ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«Πληροφορική και Δίκτυα »

Διπλωματική εργασία

«Ασφάλεια δικτύου υπολογιστών, υλοποίηση σε επιχειρηματικό περιβάλλον»

Του Θεοφάνη Γκαναβία, Α.Μ.: 151

Επιβλέπων: Στεργίου Ελευθέριος

Στους ανθρώπους που πίστεψαν σε εμένα
και με στήριξαν.

Περιεχόμενα

Περίληψη 7

Abstract 8

Εισαγωγή 9

Κεφάλαιο 1 - Τεχνολογίες και μέθοδοι 11

1.1.Telnet και Secure Shell 13

1.1.Εναλλαγή ετικετών πολλαπλών πρωτοκόλλων 14

1.2.Εικονικό ιδιωτικό δίκτυο 15

1.4 Έλεγχος ταυτότητας 21

1.5 Κρυπτογράφηση και αποκρυπτογράφηση 23

1.6 Συμπέρασμα για τις τεχνολογίες 25

ΚΕΦΑΛΑΙΟ 2 - ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΡΓΟΥ 27

ΚΕΦΑΛΑΙΟ 3 - "Σχεδιασμός, Υλοποίηση και Αξιολόγηση Ασφαλούς Εικονικού Ιδιωτικού Δικτύου με WireGuard: Μια Πρακτική Προσέγγιση" 30

3.1 Εισαγωγή 30

3.2 Μεθοδολογία 30

3.2.1 Προετοιμασία και Διαμόρφωση του Περιβάλλοντος 30

3.2.2 Δοκιμές Συνδεσιμότητας και Επαλήθευση Λειτουργικότητας 30

3.2.3 Εισαγωγή και Περιγραφή Περιβάλλοντος Δοκιμών 31

3.2.4 Γιατί Επιλέξαμε το WireGuard 31

3.2.5 Τεχνικά Πλεονεκτήματα του WireGuard 31

3.3 Εφαρμογές και Σενάρια Χρήσης 32

3.4 Λόγοι Επιλογής του WireGuard 32

3.5 Βήματα Υλοποίησης του VPN 33

3.5.1 Προετοιμασία του Kali Linux ως VPN Server 33

3.5.2 Δημιουργία Κλειδιών Κρυπτογράφησης Server 33

3.5.3 Ρύθμιση Διασύνδεσης WireGuard Server 34

3.6 Ενεργοποίηση IP Forwarding και Ρύθμιση NAT 35

3.7 Εκκίνηση του VPN Server 36

3.8 Δημιουργία και Ρύθμιση Clients ... 37
3.9 Σύνδεση και Έλεγχος ... 38
3.10 Firewall και Ασφάλεια ... 39
3.10.1 Δοκιμές Ασφαλείας και Packet Capture ... 39
3.10.2 Απόδοση και Αποτελέσματα ... 43
3.11 Αξιολόγηση Ασφάλειας ... 43
3.11.1 Πλεονεκτήματα και Μειονεκτήματα που παρατηρήθηκαν ... 44
3.11.2 Μελλοντική βελτίωση και ανάπτυξη ... 44
3.12 Διαλειτουργικότητα και Αντιμετώπιση Προβλημάτων ... 44
3.13 Αξιολόγηση και Ανάλυση Κίνησης Δικτύου ... 45
3.14 Συμπεράσματα ... 45
Ξενόγλωσσες βιβλιογραφικές αναφορές ... 47

Περιεχόμενα Πινάκων

Πίνακας 1: Τεχνολογίες και η καταλληλότητά τους ... 25
Πίνακας 2: Απαιτήσεις για τις προσφερόμενες υπηρεσίες των παρόχων Διαδικτύου: τύπος τεχνολογίας, ταχύτητα και τιμή ... 28

Περιεχόμενα Εικόνων

Εικόνα 1: Αφηρημένο μοντέλο δικτύου ... 11
Εικόνα 2: Τα τοπικά δίκτυα χωρίζονται από το Διαδίκτυο ... 12
Εικόνα 3: Αφηρημένη μετάδοση δεδομένων χωρίς ασφάλεια ... 15
Εικόνα 4: Δημιουργία κρυπτογραφημένης σήραγγας μεταξύ του Router1 και του Router2 ... 16
Εικόνα 5: Απομακρυσμένο (Remote) VPN ... 18
Εικόνα 6: Intranet VPN ... 19
Εικόνα 7: Extranet VPN ... 19

Περίληψη

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι η διερεύνηση των υφιστάμενων τεχνολογιών ασφάλειας πληροφοριών και η εφαρμογή αυτών σε ένα δίκτυο υπολογιστών. Η διπλωματική εργασία έχει δύο βασικά μέρη: το ερευνητικό μέρος και την υλοποίηση. Κάθε μέρος της εργασίας έχει διαφορετικούς στόχους.

Στο ερευνητικό μέρος, οι στόχοι αναφέρονται στον προσδιορισμό των σύγχρονων τεχνολογιών που υπάρχουν για την ενίσχυση της ασφάλειας ενός δικτύου και στο συμπέρασμα τι είδους τεχνολογία θα πρέπει να εγκατασταθεί στο μέρος υλοποίησης. Στο μέρος της υλοποίησης, οι στόχοι ήταν η δημιουργία πινάκων με δεδομένα που θα μπορούσαν να χρησιμοποιηθούν, η δημιουργία ενός περιβάλλοντος προσομοίωσης, η απόφαση μεταξύ της χρήσης μιας διεπαφής και μιας διεπαφής γραμμής εντολών, καθώς και η χρήση εντολών που θα μπορούσαν να εκτελεστούν για την εγκατάσταση του επιλεγμένου εργαλείου ασφαλείας. Ωστόσο, είναι σημαντικό να σημειωθεί ότι ενώ οι επιλεγμένες εντολές χρησιμοποιούνται για μια συγκεκριμένη συσκευή, ωστόσο μπορούν να εφαρμοστούν σε οποιαδήποτε συσκευή, οι απαιτήσεις υλικού και λογισμικού, καθώς η αρχή λειτουργίας τους παραμένει η ίδια.

Στη παρούσα εργασία χρησιμοποιήθηκαν ποιοτικές μέθοδοι για τη λήψη συγκεκριμένων πληροφοριών σχετικά με τις τεχνολογίες και τα μέτρα ασφαλείας. Η διπλωματική εργασία έχει διαμορφωθεί για να χρησιμοποιηθεί ως οδηγός εγκατάστασης τεχνολογίας σε επιχειρηματικό περιβάλλον.

Η διπλωματική εργασία ολοκληρώθηκε μετά από ανάλυση και υλοποίηση μετάδοσης δεδομένων με μέσα ασφαλείας, σε ένα σχεδιασμένο περιβάλλον με ένα σύνολο παραμέτρων που αντιστοιχούν σε υφιστάμενες προδιαγραφές.

Λέξεις-κλειδιά

εικονικό ιδιωτικό δίκτυο, ασφάλεια πληροφοριών, ομάδες χρηστών, σχεδιασμός ασφάλειας, έλεγχος ταυτότητας

Abstract

The purpose of this thesis is to investigate existing information security technologies and their application in a computer network. The thesis consists of two main parts: the research section and the implementation section, each with distinct objectives.

In the research section, the goals focus on identifying modern technologies available for enhancing network security and determining which technology should be deployed in the implementation phase. In the implementation section, the objectives include creating data tables for practical use, developing a simulation environment, deciding between the use of a graphical user interface (GUI) and a command-line interface (CLI), and executing commands for the installation of the selected security tool. It is important to note that while the chosen commands are applied to a specific device, they can be adapted to any device, as their hardware and software requirements, as well as their operational principles, remain consistent.

Qualitative methods were employed to gather specific information about security technologies and measures. This thesis is designed to serve as an installation guide for deploying technology.

The thesis was completed following the analysis and implementation of secure data transmission within a designed environment, using a set of parameters that align with existing specifications.

Keywords: Virtual Private Network (VPN), information security, user groups, security design, authentication.

Εισαγωγή

Η ασφάλεια δικτύων υπολογιστών είναι ζωτικής σημασίας σε ένα εργαστηριακό περιβάλλον για τη διαφύλαξη ευαίσθητων πληροφοριών, τη διατήρηση της εργαστηριακής έρευνας και την προστασία από απειλές στον κυβερνοχώρο. Η εφαρμογή ισχυρών μέτρων ασφαλείας περιλαμβάνει διάφορες βασικές πτυχές:

Οι νέες επιχειρήσεις έσπευσαν να ενσωματώσουν τις σύγχρονες τεχνολογίες στο χώρο εργασίας τους. Καθώς το δίκτυο των εταιριών αυτών επεκτείνονταν γρήγορα, δημιουργήθηκαν πρόσθετες λειτουργίες εργασίας. Αυτά τα νέα χαρακτηριστικά συνίστανται στη μείωση του χρόνου που δαπανάται για τις εργαστηριακές εργασίες όσο το δυνατόν περισσότερο και στην αύξηση της ποιότητας της εργασίας των σπουδαστών.

Καθώς η αξία των συλλεγόμενων πληροφοριών μεγάλωνε, παρουσιάστηκε ένας νέος κίνδυνος. Οι σύγχρονες τεχνολογίες στις επιχειρήσεις όχι μόνο μεγιστοποίησαν την ποιότητα της εργασίας και μείωσαν τη διάρκειά της, αλλά δημιούργησαν επίσης ένα πρόβλημα που αφορούσε την ασφάλεια τους. Η παραβιάσεις ασφαλείας δημιούργησαν μεγάλη πιθανότητα μη εξουσιοδοτημένης πρόσβασης στα δεδομένα που θα οδηγούσε σε παράνομη χρήση, αποκάλυψη δεδομένων, διαγραφή, τροποποίηση ή ακόμη και διαφθορά.

Επειδή τις περισσότερες φορές η ασφάλεια υφίσταται εισβολή με τη χρήση σύγχρονων τεχνολογιών, αναπτύχθηκαν λίγες λύσεις για την παρεμπόδιση των επιθέσεων.

Μια λύση για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στα δεδομένα θα ήταν η δημιουργία ενός κλειστού δικτύου — ενός τοπικού δικτύου επικοινωνίας. Ωστόσο, αυτό δεν λύνει τα πάντα επειδή προκύπτουν πρόσθετα προβλήματα — τι να κάνετε εάν τα τμήματα της επιχείρησης είναι γεωγραφικά διάσπαρτα στην πόλη ή αν ακόμα υπάρχουν συνεργαζόμενες σχολές ή επιχειρήσεις σε άλλες χώρες ή ηπείρους; Πώς να διασφαλιστεί ότι δεν θα γίνει παράνομη πρόσβαση στις κοινοποιημένες πληροφορίες; Οι φυσικές λύσεις, όπως η τοποθέτηση καλωδίων Διαδικτύου, θα απαιτούσαν τεράστιους πόρους.

Είναι δύσκολο να αξιολογήσουμε ποιες σύγχρονες τεχνολογίες πρόκειται να επικρατήσουν στο μέλλον, και γι' αυτό είναι πολύ σημαντικό να λυθεί αυτό το πρόβλημα με τις υπάρχουσες λύσεις.

Αν και υπάρχουν λίγες λύσεις σε αυτό το πρόβλημα, μία λύση διαφέρει από όλες. Η λύση ονομάζεται τεχνολογία '**εικονικού ιδιωτικού δικτύου'**. Ένα '**εικονικό ιδιωτικό δίκτυο'** είναι τοπικά δίκτυα ή ξεχωριστοί κόμβοι που συζευγνύονται σε ένα μεγάλο χρησιμοποιώντας τον παγκόσμιο δίκτυο. Με αυτήν την τεχνολογία δημιουργούνται ασφαλείς 'σήραγγες' μετάδοσης δεδομένων, τα δεδομένα κρυπτογραφούνται και απαιτείται έλεγχος ταυτότητας ενός χρήστη. Ένα από τα μεγαλύτερα πλεονεκτήματα αυτής της τεχνολογίας είναι ότι δεν απαιτεί συμπληρωματικές νέες φυσικές καλωδιακές γραμμές — η 'εικονικοποίηση' είναι το

κλειδί.

Μια λειτουργία '***εικονικού ιδιωτικού δικτύου***' μπορεί να δηλωθεί ως μία υπηρεσία, η οποία καθιστά δυνατή τη δημιουργία κλειστών ομάδων χρηστών και η οποία επιτρέπει την επικοινωνία μεταξύ των χρηστών οι οποίοι ανήκουν στην ίδια ομάδα (Perez 2014).

Λόγω του χαρακτηριστικού της να συνδέει χωριστούς κόμβους σε έναν, δημιουργώντας ένα εικονικό τοπικό δίκτυο, αυτή η υπηρεσία είναι πολύ χρήσιμη σε σχολές που διατηρούν προσωπικά δεδομένα όπως εργασίες ομάδων φοιτητών ή ερευνητών όπως η ΕΕΠΕΚ.

Τα 'εικονικά ιδιωτικά δίκτυα' ονομάζονται SecureNet IT Services.

Μία εταιρία μπορεί να συνεργάζεται με άλλες εταιρίες και συμβάλλουν στη συντήρηση της βασικής πληροφορικής υποδομής τους. Μια SecureNet IT Services χειρίζεται λογισμικό και υλικό υπολογιστών και άλλων συσκευών, και διατηρεί την δικτυακή υποδομή σε ικανοποιητικό επίπεδο. Επειδή η μία εταιρία μπορεί να διενεργεί τις δραστηριότητές της εξ αποστάσεως και έχει πρόσβαση σε ευαίσθητες και εμπιστευτικές πληροφορίες άλλων επιχειρήσεων απαιτείται η απομακρυσμένη πρόσβαση να είναι ασφαλής.

Ως εκ τούτου, ο κύριος στόχος αυτής της εργασίας είναι: να καταδείξει στο γιατί το 'εικονικό ιδιωτικό δίκτυο' έχει και πρέπει να έχει την καλύτερη προστασία δεδομένων, τον έλεγχο πρόσβασης και την 'απομόνωση' ενός δικτυακού domain, και γιατί πρέπει να επιλέγεται ως τεχνολογία για την ασφάλεια των δικτύων. Ο άλλος στόχος αυτής της εργασίας είναι να δημιουργήσει πρακτικά ένα 'εικονικό ιδιωτικό δίκτυο' σε ένα επιλεγμένο περιβάλλον, με σκοπό να το χρησιμοποιήσει για την SecureNet IT Services και άλλες εταιρείες.

Άλλοι στόχοι:

1. Προσδιοριστούν ποιες τεχνολογίες και πρακτικές χρησιμοποιούνται για τη σύνδεση σε άλλο δίκτυο εξ αποστάσεως. ποια πρωτόκολλα χρησιμοποιούνται για αυτό, και ποιες διαδικασίες ασφαλείας χρησιμοποιούν σε αυτές τις τεχνολογίες (έλεγχος ταυτότητας και κρυπτογράφηση)·

2. Να καταλήξουμε συμπερασματικά ποια τεχνολογία απομακρυσμένης συνδεσιμότητας είναι καλύτερη για χρήση σε εταιρία.

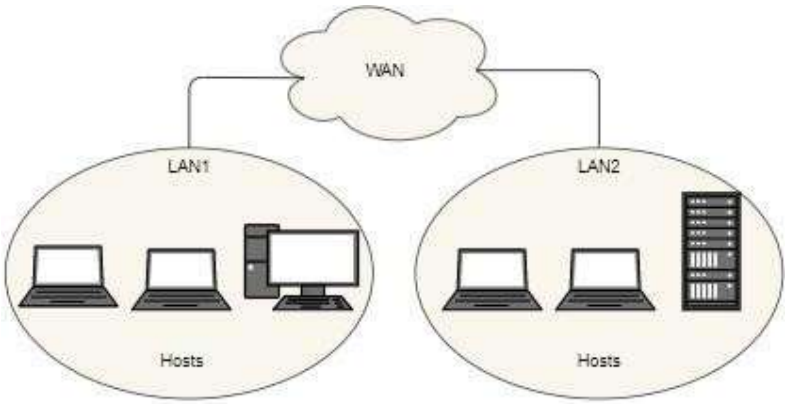
3. Να αναλυθεί το υλικό των επιχειρήσεων και να αποφασιστεί εάν αυτό είναι επαρκές ή εάν απαιτείται νέο υλικό.

4. Να εφαρμοστεί μια καλύτερη τεχνολογία.

Κεφάλαιο 1 - Τεχνολογίες και μέθοδοι

Σε αυτό το μέρος αναλύονται αντικείμενα, όπως: προσδιορισμένοι στόχοι, τεχνολογίες απομακρυσμένης πρόσβασης, μέθοδοι κρυπτογράφησης και μέθοδοι ελέγχου ταυτότητας. Επίσης, αφού ληφθούν όλα υπόψη, σχηματίζεται μια συνολική άποψη.

Ο κύριος στόχος του δικτύου θα μπορούσε να απλοποιηθεί σε ανταλλαγή δεδομένων μεταξύ ενός αποστολέα και ενός παραλήπτη. Αυτό φαίνεται στο Σχήμα 1. Οι πληροφορίες που αποστέλλονται πρέπει να περάσουν από ένα τοπικό δίκτυο (LAN), όπου βρίσκεται ο αποστολέας, σε ένα άλλο LAN, όπου βρίσκεται ο δέκτης. Στη συνέχεια, τα δεδομένα που αποστέλλονται πρέπει να ταξιδεύουν από το ένα σημείο στο άλλο μέσω δικτύων ευρείας περιοχής (WAN).



Εικόνα 1: Αφηρημένο μοντέλο δικτύου

Οι εταιρίες που έχουν εργαστηριακά τμήματα που απέχουν γεωγραφικά. Αυτό οδηγεί στο ότι όλα τα εργαστήρια των επιχειρήσεων να έχουν διαφορετικά LAN. Έτσι το δίκτυο υπολογιστών απαιτεί τότε μεγάλες ποσότητες πόρων: ξεχωριστές βάσεις δεδομένων, mail servers, διαφορετικό εξοπλισμό σάρωσης, εκτύπωσης κλπ. Επίσης, υπό αυτές τις συνθήκες, ο φόρτος εργασίας του διαχειριστή του δικτύου υπολογιστών αυξάνεται, επειδή τα διάφορα υπό-δίκτυα που προκύπτουν έχουν πρόσθετη δυσκολία να επιβλέπονται και να διατηρούνται.

Σχετικά προβλήματα εμφανίζονται όταν η επιχείρηση θέλει να επεκταθεί — για παράδειγμα, ένα υποκατάστημα που εμφανίστηκε πρόσφατα απαιτεί πρόσθετους πόρους: υλικό, λογισμικό, ανθρώπινους πόρους. Εκτός από τα

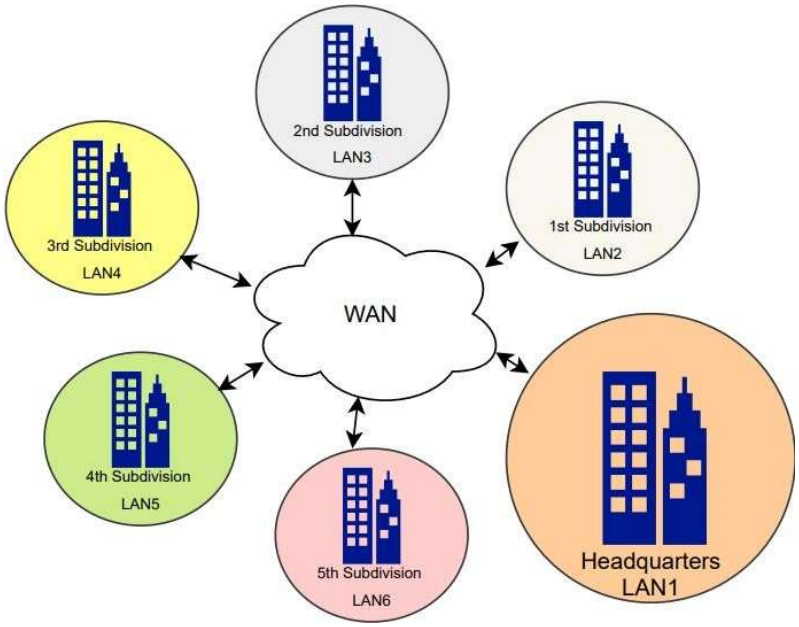
προβλήματα που αναφέρονται παραπάνω, υπάρχουν και άλλοι τομείς ανησυχίας όπως είναι για παράδειγμα η εμπιστευτικότητα και η ασφάλεια δεδομένων.

Μπορούμε να δούμε ένα απλό μοντέλο στην παρακάτω Εικόνα 2, το οποίο μας δείχνει την έδρα με γεωγραφικά απομακρυσμένα τοπικά υποδίκτυα. Κάθε εικονιζόμενο κτίριο έχει το δικό του LAN και αυτές οι μονάδες επικοινωνούν με την κύρια βάση, μέσω ενός WAN. Στο σχήμα, τα απλά βέλη αντιπροσωπεύουν όχι μόνο ότι τα δεδομένα μεταδίδονται αλλά, επίσης, ότι κοινοποιούνται χωρίς πρόσθετα

μέτρα ασφαλείας. Σε αυτό το πλαίσιο, τα μέτρα ασφαλείας χρίζουν κρυπτογράφησης.

Αυτή η περίπτωση εγείρει επίσης ένα ερώτημα — θα φτάσουν τα μεταδιδόμενα δεδομένα στον προορισμό με ασφάλεια; Εναλλακτικά, τα δεδομένα μπορεί να τροποποιηθούν, να προκαλέσουν παραπλάνηση, να εξεταστούν από μη εξουσιοδοτημένα άτομα και μηχανήματα, ενώ ταξιδεύουν στον προορισμό τους. Ποιο μπορεί να είναι τελικά το κόστος όλων αυτών των χαμένων πληροφοριών;

Αν και όλες οι πληροφορίες που αποστέλλονται δεν περιέχουν εμπιστευτικά δεδομένα, ωστόσο οι πληροφορίες που θα μπορούσαν ενδεχομένως να είναι επιβλαβείς για την εταιρεία -αν αλλοιωθούν ή χαθούν-, θα πρέπει να προστατεύονται ώστε να διατηρηθεί η ασφάλεια τους και το απόρρητο.



Εικόνα 2: Τα τοπικά δίκτυα χωρίζονται από το Διαδίκτυο

Οι εταιρίες θα πρέπει να καθορίσουν την απαιτούμενη ασφάλεια των δεδομένων τους. Διότι στο παρουσιαζόμενο δίκτυο ένα μη εξουσιοδοτημένο τρίτο μέρος θα μπορούσε να παραβιάσει την ασφάλεια και να δει τις πληροφορίες των απεσταλμένων πακέτων και να τις τροποποιήσει.
Εάν οι επιχειρήσεις αποφασίσουν ότι τα εργαστήρια τους χρειάζονται αναβάθμιση ασφαλείας, μία από τις μεθόδους προστασίας του δικτύου τους θα μπορούσε να είναι η λειτουργία και η μετάδοση δεδομένων μόνο στο ίδιο LAN.

Υπάρχουν λίγες τεχνολογίες που επιτρέπουν σε έναν χρήστη, ή σε μια ομάδα χρηστών, να εμφανιστεί ουσιαστικά στο απαραίτητο ‘ιδιωτικό δίκτυο’.

Οι μεμονωμένοι απομακρυσμένοι χρήστες που συνδέονται σε ένα απομακρυσμένο LAN θα μπορούσαν να περιγραφούν ως ‘πελάτες’ που εισέρχονται με μια συσκευή σε ένα άλλο LAN, χρησιμοποιώντας τεχνολογίες, όπως: Telnet, SSH ή VPN.

Αυτές οι τεχνολογίες όχι μόνο επιτρέπουν σε ξεχωριστό ιδιωτικό δίκτυο εργαστηρίων να μοιράζεται ένα κοινό δίκτυο, αλλά προστατεύει επίσης τα δεδομένα από τη διαρροή, την τροποποίηση και τη διαγραφή τους.

Ωστόσο, είναι απαραίτητο να ληφθούν υπόψη όχι μόνο οι κύριες πτυχές ασφάλειας, όπως είναι η κρυπτογράφηση, η πιθανή παρέμβαση τρίτων και η πιθανή τροποποίηση πληροφοριών, η αναγνώριση του χρήστη, κλπ., αλλά θα πρέπει να ληφθούν υπόψιν και οι παράμετροι όπως:

1) Εάν ένας χρήστης με χαμηλό επίπεδο παιδείας υπολογιστών θα μπορεί να χρησιμοποιήσει την τεχνολογία.

2) εάν η τεχνολογία θα απαιτήσει μεγάλες ποσότητες πόρων (τόσο λογισμικού όσο και υλικού).

3) εάν θα δαπανηθεί ένα μεγάλο χρηματικό ποσό για την εισαγωγή της τεχνολογίας στο δίκτυο υπολογιστών.

Ως εκ τούτου, τα κύρια θέματα αυτής της εργασίας είναι να ανακαλύψει ποια μέτρα θα μπορούσαν να χρησιμοποιηθούν για τη σύνδεση μεμονωμένων δικτύων υπολογιστών μέσω Διαδικτύου, σε ένα δίκτυο οργανισμού και να αναλύσει τα πρότυπα αξιοπιστίας και ασφάλειας της επιλεγμένης τεχνολογίας.

Ένα από τα πιο σημαντικά θέματα είναι: πώς αυτά τα μέτρα παρέχουν ασφάλεια στη λειτουργία του ολικού δικτύου. Πώς προστατεύονται οι πληροφορίες που αποστέλλονται μέσα στα πακέτα; Πώς επαληθεύονται τα πακέτα που ελήφθησαν από εξουσιοδοτημένο χρήστη;

1.1. Telnet και Secure Shell

Ένα άλλο εργαλείο απομακρυσμένης πρόσβασης ονομάζεται Telnet. Το Telnet είναι μια παλιά τεχνολογία, η οποία επιτρέπει στους χρήστες να έχουν πρόσβαση σε συσκευές μέσω του δικτύου δημιουργώντας σύνδεση TCP, η οποία χρησιμοποιείται για τη μετάδοση δεδομένων με πληροφορίες Telnet. Υπάρχουν τρεις αρχές της διαδικασίας εργασίας του: όταν πραγματοποιείται σύνδεση την πρώτη φορά, κάθε συσκευή τερματίζει πρέπει να λειτουργεί στο NetworkVirtual Terminal, συνάπτεται συμφωνία για τις διαπραγματευτικές επιλογές. δημιουργείται μια συμμετρική άποψη του τερματικού και της διαδικασίας του (Postel, J.; Reynolds, J.; ISI 1983). Ωστόσο, αυτή η τεχνολογία δεν διαθέτει μηχανισμούς ασφαλείας και οι πληροφορίες που μεταδίδονται είναι διαφανείς. Εξαιτίας αυτού, αυτή η τεχνολογία άλλαξε με το SecureShell (SSH).

Το SSH έχει απλά στοιχεία, όπως — ένα πρωτόκολλο δικτύου, όπου οι πληροφορίες είναι κρυπτογραφημένες, μια γραμμή εντολών και λογισμικό client\server (Dwivedi 2004).

Ενώ το SSH μπορεί να παρέχει στους χρήστες πρόσβαση σε άλλες συσκευές μέσω του διαδικτύου, ο κύριος σκοπός του είναι να προστατεύει τη σύνδεση TCP. Αυτό το

κάνει έχοντας τρία κύρια πρωτόκολλα : το SSH— TRANS πρωτόκολλο μεταφοράς, το πρωτόκολλο SSH—USERAUTH και το πρωτόκολλο SSH—CONNECT.

Τα πρωτόκολλα λειτουργούν συνήθως μέσω της θύρας TCP/UDP. (T. Ylonen, SSH Communications Security Corp, C. Lonvick, Ed., Cisco Systems, Inc. 2006a)

Το πρωτόκολλο SSH—TRANS χρησιμοποιείται για τον έλεγχο ταυτότητας server και την υλοποίηση προστασίας δεδομένων (που περιλαμβάνει αλγόριθμους συμπίεσης και κλειδιά). Όταν ένας client και ένας server αρχίζουν να ανταλλάσσουν μηνύματα, αυτό το πρωτόκολλο ενσωματώνει τα πακέτα και προσθέτει τη δική του κεφαλίδα, η οποία περιέχει τις πληροφορίες σχετικά με το μήκος του πακέτου, το μήκος του padding, MAC και του Sequence Number (SN).

Για να παρεμποδιστούν μη εξουσιοδοτημένα τρίτα μέρη, προστίθενται πρόσθετες πληροφορίες στην αρχή, τη μέση και το τέλος των μηνυμάτων, πριν από την κρυπτογράφηση, με την ελπίδα ότι το τρίτο μέρος θα αντιμετωπίσει όσο το δυνατόν μεγαλύτερη δυσκολία προσπαθώντας να μαντέψει το μήκος των δεδομένων.

Η κρυπτογράφηση εφαρμόζεται στα δεδομένα πριν από τα πεδία ενθυλάκωσης, το μήκος πακέτου, το padding και το μήκος τους.

Η αρχή λειτουργίας SSH—TRANS μπορεί να περιγραφεί ως εξής: συνήθως, μετά από ανταλλαγή ενός μηνύματος αναγνώρισης (μεταξύ του client και του server), ακολουθεί η διαπραγμάτευση των αλγορίθμων και μόνο αφού αποφασίσει ποιοι αλγόριθμοι θα χρησιμοποιηθούν, ανταλλάσσονται τα κλειδιά.

Μετά την εναλλαγή των κλειδιών, τα δύο επικοινωνούντα σημεία ξεκινούν την αλλαγή του κύριου κλειδιού που δημιουργείται και στη συνέχεια, τα δεδομένα ενθυλακώνονται, κρυπτογραφούνται και επαληθεύονται. (T. Ylonen SSH Communications Security Corp C. Lonvick, Ed. Cisco Systems, Inc. 2006b)

Εν τω μεταξύ, το SSH— USERAUTH πρωτόκολλο χρησιμοποιείται για τον έλεγχο ταυτότητας ενός client—ένας client υποβάλλει την αναγνώρισή του στον server και, στη συνέχεια, ο server ελέγχει τις ληφθείσες πληροφορίες— απαντά με ένα μήνυμα σφάλματος εάν οι πληροφορίες δεν είναι σωστές, ή απαντά με ένα μήνυμα επιτυχίας εάν ο έλεγχος ταυτότητας είναι επιτυχής.

1.1. Εναλλαγή ετικετών πολλαπλών πρωτοκόλλων

Η εναλλαγή ετικετών πολλαπλών πρωτοκόλλων (Multiprotocol Label Switching

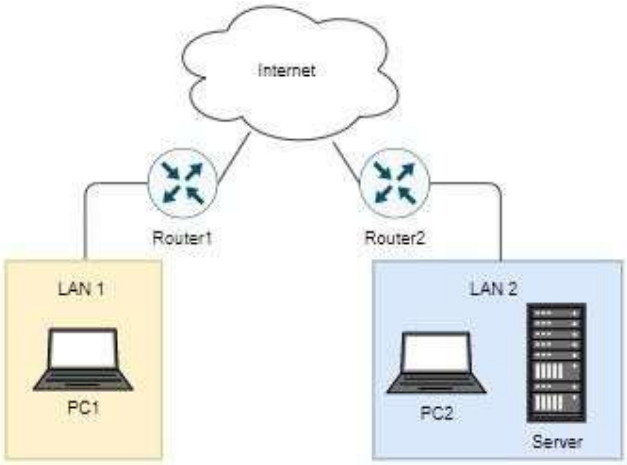
- MPLS) είναι ένα πρωτόκολλο το οποίο χρησιμοποιεί μεθόδους ενθυλάκωσης και ετικετών για τη μετάδοση των πληροφοριών. Αυτή η τεχνολογία λειτουργεί προωθώντας πακέτα που αποστέλλονται για πρώτη φορά σε συγκεκριμένη κλάση ισοδυναμίας, η οποία βάζει ετικέτες στα πακέτα. (Rosen and Rekhter 1999). Το πακέτο δρομολογείται από τον έναν κόμβο στον άλλο με βάση την εκάστοτε ετικέτα. Αυτή η τεχνική χρησιμοποιείται για την αποφυγή περίπλοκης επιθεώρησης

και την επιτάχυνση της ροής μεταφοράς πληροφοριών. (Ghein 2007).

Ωστόσο, το ίδιο το MPLS πρωτόκολλο δεν παρέχει καμία μέθοδο κρυπτογράφησης, επειδή ένας τρόπος για να παρέχει οποιαδήποτε προστασία είναι η χρήση χαρακτηριστικών 'εικονικού ιδιωτικού δικτύου'. Αυτός ο συνδυασμός ονομάζεται 'εικονικό ιδιωτικό δίκτυο' MPLS. Χρησιμοποιεί τις κρυπτογραφημένες 'σήραγγες' του εικονικού ιδιωτικού δικτύου για να διασφαλίσει ότι τα πακέτα προωθούνται προς τις τοποθεσίες προορισμός. Ωστόσο, αυτή η τεχνολογία είναι επικίνδυνη επειδή οι χρήστες χάνουν την ορατότητα των βασικών δικτύων και αυτό θα μπορούσε να οδηγήσει στην εισαγωγή πρόσθετων δρομολογητών από κακόβουλους servers. (Behringer and Morrow 2005).

1.2. Εικονικό ιδιωτικό δίκτυο

Η παρακάτω Εικόνα 3, απεικονίζει αφηρημένα τη μετάδοση πληροφοριών χωρίς πρόσθετα μέτρα ασφαλείας. Λειτουργεί καλά αν φανταστούμε μια κατάσταση - ένας υπάλληλος της εταιρίας που ονομάζεται "X", πρέπει να ταξιδέψει με το πλοίο για ένα Διεθνές Συνέδριο. Ο σπουδαστής θέλει να περάσει τον ελεύθερο χρόνο του δουλεύοντας στα υπόλοιπα μέρη του έργου εργασίας του. Το μέσο μεταφοράς που χρησιμοποιεί ο εργαζόμενος παρέχει δωρεάν πρόσβαση σε WiFi.



Εικόνα 3: Αφηρημένη μετάδοση δεδομένων χωρίς ασφάλεια

Τα έγγραφα, που χρειάζεται ο σπουδαστής, αποθηκεύονται στον διακομιστή του οργανισμού. Ο εργαζόμενος μπορεί εύκολα να έχει πρόσβαση στον διακομιστή ενώ παρέχει τον έλεγχο ταυτότητας και έτσι μπορεί να συνεχίσει να εργάζεται. Χρησιμοποίησε το παρεχόμενο ασύρματο δίκτυο και κατέβασε τα απαραίτητα έγγραφα στον φορητό υπολογιστή του με πρωτόκολλο μεταφοράς αρχείων.

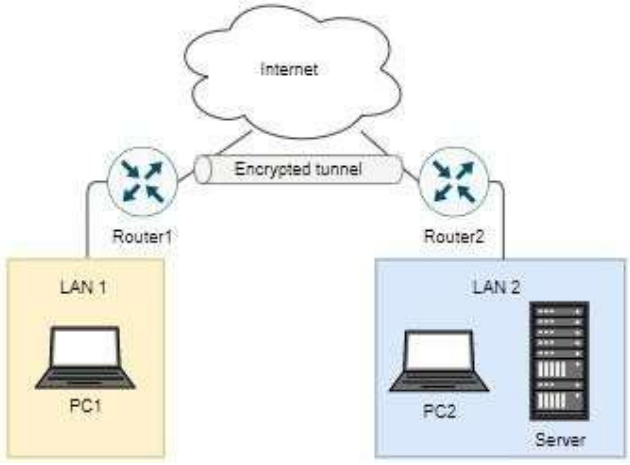
Στο ίδιο όχημα μεταφοράς ένας χάκερ σάρωνε τα πακέτα του ασύρματου δικτύου ελεύθερης πρόσβασης (Wi-Fi) και διότι ο χάκερ αποφάσισε να υποκλέψει (sniffing) τα πακέτα των εργαζομένων. Επειδή ο εργαζόμενος δεν είχε επαρκείς γνώσεις ασφάλειας και κατέβασε ένα εμπιστευτικό έγγραφο χωρίς μέτρα ασφαλείας, ύποπτες υποθέσεις για έναν έμπειρο χάκερ, ο οποίος θα μπορούσε να είχε λάβει τις

πληροφορίες των πακέτων και να είχαν βρει την τοποθεσία από όπου στάλθηκαν. Ο χάκερ θα μπορούσε επίσης να έχει εγχύσει το πακέτα με τις δικές του κακόβουλες πληροφορίες και να τα υποβάλλει ως αποκρινόμενα πακέτα.

Μπορούμε τώρα να φανταστούμε την ίδια κατάσταση να συμβαίνει ξανά, έστω ότι ωστόσο, αυτή τη φορά, η επιχείρηση ανησύχησε για την ασφάλεια του δικτύου της και εγκατέστησε μια πρόσθετη τεχνολογία ασφάλειας — ένα εικονικό ιδιωτικό δίκτυο (VPN). Ο εργαζόμενος είχε πρόσβαση στο δημόσιο Wi-Fi, αλλά, επίσης, έχει χρησιμοποιήσει και το VPN. Με ένα VPN είχε εύκολη πρόσβαση στην κρυπτογραφημένη 'σήραγγα' (tunnel) και ο υπολογιστής του έγινε μέρος του τομέα της εταιρείας - όλη η ασφάλεια που υπήρχε στη ζώνη της επιχείρησης εφαρμόστηκε στη σύνδεση του σπουδαστή στο Διαδίκτυο.

Το μη εξουσιοδοτημένο άτομο, το οποίο προσπαθούσε να δει την ανταλλαγή δεδομένων μεταξύ του server και του client, δεν μπόρεσε να έχει πρόσβαση στις πληροφορίες του πακέτου επειδή, όπως βλέπουμε στην παρακάτω (Εικόνα 4), δημιουργήθηκε μια κρυπτογραφημένη 'σήραγγα', μέσω της οποίας τα δεδομένα ταξιδεύουν.

Τώρα, ο εργαζόμενος μπορούσε να κατεβάσει με ασφάλεια τα απαραίτητα έγγραφα στη συσκευή του και να συνεχίσει την εργασία του χωρίς προβλήματα, ανεξάρτητα από την ασφάλεια (DaleLiu; Syngress; StephanieMillers; MarkLucas; AbhishekSingh; JenniferDavis 2006).



Εικόνα 4: Δημιουργία κρυπτογραφημένης σήραγγας μεταξύ του Router1 και του Router2

Η τεχνολογία VPN παρέχει μια ικανοποιητική ασφάλεια σε σύνθετα δίκτυα. Και συγκεκριμένα: Πρώτον, ένα VPN είναι μια τεχνολογία η οποία δημιουργεί ένα 'ιδιωτικό δίκτυο' από μεμονωμένα τοπικά δίκτυα με την χρήση ενός δημόσιου δικτύου χρησιμοποιώντας εικονικές συνδέσεις αντί για αποκλειστικές φυσικές συνδέσεις. Πριν σταλούν τα δεδομένα, από έναν πελάτη VPN σε έναν server VPN, μέσω της 'σήραγγας', τα πακέτα περνούν τις διαδικασίες ενθυλάκωσης και κρυπτογράφησης. Παρόλο που τα δεδομένα έχουν τροποποιηθεί, εξακολουθούν να μπορούν να επιβεβαιωθούν ως έγκυρα και μπορούν κανονικά να δρομολογηθούν - ο προορισμός του πακέτου είναι κρυφός, ωστόσο η διεύθυνση του VPN server

εμφανίζεται για να λάβει το πακέτο. Όταν το πακέτο παραδίδεται στον VPN server, μόνο ο VPN server μπορεί να χρησιμοποιήσει ένα συμμετρικό κλειδί για να αποκρυπτογραφήσει τα περιεχόμενα του πακέτου και να το παραδώσει στον τελικό προορισμό.

Αυτό παρέχει ένα συμπέρασμα ότι αυτό που κάνει μια τεχνολογία VPN ασφαλή είναι δύο σημεία: το πρωτόκολλο 'σήραγγας' (μέσω του οποίου ταξιδεύουν τα δεδομένα) και ο κρυπτογραφημένος έλεγχος ταυτότητας.

Οι γενικές κατηγορίες εικονικών δικτύων VPN θα μπορούσαν να διαχωριστούν σε τέσσερα μέρη (Andrea 2014):

1) VPN που βασίζεται στην πολιτική.

2) VPN που βασίζεται στη Διαδρομή.

3) Secure Socket Layer-Based VPN.

4) DynamicMultiport VPN.

- Το VPN με βάση την πολιτική θα μπορούσε να οριστεί ως τύπος VPN που χρησιμοποιεί καθορισμένες πολιτικές, όπως Λίστα ελέγχου πρόσβασης. Η ροή της κυκλοφορίας είναι ενθυλακωμένη και κρυπτογραφημένη σύμφωνα με τις καθορισμένες πολιτικές. Αυτός ο τύπος μπορεί να χωριστεί σε δύο υποκατηγορίες, μια κατηγορία είναι: Site—to—Site VPN και Hub και Spoke VPN. Μια άλλη κατηγορία είναι: VPN Απομακρυσμένης Πρόσβασης Πελάτη. Ένα από τα πλεονεκτήματα αυτού του τύπου είναι ότι διαθέτει ισχυρή ασφάλεια και υποστηρίζεται από τις περισσότερες συσκευές δικτύου.

- Δεύτερον, υπάρχει ένας τύπος VPN με βάση τη διαδρομή, ο οποίος δεν χρειάζεται πολιτικές για να υπαγορεύει ποια κίνηση εισέρχεται στον VPN server. Το VPN βασίζεται σε διεπαφές σήραγγας και στατικές και δυναμικές διαδρομές. Βασίζεται σε μια διεπαφή εικονικής σήραγγας (γνωστή ως VTI) και σε Generic Routing Encapsulation (GRE). Ωστόσο, αυτός ο τύπος VPN υποστηρίζεται μόνο από δρομολογητές Cisco11. Ένα άλλο μείον αυτού του τύπου είναι ότι το VTI και το GRE δεν μπορούν να παρέχουν ασφάλεια από μόνα τους και πρέπει να συνδυαστούν με την Ασφάλεια Πρωτοκόλλου Διαδικτύου.

- Στη συνέχεια, υπάρχει ένα Secure Socket Layer (SSL)—Βασισμένο VPN που επιτρέπει στους απομακρυσμένους χρήστες να συνδέονται σε άλλο δίκτυο μέσω του προγράμματος περιήγησης Ιστού ενώ χρησιμοποιεί κρυπτογράφηση SSL. Ο τύπος χωρίς client έχει περιορισμένες λειτουργίες, καθώς ο client μπορεί να έχει πρόσβαση μόνο σε εσωτερικές εφαρμογές Web, servers ηλεκτρονικού ταχυδρομείου κ.λπ. Παρόλα αυτά, εάν οι χρήστες θέλουν να έχουν πλήρη πρόσβαση, ο χρήστης πρέπει να πραγματοποιήσει λήψη μιας εφαρμογής clients και να την εγκαταστήσει στον υπολογιστή του. Τα κύρια μειονεκτήματα αυτού του τύπου είναι ότι οδηγεί σε κακή απόδοση υπό υψηλό φορτίο και ότι όταν ένας χρήστης

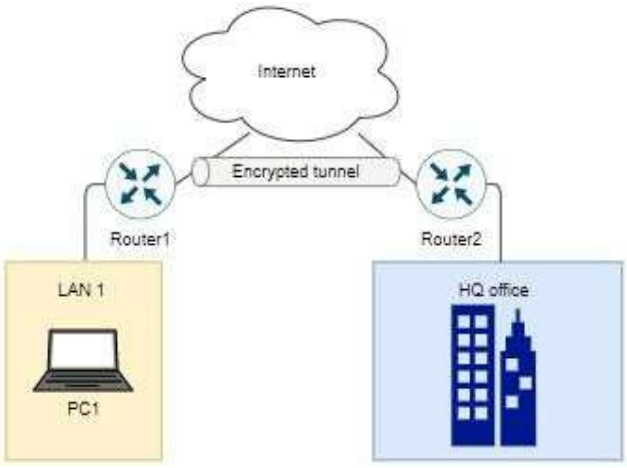
χρειάζεται πλήρη έλεγχο, χρειάζεται να κατεβάσει με μη αυτόματο τρόπο το αρχείο Java ή ActiveX και να το εγκαταστήσει. Αυτό μπορεί να είναι πρόβλημα εάν ένα τείχος προστασίας τον εμποδίζει.

- Τέλος, υπάρχει ένας τύπος DynamicMultiport VPN που δεν απαιτεί κίνηση για τη διέλευση μέσω server VPN ή δρομολογητή και χρησιμοποιεί προστασία Multipoint GRE και Internet ProtocolSecurity. Ένα από τα κύρια μειονεκτήματα αυτής της τεχνολογίας είναι ότι υποστηρίζεται μόνο σε δρομολογητές Cisco.

Ουσιαστικά, ένας τύπος VPN βάσει πολιτικής είναι καλύτερο να χρησιμοποιείται όταν υπάρχει ανάγκη δημιουργίας VPN μεταξύ συσκευών οι οποίες έχουν διαφορετικούς προμηθευτές. Οι τύποι VPN που βασίζονται στη διαδρομή πρέπει να χρησιμοποιούνται όταν υπάρχει ανάγκη για ένα VPN να υποστηρίζει πρωτόκολλα Διαδικτύου (IP) πρωτόκολλα unicast, multicast και non-IP. Ένα VPN που βασίζεται σε SSL είναι καλύτερο για χρήση με λίγους χρήστες και χαμηλή δραστηριότητα δικτύου. Τέλος, ένα DynamicMultiport VPN είναι καλύτερο για χρήση σε πολύ μεγάλες τοπολογίες VPN.

Το VPN έχει τρεις ενδιαφέροντες τύπους σύνδεσης για μεμονωμένους χρήστες και ομάδες χρηστών (Battu 2014). Οι παρακάτω εικόνες θα βοηθήσουν στην περιγραφή αυτών των τύπων.

Το VPN -ανάλογα με το τύπο σύνδεσης - θα μπορούσε να χωριστεί σε τρεις περιπτώσεις : Remote, Intranet, Extranet.

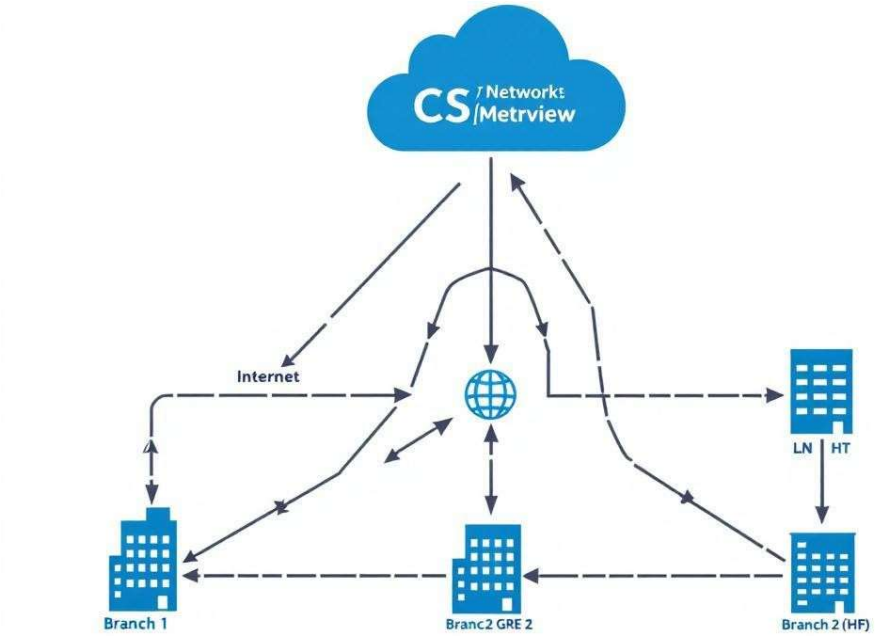


Εικόνα 5: Απομακρυσμένο (Remote) VPN

Η Εικόνα 5 απεικονίζει έναν **απομακρυσμένο (Remote) τύπο VPN** που επιτρέπει σε έναν μεμονωμένο χρήστη να φτάσει σε ένα ιδιωτικό δίκτυο παρέχοντας έναν κωδικό πρόσβασης (υπάρχει επίσης η δυνατότητα αναγνώρισης του 'αναγνωριστικού' συσκευής).

Η Εικόνα 6 απεικονίζει έναν τύπο **VPN intranet** που επιτρέπει τη σύνδεση των υποκαταστημάτων της εταιρείας και των θυγατρικών εταιρειών ενώ είναι γεωγραφικά απομεμακρυσμένες. Αυτός ο τύπος επιτρέπει όχι μόνο σε έναν χρήστη να χρησιμοποιήσει μια τεχνολογία VPN, αλλά επιτρέπει επίσης σε μια ομάδα

χρηστών, που υπάρχει στο ίδιο LAN, να συνδεθεί. Επίσης, αξίζει να αναφέρουμε ότι αυτός ο τύπος δεν απαιτεί μεμονωμένες διαμορφώσεις για όλες τις συσκευές.



Εικόνα 6: Intranet VPN

Η Εικόνα 7 απεικονίζει ένα **VPN τύπου Extranet**, το οποίο παρέχει μια ασφαλή και ελεγχόμενη σύνδεση μεταξύ μιας εταιρείας και των εξωτερικών συνεργατών της. Αυτή η λύση είναι ιδανική για επιχειρήσεις που χρειάζεται να μοιραστούν συγκεκριμένες πληροφορίες ή πόρους με εξωτερικούς εταίρους, διατηρώντας ταυτόχρονα υψηλά επίπεδα ασφάλειας.

Εικόνα 7: Extranet VPN

Επιπλέον, στους διαφόρους τύπους VPN υπάρχουν διαφορετικά πρωτόκολλα αφιερωμένα σε διαφορετικές περιστάσεις.

- Το 1994 η Cisco Systems παρουσίασε ένα νέο πρωτόκολλο που ονομάζεται **Generic Routing Encapsulation** (**GRE**). Το πρωτόκολλο GRE ενσωματώνει τα πακέτα, ενώ

προσθέτει επιπλέον διευθύνσεις IP και μια κεφαλίδα GRE και τα στέλνει μέσω του Διαδικτύου. Αυτό το πρωτόκολλο παρέχει μια 'σήραγγα', ωστόσο, δεν παρέχει κανένα μέτρο ασφαλείας.

- Στη συνέχεια, υπάρχει το **Internet ProtocolSecurity** (**IPSec**) το οποίο είναι μια σουίτα πρωτοκόλλων που χρησιμοποιούνται για την ενεργοποίηση της ασφαλούς και κρυπτογραφημένης επικοινωνίας παρέχοντας εμπιστευτικότητα, ακεραιότητα και έλεγχο ταυτότητας δεδομένων. Μπορεί να λειτουργήσει με δύο τρόπους: *λειτουργία μεταφοράς* (μόνο οι κεφαλίδες είναι πιστοποιημένες και οι πληροφορίες είναι κρυπτογραφημένες) και *λειτουργία σήραγγας*.

  Το IPSec αποτελείται από ενθυλάκωση ωφέλιμου φορτίου ασφαλείας (χρησιμοποιείται για την κρυπτογράφηση του ωφέλιμου φορτίου δεδομένων των πακέτων IP), κεφαλίδα ελέγχου ταυτότητας, ανταλλαγή κλειδιών Διαδικτύου (χρησιμοποιείται για συναλλαγές κλειδιών κρυπτογράφησης, ομοτίμων IPSec και συναλλαγών παραμέτρων ασφαλείας), αλγόριθμοι κρυπτογράφησης (DES, 3DES , AES, κ.λπ.), Diffie—HellmanGroup (πρωτόκολλο κρυπτογράφησης δημόσιου κλειδιού για τη δημιουργία κλειδιών περιόδου λειτουργίας), αλγόριθμοι κατακερματισμού (MD15, SHA16), συσχέτιση ασφαλείας (αποθήκευση αναγνώρισης ομοτίμων). (Bollapragada, Khalid and Wainner 2005)

  Η κεφαλίδα ελέγχου ταυτότητας είναι ιδανική για το IPSec επειδή μετράει τα αθροίσματα ελέγχου των κεφαλίδων TCP/IP. Εάν τα αθροίσματα ελέγχου δεν είναι πανομοιότυπα, το πακέτο ολοκληρώνεται. Το μόνο πρόβλημα είναι ότι εάν η Network Address Translation (NAT) αλλάξει τις πληροφορίες των κεφαλίδων, τότε, επίσης το πακέτο μπορεί επίσης να απορριφθεί. (Prasad και Prasad 2005).

  Στο IPSec η αρχή λειτουργίας του αποτελείται από λίγα βήματα: φάση 1, φάση 2, μεταφορά δεδομένων και τερματισμός σήραγγας IPSec. Για παράδειγμα, το βήμα της φάσης 1 συμβαίνει όταν οι συσκευές δημιουργούν ένα κανάλι για να επικοινωνούν μετά από διαπραγμάτευση πολιτικής ασφαλείας για Internet Key Exchange (IKE). Η φάση 2 εμφανίζεται όταν οι συσκευές διαπραγματεύονται πώς να προστατεύσουν τα δεδομένα. (Tiller 2004). Το IKE χρησιμοποιείται για τον έλεγχο ταυτότητας μεταξύ δύο μερών και τη δημιουργία κλειδιού ασφαλείας. Η επικοινωνία IKE αποτελείται από ανταλλαγή μηνυμάτων αιτήματος και απάντησης. (D. Harkins, D. Carrel, cisco Systems 1998).

  Ένα άλλο πρωτόκολλο, το οποίο είναι από τα παλαιότερα πρωτόκολλα VPN, ονομάζεται πρωτόκολλο Point-to-Point Tunneling Protocol (γνωστό ως PPTP). Αυτό το πρωτόκολλο δεν χρησιμοποιείται τόσο πολύ στον σημερινό κόσμο, επειδή οι μηχανισμοί ασφαλείας του δεν ήταν τόσο ανεπτυγμένοι όσο άλλα πρωτόκολλα. Το PPTP βασίζεται κυρίως στον έλεγχο ταυτότητας και συνήθως χρησιμοποιεί τη μέθοδο ελέγχου ταυτότητας MSCHAP—v2 (Microsoft Challenge Handshake Authentication Protocol). Αξίζει να σημειωθεί ότι επιτρέπει και πιστοποιητικά X.509.

  Η αρχή λειτουργίας του PPTP βασίζεται σε δύο κανάλια: την ρύθμιση της σύνδεσης

και την μεταφορά δεδομένων μέσω πρωτοκόλλου GRE. (K. Hamzeh, Ascend Communications, G. Pall, Microsoft Corporation, W. Verthein, 3Com, J. Taarud, Copper Mountain Networks, W. Little, ECI Telematics, G. Zorn 1999).

- Για την εξάλειψη των αδύνατων σημείων των πρωτοκόλλων προώθησης PPTP δημιουργήθηκε το πρωτόκολλο σήραγγας επιπέδου δύο (αργότερα αναφέρεται ως **L2TP**). Επειδή δεν προσφέρει μηχανισμούς κρυπτογράφησης, συνήθως συνδυάζεται με IPSec. Όπως και το PPTP, το L2TP χρησιμοποιεί δύο κανάλια ελέγχου για την εγκατάσταση, τη συντήρηση και τον καθαρισμό των 'σηράγγων'. (W. Townsley A. Valencia cisco Systems A. Rubens Ascend Communications G. Pall G. Zorn Microsoft Corporation B. Palter Redback Networks 1999).
- Στη συνέχεια, υπάρχει ένα **OpenVPN** που είναι ένα πρωτόκολλο VPN ανοιχτού κώδικα, που συχνά ονομάζεται VPN με βάση το SSL, που χρησιμοποιεί HMAC18. Χρησιμοποιεί εικονικούς προσαρμογείς δικτύου ως διεπαφή. Αυτό το πρωτόκολλο έχει πολύ ισχυρή κρυπτογράφηση κλειδιού που ονομάζεται AES—256, έλεγχος ταυτότητας 2048—bitRSA και αλγόριθμος κατακερματισμού SHA1. Το μεγαλύτερο πρόβλημα του πρωτοκόλλου OpenVPN είναι ότι η ταχύτητά του είναι πιο αργή από άλλα πρωτόκολλα λόγω της ισχυρής ασφάλειάς του. (CristandKeijser 2015).
- Τέλος, υπάρχει το πρωτόκολλο Microsoft SecureSocketTunneling (SSTP) το οποίο επιτρέπει σε έναν χρήστη να έχει πρόσβαση σε ένα ιδιωτικό δίκτυο μέσω HTTPS, ενώ ενσωματώνει το πρωτόκολλο Point-to-Point. Χρησιμοποιεί πιστοποιητικά 2048-bit SSL/TLS19 για έλεγχο ταυτότητας και κλειδιά SSL 256-bit για κρυπτογράφηση. (Microsoft Corporation 2021)

Οι προαναφερθείσες τεχνολογίες έχουν τις δικές τους αρχές λειτουργίας, ωστόσο, ο έλεγχος ταυτότητας των χρηστών, η κρυπτογράφηση και η αποκρυπτογράφηση δεδομένων είναι ένα τεράστιο μέρος της.

1.4 Έλεγχος ταυτότητας

Ο έλεγχος ταυτότητας είναι ένα από τα πιο σημαντικά μέρη της ασφάλειας, επειδή αυτή η διαδικασία επιτρέπει την επιβεβαίωση της ταυτότητας ενός χρήστη και της προέλευσης των δεδομένων. Για να είναι επιτυχής ο έλεγχος ταυτότητας πρέπει να συμμορφώνεται με λίγες αρχές που ορίζονται από ένα πρότυπο ασφαλείας που ονομάζεται **CIA** (**Confidentiality**, **Integrity** and **Availability**). «Το μοντέλο ορίζει χαρακτηριστικά που πρέπει να έχει στον κυβερνοχώρο για να μπορεί να θεωρηθεί ασφαλές. Αρχικά, το μοντέλο της CIA αποτελείται από τρία χαρακτηριστικά: εμπιστευτικότητα (το C), ακεραιότητα (το I) και διαθεσιμότητα (το A)» (Boonkrong 2021).

Η αναγνώριση των χρηστών μπορεί να χωριστεί σε μέρη, όπως: **RSA**, **ψηφιακή υπογραφή**, **προ-κοινόχρηστο κλειδί**, **EAP και RADIUS**.

- Το **RSA** (Rivest—Shamir—Adleman20) είναι ένα κρυπτοσύστημα δημόσιου κλειδιού που ακολουθεί τέσσερα βήματα: δημιουργία κλειδιού, κλειδί διανομής,

κρυπτογράφηση και αποκρυπτογράφηση κλειδιού. Σε αυτήν την περίπτωση, χρησιμοποιείται ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση του ληφθέντος μηνύματος. Το RSA πρέπει να ακολουθεί μερικούς κανόνες: η οντότητα για τη δημιουργία ζεύγους κλειδιών (ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί) πρέπει να είναι εύκολη, επίσης, θα πρέπει να είναι εύκολη η δημιουργία του αντίστοιχου κρυπτογραφημένου κειμένου. Δεν θα πρέπει να παρέχονται πρόσθετες προκλήσεις για την αποκρυπτογράφηση του μηνύματος χρησιμοποιώντας το κοινόχρηστο ιδιωτικό κλειδί. Ενώ η δημιουργία των κλειδιών θα πρέπει να είναι εύκολη, ωστόσο, η αναγνώριση του εσωτερικού ενός ιδιωτικού κλειδιού θα πρέπει να είναι αδύνατη και οποιαδήποτε ανάκτηση του απλού κειμένου σε τρίτους θα πρέπει να είναι ανέφικτη. Τα μαθηματικά πίσω από τη δημιουργία των κλειδιών είναι τα εξής: πρώτον, δύο μεγάλοι πρώτοι αριθμοί επιλέγονται τυχαία (σημειώνοντας ότι θα πρέπει να έχουν παρόμοιο μέγεθος) p και q, στη συνέχεια, πολλαπλασιάζονται και οι δύο και αποθηκεύονται σε μια μεταβλητή που ονομάζεται n. Στη συνέχεια, χρησιμοποιείται η συνάρτηση phi του Euler: $\phi(n)=(p —1) * (q – 1)$. Για τον πλήρη υπολογισμό του μεγαλύτερου κοινού διαιρέτη του δημόσιου κλειδιού χρησιμοποιείται μια άλλη νέα μεταβλητή: $\gcd(k, \phi(n))$, η οποία οδηγεί στις μεταβλητές n και k ως πλήρες δημόσιο κλειδί. Για τη δημιουργία ενός ιδιωτικού κλειδιού, ο εκτεταμένος ευκλείδειος αλγόριθμος χρησιμοποιείται με μια νέα πρόσθετη μεταβλητή που ονομάζεται d: $d=(1/k) \bmod \phi$.

- Ένας αλγόριθμος **ψηφιακής υπογραφής** είναι μια άλλη μέθοδος κρυπτογράφησης ασύμμετρου κλειδιού. Αυτή η τεχνική είναι πολύ παρόμοια με το RSA—δημιουργείται ένα ζεύγος κλειδιών, ένα ιδιωτικό και ένα δημόσιο κλειδί και το ιδιωτικό κλειδί χρησιμοποιείται για τη δημιουργία μιας ψηφιακής υπογραφής. Η υπογραφή μπορεί να επαληθευτεί χρησιμοποιώντας ένα δημόσιο κλειδί.

- Μια άλλη μέθοδος αναγνώρισης χρήστη που ονομάζεται **προ-κοινόχρηστο κλειδί** είναι ένας καθορισμένος κωδικός πρόσβασης που χρησιμοποιείται και από τα δύο μηχανήματα (έναν εκκινητή και έναν δέκτη) ταυτόχρονα. Αν και είναι μια από τις πιο εύκολες μεθόδους διαμόρφωσης, επιπλέον, έχει λίγα σφάλματα από μόνη της—αυτή η μέθοδος παρεμβαίνει στην επεκτασιμότητα καθώς πρέπει να ρυθμιστεί μηχανικά. θα μπορούσε να εμποδίσει την ασφάλεια καθώς ο κωδικός πρόσβασης που δημιουργήθηκε πρέπει να πληροί το πρότυπο, το οποίο αποτελείται από κανόνες πολυπλοκότητας, μοναδικότητας και μυστικότητας.

- Επίσης, υπάρχει το **EAP** (ExtensibleAuthenticationProtocol) που είναι μάλλον ένα πλαίσιο ελέγχου ταυτότητας παρά ένας συγκεκριμένος μηχανισμός ελέγχου ταυτότητας. Μπορεί από μόνο του να υποστηρίξει πολλαπλά συστήματα ελέγχου ταυτότητας χωρίς να απαιτείται προδιαπραγμάτευση. Η αρχή λειτουργίας του EAP είναι ότι ο επαληθευτής στέλνει ένα μήνυμα Αίτησης για τον έλεγχο ταυτότητας ενός ομότιμου, ενώ ο ομότιμος απαντά με ένα έγκυρο μήνυμα απάντησης. Ανταλλάσσουν συνεχώς πρόσθετα μηνύματα έως ότου ο επαληθευτής μπορεί ή/και δεν μπορεί να ελέγξει την ταυτότητα του ομοτίμου. (B. Aboba, Microsoft, L. Blunk, Merit Network, Inc, J. Vollbrecht, Vollbrecht Consulting LLC 2004).

- Τέλος, υπάρχει η **RADIUS** (Remote Authentication Dial In User Service). Αυτό το πρωτόκολλο χρησιμοποιείται για τον έλεγχο της πρόσβασης στο δίκτυο με έλεγχο ταυτότητας, εξουσιοδότηση και καταμέτρηση λογαριασμού, που ονομάζεται επίσης διαδικασία AAA. Το πρωτόκολλο RADIUS είναι ένα πρωτόκολλο χωρίς σύνδεση που βασίζεται σε UDP21, το οποίο χρησιμοποιεί ένα μοντέλο ασφαλείας hop-by-hop. Αυτό το πρωτόκολλο είναι ανιθαγενές (δεν παρακολουθεί κοινές πληροφορίες από προηγούμενες συνεδρίες) και υποστηρίζει ελέγχους ταυτότητας PAP22 και CHAP23 μέσω PPP24, χρησιμοποιεί αλγόριθμο ασφαλείας MD525. (Hassel 2010).

1.5 Κρυπτογράφηση και αποκρυπτογράφηση

Η κρυπτογράφηση είναι εξίσου σημαντική με τον έλεγχο ταυτότητας. Είναι ένα εργαλείο κρυπτογραφίας που διασφαλίζει την εμπιστευτικότητα καθιστώντας τα δεδομένα (απλό κείμενο— ένα μη κρυπτογραφημένο μήνυμα) ακατανόητα. Αποτελείται από έναν αλγόριθμο που ονομάζεται *κρυπτογράφηση* και μια μυστική τιμή που ονομάζεται *κλειδί*. Εν τω μεταξύ, η αποκρυπτογράφηση είναι μια αντίστροφη τεχνολογία που επαναφέρει τα κρυπτογραφημένα μηνύματα στην αρχική τους κατάσταση.

Οι αλγόριθμοι κρυπτογράφησης χωρίζονται σε δύο κατηγορίες:

- την συμμετρική κρυπτογράφηση και
- την ασύμμετρη κρυπτογράφηση.

Ενώ η συμμετρική κρυπτογράφηση χρησιμοποιεί το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, η ασύμμετρη κρυπτογράφηση χρησιμοποιεί δύο ξεχωριστά κλειδιά — ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί.

Η συμμετρική κρυπτογράφηση αποτελείται από: ***κρυπτογράφηση μπλοκ***, ***κρυπτογράφηση ροής***, ***συναρτήσεις κατακερματισμού***, ***συνάρτηση κατακερματισμού με μυστικό κλειδί***, ***επικυρωμένη κρυπτογράφηση***.

Μία **κρυπτογράφηση μπλοκ** αποτελείται από αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης. Ο αλγόριθμος κρυπτογράφησης χρησιμοποιεί ένα κλειδί και ένα μπλοκ απλού κειμένου για την παραγωγή ενός μπλοκ κρυπτογραφημένου κειμένου, ενώ ο αλγόριθμος αποκρυπτογράφησης είναι η αντιστροφή του αλγορίθμου κρυπτογράφησης. Ο κρυπτογράφηση μπλοκ χρησιμοποιεί δύο τιμές: ένα μέγεθος μπλοκ και ένα μέγεθος κλειδιού.

Μία **κρυπτογράφηση ροής** χρησιμοποιεί ντετερμινισμό για να επιτρέψει την αποκρυπτογράφηση δημιουργώντας bits ψευδοτυχών που χρησιμοποιούνται για κρυπτογράφηση. Χρησιμοποιεί ένα κλειδί (μια μυστική τιμή) και ένα nonce (μια μοναδική τιμή που προορίζεται για το κλειδί), στη συνέχεια παράγει μια ψευδοτυχαία ροή bit (μια ροή κλειδιού).

Μια συνάρτηση κατακερματισμού χρησιμοποιεί μια μεγάλη τιμή εισόδου και παράγει μια σύντομη τιμή εξόδου που ονομάζεται τιμή κατακερματισμού. "Οι

συναρτήσεις κατακερματισμού είναι μακράν οι πιο ευέλικτοι και πανταχού παρόντες από όλους τους αλγόριθμους κρυπτογράφησης." (Aumasson 2018), ο συγγραφέας έκανε αυτή τη δήλωση επειδή ο σκοπός της κύριας συνάρτησης κατακερματισμού είναι να είναι απρόβλεπτη. Ένα άλλο πλεονέκτημα της συνάρτησης κατακερματισμού είναι ότι μπορεί να αναστραφεί.

Εν τω μεταξύ, ο κατακερματισμός με κλειδί χρησιμοποιεί κωδικό ελέγχου ταυτότητας μηνυμάτων (αργότερα αναφέρεται ως MAC) ο οποίος επαληθεύει τα μηνύματα και διασφαλίζει την ακεραιότητά του. Επίσης, χρησιμοποιεί ψευδοτυχαίες συναρτήσεις που παράγουν τυχαίες τιμές κατακερματισμού-μεγέθους.

Τέλος, η **επαληθευμένη κρυπτογράφηση** έχει χαρακτηριστικά μιας κανονικής κρυπτογράφησης και ενός MAC. Μπορεί να χωριστεί σε τρία μέρη: *επαληθευμένη κρυπτογράφηση με χρήση MAC*, *κρυπτογράφηση με έλεγχο ταυτότητας*, *κρυπτογράφηση με συσχετισμένα δεδομένα*. Η επαληθευμένη κρυπτογράφηση με χρήση MAC επιτρέπει στους χρήστες να κρυπτογραφήσουν το απλό κείμενο και, επίσης, να το ελέγξουν. Η αποστολή κρυπτογράφησης με έλεγχο ταυτότητας είναι η επιστροφή μιας ετικέτας ελέγχου ταυτότητας με το κρυπτογραφημένο κείμενο. Η κρυπτογράφηση με έλεγχο ταυτότητας με έναν συσχετισμένο αλγόριθμο δεδομένων επιτρέπει την προσάρτηση δεδομένων απλού κειμένου σε ένα κρυπτογραφημένο κείμενο, το οποίο θα επικυρώνει εάν το κρυπτογραφημένο κείμενο είναι κατεστραμμένο ή όχι.

Αντίθετα από τη συμμετρική κρυπτογράφηση, **η ασύμμετρη κρυπτογράφηση** αποτελείται από **RSA**, **Diffie-Hellman**, **Ελλειπτικές Καμπύλες**.

- Η ίδια μέθοδος **RSA** χρησιμοποιείται στον έλεγχο ταυτότητας και στην κρυπτογράφηση. Με την κρυπτογράφηση, το RSA λειτουργεί ως εξής: μετά τη δημιουργία του ζεύγους κλειδιών και την κοινή χρήση του δημόσιου κλειδιού, το σχήμα padding χρησιμοποιείται για την εισαγωγή τυχαίων δεδομένων (που ονομάζεται paddle) και δημιουργείται ένα κρυπτογραφημένο μήνυμα. Μαθηματικά αυτό θα μπορούσε να γίνει παίρνοντας μια νέα μεταβλητή που ονομάζεται m και υπολογίζοντας την ακόλουθη συνάρτηση: c=me mod n. Αυτό επιτρέπει την κρυπτογράφηση του μηνύματος, ωστόσο, για να κρυπτογραφηθεί η κρυπτογραφημένη μεταβλητή m πρέπει να μετατραπεί σε απλό κείμενο με μια συνάρτηση m=cd mod n.

- Στη συνέχεια, υπάρχει το πρωτόκολλο ανταλλαγής κλειδιών **Diffie-Hellman** που επιτρέπει σε δύο μέρη να δημιουργήσουν έναν κοινόχρηστο μυστικό κωδικό πρόσβασης (ή ένα κλειδί) χωρίς προηγούμενη γνώση ενός άλλου μέρους. (Aumasson 2018)

Τέλος, υπάρχει κρυπτογραφία **ελλειπτικής καμπύλης**. Αυτή η μέθοδος κρυπτογραφίας χρησιμοποιεί ελλειπτικές καμπύλες σε πεπερασμένα πεδία26. Το κύριο πλεονέκτημα αυτής της μεθόδου είναι ότι χρησιμοποιεί μικρότερα κλειδιά για να φτάσει στο ίδιο επίπεδο ασφάλειας. (Ciesla 2020).

1.6 Συμπέρασμα για τις τεχνολογίες

Για να σχηματιστεί ένα συμπέρασμα, απαιτείται δημιουργία τεσσάρων κριτηρίων για να αποφασιστεί ποια τεχνολογία είναι η καταλληλότερη για τη συνέχιση του έργου. Τα κριτήρια είναι:

- αναγνώριση χρήστη,
- κρυπτογράφηση και
- αποκρυπτογράφηση δεδομένων,

Ο πίνακας που παρέχεται παρακάτω (αναφέρεται στον Πίνακα 1), δείχνει ότι όλες οι τεχνολογίες χρησιμοποιούν συγκεκριμένο προσδιορισμό, ωστόσο, άλλα κριτήρια δείχνουν ότι υπάρχουν ορισμένες τεχνολογίες που λείπουν σε ορισμένα μέρη.

Πίνακας 1: Τεχνολογίες και η καταλληλότητά τους

Ονομασία Τεχνολογίας	**Αναγνώριση**	**Κρυπτογράφηση**	**Ευκολία**	**Επίπεδο ειδικού πληροφορικής**
RDS	+	+	-	Μέτριο
SSH	+	+	-	Υψηλό
MPLS	+	-	-+	Χαμηλό-Μέτριο
VPN	+	+	-+	Χαμηλό

Η ίδια η τεχνολογία MPLS δεν χρησιμοποιεί κρυπτογράφηση για απεσταλμένες πληροφορίες. Αυτό οδηγεί στο ότι το MPLS δεν είναι κατάλληλο για αυτό το έργο. Η τεχνολογία VPN έχει φιλική προς τον χρήστη έλεγχο ταυτότητας, επίσης, η τεχνολογία δεν απαιτεί τεράστια εμπειρία ή γνώση, εν τω μεταξύ, η τεχνολογία SSH είναι πιο κατάλληλη για χρήστες που κατανοούν τις γραμμές εντολών.

Παρουσία μεγάλων ποσοτήτων συσκευών είναι δύσκολο να εγκαταστήσετε τεχνολογίες RDS και SSH, επειδή η μεμονωμένη διαμόρφωση θα απαιτεί όχι μόνο τεράστιο χρόνο αλλά και ανθρώπινους πόρους. Όλες οι τεχνολογίες που αναφέρονται δεν απαιτούν μεγάλα ποσά ακριβών. Ο πίνακας παρέχει πληροφορίες ότι η τεχνολογία VPN είναι η πλέον κατάλληλη για αυτό το έργο. Ωστόσο, η τεχνολογία VPN έχει ένα άλλο παράλληλο χαρακτηριστικό, το οποίο δεν

αναφέρεται παραπάνω, είναι η δυνατότητα τοποθέτησης καλωδιακής γραμμής peer-to-peer. Αυτή η μέθοδος παρέχει φυσικά την ευκαιρία να κάνετε τις συσκευές να συνδεθούν σε ένα άλλο LAN εύκολα και με ασφάλεια. Ωστόσο, το κύριο πρόβλημα peer-to-peer είναι ότι η τοποθέτηση καλωδίων ενώ υπάρχει μεγάλη γεωγραφική απόσταση κοστίζει πολύ και οι μικρότερες επιχειρήσεις δεν θα μπορούσαν να ενσωματώσουν αυτή τη μέθοδο. Επιπλέον, η χρήση αυτής της φυσικής τεχνολογίας σπαταλά περισσότερο χρόνο και πόρους από την εικονική τεχνολογία.

ΚΕΦΑΛΑΙΟ 2 - ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΡΓΟΥ

Η τεχνολογία VPN επιλέχθηκε για αυτό το έργο λόγω των προηγμένων πρωτοκόλλων ασφαλείας και της εύκολης εγκατάστασης. Δεδομένου ότι ο κύριος σκοπός αυτού του έργου είναι να συνδέσει διαφορετικά LAN μέσω του Διαδικτύου, ένας τύπος VPN που ονομάζεται site-to-site είναι μια τέλεια επιλογή. Η τεχνολογία VPN είναι η πιο προηγμένη σε πολλούς παράγοντες, όπως πχ. βοηθά τους διαχειριστές δικτύων υπολογιστών διότι αυτή η τεχνολογία είναι εύκολη στην προετοιμασία και την εγκατάσταση. Επιπλέον, αφού εφαρμοστεί η τεχνολογία, μπορεί να αφαιρεθεί χωρίς πρόσθετες συνέπειες — το δίκτυο θα εξακολουθεί να λειτουργεί χωρίς διακοπή. Με το site-to-site VPN δημιουργείται μια κρυπτογραφημένη σήραγγα (tunnel), που σημαίνει ότι τα δεδομένα μεταδίδονται με ασφάλεια μεταξύ των τοποθεσιών. Ακόμη, χρησιμοποιείται έλεγχος ταυτότητας και μόνο ο πελάτης, στον οποίο ανήκει το πακέτο, μπορεί να διαβάσει τα δεδομένα. Με τον κατάλληλο εξοπλισμό και την επιλογή ενός μη εμπορικού τύπου τεχνολογίας, αυτή η τεχνολογία δεν απαιτεί πρόσθετες χρεώσεις λογισμικού— δηλαδή, οι διαχειριστές IT μπορούν να δημιουργήσουν ένα ιδιωτικό εικονικό δίκτυο στις εταιρείες τους εντελώς δωρεάν.

Το αντικείμενο που σχεδιάστηκε με αφορμή αυτή την εργασία, είναι ένα δίκτυο υπολογιστών το οποίο όμως θα διαθέτει ισχυρή ασφάλεια. Μετά την υλοποίηση της ασφάλειας το σχεδιασμένο έργο θα έχει λειτουργίες όπως:

1) Η ασφάλεια του δικτύου υπολογιστών της ΣΑΕΚ, θα είναι εξασφαλισμένη.

2) Θα αναγνωρίζονται οι χρήστες στο δίκτυο.

3) Θα υπάρχει κρυπτογράφηση και αποκρυπτογράφηση των μεταδιδόμενων πληροφοριών.

4) Τα δεδομένα που μεταδίδονται μεταξύ των απαιτούμενων κόμβων του δικτύου θα είναι εγγυημένα, θα παραμένουν αμετάβλητα και υψηλής ποιότητας.

Υπάρχουν ορισμένες κρίσιμες ανάγκες για αυτό το έργο. Για παράδειγμα, είναι ζωτικής σημασίας το επιλεγμένο υλικό να υποστηρίζει VPN τεχνολογία και οι οικονομικές δαπάνες για αυτήν την τεχνολογία δεν θα πρέπει να υπερβαίνουν το οικονομικό όριο των μικρών επιχειρήσεων. Ένα άλλο ουσιαστικό μέρος αυτού του έργου είναι η ισχύς των συσκευών—η ισχύς επεξεργασίας πρέπει να χειρίζεται τις διαδικασίες κρυπτογράφησης/αποκρυπτογράφησης και η μέγιστη ταχύτητα μεταφοράς δεδομένων θα πρέπει να είναι επαρκής για τη μετάδοση πακέτων μέσω μιας σήραγγας VPN.

Τα κριτήρια υλικού θα πρέπει να διακριθούν σε μέρη όπως:

1) Την Υποστήριξη της τεχνολογίας VPN.

2) την Τιμή των υλικών

3) το μέγεθος μνήμης πρόσβασης (πχ. > 64 MB).

4) Την μέγιστη ταχύτητα μεταφοράς δεδομένων (πχ. > 100 Mbit/s).

Ανάλογα με τον φόρτο εργασίας ενός δικτύου, η ελάχιστη ταχύτητα μεταφοράς δεδομένων μπορεί να κυμαίνεται από 1,5 Mbps έως 15 Mbps. Σε αυτήν την περίπτωση, για λιγότερους από τέσσερις χρήστες το ελάχιστο ποσό επισκεψιμότητας θα πρέπει να είναι της τάξεως 2,5 Mbps, ενώ για περισσότερους από τέσσερις χρήστες το ελάχιστο ποσό θα πρέπει να είναι μεγαλύτερο από 3 Mbps. Η ταχύτητα μπορεί να είναι περιορισμένη, αλλά δεν θα πρέπει να υπερβαίνει το ελάχιστο όριο ροής δεδομένων.

Οι πάροχοι Διαδικτύου (ISP) θα πρέπει να επιλέγονται λαμβάνοντας υπόψη: την τιμή της υπηρεσίας, την ταχύτητα και τον τύπο του Διαδικτύου. Οι απαιτήσεις φαίνονται στον Πίνακα 2.

Πίνακας 2: Απαιτήσεις για τις προσφερόμενες υπηρεσίες των παρόχων Διαδικτύου: τύπος τεχνολογίας, ταχύτητα και τιμή.

Τύπος Δικτύου	**Mb/s**	**Τιμή €/μήνα**
Internet (με χαλκό)	<60	<10
Internet (με χαλκό)	<100	<15
Οπτική Ίνα	<100	<25
Οπτική Ίνα	<300	<30
Οπτική Ίνα	<1024	<50

Μετά την εφαρμογή της τεχνολογίας VPN, δεν θα απαιτείται πρόσθετη προηγμένη συντήρηση. Έτσι, λιγότερο έμπειροι διαχειριστές δικτύων πληροφορικής, μηχανικοί πληροφορικής, θα μπορούν να παρακολουθούν την τεχνολογία. Για να διατηρηθεί μια στενή παρατήρηση του δικτύου, θα πρέπει να γίνονται καθορισμένες καταχωρήσεις στα αρχεία καταγραφής VPN.

Στους μηχανικούς δικτύου και ορισμένους διαχειριστές, απαιτούνται να είναι γνωστές, πληροφορίες δρομολογητών και κόμβων, όπως επίσης και διευθύνσεις IP καθώς και οι κωδικοί πρόσβασης,. Για να μειωθεί η πιθανότητα του κινδύνου διαρροής δεδομένων, οι πληροφορίες πρέπει να αποθηκεύονται σε 'κλειστό' ηλεκτρονικό χώρο. Ο 'κλειστός' χώρος σημαίνει ότι οι πληροφορίες θα αποθηκεύονται σε servers, στους οποίους μόνο λίγα άτομα θα έχουν πρόσβαση και δεν θα είναι προσβάσιμος από χρήστες έξω από το intranet, ή από ένα σύννεφο (cloud).

Δεν υπάρχουν πρόσθετες απαιτήσεις για τον καθορισμό της μορφής του αρχείου αποθήκευσης πληροφοριών. Προγράμματα, με μορφή όπως το Microsoft Excel είναι μάλλον κατάλληλα. Ωστόσο, συνιστάται το αρχείο να είναι κρυπτογραφημένο και

να ορίζεται και απαιτείται κωδικός πρόσβασης για την πρόσβαση σε αυτό.

ΚΕΦΑΛΑΙΟ 3 - "Σχεδιασμός, Υλοποίηση και Αξιολόγηση Ασφαλούς Εικονικού Ιδιωτικού Δικτύου με WireGuard: Μια Πρακτική Προσέγγιση"

3.1 Εισαγωγή

Στο πλαίσιο της παρούσας διπλωματικής εργασίας, επιχειρήθηκε η σχεδίαση, υλοποίηση και αξιολόγηση ενός **ασφαλούς εικονικού ιδιωτικού δικτύου (VPN)** βασισμένου στο πρωτόκολλο **WireGuard**. Ο κύριος στόχος ήταν η ασφαλής διασύνδεση ετερογενών υπολογιστικών συστημάτων και η ανάλυση της λειτουργικότητας, της απόδοσης και της ασφάλειας του δικτύου. Η επιλογή του WireGuard ως λύσης VPN δικαιολογείται από την απλότητα, την υψηλή απόδοση και την ισχυρή κρυπτογράφηση που προσφέρει, χαρακτηριστικά που το καθιστούν ιδανικό για σύγχρονες εφαρμογές ασφαλούς επικοινωνίας.

Η πρακτική εφαρμογή της εργασίας περιελάμβανε όλα τα στάδια, από την προετοιμασία του υλικού και του λογισμικού μέχρι τη δημιουργία κρυπτογραφικών κλειδιών, τη διαμόρφωση των ρυθμίσεων και την πειραματική αξιολόγηση της λειτουργικότητας του δικτύου. Για τις ανάγκες της υλοποίησης, χρησιμοποιήθηκαν διαφορετικές πλατφόρμες, συμπεριλαμβανομένου ενός **κεντρικού server** με λειτουργικό σύστημα **Kali Linux** (Debian-based), ενός **client συστήματος** με **Ubuntu Server**, καθώς και ενός τρίτου client με **MX Linux** (Debian-based). Επιπλέον, εξετάστηκε η διαλειτουργικότητα του WireGuard με ένα **Windows-based client**, προκειμένου να αξιολογηθεί η ευελιξία του πρωτοκόλλου σε ετερογενή περιβάλλοντα.

3.2 Μεθοδολογία

3.2.1 Προετοιμασία και Διαμόρφωση του Περιβάλλοντος

Το πρώτο βήμα περιελάμβανε την εγκατάσταση και παραμετροποίηση του WireGuard τόσο στον κεντρικό server όσο και στους clients. Για κάθε σύστημα δημιουργήθηκαν **ιδιωτικά και δημόσια κλειδιά κρυπτογράφησης**, τα οποία ενσωματώθηκαν στα αντίστοιχα αρχεία ρυθμίσεων. Αυτή η διαδικασία ήταν κρίσιμη για την πιστοποίηση των συνδέσεων και την εξασφάλιση της ασφαλούς ανταλλαγής δεδομένων.

Για τη διευθυνσιοδότηση του VPN επιλέχθηκε ένα **ιδιωτικό υποδίκτυο (10.0.0.0/24)**, ώστε να διαχωρίζεται ξεκάθαρα από το φυσικό τοπικό δίκτυο (LAN). Σε κάθε peer (σύνδεσμο) ορίστηκαν οι **επιτρεπόμενες διευθύνσεις (AllowedIPs)**, ενώ στον server προστέθηκαν **πολλαπλοί peers**, επιτρέποντας τη σύνδεση περισσότερων του ενός clients. Η διαδικασία αυτή διασφάλισε ότι κάθε σύστημα θα μπορούσε να επικοινωνεί αποκλειστικά μέσα από το VPN, χωρίς να εκτίθεται σε εξωτερικούς κινδύνους.

3.2.2 Δοκιμές Συνδεσιμότητας και Επαλήθευση Λειτουργικότητας

Μετά την αρχική ρύθμιση, πραγματοποιήθηκαν δοκιμές συνδεσιμότητας με τη χρήση εντολών όπως το **ping** και το **wg show**. Οι δοκιμές αυτές επιβεβαίωσαν ότι η ανταλλαγή δεδομένων εντός του VPN ήταν εφικτή και ότι οι συνδέσεις ήταν σταθερές και ασφαλείς. Η επιτυχής επικοινωνία μεταξύ των συστημάτων αποτέλεσε ένα σημαντικό ορόσημο, καθώς επιβεβαίωσε την ορθότητα της διαμόρφωσης.

3.2.3 Εισαγωγή και Περιγραφή Περιβάλλοντος Δοκιμών

Η εργαστηριακή φάση υλοποιήθηκε σε οικιακό περιβάλλον, με τη χρήση εξοπλισμού και λογισμικού που είναι ευρέως διαθέσιμα, ώστε να αποδειχθεί ότι μια τέτοια υποδομή μπορεί να στηθεί ακόμη και με περιορισμένους πόρους.

Το δίκτυο βασίστηκε σε modem/router Speedport του παρόχου Cosmote, με σύνδεση VDSL στα ~100 Mbps download και ~10 Mbps upload. Το τοπικό LAN είχε το υποδίκτυο 192.168.1.0/24 με ενεργοποιημένο DHCP, ενώ το VPN σχεδιάστηκε να λειτουργεί σε απομονωμένο εικονικό υποδίκτυο 10.0.0.0/24.

Οι συσκευές που χρησιμοποιήθηκαν ήταν:

Kali Linux VirtualBox machine: Φορητός υπολογιστής συνδεδεμένος ενσύρματα στο router, φιλοξενούσε κύριο λειτουργικό σύστημα windows10 pro και μέσω του virtualbox λριτοθρεγικο συστημκα Kali Linux. Ο κύριος ρόλος του ήταν να λειτουργεί ως ο κεντρικός VPN server, διαχειριζόμενος τις εισερχόμενες συνδέσεις και δρομολογώντας την κίνηση μεταξύ των συνδεδεμένων πελατών μέσω WireGuard.

Ubuntu Server (client): Σταθερός υπολογιστής με εγκατεστημένο το επίσημο εργαλείο γραμμής εντολών (CLI) του WireGuard. Χρησιμοποιήθηκε ως πελάτης VPN για σύνδεση στον κεντρικό server και ασφαλή πρόσβαση στους πόρους του δικτύου.

MX Linux (client): Φορητός υπολογιστής με Debian-based διανομή (MX Linux), ο οποίος λειτούργησε επίσης ως πελάτης VPN, συνδεόμενος επίσαης στον ίδιο server.

3.2.4 Γιατί Επιλέξαμε το WireGuard

Στο πλαίσιο της παρούσας εργασίας, η επιλογή του **WireGuard** ως πρωτοκόλλου VPN δεν ήταν τυχαία. Το WireGuard αποτελεί μια **σύγχρονη, ανοιχτού κώδικα λύση**, η οποία σχεδιάστηκε από την αρχή με στόχο να ξεπερνά τις αδυναμίες παλαιότερων τεχνολογιών, όπως το **OpenVPN** και το **IPSec**. Αρχικά αναπτύχθηκε για τον πυρήνα του Linux, αλλά σήμερα υποστηρίζεται σε **όλα τα μεγάλα λειτουργικά συστήματα** (Windows, macOS, Android, iOS, BSD), καθιστώντας το μια ευέλικτη και προσβάσιμη λύση για κάθε χρήστη.

3.2.5 Τεχνικά Πλεονεκτήματα του WireGuard

Το WireGuard βασίζεται σε **πρωτοποριακά κρυπτογραφικά πρωτόκολλα**, τα οποία εξασφαλίζουν υψηλό επίπεδο ασφάλειας και απόδοσης:

- **Curve25519**: Για την ασφαλή ανταλλαγή κλειδιών.
- **ChaCha20**: Για την κρυπτογράφηση των δεδομένων.
- **Poly1305**: Για τον έλεγχο ακεραιότητας και αυθεντικότητας.
- **BLAKE2s και SipHash24**: Για γρήγορες και ασφαλείς λειτουργίες hashing.

Ένα από τα πιο εντυπωσιακά χαρακτηριστικά του WireGuard είναι ο **minimalιστικός σχεδιασμός του**. Ο κώδικάς του είναι **πολύ μικρότερος** σε σύγκριση με άλλες λύσεις VPN, γεγονός που μειώνει σημαντικά τις πιθανότητες ύπαρξης σφαλμάτων και διευκολύνει τον έλεγχο ασφαλείας. Αυτή η απλότητα δεν θυσιάζει την ασφάλεια, αλλά αντίθετα την ενισχύει, καθιστώντας το WireGuard μια από τις πιο αξιόπιστες λύσεις VPN σήμερα.

3.3 Εφαρμογές και Σενάρια Χρήσης

Το WireGuard μπορεί να εφαρμοστεί σε μια ευρεία γκάμα σεναρίων, όπως:

- **Απομακρυσμένη πρόσβαση**: Σε εταιρικά ή οικιακά δίκτυα, επιτρέποντας στους χρήστες να συνδέονται με ασφάλεια από απόσταση.
- **Site-to-site VPN**: Για τη διασύνδεση διαφορετικών υποδομών, όπως κεντρικά γραφεία με απομακρυσμένα υποκαταστήματα.
- **Προστασία ιδιωτικότητας**: Σε δημόσια δίκτυα Wi-Fi, όπου η κίνηση δεδομένων μπορεί να είναι εκτεθειμένη σε κινδύνους.
- **Κρυπτογράφηση κίνησης**: Για την αποφυγή υποκλοπών και την προστασία ευαίσθητων δεδομένων.

3.4 Λόγοι Επιλογής του WireGuard

Η επιλογή του WireGuard για την υλοποίηση της παρούσας εργασίας βασίστηκε σε μια σειρά από κρίσιμα πλεονεκτήματα:

1. **Απλότητα ρυθμίσεων**: Σε αντίθεση με το OpenVPN ή το IPSec, το WireGuard απαιτεί **ελάχιστα βήματα διαμόρφωσης**. Η χρήση δημόσιων και ιδιωτικών κλειδιών απλοποιεί τη διαδικασία, χωρίς την ανάγκη για περίπλοκα πιστοποιητικά.
2. **Σύγχρονη κρυπτογράφηση**: Χρησιμοποιεί τα πιο προηγμένα κρυπτογραφικά πρωτόκολλα, όπως το **ChaCha20** για κρυπτογράφηση και το **Poly1305** για επαλήθευση, εξασφαλίζοντας υψηλό επίπεδο προστασίας.
3. **Υψηλή απόδοση**: Είναι εξαιρετικά ελαφρύ σε κατανάλωση πόρων, κάτι που το καθιστά ιδανικό για **φορητές συσκευές** και servers με περιορισμένη ισχύ.
4. **Σταθερότητα και cross-platform υποστήριξη**: Λειτουργεί αξιόπιστα και είναι διαθέσιμο σε **όλα τα μεγάλα λειτουργικά συστήματα**, προσφέροντας ευελιξία και ευκολία χρήσης.

3.5 Βήματα Υλοποίησης του VPN

3.5.1 Προετοιμασία του Kali Linux ως VPN Server

Το πρώτο βήμα για τη δημιουργία του VPN ήταν η **εγκατάσταση και διαμόρφωση του WireGuard στον κεντρικό server**, ο οποίος βασίστηκε στο **Kali Linux**. Η διαδικασία ήταν απλή και περιελάμβανε τα εξής βήματα:

1. **Ενημέρωση των αποθετηρίων**: Πριν από την εγκατάσταση, ήταν απαραίτητο να ενημερωθούν τα αποθετήρια του συστήματος, ώστε να διασφαλιστεί η πρόσβαση στις τελευταίες εκδόσεις λογισμικού.

   sudo apt update

2. **Εγκατάσταση του WireGuard**: Μετά την ενημέρωση, ακολούθησε η εγκατάσταση του πακέτου WireGuard, το οποίο είναι διαθέσιμο απευθείας από τα επίσημα αποθετήρια του Debian.

   sudo apt install wireguard

Με την ολοκλήρωση αυτών των βημάτων, ο server ήταν έτοιμος για τη διαμόρφωση του WireGuard και τη δημιουργία των απαραίτητων κρυπτογραφικών κλειδιών. Η διαδικασία αυτή αποτέλεσε τη βάση για την ασφαλή διασύνδεση των clients και την υλοποίηση ενός λειτουργικού VPN.

Η εντολή **apt update** συγχρονίζει τις πληροφορίες διαθέσιμων πακέτων με τους επίσημους καθρέφτες (mirrors), διασφαλίζοντας ότι θα εγκατασταθεί η πιο πρόσφατη έκδοση του λογισμικού.

Η εντολή **apt install wireguard** κατεβάζει και εγκαθιστά το βασικό πακέτο WireGuard.

3.5.2 Δημιουργία Κλειδιών Κρυπτογράφησης Server

Η ασφάλεια ενός VPN εξαρτάται θεμελιωδώς από την κρυπτογράφηση, καθώς αυτή προστατεύει την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας. Στο WireGuard, κάθε κόμβος διαθέτει ένα ζεύγος κλειδιών ένα **ιδιωτικό** και ένα

δημόσιο που δημιουργούνται τοπικά στη συσκευή. Η ταυτοποίηση μεταξύ δύο κόμβων πραγματοποιείται μέσω της ανταλλαγής των δημοσίων κλειδιών, ενώ η ασφάλεια διασφαλίζεται απόλυτα μέσω της διατήρησης του ιδιωτικού κλειδιού ως απόρρητου.

Η ανταλλαγή κλειδιών βασίζεται στο **Curve25519** Elliptic Curve Diffie–Hellman (ECDH), που επιτρέπει τη δημιουργία ενός συμμετρικού "shared secret" το οποίο δεν μεταδίδεται ποτέ αυτούσιο μέσω του δικτύου. Αυτό το shared secret χρησιμοποιείται στη συνέχεια από το **ChaCha20** για την κρυπτογράφηση των δεδομένων, ενώ ο αλγόριθμος **Poly1305** επαληθεύει την αυθεντικότητα και ακεραιότητα κάθε πακέτου.

Δημιουργία κλειδιών:

sudo -i

cd /etc/wireguard

wg genkey | tee server_private.key | wg pubkey > server_public.key

Η εντολή **wg genkey** παράγει ένα ιδιωτικό κλειδί. Με το **tee** το αποθηκεύουμε και ταυτόχρονα το προωθούμε στην **wg pubkey** που υπολογίζει το αντίστοιχο δημόσιο κλειδί.

3.5.3 Ρύθμιση Διασύνδεσης WireGuard Server

Το αρχείο ρυθμίσεων **/etc/wireguard/wg0.conf** είναι η "καρδιά" του server:

[Interface]

Address = 10.0.0.1/24 ListenPort = 51820

PrivateKey = <server_private.key> SaveConfig = true

- Address: Ορίζει την IP του server στο VPN subnet.
- ListenPort: Η θύρα UDP στην οποία ακούει ο server.
- PrivateKey: Το ιδιωτικό κλειδί του server.
- SaveConfig: Εξασφαλίζει ότι αλλαγές που γίνονται δυναμικά αποθηκεύονται.

3.6 Ενεργοποίηση IP Forwarding και Ρύθμιση NAT

Η δρομολόγηση κίνησης μεταξύ VPN και Internet απαιτεί ενεργοποίηση της λειτουργίας IP forwarding:

echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf sysctl -p

Το NAT (Network Address Translation) είναι απαραίτητο για να μπορούν οι VPN clients να χρησιμοποιούν την κοινή IP του server στο Internet:

- ***iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE***
- ***iptables -A FORWARD -i wg0 -j ACCEPT***
- ***iptables -A FORWARD -o wg0 -j ACCEPT***

Οι κανόνες αυτοί καθορίζουν ότι Όλη η εξερχόμενη κίνηση από το wg0 προς το Internet μετατρέπεται ώστε να φαίνεται ότι προέρχεται από την IP του server.Η εισερχόμενη κίνηση από το VPN επιτρέπεται να δρομολογηθεί.

```
┌──(root㉿kali)-[/etc/wireguard]
└─# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

┌──(root㉿kali)-[/etc/wireguard]
└─# iptables -A FORWARD -i wg0 -j ACCEPT

┌──(root㉿kali)-[/etc/wireguard]
└─# iptables -A FORWARD -o wg0 -j ACCEPT


┌──(root㉿kali)-[/etc/wireguard]
└─# sudo apt install iptables-persistent
The following packages were automatically installed and are no longer required:
  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
  iptables-persistent

Installing dependencies:
  netfilter-persistent

REMOVING:
  ufw

Summary:
  Upgrading: 0, Installing: 2, Removing: 1, Not Upgrading: 0
  Download size: 18.5 kB
  Freed space: 783 kB

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 netfilter-persistent all 1.0.23 [7,948 B]
Get:2 http://kali.download/kali kali-rolling/main amd64 iptables-persistent all 1.0.23 [10.5 kB]
Fetched 18.5 kB in 1s (33.4 kB/s)
Preconfiguring packages ...
(Reading database ... 421197 files and directories currently installed.)
Removing ufw (0.36.2-9) ...
Skip stopping firewall: ufw (not enabled)
Selecting previously unselected package netfilter-persistent.
(Reading database ... 421100 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.23_all.deb ...
Unpacking netfilter-persistent (1.0.23) ...
```

3.7 Εκκίνηση του VPN Server

Η εκκίνηση γίνεται με:

wg-quick up wg0

Η wg-quick διαβάζει το αρχείο wg0.conf και δημιουργεί την εικονική διεπαφή wg0.

wg show

Η εντολή αυτή εμφανίζει τα στοιχεία του interface, τα ενεργά peers, και την κυκλοφορία δεδομένων.

```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/etc/wireguard]
└─# wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.0.0.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0

┌──(root㉿kali)-[/etc/wireguard]
└─# wg show
interface: wg0
  public key: 7CUZkTQmDSfmYAR3YyeojXEZ65fnOb
  private key: (hidden)
  listening port: 51820

┌──(root㉿kali)-[/etc/wireguard]
└─#
```

3.8 Δημιουργία και Ρύθμιση Clients

Κάθε client χρειάζεται δικό του ζεύγος κλειδιών και ξεχωριστή εγγραφή στο server.

Δημιουργία κλειδιών:

wg genkey | tee client1_private.key | wg pubkey > client1_public.key

Στον server, προστίθεται peer: ***[Peer]***

PublicKey = <client1_public.key> AllowedIPs = 10.0.0.2/32

Στον client, το αρχείο client1.conf: ***[Interface]***

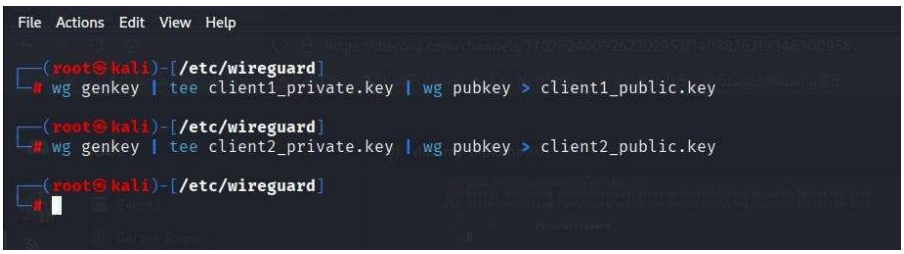
PrivateKey = <client1_private.key> Address = 10.0.0.2/24

DNS = 8.8.8.8

[Peer]

PublicKey = <server_public.key> Endpoint = 192.168.1.10:51820

AllowedIPs = 0.0.0.0/0 PersistentKeepalive = 25



3.9 Σύνδεση και Έλεγχος

Σε περιβάλλον Linux, η σύνδεση στον VPN server μέσω WireGuard έγινε με την εκτέλεση της εντολής:

sudo wg-quick up client1.conf

Η εντολή αυτή:

1. Διαβάζει το αρχείο ρυθμίσεων client1.conf, το οποίο περιέχει τα κλειδιά, τις IP διευθύνσεις και τις παραμέτρους του VPN.
2. Δημιουργεί το αντίστοιχο εικονικό interface (π.χ. wg0) και εφαρμόζει όλες τις ρυθμίσεις.
3. Εκκινεί την κρυπτογραφημένη σήραγγα (tunnel) μεταξύ του client και του server.

3.10 Firewall και Ασφάλεια

Για να διασφαλιστεί ότι όλη η δικτυακή κίνηση περνά αποκλειστικά μέσα από το VPN και να περιοριστεί η επικοινωνία εκτός αυτού, εφαρμόζονται κανόνες firewall.

Σε περιβάλλον Linux με χρήση του UFW (Uncomplicated Firewall), μπορούμε να ορίσουμε τους παρακάτω κανόνες:

sudo ufw default deny incoming: # Απορρίπτει όλες τις εισερχόμενες συνδέσεις από το εξωτερικό

sudo ufw default allow outgoing # Επιτρέπει όλες τις εξερχόμενες συνδέσεις προς το εξωτερικό

sudo ufw allow in on wg0 # Επιτρέπει εισερχόμενη κίνηση μόνο από το ***WireGuard interface (wg0)***

sudo ufw enable # Ενεργοποιεί το firewall με τους παραπάνω κανόνες

Με τους κανόνες:

- Οι συνδέσεις εκτός VPN μπλοκάρονται.
- Όλη η κίνηση προς και από τον υπολογιστή γίνεται μέσω του κρυπτογραφημένου interface wg0.
- Αποτρέπεται η ανεπιθύμητη πρόσβαση από μη εξουσιοδοτημένες πηγές.

Αυτή η ρύθμιση είναι κρίσιμη για τη διατήρηση της ασφάλειας του VPN και για την αποτροπή διαρροών δεδομένων (data leaks) εκτός της ασφαλούς σήραγγας.

```
root@mx:/etc/wireguard# sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@mx:/etc/wireguard# sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@mx:/etc/wireguard# sudo ufw allow in on wg0
Rule added
Rule added (v6)
root@mx:/etc/wireguard# sudo ufw allow ssh
Rule added
Rule added (v6)
root@mx:/etc/wireguard# sudo ufw enable
Firewall is active and enabled on system startup
```

3.10.1 Δοκιμές Ασφαλείας και Packet Capture

Για την επαλήθευση της ασφάλειας και της ορθής λειτουργίας του VPN, πραγματοποιήθηκαν διάφορες δοκιμές και αναλύσεις δικτυακής κίνησης. Αρχικά,

από τον κεντρικό server εκτελέστηκε σάρωση με το εργαλείο Nmap, με σκοπό τον εντοπισμό τυχόν ανοικτών θυρών στους πελάτες του δικτύου VPN. Η σάρωση έγινε με την εντολή:

nmap -sS 10.0.0.2

Η χρήση της σάρωσης SYN scan (–sS) επέτρεψε την ανίχνευση διαθέσιμων υπηρεσιών χωρίς να δημιουργήσει πλήρεις TCP συνδέσεις, διατηρώντας έτσι τη σάρωση διακριτική και αποτελεσματική. Παράλληλα, πραγματοποιήθηκε καταγραφή δικτυακής κίνησης (packet capture) με το εργαλείο tcpdump στο WireGuard interface wg0, χρησιμοποιώντας την εντολή:

sudo tcpdump -i wg0 -w vpn_traffic.pcap

Το αρχείο που καταγράφηκε αναλύθηκε με το Wireshark, όπου παρατηρήθηκε ότι τα πακέτα εμφανίζονται ως κρυπτογραφημένα UDP πακέτα χωρίς καμία αναγνώσιμη πληροφορία ή ευανάγνωστα headers, επιβεβαιώνοντας έτσι τη σωστή εφαρμογή και λειτουργία της κρυπτογράφησης του WireGuard VPN.

Για τη διασφάλιση της λειτουργικότητας και της σύνδεσης μεταξύ των κόμβων του VPN, πραγματοποιήθηκαν και βασικές δοκιμές δικτύου:Η εντολή ping χρησιμοποιήθηκε για την αποστολή πακέτων ICMP Echo Request από έναν πελάτη προς τον server ή ανάμεσα σε πελάτες, επιβεβαιώνοντας την απρόσκοπτη ανταλλαγή πακέτων και τη διαθεσιμότητα των συσκευών. Για παράδειγμα:

ping 10.0.0.1

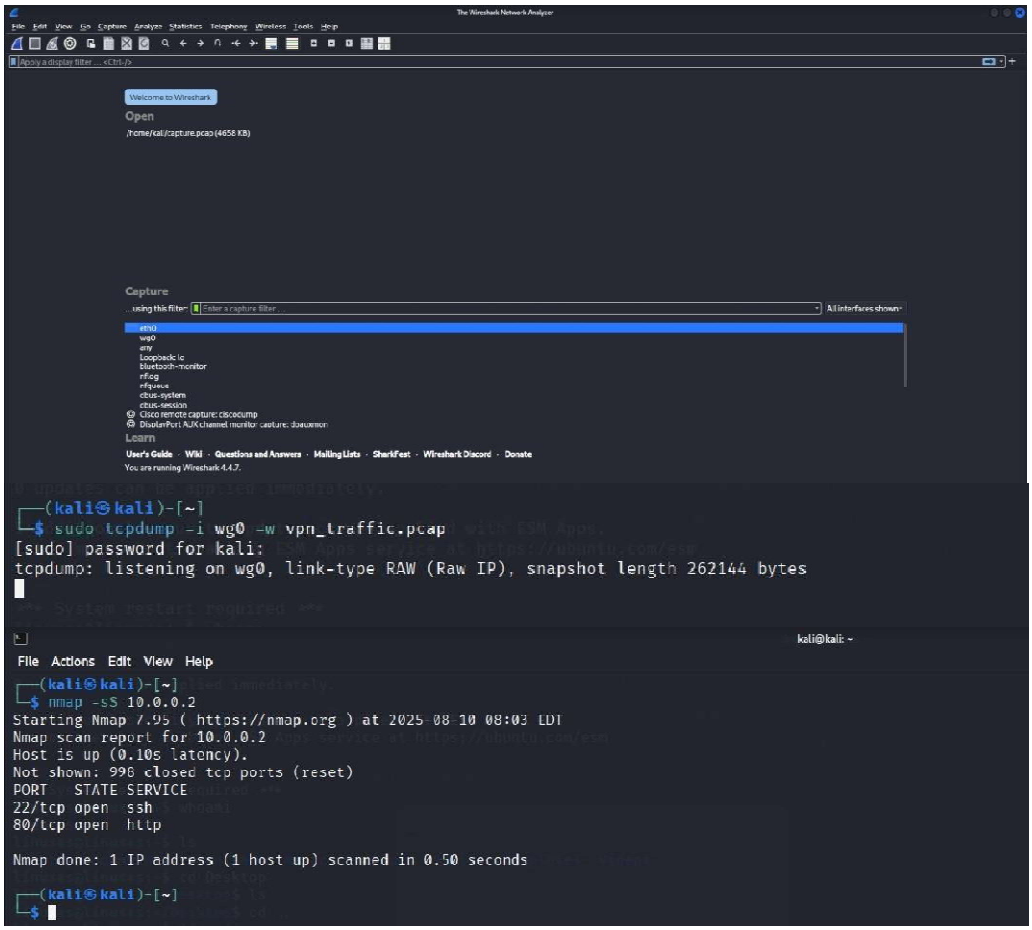
όπου 10.0.0.1 είναι η IP του VPN server. Η επιτυχημένη απάντηση (Echo Reply) αποδεικνύει τη λειτουργική σύνδεση και τη σωστή δρομολόγηση μέσω του VPN.

Επιπλέον, πραγματοποιήθηκε σύνδεση SSH μεταξύ των πελατών και του server για την ασφαλή απομακρυσμένη διαχείριση συστημάτων. Η σύνδεση γίνεται με την εντολή:

ssh user@10.0.0.1

Η επιτυχημένη σύνδεση SSH μέσω του VPN αποδεικνύει την αξιοπιστία και ασφάλεια της κρυπτογραφημένης σήραγγας για πραγματικές εφαρμογές δικτύου.

Τέλος, αξιοποιήθηκε το εργαλείο **iperf3** για τη μέτρηση της απόδοσης της σύνδεσης VPN, επιβεβαιώνοντας την ικανότητα του WireGuard να παρέχει υψηλές ταχύτητες μεταφοράς δεδομένων με ελάχιστη καθυστέρηση. Αυτές οι δοκιμές συνδυαστικά διασφαλίζουν τόσο την ασφάλεια όσο και τη λειτουργικότητα του VPN, παρέχοντας εμπιστοσύνη στην υλοποίηση και την καθημερινή χρήση του.

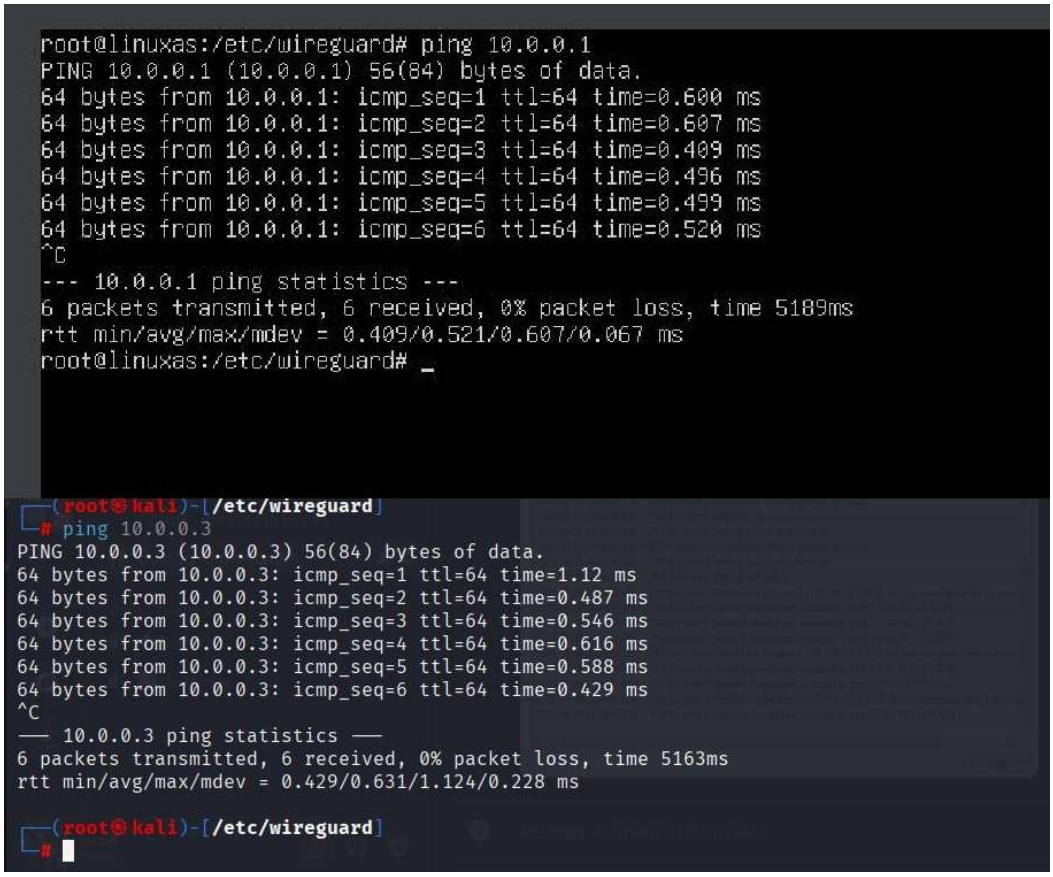

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
/home/kali/capture.pcap (4658 KB)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
wg0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.7.
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i wg0 -w vpn_traffic.pcap
[sudo] password for kali:
tcpdump: listening on wg0, link-type RAW (Raw IP), snapshot length 262144 bytes
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sS 10.0.0.2
Starting Nmap 7.95 (https://nmap.org) at 2025-08-10 08:03 EDT
Nmap scan report for 10.0.0.2
Host is up (0.10s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
┌──(kali㉿kali)-[~]
└─$

```
┌──(root㉿kali)-[/etc/wireguard]
└─# ssh linuxas@10.0.0.2
linuxas@10.0.0.2's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-63-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Aug 10 12:01:13 PM UTC 2025

  System load:             0.08
  Usage of /:              41.9% of 24.44GB
  Memory usage:            19%
  Swap usage:              0%
  Processes:               156
  Users logged in:         1
  IPv4 address for enp0s3: 192.168.1.9
  IPv6 address for enp0s3: 2a02:587:420d:c0b2:a00:27ff:fe03:b420

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

5 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


*** System restart required ***
linuxas@linuxas:~$
```

```
linuxas@mx:~/Desktop
$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.433 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.418 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.743 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.542 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.418/0.534/0.743/0.129 ms
linuxas@mx:~/Desktop
$
```

```
┌──(kali㉿kali)-[~]
└─$ cat vpn_traffic.pcap
•ò•e•h••LLEL`•@@•l
ç••\{8•9# /6•S"w•h••LLEL4•9``ç•
{•\8•$•
       H•O••CQb••/6•S"w•C       M
                                 •C     M
                                          I(I•h•LLEL•@@•
Q•"•[8••# •y•7~$&TI•hrXLLELn@6
                                Q•"
{•8•$••, ?4••>IS••v•7~$&T•C     NV•VC   NV•M•
                                             ••h•PLLELP@@+
S•u••.{80# •U••I••
                    ••h4•LLLL••@/t•S•u•
••h@LLEL}@@••••G••U••I•••C    •@•/••C •@z@
••h|dLLEL•@/••S•l•<
g•4••¿$•
    •C`••0'•••%•c•C     •y••••C •z
                          •s••h•dLLEL>•@@m
ç••3{8••# =(z•••ô••hc•LLEL•9••ç•
{•38u$•
       H•O••CQb••=(z•••ô•C      •Kcp•C  •Kc•••h•9
```

```
root@mx:/etc/wireguard# iperf3 -c 10.0.0.2
Connecting to host 10.0.0.2, port 5201
[  5] local 10.0.0.3 port 51442 connected to 10.0.0.2 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  6.95 MBytes  58.2 Mbits/sec    0    415 KBytes
[  5]   1.00-2.00   sec  7.12 MBytes  62.3 Mbits/sec   20    486 KBytes
[  5]   2.00-3.02   sec  5.64 MBytes  46.6 Mbits/sec    0    558 KBytes
[  5]   3.02-4.06   sec  5.09 MBytes  41.0 Mbits/sec    0    616 KBytes
[  5]   4.06-5.00   sec  8.52 MBytes  75.9 Mbits/sec    3    460 KBytes
[  5]   5.00-6.00   sec  5.40 MBytes  45.2 Mbits/sec    0    501 KBytes
[  5]   6.00-7.00   sec  3.86 MBytes  32.4 Mbits/sec    0    528 KBytes
[  5]   7.00-8.00   sec  6.38 MBytes  53.5 Mbits/sec    0    540 KBytes
[  5]   8.00-9.04   sec  6.87 MBytes  55.6 Mbits/sec    0    549 KBytes
[  5]   9.04-10.00  sec  6.38 MBytes  55.4 Mbits/sec    0    549 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  62.5 MBytes  52.4 Mbits/sec   23             sender
[  5]   0.00-10.08  sec  61.0 MBytes  50.8 Mbits/sec                  receiver

iperf Done.
root@mx:/etc/wireguard#
```



3.10.2 Απόδοση και Αποτελέσματα

Η απόδοση του WireGuard στο περιβάλλον δοκιμών αποδείχθηκε εξαιρετικά ικανοποιητική.

Κατά τις δοκιμές μεταφοράς αρχείων και streaming, η καθυστέρηση (latency) παρέμεινε σε πολύ χαμηλά επίπεδα, με ελάχιστη υποβάθμιση σε σχέση με την άμεση χρήση του Internet χωρίς VPN.

Η χρήση UDP στο WireGuard (θύρα 51820) συνέβαλε στην αποφυγή περιττής καθυστέρησης που θα μπορούσε να προκαλέσει το TCP. Ο μηχανισμός handshake του WireGuard, βασισμένος σε Noise Protocol Framework, λειτούργησε ομαλά και χωρίς διακοπές, επιτρέποντας τη γρήγορη δημιουργία και τερματισμό συνδέσεων.

Σε επίπεδο σταθερότητας, το VPN διατήρησε συνεχή σύνδεση για πολλές ώρες χωρίς διακοπές, ακόμη και όταν ένας από τους clients άλλαξε δίκτυο (Wi-Fi → mobile hotspot), χάρη στη ρύθμιση PersistentKeepalive.

3.11 Αξιολόγηση Ασφάλειας

Από την πλευρά της ασφάλειας, η ανάλυση πακέτων κατέδειξε ότι:

Όλη η κυκλοφορία ήταν πλήρως κρυπτογραφημένη και μη αναγνώσιμη.Η μόνη αναγνωρίσιμη πληροφορία ήταν η πηγή και ο προορισμός σε επίπεδο IP/Port (λόγω UDP μεταφοράς), ενώ το περιεχόμενο των δεδομένων παρέμεινε κρυφό.Δεν

εντοπίστηκαν διαρροές DNS.Η σάρωση θυρών με Nmap αποκάλυψε ότι οι clients δεν ήταν απευθείας εκτεθειμένοι στο Internet. Όλες οι συνδέσεις περνούσαν μέσω του server και τα ανοικτά services των clients ήταν προσβάσιμα μόνο μέσω του VPN subnet. Αυτό αποτελεί σημαντικό στρώμα άμυνας, καθώς περιορίζει το attack surface.

3.11.1 Πλεονεκτήματα και Μειονεκτήματα που παρατηρήθηκαν

Πλεονεκτήματα:

- Απλότητα – Μικρός αριθμός εντολών και αρχείων για πλήρη λειτουργία.
- Ταχύτητα – Ελάχιστη επιβάρυνση στην ταχύτητα σύνδεσης.
- Ασφάλεια – Σύγχρονα κρυπτογραφικά πρότυπα, ισχυρό handshake.
- Σταθερότητα – Συνεχής και απρόσκοπτη λειτουργία.
- Cross-platform – Υποστήριξη σε Linux, Windows, macOS, Android, iOS.

Μειονεκτήματα:

- Στατική δρομολόγηση IP – Περισσότερη χειροκίνητη εργασία.
- Περιορισμένες δυνατότητες δυναμικής διαχείρισης σε πολύπλοκα εταιρικά περιβάλλοντα.
- Απουσία ενσωματωμένου μηχανισμού πιστοποίησης μέσω username/password – βασίζεται αποκλειστικά σε key-based authentication.

3.11.2 Μελλοντική βελτίωση και ανάπτυξη

Για να επεκταθεί η λειτουργικότητα του συστήματος μελλοντικά θα μπορούσαν να προστεθούν:

- Ενσωμάτωση dynamic DNS ώστε ο server να είναι προσβάσιμος χωρίς στατική IP.
- Ανάπτυξη multi-factor authentication σε επίπεδο εφαρμογής.
- Αυτοματοποιημένη δημιουργία client configs μέσω scripts.
- Δοκιμές σε συνθήκες υψηλής καθυστέρησης (π.χ. δορυφορικό Internet) για αξιολόγηση της ανθεκτικότητας.
- Σύγκριση με WireGuard-based mesh VPNs (π.χ. Tailscale, Netmaker).

3.12 Διαλειτουργικότητα και Αντιμετώπιση Προβλημάτων

Ένα από τα βασικά ερωτήματα της εργασίας ήταν κατά πόσο το WireGuard μπορεί να λειτουργήσει αποτελεσματικά σε **ετερογενή περιβάλλοντα**. Για τον σκοπό αυτό, ο server στο Kali Linux συνδέθηκε επιτυχώς με ένα Windows client, ενώ πραγματοποιήθηκαν πρόσθετες ρυθμίσεις για τη σύνδεση ενός ακόμη Linux-based client. Κατά τη διάρκεια της διαδικασίας, αντιμετωπίστηκαν πρακτικά ζητήματα, όπως:

- Η **σωστή αντιστοίχιση κλειδιών** μεταξύ των peers.
- Η **ρύθμιση των endpoints** για την αποφυγή σφαλμάτων σύνδεσης.
- Η **διόρθωση λανθασμένων ρυθμίσεων IP** και η εγκατάσταση απαραίτητων

πακέτων λογισμικού.

Η αντιμετώπιση αυτών των προβλημάτων συνέβαλε στη βελτίωση της κατανόησης των τεχνικών λεπτομερειών του WireGuard και ενίσχυσε την εμπιστοσύνη στη σταθερότητα του δικτύου.

3.13 Αξιολόγηση και Ανάλυση Κίνησης Δικτύου

Για την αξιολόγηση της απόδοσης και της ασφάλειας του VPN, χρησιμοποιήθηκαν εργαλεία όπως το **Wireshark** και το **tcpdump**, τα οποία επέτρεψαν την καταγραφή και ανάλυση της κίνησης των πακέτων. Πραγματοποιήθηκαν πειράματα με:

- **Απλή κίνηση δεδομένων** (ping).
- **Ασφαλή σύνδεση** (SSH).
- Μεταφορά αρχείων.
- **Σάρωση θυρών** με το εργαλείο **Nmap**.

Μέσω αυτών των δοκιμών εξετάστηκε η **ανταπόκριση του δικτύου**, η **δυνατότητα ανίχνευσης ενεργών υπηρεσιών** και η **αποδοτικότητα της κρυπτογράφησης**. Τα αποτελέσματα ανέδειξαν ότι το WireGuard προσφέρει **υψηλές επιδόσεις** και **ισχυρή προστασία δεδομένων**, επιβεβαιώνοντας την καταλληλότητά του ως λύση VPN χαμηλής πολυπλοκότητας.

3.14 Συμπεράσματα

Συνοψίζοντας, η παρούσα πτυχιακή εργασία κατέστησε δυνατή την ενδελεχή ανάλυση επιλεγμένων τεχνολογιών κυβερνοασφάλειας και την εφαρμογή μιας συγκεκριμένης σε πραγματικό περιβάλλον. Στο πλαίσιο αυτό, μελετήθηκαν οι βασικές αρχές της ασφαλούς επικοινωνίας και επιλέχθηκε η υλοποίηση του **WireGuard VPN**, λόγω της απλότητας, της επεκτασιμότητας,, της υψηλής απόδοσης και της διαθεσιμότητάς του. Οι αρχές αυτές εξασφαλίζουν ότι η προσθήκη του δεν αυξάνει σημαντικά τον φόρτο διαχείρισης, εφαρμόζεται εύκολα σε διαφορετικά δίκτυα, έχει ελάχιστες επιπτώσεις στην απόδοση και είναι εύχρηστο από τους τελικούς χρήστες.

Η μελέτη έδειξε ότι το WireGuard παρέχει ένα ολοκληρωμένο πλαίσιο ασφάλειας, συνδυάζοντας προστασία δεδομένων, έλεγχο ταυτότητας και απομόνωση του εσωτερικού δικτύου από μη εξουσιοδοτημένες προσβάσεις. Παράλληλα, η αρχιτεκτονική του το καθιστά ιδιαίτερα προσαρμοστικό στις ανάγκες των χρηστών και κατάλληλο για διαφορετικά σενάρια, από προσωπική χρήση και απομακρυσμένη πρόσβαση, έως εταιρικές υλοποιήσεις και διασύνδεση υποκαταστημάτων.

Με το περιβάλλον προσομοίωσης που δημιουργήθηκε, το WireGuard εφαρμόστηκε σε πραγματικές συνθήκες και απέδειξε ότι μπορεί να αποτελέσει έναν πρακτικό οδηγό για μελλοντικές εφαρμογές. Η υλοποίηση ανέδειξε τόσο τεχνικές δεξιότητες (παραμετροποίηση, δρομολόγηση, δοκιμές ασφάλειας) όσο και την κατανόηση θεμελιωδών αρχών όπως η αυθεντικοποίηση και η κρυπτογράφηση.

Ως τελική παρατήρηση, ο σχεδιασμός του VPN μπορεί να βελτιωθεί περαιτέρω μέσα

από μελλοντική έρευνα και πειραματισμό, ώστε να απαντηθούν ερωτήματα όπως: πώς να ελαχιστοποιηθεί ο κατακερματισμός των πακέτων, πώς να περιοριστεί η επιβάρυνση της CPU σε υφιστάμενο υλικό, ποιες μέθοδοι κρυπτογράφησης και πιστοποίησης ανταποκρίνονται καλύτερα στις ανάγκες των καταναλωτών και ποιες συμπληρωματικές λειτουργίες ασφάλειας θα μπορούσαν να ενσωματωθούν. Παράλληλα, ζητήματα όπως η υποστήριξη πολυεκπομπής και η αποφυγή τερματισμού σήραγγας αποτελούν πεδία για περαιτέρω διερεύνηση.

Συνολικά, απέδειξε ότι αποτελεί μια σύγχρονη, ευέλικτη και αποδοτική λύση VPN, ικανή να καλύψει ένα ευρύ φάσμα εφαρμογών και να αποτελέσει αξιόπιστη επιλογή για μελλοντικές αναπτύξεις σε προσωπικό και επαγγελματικό επίπεδο.

Ξενόγλωσσες βιβλιογραφικές αναφορές

Andrea, Harris. 2014. *Cisco VPN Configuration Guide.*

Aumasson, Jean-Philippe. 2018. *Serious cryptogrpahy: A Practical Introduction to Modern Encryption.* William Pollock .

B. Aboba, Microsoft, P. Calhoun, Airespace. 2003. "RFC 3579." *IETF Tools.* September. Accessed March 10, 2021. https://www.ietf.org/rfc/rfc3579.txt.

B. Aboba,Microsoft, L. Blunk, Merit Network, Inc, J. Vollbrecht, Vollbrecht Consulting LLC. 2004. "RFC 3748." *IETF Tools.* June. Accessed March 10, 2021. https://tools.ietf.org/html/rfc3748.

Battu, Daniel. 2014. *New Telecom Networks : Enterprises and Security.* ISTE Ltd and John Wiley & Sons, Inc. .

Behringer, Michael H, and Monique J. Morrow. 2005. *MPLS VPN Security.* Indianapolis: Cisco Systems, Inc.

Bollapragada, Vijay, Mohamed Khalid, and Scott Wainner. 2005. *IPSec VPN Design.* Indianapolis: Cisco Systems, Inc.

Boonkrong, Sirapat. 2021. *Authentication and Access Control: Practical Cryptography Methods and Tools.* Nakhon Ratchasima: Apress.

C. Kaufman, Microsoft, P. Hoffman, VPN Consortium, Y. Nir, Check Point, P. Eronen, Independent. 2010. "RFC 5996 ." *IETF Tools.* September. Accessed March 08, 2021. https://tools.ietf.org/html/rfc5996.

Ciesla, Robert. 2020. *Encryption for Organizations and Individuals: Basics of Contemporary and Quantum Cryptography.* HELSINKI: Apress.

Crist, Eric F, and Jan Just Keijser. 2015. *Mastering OpenVPN.* Packt Publishing Ltd.

D. Harkins, D. Carrel, cisco Systems. 1998. "RFC 2409." *IETF Tools.* November. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2409.

Dale Liu; Syngress; Stephanie Millers; Mark Lucas; Abhishek Singh; Jennifer Davis. 2006. *Firewall Policies and VPN Configurations.* Rockland: Syngress Publishing, Inc.

Downie, Ken. 2020. "Extensible Authentication Protocol (EAP) for network access." *docs.microsoft.* December 28. Accessed April 02, 2021. https://docs.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access

Dwivedi, Himanshu. 2004. *Implementing SSH: Strategies for Optimizing the Secure Shell.* Wiley Publishing, Inc.

Ghein, Luc De. 2007. *MPLS fundamentals.* Indianapolis: Cisco Press. Hassel, Jonathan. 2010. *RADIUS.* O'Reilly Media, Inc.

K. Hamzeh, Ascend Communications, G. Pall, Microsoft Corporation, W. Verthein, 3Com, J. Taarud, Copper Mountain Networks, W. Little, ECI Telematics, G. Zorn . 1999. "RFC 2637." *IETF Tools.* July. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2637.

2011. *Manual:IP/Address.* Feburary 10. Accessed Feburary 15, 2021. https://wiki.mikrotik.com/wiki/Manual:IP/Address.

2020. *Manual:IP/DHCP Server.* January 21. Accessed Feburary 15, 2021. https://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Server.

2021. *Manual:IP/IPsec.* April 1. Accessed Feburary 15, 2021. https://wiki.mikrotik.com/wiki/Manual:IP/IPsec.

Maxwell, Douglas ; Noble, James S. ; Inc. Staff Syngress Media. 2003. *Check Point NG VPN-1/FireWall-1 Advanced Configuration and Troubleshooting.* Syngress Publishing, Inc.

Microsoft Corporation. 2021. "[MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)." *docs.microsoft.* April 7. Accessed March 08, 2021. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/c50ed240-56f3-4309-8e0c-1644898f0ea8.

Montoya, Christian , Elizabeth Ross, Stef Ki, Theano Petersen, Liza Poggemeyer, and Justin Hall. 2017. "Welcome to Remote Desktop Services." *docs.microsoft.com.* Feburary 22. Accessed March 12, 2021. https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds.

Perez, André. 2014. *Network Security.* ISTE Ltd and John Wiley & Sons, Inc. Postel, J.; Reynolds, J.; ISI. 1983. "RFC 854." *IETF Tools.* May. Accessed March 10, 2021. https://tools.ietf.org/html/rfc854.

Prasad, Neeli R., and Anand R. Prasad. 2005. *802.11 LANs and IP Networking : Security, QoS, and Mobility.* Artech House.

Rosen, E., and Y. Rekhter. 1999. "RFC 2547." *IETF Tools.* March. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2547.

T. Ylonen SSH Communications Security Corp C. Lonvick, Ed. Cisco Systems, Inc. 2006c. "RFC 4252." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4252.

—. 2006b. "RFC 4253." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4253.

—. 2006d. "RFC 4254." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4254. 53

T. Ylonen, SSH Communications Security Corp, C. Lonvick, Ed., Cisco Systems, Inc. 2006a. "RFC 4251." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4251.

Tiller, James S. 2004. *A Technical Guide to IPSec Virtual Private Networks.* CRC Press LLC.

W. Townsley A. Valencia cisco Systems A. Rubens Ascend Communications G. Pall G. Zorn Microsoft Corporation B. Palter Redback Networks. 1999. "RFC 2661." *IETF Tools.* August. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2661.

Zhang, Frank. 2021. "[MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting." *docs.microsoft.com.* April 07. Accessed March 10, 2021. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/5073f4ed-1e93-45e1-b039-6e30c385867c?redirectedfrom=MSDN.