ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διπλωματική Εργασία

Βέλτιστες πρακτικές υλοποίησης VPN

Δημήτρης Αντωνούλης

Επιβλέπον Καθηγητής: Σ. Γκρίτζαλης

Πειραιάς, 2024

ΠΕΡΙΛΗΨΗ

Η διπλωματική αυτή εργασία εστιάζει στην δημιουργία μιας βέλτιστης υλοποίησης εικονικού ιδιωτικού δικτύου. Επικεντρώνεται στη διαδικασία και έρευνα η οποία απαιτείται για την επιλογή των κατάλληλων πρωτοκόλλων σήραγγας, πρωτοκόλλων κρυπτογράφησης και μηχανισμών ασφαλείας αναλύοντας τις πιο ευρέως διαδεδομένες και αξιόπιστες επιλογές του σήμερα. Η μελέτη στοχεύει να αντιμετωπίσει το ερώτημα πως ένας οργανισμός ή ένας χρήστης μπορεί να πετύχει τη βέλτιστη υλοποίηση VPN που να ανταποκρίνεται και να ταιριάζει ακριβώς στις απαιτήσεις του οργανισμού ή τις ανάγκες του αντίστοιχα. Όσον αφορά τη μεθοδολογία, η διπλωματική ακολουθεί μια πολύπλευρη προσέγγιση ξεκινώντας με ένα θεωρητικό πλαίσιο το οποίο περιλαμβάνει αναλυτική περιγραφή πρωτοκόλλων κρυπτογράφησης, μηχανισμών ελέγχου ταυτότητας, πρωτοκόλλων σήραγγας, πολιτικές ελέγχου πρόσβασης καταγραφής συμβάντων καθως και ασφαλή ρύθμιση συσκευών. Η έρευνα μέσα από την ανάλυσή της υπογραμμίζει συνεχώς τη κρίσιμη σημασία της επιλογής των κατάλληλων πρωτοκόλλων και μηχανισμών ασφαλείας για να επιτευχθεί η βέλτιστη υλοποίηση ενος εικονικού ιδιωτικού δικτύου. Παρέχοντας πληροφορίες και αναλύοντας όλα τα απαραίτητα βήματα, το θεωρητικό κομμάτι της έρευνας μπορεί να χρησιμοποιηθεί ως οδηγός για την επιλογή μιας βέλτιστης υλοποίησης εικονικού ιδιωτικού δικτύου. Η μεθοδολογία συνεχίζει με ένα πρακτικό κομμάτι όπου υλοποιήθηκε ένα εικονικό ιδιωτικό δίκτυο για έναν ατομικό χρήστη με τη χρήση OpenVPN πρωτοκόλλου. Όσον αφορά τα μέτρα ασφαλείας χρησιμοποιήθηκε έλεγχος ταυτότητας πολλαπλών παραγόντων με τη χρήση κινητής συσκευής καθώς και πρόσβαση μόνο με κλειδί SSH. Η πρακτική υλοποίηση περιγράφεται αναλυτικά βήμα προς βήμα και παρέχονται στιγμιότυπα οθόνης σε κάθε βήμα εσκεμμένα έτσι ώστε να είναι εύκολη η αναπαραγωγή της διαδικασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

I. Εισαγωγή

Ιστορικό για τα VPN

1. Ορισμός του εικονικού ιδιωτικού δικτύου (VPN)

Στη σημερινή εποχή η οποία χαρακτηρίζεται ως ψηφιακή, μια απο τις μεγαλύτερες προκλήσεις αποτελεί η ασφάλεια και η ακεραιότητα της ροής των δεδομένων. Τόσο οι οργανισμοί όσο και οι καθημερινοί χρήστες αντιλαμβάνονται τη σημασία της ασφάλειας των δεδομένων τους και για αυτόν τον λόγο έχει γίνει πρωταρχικό τους μέλημα. Οι αυξανόμενες απειλές και επιθέσεις που εμφανίζονται καθημερινά στον κυβερνοχώρο αποτελούν απόδειξη της επείγουσας ανάγκης για μια άμεση λύση, την οποία και έρχονται να δώσουν τα Εικονικά Ιδιωτικά Δίκτυα(Virtual Private Networks - VPNs).

Ένα VPN έρχεται να προσφέρει μια ασφαλέστερη, ιδιωτική και κρυπτογραφημένη διαδρομή στη μεταφορά των δεδομένων, προστατεύοντάς τα έτσι από τα αμέτρητα ευπαθή σημεία που αντιστοιχούν στο διαδίκτυο. Αναλυτικότερα, ένα VPN δημιουργεί μια εικονική σήραγγα ανάμεσα σε δύο σημεία, τον χρήστη και το διακομιστή προορισμού(destination server). Με τον τρόπο αυτόν δημιουργείται έτσι μια ιδιωτική σύνδεση δικτύου ανάμεσα σε αυτά τα δύο σημεία μέσω της οποίας οι πληροφορίες μπορούν να ταξιδεύουν με ασφάλεια.

2. Τύποι VPN

Υπάρχουν διαφορετικοί τύποι Εικονικών Ιδιωτικών Δικτύων, οι οποίοι χωρίζονται σε 3 βασικές κατηγορίες, τα site to site VPNs, τα VPN απομακρυσμένης πρόσβασης(remote access) και τα προσωπικά VPN. Κάθε μια από αυτές τις κατηγορίες είναι προσαρμοσμένη για συγκεκριμένες ανάγκες και εξυπηρετεί έναν μοναδικό σκοπό όμως όλες στοχεύουν στην βελτίωση της ασφάλειας και του απορρήτου του διαδικτύου.

Όσον αφορά την πρώτη κατηγορία, τα site to site VPNs είναι ένας τύπος VPN που χρησιμοποιείται για την ασφαλή μεταφορά δεδομένων μεταξύ γεωγραφικά απομακρυσμένων τοποθεσιών ή δικτύων [1]. Αυτός ο τύπος VPN χρησιμοποιείται κυρίως από εταιρείες με παραπάνω από ένα κτίρια τα οποία είναι απαραίτητο είτε να επικοινωνούν όλα μεταξύ τους ή να επικοινωνούν όλα τα παραρτήματα με το κύριο κτίριο. Στην περίπτωση αυτή το site to site VPN τους επιτρέπει να επικοινωνούν μεταξύ των διαφορετικών τοποθεσιών και να έχουν πρόσβαση σε πόρους του δικτύου σαν να ήταν τοπικά συνδεδεμένοι. Για να εξασφαλιστεί η ακεραιότητα, η εμπιστευτικότητα καθώς και η αυθεντικότητα των δεδομένων που ταξιδεύουν μεταξύ των τοποθεσιών, τα site to site VPNs χρησιμοποιούν πρωτόκολλα κρυπτογράφησης και σήραγγας(tunneling protocols). Οι υλοποιήσεις σε τέτοιους τύπους VPN γίνονται

μέσω των τεχνολογιών SDN(Software-Defined Networking) σε πιο σύγχρονες υλοποιήσεις και MPLS(Multi-Protocol Label Switching) σε πιο παλιές. Για το λογισμικό VPN και τις κρυπτογραφικές τεχνικές που μπορούν να χρησιμοποιηθούν για να δημιουργηθούν ασφαλή σήραγγες μεταξύ των τοποθεσιών υπάρχουν διάφορες επιλογές, χαρακτηριστικά παραδείγματα αποτελούν το SSL και η σουιτα πρωτοκολλων IPSec. Αυτός ο τύπος VPN είναι απαραίτητος για οργανισμούς και εταιρείες με πολλές εγκαταστάσεις που ανταλλάσουν δεδομένα μεταξύ των εγκαταστάσεων μέσω του διαδικτύου και αναζητούν ασφάλεια.

Τα VPN απομακρυσμένης πρόσβασης, έχουν ως στόχο να προσφέρουν την δυνατότητα σε μεμονωμένους χρήστες να συνδέονται σε ένα ιδιωτικό δίκτυο από μια απομακρυσμένη τοποθεσία είτε αυτό αναφέρεται σε εργασία από το σπίτι είτε σε κάποιο ταξίδι. Η συγκεκριμένη κατηγορία VPN λειτουργεί παρέχοντας μια ασφαλή σήραγγα μέσω της οποίας μεταφέρονται δεδομένα και προστατεύει τις ευαίσθητες πληροφορίες από οποιαδήποτε πιθανή απειλή. Αυτό είναι εξαιρετικά χρήσιμο στις εταιρείες οι οποίες επιθυμούν να προσφέρουν ευελιξία στο χώρο από τον οποίο εργάζονται οι υπάλληλοί τους, παρέχοντας με τον τρόπο αυτό ασφαλή πρόσβαση στους πόρους της εταιρείας.

Τα προσωπικά VPN έρχονται να εξυπηρετήσουν τους χρήστες οι οποίοι αναζητούν ένα έξτρα επίπεδο προστασίας στις καθημερινές διαδικτυακές τους δραστηριότητες. Αυτή η κατηγορία προσφέρει κρυπτογραφημένη σύνδεση στο διαδίκτυο και με τον τρόπο αυτό προσφέρει ένα επιπλέον επίπεδο ασφάλειας στην ιδιωτικότητα του χρήστη. Οι χρήστες χρησιμοποιούν τα VPN ως ένα πολύτιμο εργαλείο για να διαφυλάξουν τα προσωπικά τους δεδομένα και να διατηρήσουν και ασφαλίσουν το απόρρητό τους χωρίς να ανησυχούν αν ο πάροχος παρακολουθεί την δραστηριότητά τους. Άλλος ένας ακόμη συχνότερος λόγος που εμφανίστηκε όταν ρωτήθηκαν οι χρήστες γιατί χρησιμοποιούν ένα VPN είναι για να παρακολουθούν περιεχόμενο το οποίο είναι περιορισμένο σε συγκεκριμένες τοποθεσίες [2].

3. Λόγοι εφαρμογής VPN

Η τεχνολογία του ψηφιακού χώρου στις μέρες μας ολοένα και εξελίσσεται και ταυτόχρονα με αναλογικό ρυθμό αυξάνονται και οι απειλές στον κυβερνοχώρο, πράγμα που φέρνει ανησυχίες τόσο στους οργανισμούς όσο και στους απλούς χρήστες. Πλέον, καθώς η ασφάλεια της πληροφορίας και του απορρήτου είναι πρωτεύον θέμα, οι υλοποιήσεις VPN αποτελούν αναγκαιότητα και όχι επιλογή. Όσον αφορά τις εταιρείες, είναι απαραίτητο να διατηρήσουν ασφαλή τα ευαίσθητα εταιρικά δεδομένα, την επικοινωνία αλλά και τις πληροφορίες που ανταλλάσσουν οι υπάλληλοι του. Με την χρήση των VPN δημιουργούν αυτόματα μια πρόσθετη αμυνα, διασφαλίζοντας έτσι κρυπτογραφία και ασφάλεια στις πληροφορίες που μεταφέρονται στο δίκτυο της εταιρείας. Ταυτόχρονα, οι απλοί χρήστες χρησιμοποιούν τα VPN για να ενισχύσουν το απόρρητο τους και να διατηρήσουν την ανωνυμία τους. Προστατεύουν την δραστηριότητά τους τόσο από τα μάτια του παρόχου σε

καθημερινή βάση, αλλά και σε περιπτώσεις χρήσης δημόσιου Wi-Fi δικτύου από οποιονδήποτε μπορεί να παρακολουθεί το δίκτυο. Ταυτόχρονα, εμποδίζουν ιστοσελίδες και διαδικτυακές υπηρεσίες απο το να καταγράφουν την πραγματική διεύθυνση IP τους και την διαδικτυακή τους δραστηριότητα. Τέλος, όπως και προαναφέρθηκε, συχνά η χρήση VPN απο απλούς χρήστες είναι ένα μέσο για επισκεφτούν περιεχόμενο ή υπηρεσίες οι οποίες είναι περιορισμένες σε συγκεκριμένες γεωγραφικές τοποθεσίες.

Στόχος διπλωματικής εργασίας

Η συγκεκριμένη διπλωματική εργασία έχει σκοπό να χρησιμεύσει ως ένας εξαντλητικός οδηγός για μια βέλτιστη υλοποίηση εικονικού ιδιωτικού δικτύου(VPN). Με έμφαση στην ασφάλεια στον κυβερνοχώρο, διερευνά και αναλύει με λεπτομέρεια όλες τις απαραίτητες πληροφορίες τόσο σε θεωρητικό όσο και πρακτικό επίπεδο, οι οποίες είναι χρήσιμες για μια βέλτιστη υλοποίηση. Η εργασία καλύπτει με λεπτομέρεια όλες τις απαραίτητες θεμελιώδης έννοιες σε θεωρητικό επίπεδο ενώ ταυτόχρονα εμβαθύνει στην περιγραφή βήμα προς βήμα μιας υλοποίησης οικιακού VPN με τη χρήση OpenVPN και την εφαρμογή πρόσθετων μηχανισμών ασφαλείας.

Δομή διπλωματικής εργασίας

Όσον αφορά τη δομή, η διατριβή ακολουθεί μια λογική εξέλιξη που έχει σχεδιαστεί με σκοπό να διευκολύνει την έρευνα και ταυτόχρονα να ελαττώσει τη πολυπλοκότητα των εφαρμογών VPN συνολικά. Η εργασία ξεκινάει με μια λεπτομερής εξερεύνηση του ορισμού, των διαφορετικών τύπων και των λόγων ανάπτυξης του VPN. Συνεχίζοντας ακολουθεί το «Θεωρητικό Πλαίσιο» το οποίο εμβαθύνει σε βασικές έννοιες όπως η ανάλυση πρωτοκόλλων κρυπτογράφησης, οι μηχανισμοί ελέγχου ταυτότητας, τα πρωτόκολλα σήραγγας, τις πολιτικές ελέγχου πρόσβασης, τα συμβάντα καταγραφής καθώς και η ασφαλής ρύθμιση των συσκευών. Μεταβαίνοντας στη "Μεθοδολογία", η διατριβή μετατοπίζεται στην πρακτική εφαρμογή, περιγράφοντας λεπτομερώς κάθε βήμα το οποίο είναι απαραίτητο για τη δημιουργία ενός οικιακού VPN με το OpenVPN. Ακολουθεί η ενότητα ανάλυσης των αποτελεσμάτων όπου με μια σύντομη ανάλυση αξιολογείται η υλοποίηση σε επίπεδο απόδοσης ασφάλειας και ευχρηστίας. Τέλος, στην τελευταία ενότητα με τα συμπεράσματα συνοψίζονται οι στόχοι και η μεθοδολογία που ακολουθησε η διπλωματική, αναφέρεται προτεινόμενη προσέγγιση στο θέμα της διπλωματικής καθώς και προτείνονται μελλοντικές βελτιώσεις και προσθήκες.

Αυτή η δομημένη προσέγγιση εξασφαλίζει μια κατανόηση όλων των στοιχείων που οι συνδυασμοί τους θα αποτελέσουν μια βέλτιστη υλοποίηση VPN, ενώ ταυτόχρονα παρέχεται ένας λεπτομερής οδηγός για την υλοποίηση ενός ασφαλούς οικιακού εικονικού ιδιωτικού δικτύου(VPN).

ΙΙ. Θεωρητικό πλαίσιο

Σε αυτή την ενότητα θα αναλυθούν με λεπτομέρεια σε θεωρητικό επίπεδο έννοιες όπως τα πρωτόκολλα κρυπτογράφησης, οι μηχανισμοί αυθεντικοποίησης, τα πρωτόκολλα σήραγγας, οι πολιτικές ελέγχου πρόσβασης, η καταγραφή συμβάντων και η ασφαλής ρύθμιση συσκευών και ασφάλεια τελικού σημείου.

Βασικές έννοιες στις βέλτιστες πρακτικές VPN

Η αναζήτηση και έρευνα για βέλτιστες πρακτικές VPN αποτελεί μια πολυσύνθετη διαδικασία, είτε αναφέρεται σε site to site VPNs, VPN απομακρυσμένης πρόσβασης(remote access) είτε σε προσωπικά VPN. Για να επιτευχθεί μια σωστή υλοποίηση θα πρέπει να γίνει μια κατάλληλη και επαρκής έρευνα σε πρωτόκολλα κρυπτογράφησης, σε μηχανισμούς ελέγχου ταυτότητας, πρωτόκολλα σήραγγας, πολιτικές ελέγχου πρόσβασης και πρακτικές καταγραφής και ελέγχου έτσι ώστε να επιλεχθεί ο κατάλληλος τρόπος υλοποίησης του VPN για να καλύπτει τις ανάγκες με τον ασφαλέστερο δυνατό τρόπο. Για κάθε ένα από αυτά οι επιλογές ποικίλουν και η κάθε επιλογή έχει θετικά και αρνητικά που την καθιστούν μοναδική. Για αυτόν τον λόγο είναι απαραίτητη η σωστή κατανόηση και αξιολόγηση της κάθε επιλογής για να επιτευχθεί η βέλτιστη υλοποίηση VPN.

Α. Πρωτόκολλα Κρυπτογράφησης

Στα εικονικά ιδιωτικά δίκτυα το θεμέλιο για μια ασφαλή επικοινωνία είναι η κρυπτογραφία. Σε κάθε έμπιστη και καλή υλοποίηση VPN κρύβεται από πίσω μια σωστή επιλογή των κατάλληλων πρωτοκόλλων κρυπτογράφησης, έτσι ώστε να διαφυλαχθούν τα ευαίσθητα δεδομένα. Για την επαρκή κατανόηση της σπουδαιότητας της κρυπτογραφίας στην διαδικασία επιλογής της βέλτιστης υλοποίησης VPN, είναι απαραίτητη μια ανάλυση των μηχανισμών κρυπτογράφησης, των τεχνικών βάσεων και των χαρακτηριστικών ασφαλείας ανάμεσα στη σουίτα πρωτοκόλλων IPSec και στο SSL/TLS καθώς και μια αναφορά στο Wireguard.

1. IPSec

Το 1995 ο οργανισμός IETF (Internet Engineering Task Force) δημοσιοποίησε ένα standard για πολλούς σκοπούς ασφάλειας του πρωτοκόλλου διαδικτύου, το IPSec (Internet Protocol Security) [3].Το IPSec είναι μια σουίτα πρωτοκόλλων η οποία παρέχει διάφορες υπηρεσίες ασφάλειας μέσω των οποίων φροντίζει για την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα της κίνησης των πακέτων [4]. Περιλαμβάνει πολλαπλές κρυπτογραφικές σουίτες, δύο πρωτόκολλα το Authentication Header (AH) και το Encrypted Security Payload (ESP) και έχει δύο τρόπους λειτουργίας και αυτοί είναι η λειτουργία μεταφοράς και η λειτουργία σήραγγας. Το IPSec αποτελεί σημαντικό υποψήφιο για επιλογή όταν πρόκειται για

θέματα κρυπτογραφίας στα VPNs καθώς αυξάνει σημαντικά την ασφάλεια και για αυτό αποδεικνύεται τόσο χρήσιμο και χρησιμοποιείται συχνά σε συνδυασμό με κάποια άλλα πρωτόκολλα σήραγγας όπως για παράδειγμα το L2TP(Layer 2 Transfer Protocol). Παρόλα αυτά, εμφανίζει μερικά αρνητικά στο τεχνικό κομμάτι καθώς οι πολλαπλές επιλογές που δίνει και η δυνατότητα για πλήρες έλεγχο των ρυθμίσεών τους, συχνά το καθιστούν αποθαρρυντικό.

2. SSL/TLS

Σημαντικό ρόλο στην κρυπτογραφία των VPN παιζουν επίσης και τα πρωτόκολλα SSL/TLS. Το 1999 κυκλοφόρησε το TLS(Transport Layer Security) το οποίο αποτελεί αναβάθμιση του SSL (Secure Sockets Layer) 3.0 το οποίο κυκλοφόρησε το 1996. Τα πρωτόκολλα SSL/TLS χρησιμοποιούνται στα VPN για να δημιουργούν μια ασφαλής σήραγγα στο διαδίκτυο από την οποία περνάνε τα δεδομένα. Παρέχουν κρυπτογραφημένη επικοινωνία και με τη χρήση τους εξασφαλίζεται η ασφαλής μεταφορά δεδομένων μεταξύ του χρήστη και του διακομιστή(server) προστατεύοντας το από οποιαδήποτε υποκλοπή επικοινωνίας. Ταυτόχρονα παρέχει και αυθεντικοποίηση η οποία επιτρέπει και στον χρήστη αλλά και στον διακομιστή να επαληθεύουν την ταυτότητα ο ένας του άλλου. Τέλος, φροντίζει για την ακεραιότητα των δεδομένων έτσι ωστε να μην μπορεί η πληροφορία να αλλοιωθεί. Το SSL/TLS καταφέρνει να παρέχει κρυπτογραφία στην επικοινωνία με κρυπτογραφικούς αλγόριθμους, αυθεντικοποίηση με ψηφιακά πιστοποιητικά και ακεραιότητα με συναρτήσεις hash προσφέροντας έναν μεγάλο βαθμό ασφάλειας.

3. Wireguard

Όσον αφορά την κρυπτογραφία στα VPN, είναι γνωστό ότι κυρίαρχες θέσεις έχουν τα πρωτόκολλα IPSec και SSL/TLS. Παρόλα αυτά μια αξιοσημείωτη προσθήκη τα τελευταία χρόνια είναι το Wireguard. Το Wireguard χρησιμοποιεί μια ξεχωριστή προσέγγιση στην ασφαλή επικοινωνία καθώς επιλέγει ένα μοντέλο peer-to-peer. Βασισμένο στην απλότητα, το wireguard είναι ένα πρωτόκολλο επικοινωνίας για την υλοποίηση ασφαλών ιδιωτικών εικονικών δικτύων και βασίζει τη κρυπτογραφία του στις curve25519 και chacha20. Χρησιμοποιεί την Poly1305 συνάρτηση κατακερματισμού για αυθεντικοποίηση και τις συναρτήσεις SipHash24 και BLAKE2 για ιδιωτικά κλειδιά. Σε αντίθεση με το IPSec και το SSL/TLS αποτελεί ένα ολόκληρο πρωτόκολλο VPN και όχι απλώς ένα πρόσθετο επίπεδο ασφαλείας. Λειτουργεί ανεξάρτητα δημιουργώντας κρυπτογραφημένες σήραγγες μεταξύ δύο peers όπου ο καθένας προσδιορίζεται με δικό του ζεύγος δημοσιου και ιδιωτικου κλειδιού, προσδίδοντας έτσι ασφάλεια. Το βασικό του πλεονέκτημα είναι η απλότητα. Διαθέτει μια μόνο κρυπτογραφική σουίτα και έχει εξαλειφθεί εντελώς η φάση διαπραγμάτευσης της έκδοσης του πρωτοκόλλου [3]. Επιπρόσθετα, ως χαρακτηριστικό πρόσθετης ασφάλειας, δεν υπάρχει συγκεκριμένη θύρα στην οποία λειτουργεί επομένως το καθιστά πιο δύσκολο για σαρώσεις στο δίκτυο να αντιληφθούν την παρουσία του.

Β. Μηχανισμοί Αυθεντικοποίησης

Η ασφαλής πρόσβαση είναι ένα από τα πρωτεύοντα θέματα στα εικονικά ιδιωτικά δίκτυα και λύση έρχονται να δώσουν οι μηχανισμοί ελέγχου ταυτότητας. Μέσω των διαφόρων μηχανισμών αυθεντικοποίησης, διασφαλίζεται η πρόσβαση αποκλειστικά και μόνο σε εξουσιοδοτημένες οντότητες. Σε αυτήν την ενότητα θα αναφερθούν και αναλυθούν τρεις συγκεκριμένοι μηχανισμοί ελέγχου ταυτότητας και αυτοί είναι ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA), ο έλεγχος ταυτότητας μέσω πιστοποιητικών και ο παραδοσιακός έλεγχος ταυτότητας με διαπιστευτήρια. Για κάθε ένα από τα παραπάνω θα αναφερθούν οι τρόποι λειτουργίας τους καθώς και ο τρόπος με τον οποίο το κάθε ένα από αυτά ενισχύει την ασφάλεια στα εικονικά ιδιωτικά δίκτυα.

1. Έλεγχος Ταυτότητας πολλαπλών παραγόντων

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων(MFA) είναι μια τεχνική η οποία ενισχύει τα μέτρα ασφαλείας που έχουμε ήδη θέσει. Αποτελεί ένα πρόσθετο βήμα στην διαδικασία σύνδεσης του χρήστη και μπορεί να γίνει με διάφορους τρόπους. Ουσιαστικά, η τεχνική αυτή έχει ως προαπαιτούμενο είτε κάτι που ξέρει ο χρήστης όπως για παράδειγμα έναν αριθμό PIN ή μια προαποφασισμένη ερώτηση που μόνο ο χρήστης μπορεί να απαντήσει, κάτι που έχει όπως είναι μια εφαρμογή ελέγχου ταυτότητας ή ένα κείμενο επιβεβαίωσης που θα του σταλεί στο κινητό, είτε τέλος κάτι που είναι, όπως ένα δακτυλικό αποτύπωμα ή σάρωση προσώπου. Όλοι οι παραπάνω παράγοντες μπορούν να υλοποιηθούν συνδυαστικά για να προσφέρουν πρόσθετη ασφάλεια στην αυθεντικοποίηση του χρήστη. Η υλοποίηση τεχνικών ελέγχου ταυτότητας πολλαπλών παραγόντων όπως αναφέρει η Microsoft μπορεί να μειώσει έως και 99% την πιθανότητα να σε παραβιάσουν [5].

2. Έλεγχος ταυτότητας μέσω πιστοποιητικών

Άλλος ένας τρόπος με τον οποίο αποφεύγεται η πρόσβαση σε μη εξουσιοδοτημένους χρήστες είναι ο έλεγχος ταυτότητας με τη χρήση πιστοποιητικών. Τα ψηφιακά πιστοποιητικά βασίζονται στην υποδομή δημοσίου κλειδιού(PKI) κάτι που τα καθιστά δύσκολα να πλαστογραφηθουν. Ταυτόχρονα, δεν κινδυνεύουν από επιθέσεις επαναλαμβανόμενων προσπαθειών όπως άλλοι μέθοδοι ελέγχου ταυτότητας και για τους λόγους αυτούς τα ψηφιακά πιστοποιητικά είναι αρκετά αποτελεσματικά.

Ο τρόπος με τον οποίο λειτουργούν ξεκινάει με τον χρήστη να ζητά ένα ψηφιακό πιστοποιητικό από μια αρχή έκδοσης πιστοποιητικών(CA). Η αρχή έκδοσης πιστοποιητικών σε μια εταιρεία αποτελεί μια ομάδα η οποία είναι υπεύθυνη για την διαχείριση και την έκδοση ψηφιακών πιστοποιητικών σε όποιον το χρειάζεται μέσα στην εταιρεία, είτε αυτός είναι υπάλληλος είτε κάποιος συνεργάτης. Στη συνέχεια, η CA επαληθεύει την ταυτότητα του χρήστη με αυστηρότητα το οποίο συνήθως γίνεται

απαιτώντας νόμιμα έγγραφα που να επαληθεύουν την ταυτότητά του. Μετά την επαλήθευση ο χρήστης δημιουργεί ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού όπου το δημόσιο κλειδι περιλαμβάνεται στο πιστοποιητικό ενώ το ιδιωτικό είναι μυστικό και χρησιμοποιείται για αποκρυπτογράφηση και ψηφιακή υπογραφή. Τέλος, η αρχή έκδοσης πιστοποιητικών εκδίδει το ψηφιακό πιστοποιητικό με το δημόσιο κλειδί του χρήστη, πληροφορίες του χρήστη και την ψηφιακή υπογραφή της αρχής ώστε να αποδεικνύεται ότι είναι γνήσιο το πιστοποιητικό. Έτσι η ταυτότητα του χρήστη μπορεί να επαληθεύεται δημιουργώντας μια ασφαλή και αξιόπιστη σύνδεση.

Αξίζει να αναφερθεί ότι τα πιστοποιητικά έχουν συγκεκριμένη περίοδος ισχύος που ορίζεται κατα την έκδοση και πρέπει να ανακαλούνται σε περίπτωση λήξης της συνεργασίας με τον χρήστη ή να ανανεώνονται σε περίπτωση που λήγουν πριν να είναι απαραίτητο. Η χρήση των ψηφιακών πιστοποιητικών αποτελούν μια πολύ καλή τεχνική για ασφαλή επικοινωνία βοηθούν στην αποφυγή μη εξουσιοδοτημένης πρόσβασης και ταυτόχρονα ενισχύουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων που μεταδίδονται μέσω των εικονικών ιδιωτικών δικτύων.

3. Έλεγχος ταυτότητας με διαπιστευτήρια

Ο πιο γνωστός και ευρέως διαδεδομένος τρόπος για έλεγχο ταυτότητας των χρηστών είναι μέσω διαπιστευτηρίων. Το όνομα και κωδικός πρόσβασης είναι ότι περιμένει κάθε χρήστης όταν αναφερόμαστε σε έλεγχο ταυτότητας και παρόλο που συμβάλλει στην ασφάλεια των εικονικών ιδιωτικών δικτύων, είναι ταυτόχρονα επιρρεπές σε πολλές επιθέσεις. Τα διαπιστευτήρια και πιο συγκεκριμένα οι κωδικοί πρόσβασης αποτελούν τον πιο συχνό στόχο για επιθέσεις ωμής βίας [3] καθώς βασίζονται απόλυτα στον ανθρώπινο παράγοντα. Απαιτούν από τον χρήστη πλήρη επίγνωση του κινδύνου που διατρέχει έτσι ώστε να λαμβάνει τα κατάλληλα μέτρα όσον αφορά την τυχαιότητα και το μήκος του κωδικού του, τον τρόπο με τον οποίο τον απομνημονεύει καθώς και το πόσο συχνά τον ανανεώνει να αποτελούν αποκλειστικά δική του ευθύνη. Για τις εταιρείες κάτι τέτοιο ισοδυναμεί με μεγάλο ρίσκο καθώς από ένα και μόνο λάθος μπορεί να παραβιαστούν και εκτεθούν οι πόροι της εταιρείας, πράγμα που σημαίνει μεγάλη απώλεια για την εταιρεία σε οικονομικό και όχι μόνο επίπεδο. Αυτό καθιστά τον συνδυασμό των παραπάνω μεθόδων απαραίτητο για τον σωστό έλεγχο ταυτότητας των χρηστών και την κατάλληλη προστασία στην ακεραιότητα και εμπιστευτικότητα των δεδομένων.

Γ. Πρωτόκολλα Σήραγγας

Στα εικονικά ιδιωτικά δίκτυα το θεμελιώδες στοιχείο το οποίο είναι υπεύθυνο για την μεταφορά πληροφοριών με ασφάλεια στο διαδίκτυο είναι τα πρωτόκολλα σήραγγας. Στην παρακάτω ενότητα θα ακολουθήσει μια ανάλυση και διερεύνηση του τρόπου λειτουργίας αλλά και της ασφάλειας την οποία παρέχουν πρωτόκολλα όπως

είναι το Layer 2 Tunneling Protocol(L2TP), Point-To-Point Tunneling Protocol(PPTP) και το OpenVPN. Για κάθε ένα από αυτά θα αναφερθούν πληροφορίες όπως τα πλεονεκτήματα και τα μειονεκτήματα του καθενος καθώς και τρωτά σημεία που σχετίζονται με το κάθε πρωτόκολλο. Θα καλυφθούν επίσης τεχνικές αρχιτεκτονικές καθώς και τα χαρακτηριστικά ασφάλειας έτσι ώστε να υπάρχει μια σαφής αντίληψη για το κάθε ένα πρωτόκολλο. Η ανάλυση αυτή είναι απαραίτητη όταν πρόκειται να αποφασίσουμε την βέλτιστη υλοποίηση εικονικού ιδιωτικού δικτύου καθώς είναι σημαντικό να έχουν αναλυθεί οι επιλογές που υπάρχουν στα πρωτόκολλα σήραγγας απο τις οποίες θα γίνει η τελική επιλογή.

1. Layer 2 Tunneling Protocol

Το L2TP είναι ένα πρωτόκολλο σήραγγας το οποίο κάνει encapsulate(ενθυλακώνει) τα δεδομένα που μεταδίδονται και δημιουργεί μια σήραγγα μεταξύ του αποστολέα και του παραλήπτη. Λειτουργεί στο επίπεδο 2 του μοντέλου OSI και χρησιμοποιεί συνήθως την θύρα UDP 1701 για επικοινωνία, πληροφορία η οποία είναι αρκετά χρήσιμη όταν διαμορφώνονται οι ρυθμίσεις του τείχους προστασίας. Όσον αφορά τα πλεονεκτήματά του, το L2TP υποστηρίζεται ευρέως πράγμα που είναι πολύ βολικό, είναι γνωστό για την απλότητα και την ευκολία με την οποία ρυθμίζεται. Το πιο σημαντικό από όλα ωστόσο τα θετικά του είναι ότι δεν υπάρχουν έως τώρα γνωστές ευπάθειες [6] κάτι που το καθιστά αξιόπιστο και επιλέγεται συχνά για υλοποίησης απομακρυσμένης σύνδεσης καθώς και site-to-site. Παρόλα αυτά, το L2TP από μόνο του, δεν παρέχει κάποια κρυπτογράφηση ούτε επαληθεύει μεμονωμένα μηνύματα. Για να ξεπεραστεί αυτή η αδυναμία συνήθως χρησιμοποιείται σε συνδυασμό με το IPSec. Με τον τρόπο αυτό προστίθεται ένα επίπεδο ελέγχου ταυτότητας και ταυτόχρονα κρυπτογράφησης καθώς τα πακέτα L2TP πακέτα είναι πλέον πακεταρισμένα σε IPSec πακέτα στο επίπεδο δικτύου [7]. Ο συνδυασμός αυτός L2TP και IPSec επιλέγεται συχνά καθώς τα παρέχει όλα αλλά το γεγονός ότι το πρωτόκολλο από μόνο του χρειάζεται και τη βοήθεια της σουίτας πρωτοκόλλων IPSec για να καλύπτει πλήρως το επίπεδο ασφάλειας μπορεί να αποτελέσει μειονέκτημα.

2. Point-To-Point Tunneling Protocol

Το PPTP δημιουργήθηκε το 1996 και τυποποιήθηκε σε RFC 2637 το 1999. Είναι ένα από τα πρώτα πρωτόκολλα VPN και ως πρωτόκολλο σήραγγας και αυτό ενθυλακώνει τα πακέτα δεδομένων μεταξύ ενός απομακρυσμένου χρήστη και ενός διακομιστή μέσω του διαδικτύου δημιουργώντας μια ασφαλή διαδρομή για τη διέλευση των δεδομένων. Χρησιμοποιεί την θύρα TCP 1723 και για την κυκλοφορία των δεδομένων το πρωτόκολλο Generic Routing Encapsulation. Απο προεπιλογή το PPTP δεν προσφέρει λειτουργίες κρυπτογράφησης ή ελέγχου ταυτότητας [8] αλλά χρησιμοποιεί το Microsoft Point-to-Point Encryption για κρυπτογραφία που και πάλι θεωρείται ασθενές. Όσον αφορά τα πλεονεκτήματα, το PPTP είναι συμβατό με τα περισσότερα λειτουργικά συστήματα και είναι γνωστό για την απλότητα στην

εγκατάσταση και στις ρυθμίσεις του πράγμα που το καθιστά μια γρήγορη λύση VPN. Παρόλα αυτά, η ασφάλεια του PPTP δεν είναι επαρκής για τα σημερινά δεδομένα. Έχει διάφορες ευπάθειες και η κρυπτογράφηση που χρησιμοποιεί είναι αδύναμη και υπάρχουν γνωστές επιθέσεις που έχει δεχτει. Πλέον το PPTP, δεν χρησιμοποιείται συχνά λόγω της αδύναμης ασφάλειας του και όσοι μικροι, μεσαιοι και μεγάλοι οργανισμοί το χρησιμοποιούν, συνίσταται να σταματήσουν [9].

3. OpenVPN

Το OpenVPN είναι ένα πρωτόκολλο VPN ανοιχτού κώδικα και αναφέρεται συχνά ως SSL VPN καθώς χρησιμοποιεί SSL/TLS για την ανταλλαγή κλειδιών. Ενθυλακώνει τα πακέτα σε σήραγγες SSL/TLS για να παρέχει ασφαλή διέλευση των δεδομένων στο διαδίκτυο [10]. Χρησιμοποιεί την βιβλιοθήκη OpenSSL για κρυπτογράφηση και έτσι υποστηρίζει διάφορους κρυπτογραφικούς αλγόριθμους παρέχοντας επιλογές στον χρήστη ο οποίος μπορεί να επιλέξει και να ορίσει αυτός το επίπεδο ασφαλείας. Για ελέγχους ταυτότητας, υποστηρίζει πολλές μεθόδους όπως είναι τα προ-κοινοποιημένα κλειδιά, τα ψηφιακά πιστοποιητικά και η χρήση διαπιστευτηρίων. Χρησιμοποιεί την θύρα 1194 και μπορεί να ρυθμιστεί να χρησιμοποιεί είτε το πρωτόκολλο TCP είτε το UDP. Όσον αφορά τα πλεονεκτήματά του, το OpenVPN επωφελείται από το γεγονός ότι είναι ανοιχτού κώδικα και έχει μια ζωντανή κοινότητα προγραμματιστών. Επίσης είναι συμβατό με διάφορα λειτουργικά συστήματα, συμπεριλαμβανομένου και των Windows, Linux, MacOS, Android και iOS. Παρά τα θετικά στην ασφάλειά του το OpenVPN όσον αφορά την απόδοση έχει χώρο για βελτίωση καθώς μπορεί να επηρεαστεί από παράγοντες όπως είναι οι συνθήκες δικτύου και οι ρυθμίσεις κρυπτογράφησης που θα επιλέξει ο χρήστης.

Γ. Πολιτικές Ελέγχου Πρόσβασης

Πολιτικές ελέγχου πρόσβασης ονομάζουμε μια ομάδα κανόνων και οδηγιών οι οποίες ορίζουν πως συσκευές, χρήστες και συστήματα μπορούν να αλληλεπιδρούν με διάφορους πόρους μέσα σε ένα σύστημα ή ένα δίκτυο. Τέτοιες πολιτικές είναι απαραίτητες σε έναν οργανισμό ιδιαίτερα σε ένα εταιρικό περιβάλλον όπου οι υπάλληλοι συνδέονται στο εταιρικό δίκτυο με απομακρυσμένη πρόσβαση μέσω εικονικών ιδιωτικών δικτύων. Περιορίζουν τη ζημιά σε περίπτωση μη εξουσιοδοτημένης πρόσβασης ή κάποιας άλλης κακόβουλης κίνησης εντός του δικτύου ή του συστήματος καθώς περιορίζουν τα προνόμια των χρηστών, των εφαρμογών και των συστημάτων. Μερικές απο τις πολιτικές ελέγχου πρόσβασης αποτελούν η Αρχή των ελαχίστων προνομίων(Principle of Least Privilege) και ο έλεγχος πρόσβασης βάση ρόλων (Role-Based Access Control).

1. Αρχή των ελαχίστων προνομίων

Ο τρόπος με τον οποίο λειτουργεί η αρχή των ελαχίστων προνομίων είναι περιορίζοντας τις άδειες των χρηστών ή του συστήματος στο ελάχιστο το οποίο είναι

απαραίτητο για τις εργασίες που είναι υπεύθυνος να φέρει εις πέρας. Αυτό είναι ιδιαίτερα κρίσιμο στα εικονικά ιδιωτικά δίκτυα καθώς διασφαλίζει ότι όλοι οι απομακρυσμένοι υπάλληλοι έχουν μόνο την απαραίτητη πρόσβαση μειώνοντας έτσι σε μεγάλο βαθμό τη ζημιά μιας κακόβουλης κίνησης ή κακής χρήσης. Έτσι γίνεται ένα πολύ καλό εργαλείο απέναντι στην μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητους πόρους της εταιρίας ενισχύοντας την ασφάλεια στην απομακρυσμένη πρόσβαση [11]. Αναλυτικότερα, η αρχή των ελαχίστων προνομίων διασφαλίζει ότι ο κάθε ένας χρήστης VPN έχει πρόσβαση μόνο σε συγκεκριμένες λειτουργίες που του είναι απαραίτητες για να διεκπεραιώσει τις εργασίες του με αποτελεσματικότητα μειώνοντας έτσι σημαντικά τον χώρο στον οποίο μπορεί να γινει μια επίθεση. Ταυτόχρονα, καθώς οι ενέργειες των χρηστών είναι συνδεδεμένες με συγκεκριμένα προνόμια που τους έχουν δοθεί ο οργανισμός μπορεί να επικαλεστεί την λογοδοσία σε περιπτώσεις στις οποίες εντοπίζει αποκλίσεις. Όσον αφορά τα αρνητικά της αρχής των ελαχίστων προνομίων μπορεί να είναι η αρνητική στάση και η δυσαρέσκεια των χρηστών με τον τρόπο λειτουργίας του συστήματος καθώς θα έχουν συνηθίσει ίσως σε μια πιο ευρύτερη πρόσβαση.

2. Έλεγχος πρόσβασης βάση ρόλων

Ακόμα μια πολύ καλή πολιτική για έλεγχο πρόσβασης είναι ο έλεγχος πρόσβασης βάση ρόλων. Η συγκεκριμένη τεχνική οργανώνει τα δικαιώματα και προνόμια των χρηστών ορίζοντας τους ρόλους. Δημιουργούνται ρόλοι με προσοχή οι οποίοι εξοπλίζονται με συγκεκριμένα προνόμια που ποικίλλουν ανάλογα με τον ρόλο και τα καθήκοντα που θα έχουν όσοι πρόκειται να περιλαμβάνονται σε αυτόν τον ρόλο. Με τη χρήση του RBAC απλοποιείται και ταυτόχρονα ενισχύεται η ασφάλεια και η διαχείριση πρόσβασης στα VPN, διασφαλίζοντας ότι ο κάθε χρήστης ο οποίος δουλεύει εξ αποστάσεως ή χρησιμοποιεί το VPN της εταιρείας, έχει τα κατάλληλα προνόμια. Μια σωστή υλοποίηση αυτού του μοντέλου η οποία λαμβάνει υπόψη την αρχή του ελάχιστου προνομίου διασφαλίζει ότι οι χρήστες έχουν πρόσβαση μόνο σε αυτά που χρειάζονται και τίποτα περισσότερο ενισχύοντας σε μεγάλο βαθμό την ασφάλεια [12]. Ταυτόχρονα, το συγκεκριμένο μοντέλο επιτρέπει στον οργανισμού να προσαρμόζει τους ρόλους καθώς εξελίσσεται η εταιρία και οι ευθύνες του κάθε ρόλου αυξάνονται ή αλλάζουν προσφέροντας έτσι μια ευελιξία. Όσον αφορά τις προκλήσεις που έχει η υλοποίηση του ελεγχου προσβασης βαση ρόλων είναι η σωστή και στρατηγικά μελετημένη δημιουργία των ρόλων με τον κατάλληλο τρόπο ώστε να είναι αρκετός για την αποτελεσματική εργασία των υπαλλήλων εξ αποστασεως αλλά ταυτόχρονα να προστατεύει την εταιρία απο περιττή πρόσβαση που δεν χρειάζεται να έχουν οι ρόλοι αυτοί.

Δ. Καταγραφή Συμβάντων

Οι δύο σημαντικότεροι τρόποι καταγραφής συμβάντων είναι το logging και το auditing. Ξεκινώντας με το logging, ονομάζεται η διαδικασία κατα την οποία καταγράφονται συστηματικά τα γεγονότα, οι δραστηριότητες και οι συναλλαγές σε μια

υποδομή εικονικού ιδιωτικού δικτύου. Καταγράφονται πληροφορίες οι οποίες αποθηκεύονται σε αρχεία καταγραφής και μέσα σε αυτά περιλαμβάνονται δεδομένα όπως οι συνδέσεις χρηστών καθώς και η ώρα σύνδεσης και όλες οι προσπάθειες πρόσβασης ενός χρήστη λόγω εσφαλμένου κωδικού καθώς και άλλες ενέργειες. Αυτά τα αρχεία είναι πολύ χρήσιμα σε περίπτωση κάποιου περιστατικού ασφαλείας καθώς μπορούν να χρησιμοποιηθούν μετά το περιστατικό και να μελετηθούν οι καταγεγραμμένες πληροφορίες. Με την λέξη auditing, αναφερόμαστε στην διαδικασία συστηματικής εξέτασης και αξιολόγησης των αρχείων καταγραφής για να διασφαλιστεί οτι ακολουθούνται όλοι οι κανόνες και οι πολιτικές ασφάλειας που έχουν τεθεί από τον οργανισμό. Η διαδικασία περιλαμβάνει τον έλεγχο των δραστηριοτήτων ενός χρήστη, των συμβάντων του συστήματος καθώς και όποιας άλλης πληροφορίας περιλαμβάνεται στα αρχεία συμβάντων. Αυτή η διαδικασία είναι πολύ σημαντική για την ασφάλεια καθώς αναλύει την συμπεριφορά των χρηστών και εντοπίζει νωρίς την ύποπτη συμπεριφορά που συχνα σημαίνει μη εξουσιοδοτημένη πρόσβαση.

Ο συνδυασμός των δύο αυτών τεχνικών στα εικονικά ιδιωτικά δίκτυα είναι απαραίτητος για την ασφάλεια του οργανισμού. Με τη διαδικασία καταγραφής του logging, ο οργανισμός έχει στη διάθεση του αρχεία με χρονολογικά ταξινομημένες τις ενέργειες του χρήστη πράγμα που στην ασφάλεια είναι πολύ χρήσιμο. Τέτοιες πληροφορίες μπορούν να χρησιμοποιηθούν για εγκληματολογική ανάλυση πράγμα που αυτόματα αναβαθμίζει την ασφάλεια σε επίπεδο εντοπισμού, απόκρισης και πρόληψης συμβάντων ασφαλείας. Ταυτόχρονα, με το auditing να γίνεται συστηματικά, διασφαλίζεται ότι οι ενέργειες των χρηστών είναι ευθυγραμμισμένες με τις πολιτικές του οργανισμού παρέχοντας έτσι μια ζωντανή εικόνα για την ασφάλεια του οργανισμού ενώ ταυτόχρονα διευκολύνεται η διαδικασία λογοδοσίας σε περίπτωση λάθους ή κακόβουλης κίνησης. Μαζί οι δύο αυτές τεχνικές βοηθούν κάθε εταιρεία να βελτιώνεται, αναβαθμίζει και διορθώνει συνεχώς τις τεχνικές ασφαλείας.

Ε. Ασφαλής ρύθμιση συσκευών και ασφάλεια τελικού σημείου

Στη συνέχεια, αναλύονται δυο πολύ κρισιμοι παράγοντες για την ασφάλεια στην αναζήτηση για μια υλοποίηση εικονικού ιδιωτικού δικτύου, η ασφαλής ρύθμισης των συσκευών και η ασφάλεια τελικού σημείου(Endpoint Security). Αναφερόμενοι σε διακομιστές, δρομολογητές και όλες τις συσκευές ενός οικοσυστήματος εικονικού ιδιωτικού δικτύου, η σωστή ρύθμιση όλων αυτών με έμφαση στην ασφάλεια είναι αυτό που στοχεύει να πετυχει η ασφαλής ρύθμιση των συσκευών. Με τον τρόπο αυτό ο οργανισμός ελαχιστοποιεί τους κινδύνους ασφαλείας με μια διαδικασία αναζήτησης των κατάλληλων πρωτοκόλλων κρυπτογράφησης, μηχανισμών ελέγχου πρόσβασης και τη σωστή υλοποίησή τους, η οποία χρειάζεται να γίνει μια φορά κατά την εγκατάσταση των συσκευών. Ταυτοχρόνως, η ασφάλεια τελικού σημείου εστιάζει να προστατεύει μεμονωμένες συσκευές που συνδέονται στο εικονικό ιδιωτικό δίκτυο οι οποίες συνήθως είναι χρήστες που εργάζονται με απομακρυσμένη πρόσβαση.

1. Ασφαλής ρύθμιση και διαμόρφωση συσκευών

Όταν ο οργανισμός ή ενας χρήστης χρειάζεται μια υλοποίηση εικονικού ιδιωτικού δικτύου η ασφάλεια θα πρέπει να είναι πρωτεύον ζήτημα απο την πρώτη μέρα. Η ασφαλής ρύθμιση και διαμόρφωση των συσκευών αναφέρεται στην ελαχιστοποίηση των κινδύνων ασφαλείας από την αρχή της υλοποίησης. Η διαδικασία περιλαμβάνει τη σωστή ρύθμιση των συσκευών όπως δρομολογητές και διακομιστές με προτεραιότητα στην ασφάλεια αλλά και η σωστή επιλογή των μεθόδων ασφαλείας. Με στόχο την ασφάλεια στο οικοσύστημα του εικονικού ιδιωτικού δικτύου θα πρέπει γίνει εκτενής εξερεύνηση για τις κατάλληλες και πιο συνήθης τάσεις για το είδος του εικονικού ιδιωτικού δικτύου που θα υλοποιηθεί. Για μια σωστή υλοποίηση θα πρέπει να διερευνηθούν οι επιλογές που υπάρχουν σε πρωτόκολλα κρυπτογράφησης, μηχανισμούς ελέγχου πρόσβασης και να επιλεχθούν οι κατάλληλες και πιο ασφαλής επιλογές για το κάθε ένα από αυτά. Η έρευνα θα πρέπει να καλύπτει μεχρι και τις πιο πρόσφατες απειλές στον κυβερνοχώρο για να γίνει μια σωστή ανάλυση των πρωτοκόλλων που δεν πάσχουν από ευπάθειες και τέλος μια κατάλληλη επιλογή ενος απο αυτά. Ταυτόχρονα, θα αφού επιλεχθεί το πρωτόκολλο κρυπτογράφησης, οι μηχανισμοί ελέγχου πρόσβασης το πρωτόκολλο σήραγγας και όλα τα υπόλοιπα μέτρα ασφαλείας, θα πρέπει να ρυθμιστούν με ασφαλή τρόπο όλες οι συσκευές εντός του οικοσυστήματος του εικονικού ιδιωτικού δικτύου έτσι ώστε να μην υπάρξουν κενά ασφαλείας λόγω κακών ρυθμίσεων, να παρακολουθούνται οι τελευταίες εξελίξεις για καινούργιες ευπάθειες στον κυβερνοχώρο και να ενημερώνονται καταλλήλως τα λογισμικά των συσκευών.

2. Ασφάλεια τελικού σημείου

Πιο έντονα εφαρμόσιμη σε περιπτώσης απομακρυσμένης πρόσβασης αλλά εξίσου σημαντική είναι κ η ασφάλεια τελικού σημείου. Η ασφάλεια τελικού σημείου αναφέρεται κυρίως σε μεμονωμένες συσκευές τελικού σημείου οι οποίες είναι συνδεδεμένες με το εικονικό ιδιωτικό δίκτυο. Εστιάζει κυρίως σε περιπτώσεις που αφορούν συνδέσεις εξ αποστάσεως, συνθήκες αρκετά συνηθισμένες σε έναν οργανισμό και φροντίζει να ασφαλίζει τις συσκευές αυτές είτε είναι λάπτοπ, τάμπλετ ή κινητό. Ως στόχο έχει να προστατεύσει αυτές τις συσκευές από απειλές όπως κακόβουλο λογισμικό ή υποκλοπή πληροφορίας. Αυτό μπορεί να το πετυχει με διάφορους τρόπους όπως η χρήση antivirus και anti malware λογισμικών, ρυθμίσεις firewalls που εντοπίζουν και αποτρέπουν απειλές καθώς και μηχανισμούς αυθεντικοποίησης όπως τα ψηφιακά πιστοποιητικά και ο έλεγχος ταυτότητας πολλαπλών παραγόντων για να επαληθεύεται η ταυτότητα των χρηστών αλλά και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση. Όλοι αυτοί η μηχανισμοί ασφαλείας που προσφέρει η ασφάλεια τελικού σημείου, είναι πολύ σημαντικοί καθώς ενισχύουν σε μεγάλο βαθμό την ασφάλεια του οικοσυστήματος του εικονικού ιδιωτικού δικτύου.

III. Μεθοδολογία

Στην ενότητα αυτή θα ακολουθήσει λεπτομερής παρουσίαση βήμα προς βήμα της υλοποίησης του εικονικού ιδιωτικού δικτύου με OpenVPN. Αναφέρονται εκτός απο τα βήματα και οι εντολές που θα εκτελεστούν ενώ ταυτόχρονα παρουσιάζονται πολλά κομμάτια και σε στιγμιότυπα οθόνης.

Α. Περιγραφή Εφαρμογής Οικιακού VPN

Στη συγκεκριμένη ενότητα παρουσιάζεται η προσέγγιση που ακολουθήθηκε για την υλοποίηση ενός οικιακού εικονικού ιδιωτικού δικτύου με πρόσθετα μέτρα ασφαλείας. Ο στόχος της υλοποίησης ήταν να δημιουργηθεί μια ασφαλής και πρακτική λύση εικονικού ιδιωτικού δικτύου και να περιγραφεί ώστε να λειτουργήσει ως εγχειρίδιο για όλους τους χρήστες που επιθυμούν να δημιουργήσουν ένα αποκλειστικά δικό τους εικονικό ιδιωτικό δίκτυο χωρίς να βασίζονται στις εμπορικές επιλογές. Η υλοποίηση ακολουθεί μια σειρά από βήματα η οποία ξεκινάει με την επιλογή ενός παρόχου εικονικού ιδιωτικού διακομιστή και τελειώνει με τη ρύθμιση αυτόματων ενημερώσεων και ειδοποιήσεων στο προσωπικό ηλεκτρονικό ταχυδρομείο όποτε αυτά γίνονται. Στην ενότητα θα περιγραφούν με ακρίβεια τα βήματα ενοικίασης και ρύθμισης ενός εικονικού ιδιωτικού διακομιστή, η δημιουργία κλειδιών SSH και η εγκατάσταση και ρύθμιση του OpenVPN με ένα script για μεγαλύτερη αυτοματοποίηση. Όσον αφορά την ασφάλεια, χρησιμοποιήθηκε έλεγχος ταυτότητας δύο παραγόντων μέσω του Google Authenticator και μιας κινητής συσκευής και ταυτόχρονα έγιναν κάποιες ρυθμίσεις για να αποφευχθούν οι επιθέσεις ωμής βιας απο bots.

1. Ενοικίαση Διακομιστών

Για την επιλογή του κατάλληλου παρόχου εικονικού ιδιωτικού διακομιστή, χρειάζεται να ληφθούν κάποιοι παράγοντες υπόψη. Αρχικά ο πρώτος παράγοντας είναι το κόστος ή καλύτερα, η σχέση κόστους-ποιότητας. Στη συνέχεια ελέγχεται η τεχνολογία την οποία παρέχουν όπου και προτιμήθηκαν σύγχρονες τεχνολογίες εικονικοποίησης (virtualization) όπως είναι οι Kernel-based Virtual Machine(KVM) και η Xen και απορριφθηκε η OpenVZ. Αυτό συνέβη καθώς η OpenVZ έχει παλιότερο Linux Kernel και δεν υποστηρίζει τεχνολογίες όπως Docker και WireGuard και επίσης καθιστά πιο εύκολη την παρακολούθηση από τον πάροχο. Ακόμα ένας παράγοντας για την επιλογή του εικονικού ιδιωτικού διακομιστή είναι η γεωγραφική τοποθεσία του διακομιστή καθώς αυτή θα πρέπει να είναι σε αντιστοιχία με το σκοπό χρήσης του εικονικού ιδιωτικού δικτύου που θέλουμε να υλοποιήσουμε ενώ ταυτόχρονα συνδέεται με την απόδοση και την καθυστέρηση ανάλογα με το πόσο μακριά είναι γεωγραφικά απο την τοποθεσία μας. Τέλος, ρόλο παίζει και το χαρακτηριστικό αποκλειστικής διεύθυνσης IPv4 λόγω της σπανιότητας των διευθύνσεων IPv4 τελευταία.

Για την συγκεκριμένη υλοποίηση επέλεξα έναν εικονικό ιδιωτικό διακομιστή με λογισμικό Ubuntu 20.04 LTS και αποκλειστική διεύθυνση IPv4 με επιλογή χαρακτηριστικών όπως χωρητικότητα, αριθμός πυρήνων και μνήμη Ram τα ελάχιστα.

2. Δημιουργία κλειδιών SSH

Η χρήση κωδικού πρόσβασης σε μορφή καθαρού κειμένου είναι αρκετά ευπαθής και επικίνδυνη καθώς η πληροφορία διασχίζει ανασφαλή μη κρυπτογραφημένα δίκτυα κάτι που την καθιστά επιρρεπή σε επιθέσεις υποκλοπής(Man in the middle attacks). Για τον λόγο αυτό η χρήση του πρωτοκόλλου Secure Shell με την δημιουργία κλειδιών SSH είναι μια καλή λύση καθώς τα κλειδιά SSH δημιουργούν μια διαδικασία ελέγχου ταυτότητας σε δύο επίπεδα η οποία απαιτεί εκτός από κωδικό πρόσβασης, ο χρήστης να κατέχει και το αρχείο με το κλειδί. Με τον τρόπο αυτό διασφαλίζεται ένα πρόσθετο βήμα ασφάλειας κατά το οποίο η ύπαρξη του αρχείου του κλειδιού καθορίζει την αποκλειστικότητα της πρόσβασης στον διακομιστή μόνο σε όσους χρήστες έχουν το αντίστοιχο κρυπτογραφικό κλειδί. Η συγκεκριμένη μεθοδολογία χρησιμοποιήθηκε καθώς με τη δημιουργία των κλειδιών κρυπτογραφείται η διαδικασία ελέγχου ταυτότητας με αποτέλεσμα να προστατευεται σε περίπτωση που κάποιος προσπαθεί να υποκλέψει την επικοινωνία μεταξύ της συσκευής και του διακομιστή καθώς ο επιτιθέμενος χρειάζεται και το ιδιωτικό κλειδί για να αποκρυπτογραφήσει την διαδικασία ελέγχου ταυτότητας.

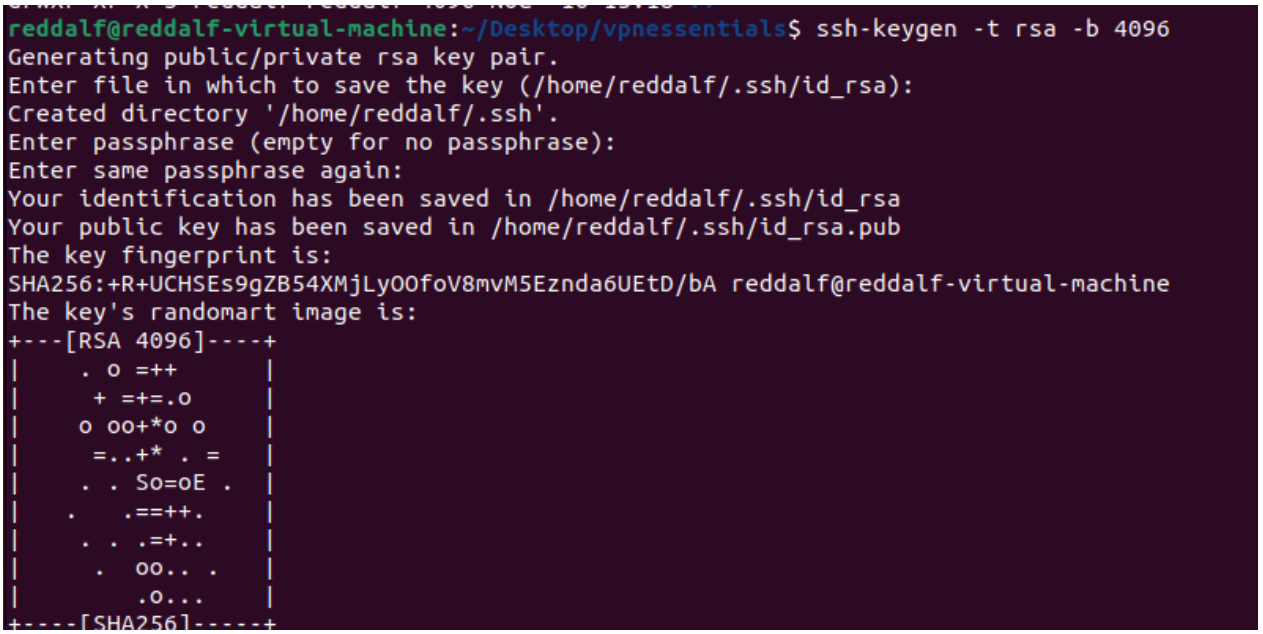
Οδηγίες

Για την δημιουργία των κλειδιών SSH χρησιμοποιήθηκαν τα ακόλουθα βήματα:

A. Άνοιγμα παραθύρου τερματικού:
    - Ανοίχτηκε ένα παράθυρο τερματικού για να χρησιμοποιηθούν οι απαραίτητες εντολές με ευκολία.
B. Δημιουργία κλειδιών SSH:
    - Χρησιμοποιήθηκε η ακόλουθη εντολή για να δημιουργηθεί ένα RSA κλειδί με μήκος 4096 bit:

        $ ssh-keygen -t rsa -b 4096
C. Διαμόρφωση θέσης κλειδιού:
    - Με κενό το πεδίο και την χρήση του “enter” διατηρήθηκε η προεπιλεγμένη τοποθεσία αποθήκευσης του κλειδιού.
D. Ορισμός κωδικού πρόσβασης:

- Ο κωδικός πρόσβασης που επιλέχθηκε, εισήχθη δύο φορές όπως ζητείται, μια φορά για τον ορισμό του κωδικού και μια για την επιβεβαίωση.

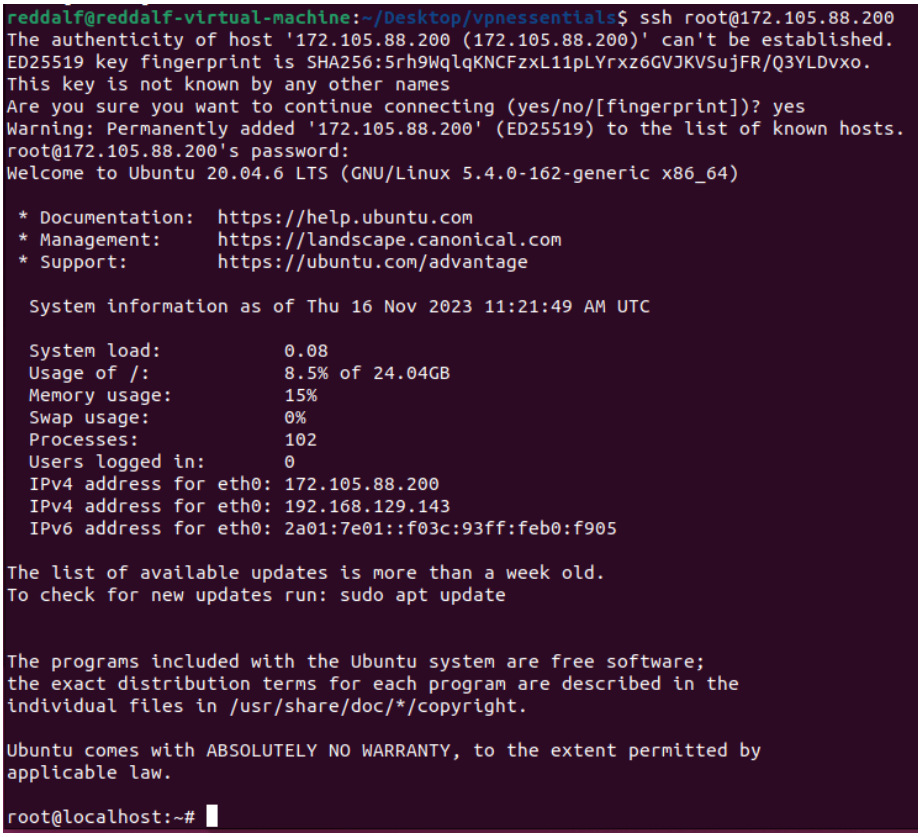


Σ1. Δημιουργία κλειδιών SSH

3. Ενημέρωση λειτουργικού συστήματος διακομιστή

A. Σύνδεση στο διακομιστή με SSH:
   - Η πρόσβαση στο διακομιστή έγινε μέσω SSH και τη χρήση των διαπιστευτηρίων του χρήστη root που παρέχονται απο τον παροχο εικονικού ιδιωτικού διακομιστή(VPS):
     “$ ssh root@172.105.88.200”

Με την εντολή αυτή το σύστημα ζήτησε την εισαγωγή του κωδικού πρόσβασης ο οποίος πληκτρολογήθηκε και η σύνδεση είναι επιτυχής.



Σ2. Επιτυχής σύνδεση στο διακομιστή μέσω SSH.

B. Εκτέλεση ενημερώσεων λειτουργικού συστήματος:

- Πρώτη ενέργεια που έγινε στο διακομιστή ήταν η ενημέρωση και αναβάθμιση του λειτουργικού συστήματος η οποία έγινε με την ακόλουθη εντολή:
  “$ apt-get update && apt-get upgrade”

Με την ενημέρωση και αναβάθμιση του συστήματος εξασφαλίστηκε η βέλτιστη λειτουργικότητα του συστήματος με τις νεότερες εκδόσεις στις εφαρμογές της.

4. Δημιουργία απλού χρήστη χωρίς δικαιώματα root

A. Βήματα δημιουργίας non-root χρήστη

Στο βήμα αυτό, δημιουργήθηκε ένας νέος χρήστης χωρίς δικαιώματα διαχειριστή. Παρά την ευκολία και τις ανέσεις που παρέχει η άμεση πρόσβαση σε χρήστη με δικαιώματα root, η λογική αυτή είναι επικίνδυνη και κρύβει κενά στην ασφάλεια για αυτό και υλοποιήθηκε αυτή η στρατηγική σαν πρόσθετο βήμα ασφαλείας.

- Η δημιουργία του νέου non-root χρήστη έγινε με την ακόλουθη εντολή στο τερματικό:

“$ useradd -G sudo -m reddalf -s /bin/bash”

Με την εντολή αυτή δημιουργήθηκε ένας καινούργιος λογαριασμός χρήστη με δικαιώματα sudo, όνομα χρήστη “reddalf” και το bash shell ως προεπιλογή διασφαλίζοντας έτσι ένα ελεγχόμενο περιβάλλον.

Β. Ορισμός κωδικού πρόσβασης στο νέο χρήστη

Ορίστηκε ένας κωδικός πρόσβασης για τον καινούργιο χρήστη “reddalf” που δημιουργήθηκε στο προηγούμενο βήμα με την ακόλουθη εντολή:

“$ passwd reddalf”

Αμέσως μετά την εντολή εισήχθη ο επιθυμητός, ασφαλής κωδικός πρόσβασης δύο φορές όπως ζητήθηκε.

```
root@localhost:~# useradd -G sudo -m reddalf -s /bin/bash
root@localhost:~#
root@localhost:~# passwd reddalf
New password:
Retype new password:
passwd: password updated successfully
root@localhost:~#
```

Σ3. Δημιουργία non-root χρήστη και ορισμός κωδικού πρόσβασης.

5. Διαμόρφωση ελέγχου ταυτότητας κλειδιού SSH

Α. Αντιγραφή κλειδιού SSH στον διακομιστή

Σε αυτό το βήμα, αντιγράφηκε το κλειδί SSH του χρήστη “reddalf” από το τοπικό μηχάνημα στον διακομιστή, δημιουργώντας έτσι έναν ασφαλή έλεγχο ταυτότητας. Με τη διαδικασία αυτή, απλοποιείται η πρόσβαση ενώ ταυτόχρονα υλοποιούνται ισχυρά πρωτόκολλα ασφάλειας. Το βήμα αυτό έγινε με την ακόλουθη εντολή στο τερματικό τοπικού υπολογιστή:

“$ ssh-copy-id reddalf@172.105.88.200”

Β. Έλεγχος ταυτότητας και οριστικοποίηση

Το αποτέλεσμα που προκύπτει απο την επιτυχή μεταφορά του κλειδιού SSH στον διακομιστή είναι πως ο νέος χρήστης “reddalf” μπορεί πλέον να πραγματοποιήσει έλεγχο ταυτότητας με ασφάλεια. Αυτό το βήμα είναι πολύ σημαντικό καθώς στη συνέχεια θα ρυθμίσουμε τον διακομιστή με τέτοιο τρόπο ώστε να διασφαλιστεί ότι

μόνο οι χρήστες που διαθέτουν τα κατάλληλα κλειδιά SSH μπορούν να δημιουργήσουν ασφαλείς συνδέσεις σε αυτόν.

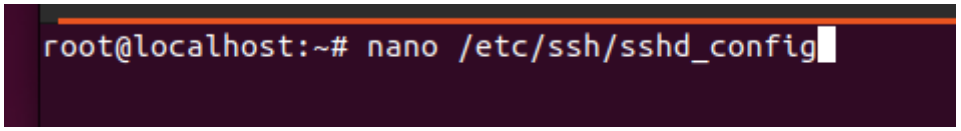
6.Ρύθμιση παραμέτρων ελέγχου ταυτότητας μόνο με κλειδί SSH και βελτιώσεων ασφαλείας

Μετά την εφαρμογή του ελέγχου ταυτότητας κλειδιού SSH στο προηγούμενο βήμα, ακολούθησε η ρύθμιση του διακομιστή ώστε να περιορίζει την πρόσβαση SSH αποκλειστικά στον έλεγχο ταυτότητας μέσω κλειδιού για τον χρήστη “reddalf”. Με τον τρόπο αυτόν, ελαχιστοποιούνται οι κίνδυνοι που σχετίζονται με τον έλεγχο ταυτότητας μέσω κωδικών πρόσβασης. Ακολουθούν τα βήματα:

Α. Τροποποίηση του αρχείου ρυθμίσεων SSH

- Στο βήμα αυτό ανοίχτηκε για επεξεργασία το αρχείο διαμόρφωσης SSH με την χρήση του nano ως πρόγραμμα επεξεργασίας κειμένου με την εντολή:

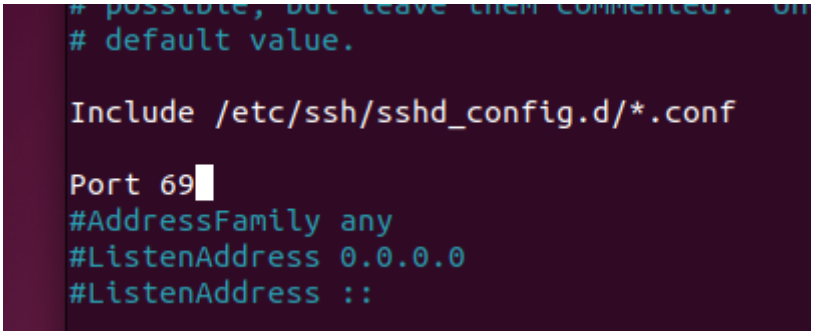
“$ nano /etc/ssh/sshd_config”



Σ4. Επεξεργασία αρχείου sshd_config.

- Έγινε αλλαγή από την προεπιλεγμένη θύρα SSH σε μια άλλη τυχαία θύρα:

“# Port 22
Port 69”

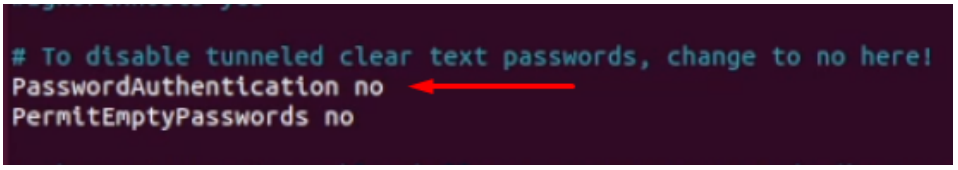


Σ5. Αλλαγή θύρας στο αρχείο sshd_config.

Ο σκοπός αυτής της κίνησης δεν εξυπηρετεί σε μεγάλο βαθμό την ασφάλεια αλλά αποτρέπει την στοχοποίηση από ρομπότ σαρωτές που ψάχνουν για την προεπιλεγμένη θύρα SSH(θύρα 22) και δοκιμάζουν γνωστά διαπιστευτήρια.

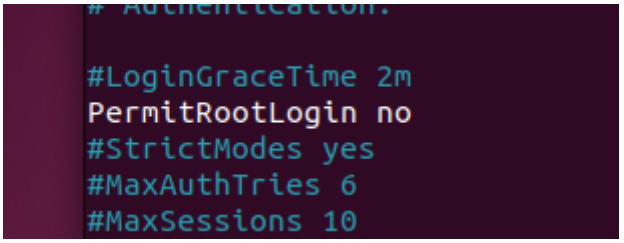
- Στη συνέχεια, απενεργοποιήθηκε ο έλεγχος ταυτότητας με κωδικό πρόσβαση έτσι ώστε να επιβληθεί η πρόσβαση μόνο με κλειδί:

“PasswordAuthentication no”



Σ6. Απενεργοποίηση ελέγχου ταυτότητας με κωδικό πρόσβασης στο αρχείο sshd_config

- Για ενίσχυση της ασφάλειας, απενεργοποιήθηκε η σύνδεση root:
  "PermitRootLogin no"



Σ7. Απενεργοποίηση σύνδεσης root στο αρχείο sshd_config.

Μετά και από αυτή την αλλαγή, ακολούθησε η αποθήκευση των αλλαγών και η έξοδος από το αρχείο.

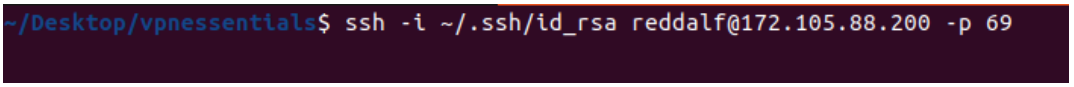
Β. Επανεκκίνηση υπηρεσιών SSH και επαλήθευση

Μετά την έξοδο από το αρχείο έγινε μια επανεκκίνηση των υπηρεσιών SSH με την ακόλουθη εντολή:

"$ systemctl restart sshd"

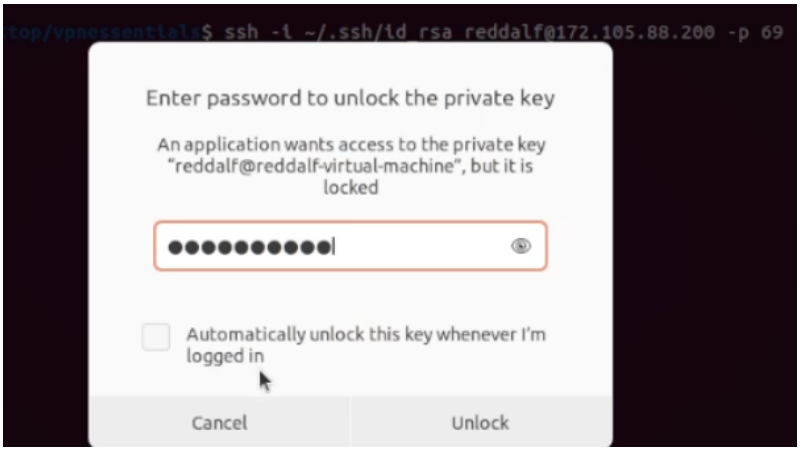
Στην συνέχεια, έγινε μια επαλήθευση απο το τοπικό μηχάνημα για να επιβεβαιωθεί οτι έχουν τεθεί σε λειτουργία οι καινούργιες ρυθμίσεις που έχουν τεθεί. Αυτό έγινε με την εντολή:

"$ ssh -i ~/.ssh/id_rsa reddalf@172.105.88.200 -p 69"



Σ8. Επαλήθευση εφαρμογής αλλαγών στην επαλήθευση μέσω κλειδιού

Στο σημείο αυτό ζητήθηκε επαλήθευση με κωδικό πρόσβασης κάτι που υποδηλώνει ότι ο έλεγχος ταυτότητας είναι επιτυχής.



Σ9. Επαλήθευση σύνδεσης με κωδικό πρόσβασης

Έπειτα έγινε και επαλήθευση από άλλο μηχάνημα χωρίς το κλειδί με την ακόλουθη εντολή, όπου και εμφανίστηκε ένα μήνυμα “Permission denied” επιβεβαιώνοντας την επιτυχία της διαδικασίας.

“$ ssh reddalf@172.105.88.200 -p 69”

Με τις ρυθμίσεις αυτές βελτιώνεται η ασφάλεια και η πρόσβαση SSH ενισχύεται καθώς απαιτείται ο χρήστης να έχει τα απαραίτητα κλειδιά. Ταυτόχρονα, ενισχύεται η ασφάλεια του διακομιστή με πρόσθετα μέτρα όπως η αλλαγή της προεπιλεγμένης θύρας και η αποτροπή σύνδεσης root.

7. Βελτιστοποίηση απομακρυσμένης πρόσβασης

Α. Διευκόλυνση σύνδεσης του χρήστη στο διακομιστή

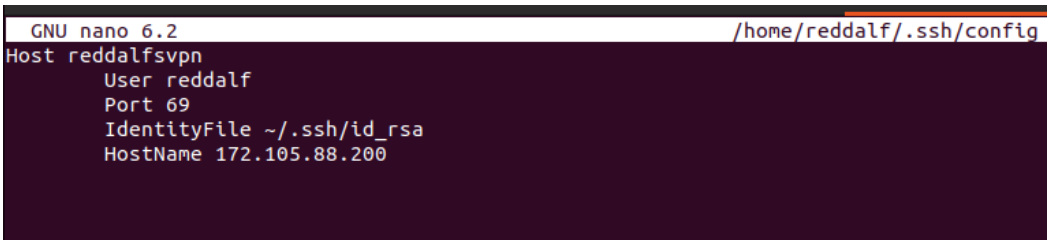
Για την βελτιστοποίηση της εμπειρίας του χρήστη, σε αυτό το σημείο υλοποιήθηκε ένα προαιρετικό βήμα για τη δημιουργία ενός alias για τον χρήστη “reddalf” στον διακομιστή στη IP διεύθυνση 172.105.88.200. Με τη διαδικασία αυτή απλοποιείται και επισπεύδεται η διαδικασία σύνδεσης στοχεύοντας στην βελτίωση της εμπειρίας του χρήστη χωρίς κάποιο αντίκτυπο στην ασφάλεια. Παρόλο που δεν βελτιώνεται η ασφάλεια της υλοποίησης VPN με αυτό το βήμα, υλοποιήθηκε καθώς συμβάλλει σε μια καλύτερα οργανωμένη ροή εργασίας για τους χρήστες. Αυτό έγινε με τα ακόλουθα βήματα:

- Δημιουργήθηκε ένα αρχείο διαμόρφωσης με το όνομα “config” στον φάκελο “.ssh” στον φάκελο home του χρήστη reddalf.

  “$ nano ~/.ssh/config”
- Μέσα στο αρχείο ορίστηκε ένα alias για το VPS το οποίο περιέχει τις ακόλουθες πληροφορίες:

  “Host reddalfsvpn
  User reddalf

Port 69
IdentityFile ~/.ssh/id_rsa
Hostname 172.105.88.200”



Σ9. Αρχείο config με ρυθμίσεις alias για συνδεση στο διακομιστή.

Μετά τη συμπλήρωση των παραπάνω πληροφοριών έγινε αποθήκευση του αρχείου και έξοδος.

Β. Απλοποιημένη σύνδεση

- Με το alias σωστά ρυθμισμένο, πλέον η πρόσβαση στον διακομιστή απλοποιείται σε μια σύντομη εντολή:

“$ ssh reddalfsvpn”

Γ. Σίγαση κειμένου σύνδεσης

- Για περαιτέρω βελτίωση, έγινε και σίγαση του περιττού κειμένου που εμφανίζεται όταν γίνεται η σύνδεση στο διακομιστή με την δημιουργία του αρχείου hustlogin και την εντολή:

“$ touch .hushlogin”

8. Εφαρμογή OpenVPN

Α. Αυτοματοποίηση της εγκατάστασης OpenVPN

Η διαδικασία εγκατάστασης ενός διακομιστή OpenVPN είναι μια διαδικασία η οποία λόγω της πολυπλοκότητας και της πολύωρης διάρκειας της διαδικασίας της υποκρύπτει τον κίνδυνο να γίνουν λάθη. Η διαδικασία περιλαμβάνει εγκατάσταση πακέτων(packages), διαμόρφωση των IP Tables του διακομιστή και την χειροκίνητη δημιουργία αρχείων διαμόρφωσης διακομιστή και πελάτη. Στη συγκεκριμένη διατριβή, για να εξαλειφθεί η πιθανότητα ανθρώπινου λάθους και να επιταχυνθεί η διαδικασία υλοποίησης χωρίς να διακυβεύεται η ασφάλεια, ελήφθη η απόφαση να αξιοποιηθεί μια αυτοματοποιημένη προσέγγιση. Η ενότητα εμβαθύνει στα βήματα που έγιναν από την απόφαση του αυτοματισμού μέχρι την λεπτομερή ανάλυση της μεθόδου αυτοματοποίησης.

Β. Απόφαση αυτοματισμού

Για να βελτιωθεί σε ακόμα μεγαλύτερο βαθμό η αποτελεσματικότητα και ταυτόχρονα να μειωθεί το ανθρώπινο λάθος, λήφθηκε η αποφαση η διαδικασία εγκατάστασης του OpenVPN να αυτοματοποιηθεί. Ο αυτοματισμός είναι ο βέλτιστος τρόπος να διασφαλιστεί μια συνεπής αλλά και εύκολα αναπαραγώγιμη εγκατάσταση ενώ ταυτόχρονα επιταχύνει την ανάπτυξη εστιάζοντας έτσι στην ασφάλεια και την αξιοπιστία, κάτι που ευθυγραμμίζεται με τους σκοπούς και την εστίαση της έρευνας.

Η επιλογή μιας αυτοματοποιημένης διαδικασίας εγκατάστασης του OpenVPN στηρίζεται από έναν μεγάλο αριθμό πλεονεκτημάτων. Αρχικά η αυτοματοποιημένη εγκατάσταση με τη χρήση ενός script, μειώνει σημαντικά τον χρόνο ο οποίος απαιτείται για να διεκπεραιωθούν επαναλαμβανόμενες ενέργειες στις ρυθμίσεις του. Ταυτόχρονα, επιτρέπει όχι μόνο γρηγορότερη ανάπτυξη αλλά και ελαχιστοποιεί την πιθανότητα να εμφανιστούν λάθη και επιπλοκές που οφείλονται στον ανθρώπινο παράγοντα και σχετίζονται με λανθασμένες ρυθμίσεις. Άλλο ένα θετικό αποτελεί η συνεπή και ομοιόμορφη διαμόρφωση που προκύπτει από την χρήση ενός script η οποία μετριάζει τον κίνδυνο να υπάρχουν αποκλίσεις από μια εγκατάσταση σε μια άλλη σε περίπτωση που χρειαστούν παραπάνω από μια εγκαταστάσεις καθώς οι ρυθμίσεις παραμένουν ίδιες. Τελευταίο και σημαντικότερο κριτήριο αποτελεί η αναπαραγωγιμότητα. Καθώς ένα μέρος της υλοποίησης της έρευνας εστιάζει στην ευκολία αναπαραγωγής της διαδικασίας, η χρήση script για την εγκατάσταση του OpenVPN είναι η κατάλληλη λύση για να μπορέσει ο καθένας να αναπαράγει τη διαδικασία πιστά, συμβάλλοντας στην ακεραιότητα της έρευνας.

Γ. Επιλογή script

Το script το οποίο χρησιμοποιήθηκε για αυτοματοποίηση της διαδικασίας εγκατάστασης του OpenVPN είναι το OpenVPN road warrior script απο το Nyr Github repository(“**https://github.com/Nyr/openvpn-install”**). Αυτό το script αυτοματοποιεί τις περίπλοκες εργασίες όπως είναι η εγκατάσταση διαφόρων απαραίτητων πακέτων και η διαμόρφωση τους, απαιτώντας από τον χρήστη να απαντήσει σε μερικές ερωτήσεις και τελειώνει τη διαδικασία δίνοντας στον χρήστη την επιλογή λήψης του αρχείου ρυθμίσεων. Πριν την χρήση του συγκεκριμένου script υπήρξε μια εκτενής διαδικασία ελέγχου και ανάλυσής του. Είναι πολύ σημαντικό σε τέτοιες περιπτώσεις αυτοματοποίησης μέσω script να γίνεται εκτενής έλεγχος των εντολών που περιλαμβάνονται στο script έτσι ώστε να διασφαλίζεται η διαφάνεια και η αξιοπιστία του. Η λήψη τέτοιων μέτρων προφύλαξης είναι απαραίτητη έτσι ώστε να αποτρέπονται πιθανόν κακόβουλες γραμμές κώδικα απο το να εκτελούνται και να τονίζεται χωρίς αμφιβολία σε έντονο βαθμό η ασφάλεια στην διαδικασία.

Δ. Βήματα εγκατάστασης OpenVPN

Στη διαδικασία της εγκατάστασης ακολουθήθηκαν κάποια βήματα τα οποία αποτελούνται από την σύνδεση στο διακομιστή, την επιβεβαίωση ύπαρξης του προγράμματος ‘wget’, τη λήψη του script και την εκτέλεσή του όπου αφού

απαντήθηκαν κάποιες στοιχειώδης ερωτήσεις, το script ξεκίνησε την διαδικασία εγκατάστασης:

1. Εκτέλεση του script

- Η διαδικασία ξεκίνησε διασφαλίζοντας την ύπαρξη του προγράμματος ‘wget’ το οποίο είναι απαραίτητο στη συνέχεια,μέσω της προσπάθειας εγκατάστασής του. Αυτό έγινε με την ακόλουθη εντολή:

“$ sudo apt install wget”

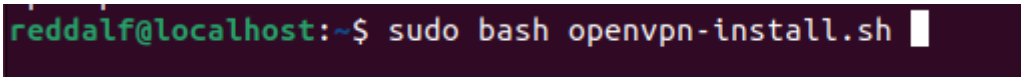
- Στη συνέχεια, έγινε λήψη του OpenVPN road warrior script με την χρήση του ‘wget’ και την ακόλουθη εντολή:

“$ sudo wget https://github.com/Nyr/openvpn-install/raw/master/openvpn-install.sh”

Σ10. Εγκατάσταση του ‘wget’ και λήψη του OpenVPN road warrior script.

- Ακολουθεί η εκκίνηση του script και η απάντηση στις ερωτήσεις και οδηγίες:

“$ sudo bash openvpn-install.sh”



Σ11. Εκκίνηση του OpenVPN road warrior script.

Με την εκκίνηση του script θα γίνουν κάποιες βασικές ερωτήσεις τις οποίες θα πρέπει να απαντήσει ο χρήστης, ξεκινώντας με ποια IPv4 διεύθυνση θα πρέπει να χρησιμοποιηθεί(‘Which IPv4 address should be used?’) όπου και επιλέχθηκε η προκαθορισμένη απάντηση που ήταν η διεύθυνση ‘*172.105.88.200*’. Στη συνέχεια ακολούθησε η ερώτηση ποιό πρωτόκολλο θα π΄ρεπει να χρησιμοποιεί το OpenVPN(‘Which protocol should OpenVPN use?’) όπου θα επιλέχθηκε το UDP το

οποίο είναι και η προτεινόμενη επιλογή. Έπειτα έγινε η ερώτηση για το ποιά θύρα θα πρέπει να ακούει το OpenVPN(‘What port should OpenVPN listen to?’) όπου η προτεινόμενη θύρα είναι η 1194 αλλά καθώς αυτή είναι ευρέως γνωστή ως η θύρα του OpenVPN επιλέχθηκε η θύρα 443 η οποία είναι η ίδια θύρα που χρησιμοποιεί το HTTPS πρωτόκολλο αλλά καθώς το HTTPS χρησιμοποιεί TCP και το OpenVPN UDP, δεν υπάρχει πρόβλημα. Τελευταίες δύο ερωτήσεις είναι ο DNS διακομιστής που θα πρέπει να επιλεγεί(‘Select a DNS server for the clients:’) που επιλέχθηκε του Google και το όνομα του πρώτου πελάτη(‘Enter a name for the first client:’) στο οποίο επιλέχθηκε το όνομα thinkpad.

```
Welcome to this OpenVPN road warrior installer!

Which IPv4 address should be used?
     1) 172.105.88.200
     2) 192.168.129.143
IPv4 address [1]: 1

Which protocol should OpenVPN use?
   1) UDP (recommended)
   2) TCP
Protocol [1]:

What port should OpenVPN listen to?
Port [1194]: 443

Select a DNS server for the clients:
   1) Current system resolvers
   2) Google
   3) 1.1.1.1
   4) OpenDNS
   5) Quad9
   6) AdGuard
DNS server [1]: 2

Enter a name for the first client:
Name [client]: thinkpad
```

Σ12. Ερωτήσεις και απαντήσεις του OpenVPN road warrior script.

Μετά τις ερωτήσεις, το script έτρεξε και ξεκίνησε η αυτοματοποιημένη διαδικασία εγκατάστασης του OpenVPN κατά τη διάρκεια της οποίας δεν υπήρξε καμία επιπλοκή. Όταν η διαδικασία τελείωσε, ένα μήνυμα σε ενημερώνει πως για την προσθήκη νέων χρηστών θα χρειαστεί απλώς να τρέξει άλλη μια φορά το ίδιο script καθώς και ότι το αρχείο το οποίο θα χρειαστεί να μεταφερθεί στο τοπικό μηχάνημα αποθηκεύτηκε στο φάκελο ‘/root/thinkpad.ovpn’. Καθώς η διαδικασία έγινε με τον χρήστη “reddalf”, χρειάστηκε να μεταφερθέι το αρχείο στο παρόν φάκελο και να

δωθούν στον χρήστη “reddalf” τα κατάλληλα δικαιώματα κάτι το οποίο έγινε με τις ακόλουθες εντολές:

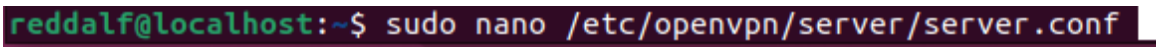
1. *“$ sudo mv /root/thinkpad.ovpn .”*
2. *“$ sudo chown reddalf thinkpad.ovpn”*

2. Απενεργοποίηση αρχείων καταγραφής

Ακολουθεί ένα βήμα απενεργοποίησης των αρχείων καταγραφής. Μια τέτοια κίνηση προσφέρει θετικά σε πολλούς διαφορετικούς τομείς. Αρχικά τα αρχεία καταγραφής περιέχουν λεπτομερείς πληροφορίες σχετικά με τη δραστηριότητα και τις συνδέσεις του διακομιστή και του χρήστη. Τέτοιες πληροφορίες σε περίπτωση μη εξουσιοδοτημένης πρόσβασης είναι σίγουρα πολύ χρήσιμες σε κάποιο κακόβουλο χρήστη ο οποίος θα τις χρησιμοποιήσει για να βρει εκτεθειμένες ευαίσθητες πληροφορίες ή να διεισδύσει βαθύτερα στον διακομιστή μέσω πιθανών ευπαθειών που θα ανακαλύψει. Με την απενεργοποίηση της καταγραφής ωστόσο μετριάζεται ο κίνδυνος καθώς αυτόματα μειώνεται η επιφάνεια επίθεσης στην οποία είναι εκτεθειμένος ο χρήστης. Επιπρόσθετα, στο πλαίσιο της υλοποίησης VPN απο το σπίτι το απόρρητο του χρήστη είναι πρωταρχικής σημασίας και η απενεργοποίηση της λεπτομερής καταγραφής της δραστηριότητας του χρήστη όπως διευθύνσεις IP ή καταγραφή του χρόνου συνδέσεις είναι σημαντικό να μην αποθηκεύονται ασκοπα. Τέλος, μια τέτοια κίνηση αν και λιγότερο σημαντικό, ενισχύει την απόδοση του διακομιστή καθώς αποφεύγεται η πρόσθετη κατανάλωση πόρων του συστήματος που προορίζονταν στην καταγραφή των συμβάντων διασφαλίζοντας μια αποτελεσματικότερη λειτουργία. Η απενεργοποίηση των αρχείων καταγραφής έγινε με την παρακάτω διαδικασία:

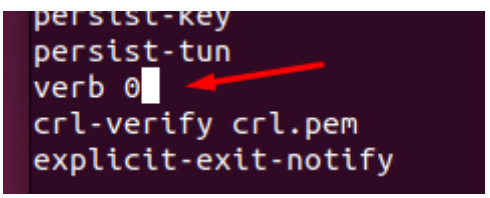
- Πρώτα έγινε επεξεργασία του αρχείου server.conf με το πρόγραμμα επεξεργασίας κειμένου nano:

“$ sudo nano /etc/openvpn/server/server.conf”



Σ11. Επεξεργασία αρχείου server.conf.

- Στο αρχείο έγινε η αλλαγή της τιμής του verb(verbose) από 3 σε 0:



Σ12. Αλλαγή τιμής του verb απο 3 σε 0.

Τέλος για οριστικοποίηση των αλλαγών έγινε μια επανεκκίνηση της υπηρεσίας OpenVPN:

```
reddalf@localhost:~$ sudo nano /etc/openvpn/server/server.conf
reddalf@localhost:~$ sudo systemctl restart openvpn-server@server.service
reddalf@localhost:~$
```

Σ13. Επανεκκίνηση της υπηρεσίας OpenVPN.

3. Λήψη του αρχείου

Στη συνέχεια ακολούθησε η λήψη του αρχείου διαμορφώνοντας μια sftp σύνδεση στον διακομιστή και στη συνέχεια λήφθηκε το αρχείο στο τοπικό μηχάνημα με την εντολή get και το όνομα του αρχείου όπως φαίνεται στις παρακάτω εντολές:

- Σύνδεση sftp με τον διακομιστή απο το τοπικό μηχάνημα:

“$ sftp reddalfsvpn”

- Λήψη του αρχείου:

“$ get thinkpad.ovpn”

- Κλείσιμο της σύνδεσης sftp:

“$ exit”

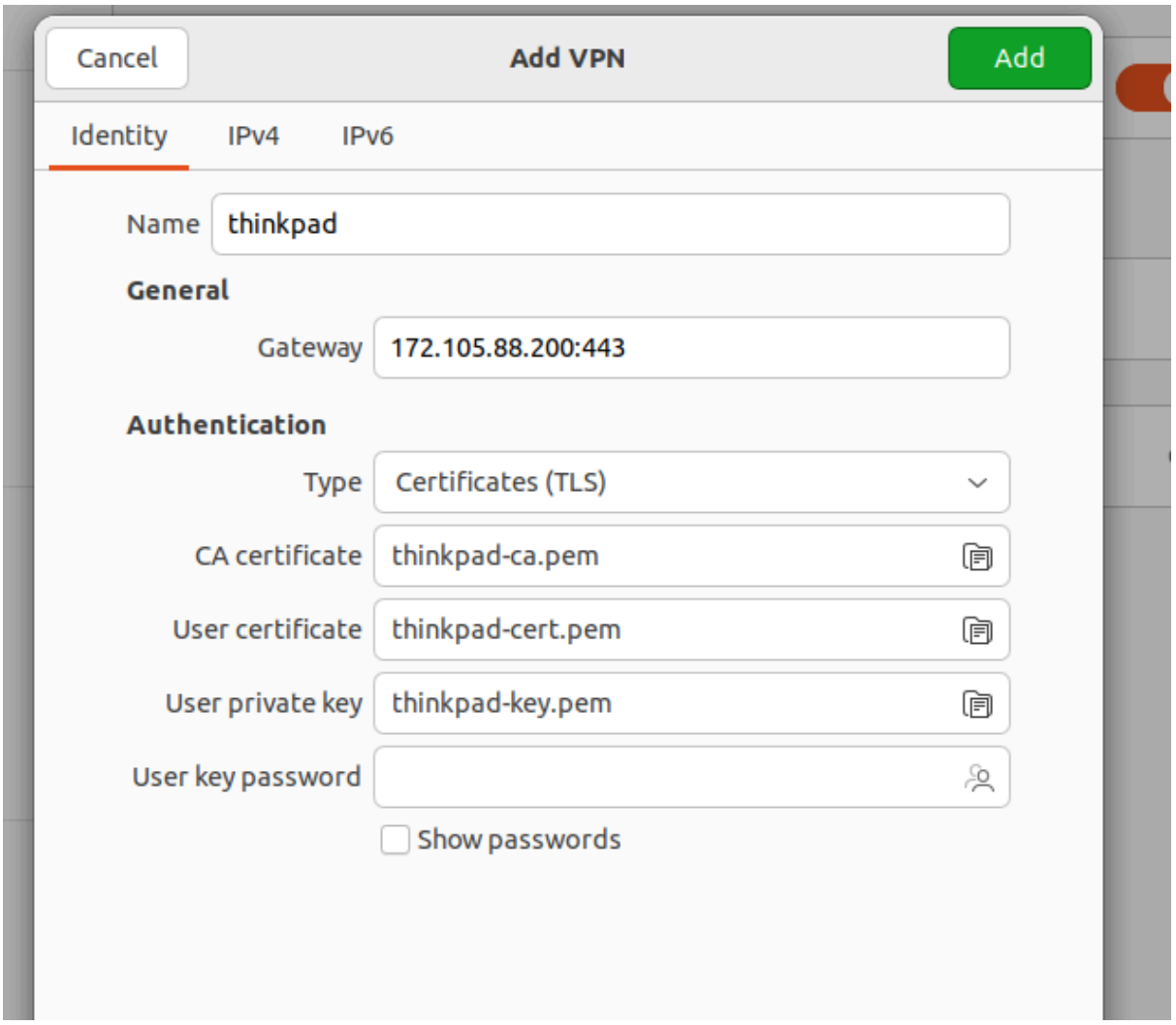
```
reddalf@reddalfsvpn: ~                                                redd
reddalf@reddalf-virtual-machine:~/Desktop/vpnessentials$ sftp reddalfsvpn
Connected to reddalfsvpn.
sftp> get thinkpad.ovpn
Fetching /home/reddalf/thinkpad.ovpn to thinkpad.ovpn
thinkpad.ovpn
sftp> exit
reddalf@reddalf-virtual-machine:~/Desktop/vpnessentials$ ls
thinkpad.ovpn
reddalf@reddalf-virtual-machine:~/Desktop/vpnessentials$
```

Σ13. Λήψη του αρχείου διαμόρφωσης του OpenVPN.

4. Φόρτωση του αρχείου διαμόρφωσης στο Network Manager

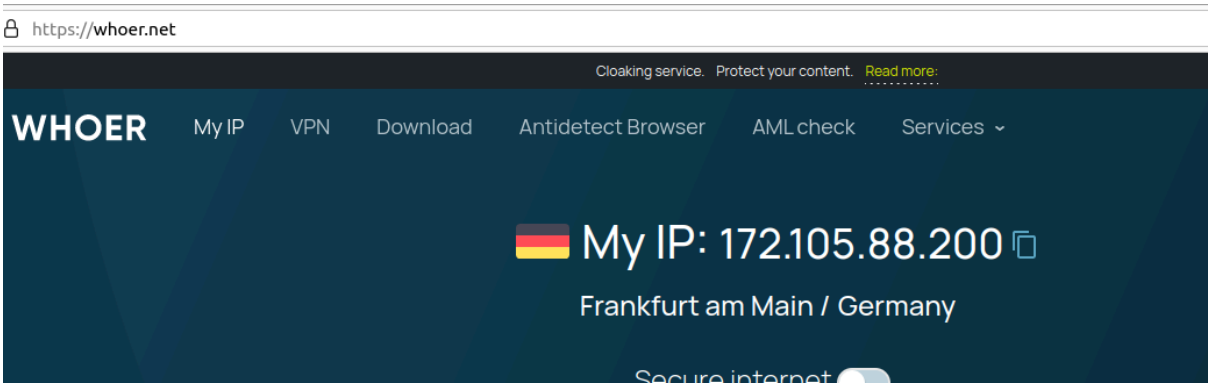
Καθώς το τοπικό μηχάνημα έχει λειτουργικό σύστημα Linux, το μόνο που χρειάζεται για την χρήση του OpenVPN που εγκαταστάθηκε στο διακομιστή είναι η φόρτωση του αρχείου διαμόρφωσης στον NetworkManager. Για να γίνει αυτό, ακολουθήθηκε η εξής διαδικασία Settings -> Network -> Add VPN -> Import from file -> επιλογή του

thinkpad.ovpn -> Προσθήκη του ιδιωτικού κλειδιού thinkpad-key.pem -> Add όπως φαίνεται και στο στιγμιότυπο οθόνης 14 που ακολουθεί.



Σ14. Προσθήκη του thinkpad.ovpn στον NetworkManager.

Με την ολοκλήρωση αυτού του βήματος, η διαδικασία έχει λάβει τέλος και η επαλήθευση έγινε με μια απλή αναζήτηση της διεύθυνσης IP στο Google την οποία και αναγνωρίζει ως την IP του VPN.



Σ15. Επαλήθευση ορθής λειτουργίας του VPN.

Ε. Ενίσχυση της ασφάλειας του διακομιστή με έλεγχο ταυτότητας πολλαπλών παραγόντων

Αναγνωρίζοντας το γεγονός ότι ο διακομιστής αποτελεί το σημείο τομής της ασφάλειας τόσο του ίδιου του διακομιστή όσο και της OpenVPN υλοποίησης σε αυτό το σημείο επιλέχθηκε να ενσωματωθεί ο έλεγχος ταυτότητας πολλαπλών παραγόντων(MFA) για να ενισχυθεί η στάση ασφάλειας του. Η συγκεκριμένη ενότητα εμβαθύνει στα βήματα που ακολουθήθηκαν για να εφαρμοστή ο έλεγχος ταυτότητας πολλαπλών παραγόντων αξιοποιόντας το πακέτο google-authenticator-libpam. Η στρατηγική κίνηση αυτή διασφαλίζει πως η πρόσβαση είναι αποκλειστική και ελέγχεται με την επιβολή μιας διαδικασίας ελέγχου ταυτότητας σε δυο επιπεδα. Ο χρήστης για να έχει πρόσβαση στον διακομιστή χρησιμοποιεί όχι μόνο το δημόσιο κλειδί του αλλά και έναν κωδικό πρόσβασης που δημιουργείται μια φορά στην αξιόπιστη συσκευή τηλεφώνου που έχει οριστεί κατά την υλοποίηση. Η κίνηση αυτή προσφέρει πολλά οφέλη για την ασφάλεια και τονίζει την χρησιμότητα του ελέγχου ταυτότητας πολλαπλών παραγόντων για το σκοπό μιας ισχυρής προστασίας στο διακομιστή. Παρακάτω παρατίθενται λεπτομερώς τα βήματα που έγιναν για την υλοποίηση αυτού του μέτρου:

1. Εγκατάσταση ελέγχου ταυτότητας πολλαπλών παραγόντων

- Η διαδικασία ξεκιναει με την εγατάσταση του πακέτου “google-authenticator-libpam” με την αντίστοιχη εντολή:

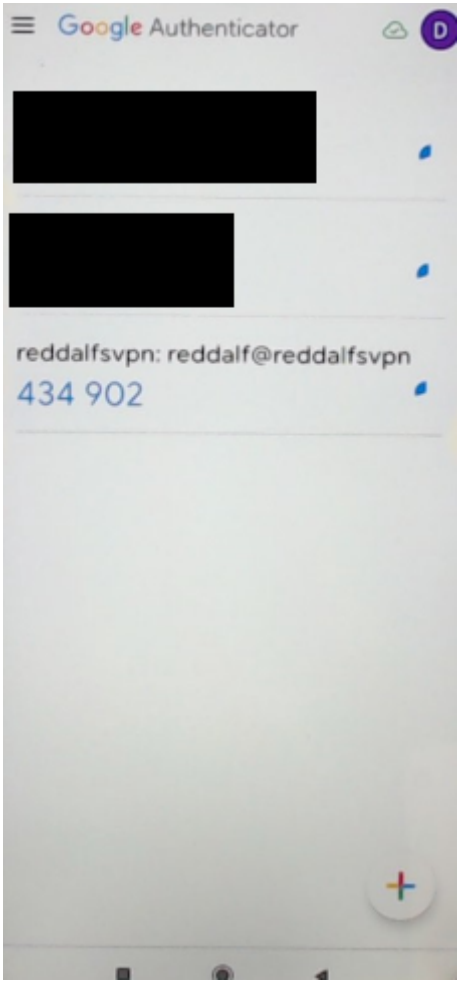
“$ sudo apt install libpam-google-authenticator”

2. Διαμόρφωση του ελέγχου ταυτότητας πολλαπλών παραγόντων

- Εκκίνηση του initialization script για την διαμόρφωση του ελέγχου ταυτότητας πολλαπλών παραγόντων:

“$ google-authenticator”

Στο σημείο αυτό το script εμφάνισε μια σειρά ερωτήσεων οι οποίες ήταν απαραίτητες για την εγκατάσταση του και απαντήθηκαν όλες θετικά εκτός από την ερώτηση για πολλαπλούς χρήστες και την ερώτηση για τα 30-δευτερόλεπτα tokens. Μαζί με τις ερωτήσεις εμφανίστηκε και το QR Code ο οποίος χρησιμοποιήθηκε σε συνδυασμό με τη χρήση της εφαρμογής Google Authenticator στο κινητό έτσι ώστε να γίνει η σάρωση και να προστεθεί ο λογαριασμός στην εφαρμογή.



Σ16. Προσθήκη λογαριασμού στην εφαρμογή Google Authenticator στο κινητό.

3. Προσθήκη του ελέγχου με Google authenticator στο ssh αρχείο διαμορφωσης

Μετά την επιτυχή υλοποίηση του google authenticator, ακολούθησε η επεξεργασία του αρχείου διαμορφώσεων του ssh έτσι ώστε να ζητείται ο κωδικός από την εφαρμογή κάθε φορά που γίνεται σύνδεση μέσω ssh.

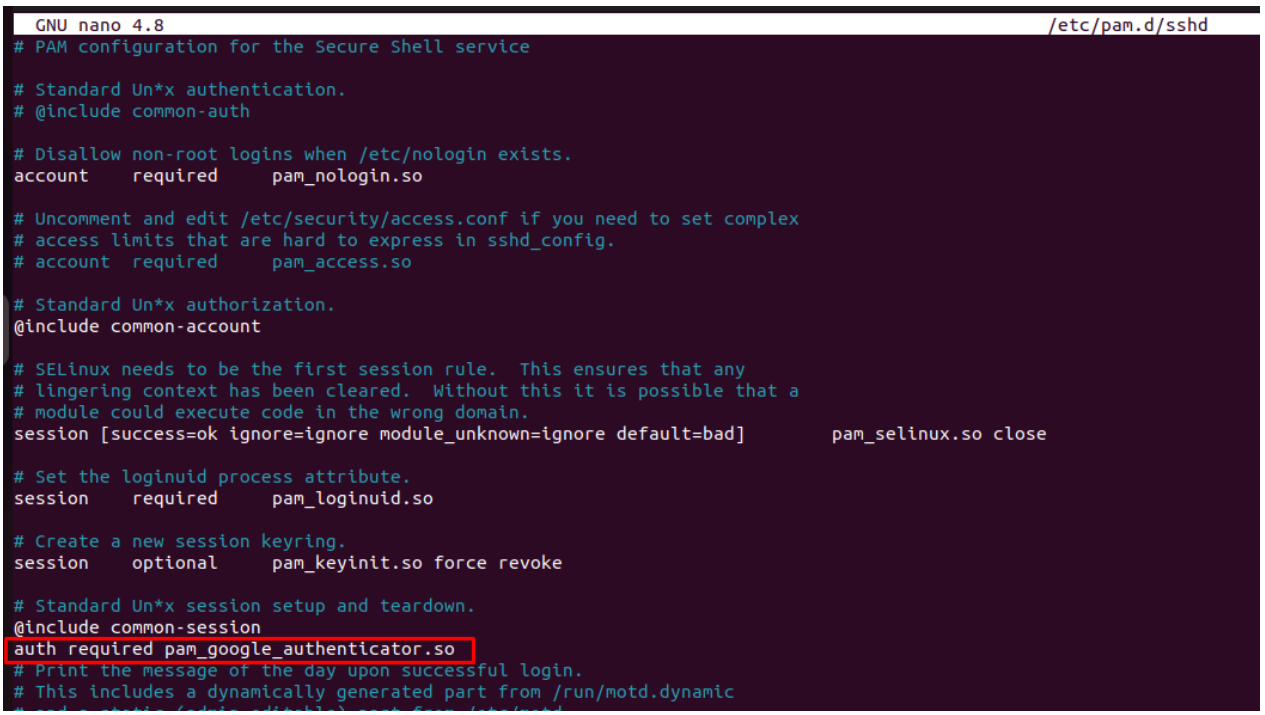
- Επεξεργασία του αρχείου “/etc/pam.d/sshd” με την βοήθεια του προγράμματος επεξεργασίας κειμένου nano και την ακόλουθη εντολή:

“$ sudo nano /etc/pam.d/sshd”

```
reddalf@reddalfsvpn:~$ sudo nano /etc/pam.d/sshd
```

Σ17. Επεξεργασία αρχείου sshd.

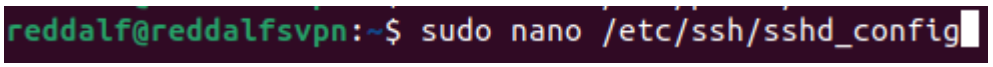
- Προσθήκη της γραμμής auth required pam_google_authenticator.so μέσα στο αρχείο.



Σ18. Προσθήκη απαιτούμενης κίνησης της χρήσης google authenticator στη διαδικασια σύνδεσης.

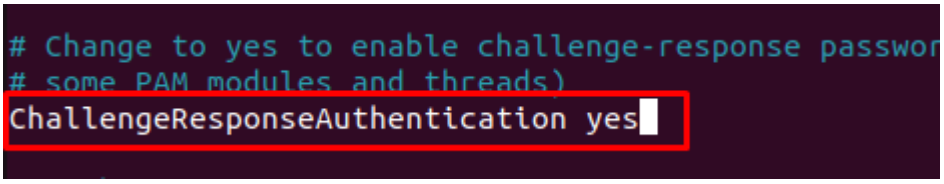
Μετά έγινε η επεξεργασία του αρχείου “/etc/ssh/sshd_config” όπου έγιναν κάποιες αλλαγές έτσι ωστε να αντιληφθεί το ssh την καινούργια μέθοδο ελέγχου ταυτότητας.

“$ sudo nano /etc/ssh/sshd_config”

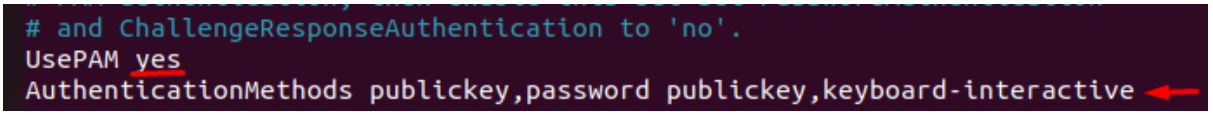


Σ19. Εντολή επεξεργασίας αρχείου sshd_config.

Στο σημείο αυτό τροποποιήθηκε η γραμμή ChallengeResponseAuthentication απο no σε yes καθώς και η γραμμή UsePAM απο no σε yes και προστέθηκε η γραμμή AuthenticationMehtods publickey, password publickey, keyboard-interactive:



Σ19. Αλλαγή του ChallengeResponseAuthentication σε yes.



Σ20. Αλλαγή του UsePAM σε yes και προσθήκη της γραμμής AuthenticationMethods.

Η διαδικασία ολοκληρώθηκε με επιτυχία με τελευταίο βήμα την επανεκκίνηση του sshd με την εντολή:

“$ sudo systemctl restart sshd”

ΣΤ. Ανάλυση λειτουργίας του OpenVPN road warrior script

Το συγκεκριμένο script είναι σχολαστικά γραμμένο με σκοπό να αυτοματοποιήσει τη διαδικασία εγκατάστασης αλλά και ρύθμισης του OpenVPN σε έναν διακομιστή Linux. Σε αυτή την ενότητα θα ακολουθήσει μια ανάλυση της λειτουργικότητας του script η οποία περιλαμβάνει μια συνοπτική περίληψη κάθε ενος απο τα στάδια εκτέλεσης στα οποία έγινε αναλυτική μελέτη κατά τη διάρκεια της έρευνας.

1. Έλεγχος έκδοσης λειτουργικού συστήματος και πυρήνα

Το script ξεκινάει κάνοντας έναν λεπτομερή έλεγχο του συστήματος για να διασφαλίσει ότι υπάρχει συμβατότητα η οποία και υπήρχε καθώς ο διακομιστής έχει λειτουργικό σύστημα Ubuntu 20.04. Ταυτόχρονα, δίνει έμφαση στην εκτέλεση του με το bash κελυφος(shell) και πραγματοποιεί έλεγχο έκδοσης του πυρήνα(kernel) του συστήματος για να ελέγξει για προβλήματα συμβατότητας. Το script είναι ρυθμισμένο έτσι ωστε να ακολουθεί μια σειρά βημάτων ανάλογα με το περιβάλλον το οποίο ανιχνεύει ενώ ταυτόχρονα προστατεύει από εγκατάσταση του script σε μη συμβατά συστήματα επομένως αυτό το πρώτο βήμα είναι πολύ σημαντικό.

2. Προνόμια χρήστη και επαλήθευση συσκευής TUN

Για την λειτουργήσει χωρίς σφάλματα το script επικυρώνει οτι εκτελείται με δικαιώματα root. Την ίδια στιγμή εκτελεί και έναν δεύτερο έλεγχο ο οποίος ελέγχει την ύπαρξη συσκευής TUN η οποία είναι κρίσιμη για τη λειτουργικότητα του OpenVPN καθώς βοηθάει σε πολλά καθήκοντα που αφορούν το δίκτυο.

3. Εκκίνηση και ρύθμιση του προγράμματος εγκατάστασης

Αφού αναγνώρισε το σύστημα, το script συνεχίζει και προετοιμάζει μεταβλητές αντίστοιχες του ανιχνευμένου λειτουργικού συστήματος και προετοιμάζεται για τα επόμενα βήματα της εγκατάστασης.

4. Αλληλεπίδραση με τον χρήστη

Στο σημείο αυτό το script ξεκινάει να κάνει μια σειρά ερωτήσεων όπως αναφέρθηκαν και παραπάνω. Στο στάδιο αυτό ο χρήστης επιλέγει μια διεύθυνση IPv4 ενώ του παρέχονται ως επιλογές οι ανιχνευμένες διευθύνσεις. Αντίστοιχα, επιλέγει και πρωτόκολλο UDP ή TCP, τη θύρα λειτουργίας και τη ρύθμιση του DNS του διακομιστή. Με τις επιλογές αυτές το script θα συνεχίσει στην δημιουργία ενός

αρχείου διαμορφώσεων ‘server.conf’ το οποίο θα είναι έτσι ρυθμισμένο ώστε να ανταποκρίνεται στις επιλογές που παρείχε ο χρήστης.

5. Ρυθμίσεις του τείχους προστασίας

Στο βήμα αυτό το script ανιχνεύει για την ύπαρξη του firewall και το εγκαθιστά αν δεν υπάρχει. Συνεχίζει ορίζοντας τις κατάλληλες ρυθμίσεις για το firewall και φροντίζει να διευκολύνουν την ασφαλή λειτουργία του OpenVPN κάνοντας τις κατάλληλες προσαρμογές στις ρυθμίσεις έτσι ωστε η κίνηση του OpenVPN να είναι επιτρεπτή.

6. Εγκατάσταση του OpenVPN και των απαραίτητων Dependencies

Το script ξεκινάει με την εγκατάσταση των OpenVPN, OpenSSL και των CA πιστοποιητικών καθώς και όλων των απαραίτητων πακέτων για το τείχος προστασίας. Αυτή η διαδικασία αποτελεί την πλειονότητα του script καθώς και τη βάση μιας ασφαλής και λειτουργικής εγκατάστασης OpenVPN.

7. Εγκατάσταση Easy-RSA και διαχείριση πιστοποιητικών

Για να διαχειριστούν αποτελεσματικά τα πιστοποιητικά το script κάνει λήψη του Easy-RSA και εκτελεί τις κατάλληλες ρυθμίσεις. Το βήμα αυτό είναι πολύ σημαντικό καθώς βελτιστοποιεί την δημιουργία και διαχείριση των πιστοποιητικών ενώ ταυτόχρονα δημιουργεί ένα ασφαλές κανάλι επικοινωνίας εντός του OpenVPN.

8. Διαμόρφωση πελάτη

Ένα από τα βήματα που χαρακτηρίζουν το script είναι η διαδικασία δημιουργίας αρχείων διαμόρφωσης OpenVPN εξατομικευμένων σε κάθε χρήστη. Η προσέγγιση αυτή διευκολύνει την ασφαλή σύνδεση των χρηστών με τον διακομιστή OpenVPN.

9. Διαμόρφωση δικτύου

Πέρα από την άμεση ρύθμιση του OpenVPN το script κάνει τις απαραίτητες ρυθμίσεις επίσης και στο δίκτυο επιτρέποντας την προώθηση IP και ορίζοντας του απαραίτητους κανόνες NAT.

10. Πρόσθετες επιλογές για υπάρχουσες εγκαταστάσεις

Τέλος, το script σε περιπτώσεις που το OpenVPN είναι ήδη εγκατεστημένο προσφέρει επιλογές οι οποίες δίνουν τη δυνατότητα στους χρήστες να μπορούν με ευκολία να προσθέτουν ή να ανακαλούν πελάτες καθώς επίσης και να καταργούν το OpenVPN.

IV. Ανάλυση αποτελεσμάτων

Σε αυτή την ενότητα θα εξεταστούν τα αποτελέσματα της υλοποίησης του οικιακού εικονικού ιδιωτικού δικτύου αξιολογώντας διάφορες πτυχές του όπως η επίδοση, η ασφάλεια, η ευκολία χρήσης καθώς και η συνοχή του με το θεωρητικό κομμάτι.

1. Αξιολόγηση απόδοσης

Έπειτα από εκτενής χρήση και ελέγχους με εξειδικευμένα εργαλεία, μετρήθηκε η ταχύτητα αλλά και η αξιοπιστία της υλοποίησης. Τα αποτελέσματα των μετρήσεων απέδειξαν πως η υλοποίηση παρέχει σταθερές ταχύτητες και έχει ελάχιστο latency χαρακτηρίζοντας την απόδοσή του εξαιρετική. Η απόδοση αυτή ευθυγραμμίζεται με τα ευρέως διαδεδομένα και αναμενόμενα αποτελέσματα που υπάρχουν για τέτοιες υλοποιήσεις επιβεβαιώνοντας τη σωστά διαμορφωμένη υλοποίηση.

2. Αξιολόγηση ασφάλειας

Όσον αφορά την ασφάλεια χρησιμοποιήθηκε ένας συνδυασμός από μέτρα ασφαλείας τόσο για την ενίσχυση ασφάλειας του VPN όσο και της πρόσβασης στο διακομιστή. Αρχικά έγινε χρήση του OpenVPN το οποίο είναι ευρέως χρησιμοποιούμενο και ισχυρό πρωτόκολλο το οποίο εγγυήθηκε μια ασφαλή επικοινωνία. Επιπλέον, περιορίστηκε σκόπιμα η καταγραφή των συμβάντων σε αρχείο έτσι ώστε η περιήγηση να είναι πραγματικά ελεύθερη και πουθενά καταγεγραμμένη προσφέροντας ιδιωτικότητα.Ταυτόχρονα βελτιώθηκε και η ασφάλεια στο διακομιστή ξεκινώντας με τον πολλαπλό έλεγχο ταυτότητας των χρηστών ο οποίος έγινε με τη χρήση κωδικού πρόσβασης αλλά και κωδικού μιας χρήση μέσω του google-authenticator. Επίσης έγινε χρήση κλειδιών SSH αλλά και έγιναν αλλαγές στις προκαθορισμένες ρυθμίσεις που καθιστούσαν το διακομιστή επιρρεπή σε επιθέσεις απο αυτοματοποιημένα ρομπότ ενισχύοντας σε περαιτέρω επίπεδα την ασφάλεια. Ο συνδυασμός των μέτρων αυτών ασφαλείας ακολουθά τα προβλεπόμενα που αναλύθηκαν στο θεωρητικό κομμάτι ενώ ταυτόχρονα κάνει ξεκάθαρη την ιδιαίτερη βαρύτητα που δόθηκε στην ασφάλεια του οικιακού εικονικού ιδιωτικού δικτύου.

3. Αξιολόγηση ευχρηστίας

Η εμπειρία χρήσης της υλοποίησης αποδείχτηκε μια φιλική προς τον χρήστη και εύκολη σε δυσκολία διαδικασία. Η διαδικασία ρύθμισης του εικονικού ιδιωτικού δικτύου ήταν αυτοματοποιημένη και εύκολη και οι περαιτέρω προσθήκες για ενίσχυση της ασφάλειας αν και χρονοβόρες σε μερικά σημεία δεν αποτελεσαν πολύπλοκη διαδικασία. Συνολικά ήταν μια απλοποιημένη και εύκολα αναπαραγώγιμη διαδικασία ιδιαίτερα με την αναλυτική περιγραφή που αναπτύχθηκε στην εργασία.

V. Συμπεράσματα

Ολοκληρώνοντας αυτήν τη έρευνα στο θέμα των βέλτιστων πρακτικών εικονικών ιδιωτικών δικτύων η μελέτη έχει αναλύσει το θεωρητικό κομμάτι και έχει εστιάσει και σε πρακτική υλοποίηση. Ως πρωτεύον στόχο η διπλωματική έχει τη συμβολή στην ανάπτυξη ασφαλέστερων και καλύτερων υλοποιήσεων VPNs παρέχοντας μια ολοκληρωμένη έρευνα γύρω από όλες τις διαφορετικές πτυχές που πρέπει να διερευνηθούν για την υλοποίηση VPN σε βέλτιστο επίπεδο. Ταυτόχρονα, από τη θεωρία στην πράξη, υλοποιήθηκε ένα οικιακό VPN με τη χρήση του πρωτοκόλλου OpenVPN. Λαμβάνοντας υπόψη την ασφάλεια και τη θεωρητική ανάλυση που προηγήθηκε, χρησιμοποιήθηκαν μέτρα ασφαλείας όπως πολιτικές ελέγχου ταυτότητας πολλαπλών παραγόντων(MFA) και έλεγχοι πρόσβασης μέσω κλειδιών SSH δίνοντας στην ασφάλεια την βαρύτητα που απαιτείται. Η μελετημένη επιλογή των πρωτοκόλλων και των μέτρων ασφαλείας έγινε σε ευθυγράμμιση με τη θεωρητική ανάλυση βάζοντας σε λειτουργία τις έννοιες που αναλύθηκαν στο θεωρητικό κομμάτι.

Για κάθε χρήστη ή οργανισμό που ο σκοπός του είναι να επιτύχει τη βέλτιστη δυνατή υλοποίηση VPN, θα πρέπει να κατανοήσει σε βάθος τις οργανωτικές ανάγκες του οργανισμού να επιλέξει προσεκτικά τα πρωτόκολλα που θα χρησιμοποιήσει όπως επίσης και τα μέτρα ασφαλείας. Αρχικά, θα πρέπει να υπάρχει πλήρης κατανόηση των ποικίλων διαθέσιμων τύπων VPN έτσι ώστε για να υπάρξει η σωστή επιλογή του τύπου VPN που αντιστοιχεί καλύτερα στην περίπτωση με βάση τις ανάγκες. Στη συνέχεια και σύμφωνα με το θεωρητικό πλαίσιο θα πρέπει να αξιολογηθούν τα πρωτόκολλα όπως το IPSEC, το SSL/TLS και το Wireguard και σύμφωνα με την μελέτη στα πλεονεκτήματα και αδυναμίες της κάθε επιλογής να επιλεχθεί το κατάλληλο πρωτόκολλο που θα συνεισφέρει καλύτερο στο επιθυμητό αποτέλεσμα. Τέλος, καθώς η ασφάλεια είναι πρωταρχικής σημασίας η μεγαλύτερη έρευνα θα πρέπει να αφορά την επιλογή και εφαρμογή των μέτρων ασφαλείας. Απο τις μεθόδους ελέγχου ταυτότητα όπως είναι ο έλεγχος ταυτότητας πολλαπλών παραγόντων, ο έλεγχος ταυτότητας με βάση τα πιστοποιητικά και ο έλεγχος ταυτότητας μέσω διαπιστευτηρίων μέχρι τις πολιτικές ελέγχου πρόσβασης θα πρέπει να αφιερωθεί ο χρόνος και η απαραίτητη έρευνα για να διασφαλιστεί μια μελετημένη απόφαση και υλοποίηση των μέτρων ασφαλείας.

Προτάσεις για βελτίωση

Παρόλο που η συγκεκριμένη υλοποίηση αποδείχθηκε αρκετά καλή και τα μέτρα ασφαλείας ικανοποιητικά, περιθώρια για βελτίωση υπάρχουν σε κάθε υλοποίηση. Ως προτεινόμενες κινήσεις είναι η περαιτέρω διερεύνηση πρωτοκόλλων κρυπτογράφησης, η βελτίωση και προσθήκη περισσότερων ελέγχων ταυτότητας του χρήστη καθώς και η χρήση και έλεγχος της απόδοσης και ευχρηστίας της συγκεκριμένης υλοποίησης εικονικού ιδιωτικού δικτύου σε ένα ευρύτερο φάσμα

συσκευών. Με τις παραπάνω προτεινόμενες βελτιώσεις, θα διερευνηθεί και ταυτόχρονα εξελιχθεί σε μεγαλύτερο βαθμό η ασφάλεια της υλοποίησης του εικονικού ιδιωτικού δικτύου ενώ ως καινούργια αποτελέσματα θα προκύψουν από την απόδοση και το επίπεδο ευχρηστίας στις καινούργιες συσκευές που θα διερευνηθούν.

VI. Βιβλιογραφία

[1] “Open source system OpenVPN in a function of Virtual Private Network”, Skendzic, Kovacic

[2] “Common Vulnerabilities Exposed in VPN – A Survey”, Rama Bansode, Anup Girdhar

[3] “Everything VPN is New Again”, David Crawshaw

[4] “Overview of quantum key distribution technique within IPSec architecture”, Emir Dervisevic, Miralem Mehic

[5] “More than a Password” CISA, https://www.cisa.gov/MFA

[6] “Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks”, Si Thu Aung, Thandar Thein

[7] “VPN site to site implementation using protocol L2TP and IPSEC”, Budi Santoso, Asrul Sani, T. Husain, Nedi Hendri

[8] “MPLS based VPN Implementation in a Corporate Environment”, Farooq Ahmed, Zain Ul Abedin Butt, Uzair Ahmad Siddiqui

[9] “Cybersecurity of remote work migration: A study on the VPN security landscape post covid-19 outbreak”, Kushtrim Qollakaj, Lukas Einler Larsson

[10] “Analysis of Security Virtual Private Network (VPN) Using OpenVPN”, Muhammad Iqbal , Imam Riadi

[11] “Protecting Information with Cybersecurity”, John M. Borky, Thomas H. Bradley

[12] “Role-Based Access Control”, Ravi S. Sandhu