παράρτημα 1
Ερωτηματολόγιο

VPN – ΕΙΚΟΝΙΚΑ ΔΙΚΤΥΑ

1. Φύλο

- ☐ Άντρας
- ☐ Γυναίκα

2. Ηλικία

- ☐ 18-25
- ☐ 26-35
- ☐ 36-45
- ☐ 46-55
- ☐ πάνω από 56

3. Σε ποιον τομέα εργάζεσαι;

- ☐ Πληροφορική
- ☐ Τηλεπικοινωνίες
- ☐ Εκπαίδευση
- ☐ Κυβερνητική υπηρεσία εξυπηρέτησης πολιτών

4. Χρησιμοποιείς VPN (εικονικό δίκτυο) για σύνδεση στο διαδίκτυο;

- ☐ Ναι
- ☐ Όχι

5. Πόσες ώρες την ημέρα χρησιμοποιείς το VPN;

- ☐ 1-5
- ☐ 6-10
- ☐ 10-15
- ☐ πάνω από 15

6. Τι τεχνολογία VPN χρησιμοποιείς;

- [ ] Δε γνωρίζωIPsec
- [ ] L2TP
- [ ] PPTP

7. Πόσο ασφαλής θεωρείς ότι είναι η VPN σύνδεση σου;

- [ ] Δε γνωρίζω
- [ ] Καθόλου
- [ ] Λίγο
- [ ] Αρκετά Πολύ
- [ ] Πάρα πολύ

8. Γνωρίζεις αν η VPN σύνδεση σου χρησιμοποιεί τεχνολογίες κρυπτογράφησης;

- [ ] Ναι
- [ ] Όχι

9. Συνδέεσαι με VPN και χωρίς VPN. Ποια σύνδεση θεωρείς πιο γρήγορη;

- [ ] Με VPN
- [ ] Χωρίς VPN