Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Βελτίωση Ασφάλειας Δικτύου με SDN:Software Defined Networking

Λοΐζος Τσιάτταλος

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Μάιος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Βελτίωση Ασφάλειας Δικτύου με SDN:Software Defined Networking

Λοΐζος Τσιάτταλος

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2020

Περίληψη

Η τεχνολογική εξέλιξη και η ανάπτυξη της επιστήμης των υπολογιστών στη σημερινή εποχή οδήγησε στην εισαγωγή <<έξυπνων>> συσκευών σε κάθε πτυχή της καθημερινότητας. Αυτή η ραγδαία αύξηση κινητών τηλεφώνων, ηλεκτρονικών υπολογιστών και κάθε λογής συσκευής που χρησιμοποιεί το διαδίκτυο και η δικτύωση (τεχνολογίες IoT) ανέβασε κατακόρυφα τον όγκο δεδομένων που διακινούνται μέσω των δικτύων, καθώς επίσης και την ανάγκη για ταχύτητα στη διακίνηση όλων αυτών των πακέτων δεδομένων. Η πολυπλοκότητα και η στατικότητα των παραδοσιακών δικτύων αποτέλεσε τροχοπέδη στις ανάγκες των σύγχρονων χρηστών και επιχειρήσεων για την ανάπτυξη καινοτόμων παροχών προς τους πελάτες τους. Το σύγχρονο δυναμικό περιβάλλον και η ταχύτατη εξέλιξη της τεχνολογίας οδήγησε τις εταιρείες στην εξεύρεση νέων λύσεων όσων αφορά τη δικτύωση τους, ώστε να αυξηθεί η ταχύτητα, η ευελιξία και να μειωθεί το κόστος των δικτυακών εφαρμογών. Κάπως έτσι οδηγήθηκαν στις Software Define Networking (SDN) αρχιτεκτονικές.

Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι να προσδιορίσει αν μπορούν τελικά τα SDN να προσφέρουν την απαιτούμενη ασφάλεια. Αρχικά, γίνεται μια παρουσίαση της αρχιτεκτονικής των SDN δικτύων και παρουσιάζονται τα πλεονεκτήματα τους έναντι των παραδοσιακών. Στη συνέχεια, ακολουθεί μία σύντομη περιγραφή του πρωτοκόλλου OpenFlow, που αποτελεί το βασικό πρωτόκολλο επικοινωνίας στα SDN δίκτυα και γίνεται επεξήγηση των μηνυμάτων που ανταλλάσσονται. Ακολούθως, μελετώνται οι υπάρχουσες εφαρμογές που έχουν σχεδιαστεί για την παροχή ενισχυμένης ασφάλειας σε διάφορους τομείς δικτύωσης. Στο εμπειρικό-πρακτικό κομμάτι της διατριβής, γίνονται οι προσομοιώσεις ενός δικτύου SDN και ενός παραδοσιακού και πραγματοποιείται επίθεση άρνησης εξυπηρέτησης για να εξεταστεί η συμπεριφορά τους ως προς την ασφάλεια. Τέλος, γίνεται αναφορά στις προκλήσεις που αντιμετωπίζουν τα SDN δίκτυα σε θέματα ασφάλειας, παρουσιάζονται διάφορες λύσεις και προτείνονται οδηγίες ανάπτυξης για ασφαλή χρήση τους.

Λέξεις - Κλειδιά: SDN, network security, threats, software, solutions, applications

Summary

The technological advancement and development of computer science nowadays has led to the introduction of 'smart' devices in every aspect of everyday life. This rapid growth of mobile phones, computers and all kinds of devices used by the internet and networking (IoT technologies) has dramatically increased the amount of data circulating through networks as well as the need for speed in the handling of all these data packets. The complexity and staticity of traditional networks has been a stumbling block to the needs of modern users and businesses to develop innovative services to their customers. The modern dynamic environment and the rapid development of technology have led companies to find new solutions for their networking, in order to increase speed, flexibility and reduce the cost of web applications. This is how Software Define Networking (SDN) architecture was led.

The purpose of this postgraduate dissertation is to determine whether SDN can ultimately provide the required security. In the beginning, a presentation of the architecture of SDN networks is made and their advantages over traditional ones are presented. Next, there is a brief description of the OpenFlow protocol, which is the main communication protocol in SDN networks, following by an explanation of the messages that will be exchanged.
Moreover, the existing applications which designed to provide enhanced security in various networking areas are studied. In the empirical-practical part of the dissertation, the simulations of an SDN and a traditional network are implented and a distributed denial of service attack is carried out to examine their security behavior. Finally, the challenges that SDN networks facing in terms of security are addressed, various solutions are presented and guidelines are proposed for their secure use.

Key Words: SDN, network security, threats, software, solutions, applications

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια μου κα. Αδαμαντίνη Περατικού, για την χρήσιμη καθοδήγηση που μου παρείχε κατά τη διάρκεια εκπόνησης της μεταπτυχιακής μου διατριβής και για την άψογη συνεργασία που είχαμε όλο αυτό το διάστημα. Ευχαριστώ επίσης την οικογένεια και τους φίλους μου για την στήριξη και τις πολύτιμες συμβουλές τους καθ'όλη τη διάρκεια των σπουδών μου και ιδιαίτερα τον τελευταίο χρόνο.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

1.1 Σκοπός

Το Software Defined Networking παρέχει μια νέα τεχνολογία στα δίκτυα υπολογιστών. Σε αυτή τη διατριβή, θα αναλυθεί η τεχνολογία των SDN για να προσδιοριστεί αν μπορεί να προσφέρει βελτιώσεις στην ασφάλεια των δικτύων. Αναμένεται να παρουσιαστούν οι υπάρχουσες εφαρμογές που σχεδιάστηκαν για παροχή ενισχυμένης ασφάλειας, να ερευνηθούν οι υπάρχουσες λύσεις και να προταθούν οδηγίες ανάπτυξης για ασφαλή χρήση τους.

1.2 Βασικά Ερευνητικά Ερωτήματα

Τα βασικά ερευνητικά ερωτήματα που αναμένεται να απαντηθούν στην παρούσα διατριβή είναι:

1. Γιατί είναι αναγκαία η τεχνολογία των SDN Networks;

2. Ποιες είναι οι υπάρχουσες εφαρμογές που έχουν σχεδιαστεί για παροχή ενισχυμένης ασφάλειας;

3. Ποιες είναι οι υπάρχουσες λύσεις που παρέχουν καλύτερη ασφάλεια;

4. Μπορούν τελικά τα SDN να προσφέρουν την απαιτούμενη ασφάλεια;

1.3 Αναγκαιότητα και σπουδαιότητα της έρευνας

Ο αριθμός των δικτυακών συνδεδεμένων συσκευών ολοένα και αυξάνεται επιβαρύνοντας τα επικοινωνιακά δίκτυα καθιστώντας τα δυσκολότερα στη διαχείριση. Η ανάγκη για αντικατάσταση των στατικών δικτύων ethernet σε δυναμικά επίφερε στα SDN την ανάγκη για μετατροπή των ethernet δικτύων σε cloud για καλύτερο έλεγχο κυκλοφορίας. Η χρήση SDN προσφέρει τη δυνατότητα για πιο αποδοτικά και ασφαλή δίκτυα. Ο σκοπός της διατριβής είναι να προσδιορίσει αν μπορούν τα SDN να προσφέρουν την ζητούμενη ασφάλεια.

1.4 Δομή της Μεταπτυχιακής Διατριβής

Στο κεφάλαιο 2, γίνεται μια πρώτη εισαγωγή στην τεχνολογία των SDN δικτύων, επεξηγείται η αρχιτεκτονική τους, αναφέρονται οι διαφορές τους σε σχέση με τα παραδοσιακά και παρουσιάζονται τα πλεονεκτήματα τους.

Στο κεφάλαιο 3, γίνεται επεξήγηση της μεθοδολογίας που θα χρησιμοποιηθεί.

Στο κεφάλαιο 4, γίνεται αναφορά στο πρωτόκολλο OpenFlow, που αποτελεί το βασικό τρόπο επικοινωνίας στα SDN δίκτυα, επεξήγηση των τρόπων επικοινωνίας και περιγραφή των μηνυμάτων που ανταλλάσσονται.

Στο κεφάλαιο 5, περιλαμβάνονται οι βασικές εφαρμογές που σχεδιάστηκαν σε διάφορους τομείς δικτύωσης (WLAN, Campus, Data Center) για παροχή ενισχυμένης ασφάλειας.

Στο κεφάλαιο 6, παρουσιάζονται τα αποτελέσματα των πειραμάτων που εκτελέστηκαν για σύγκριση των SDN δικτύων με τα παραδοσιακά και καταγράφεται η συμπεριφορά τους ως προς την ασφάλεια μετά την εκτέλεση κακόβουλης επίθεσης.

Στο κεφάλαιο 7, γίνεται αναφορά στις προκλήσεις που αντιμετωπίζουν τα SDN δίκτυα σε θέματα ασφάλειας, προτείνονται διάφορες λύσεις καθώς και οδηγίες ανάπτυξης για ασφαλή χρήση τους.

Στο κεφάλαιο 8, η διατριβή ολοκληρώνεται με σύνοψη των θεμάτων που μελετήθηκαν και γίνεται αναφορά σε πιθανή μελλοντική έρευνα.

Κεφάλαιο 2
Βιβλιογραφική Ανασκόπηση

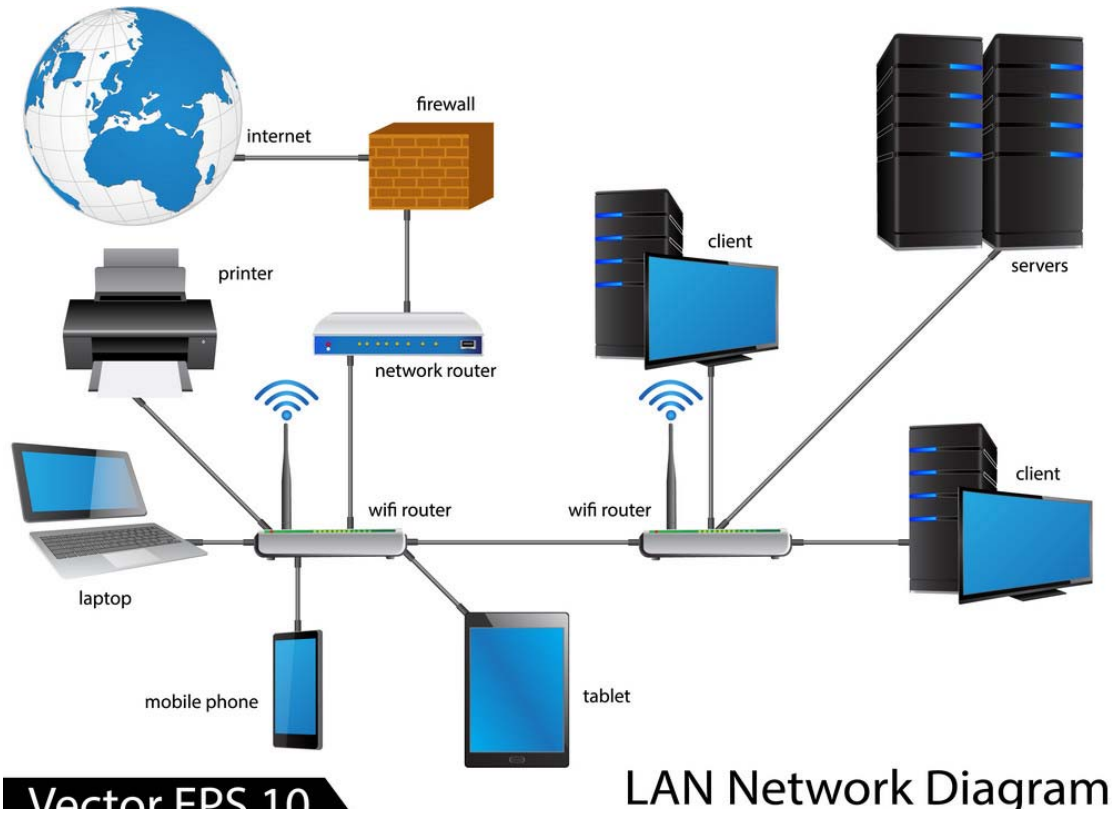
Το Software Defined Networking είναι μια συναρπαστική τεχνολογία που επιτρέπει την καινοτομία στον τρόπο σχεδιασμού και διαχείρισης των δικτύων. Αν και αυτή η τεχνολογία φαίνεται να έχει εμφανιστεί ξαφνικά, το SDN είναι μέρος μιας μακράς ιστορίας προσπαθειών για να καταστήσουν τα δίκτυα υπολογιστών περισσότερο προγραμματιζόμενα.

Σε αυτό το πρώτο κεφάλαιο θα γίνει μια πρώτη εισαγωγή στην τεχνολογία των SDN δικτύων, επεξήγηση της αρχιτεκτονικής τους, παρουσίαση των διαφορών τους καθώς και των πλεονεκτημάτων τους σε σύγκριση με τα παραδοσιακά.

2.1 Παραδοσιακά Δίκτυα και SDN

Τα υπάρχοντα δίκτυα υπολογιστών αποτελούνται από routers, switches, servers και firewalls. Κάθε μια από αυτές τις συσκευές επιτελεί ένα ξεχωριστό ρόλο μέσα στο δίκτυο. Τα switches είναι ο πυρήνας ενός LAN, καθώς είναι η συσκευή στην οποία συνδέονται τα τερματικά ενός τοπικού δικτύου, προσφέροντας υψηλές ταχύτητες διασύνδεσης μεταξύ του. Το router είναι η συσκευή που ενώνει δύο ή περισσότερα τοπικά δίκτυα. Οι servers, είτε ως συσκευές υλικού είτε ως virtual machines, περιλαμβάνουν δεδομένα και εφαρμογές στα οποία θέλουν να έχουν πρόσβαση οι

χρήστες του δικτύου. Τα firewall, είτε ως λογισμικό είτε ως συσκευές, ελέγχουν την πρόσβαση στο δίκτυο.



Εικόνα 2.1: Παραδοσιακά Δίκτυα

Για την παραμετροποίηση ενός παραδοσιακού δικτύου απαιτείται η διαμόρφωση κάθε συσκευής του δικτύου ξεχωριστά. Προκειμένου να εισαχθεί μια καινούρια συσκευή στο δίκτυο πρέπει όλες οι υπάρχουσες συσκευές να ενημερωθούν για την καινούρια συσκευή που εισέρχεται. Η ενημέρωση αυτή γίνεται χειροκίνητα, συνήθως στο CLI κάθε συσκευής. Η χειροκίνητη αυτή ενημέρωση είναι πολύ κοστοβόρα από άποψης χρόνου, χρειάζονται από κάποιες ώρες έως εβδομάδες για την ενημέρωση όλων των συσκευών του δικτύου, και εμπεριέχει μεγάλο κίνδυνο λάθους λόγω του ανθρώπινου παράγοντα.

Ένα ακόμη μεγάλο πρόβλημα που προκύπτει είναι η πιθανότητα ασυμβατότητας της νέας συσκευής που πρέπει να συνδεθεί στο δίκτυο. Το υπάρχοντα δίκτυα χρησιμοποιούν πρωτόκολλα επικοινωνίας τα οποία διαμορφώνει ο κατασκευαστής. Νέα συσκευή με νεότερο ή διαφορετικό πρωτόκολλο επικοινωνίας αντιμετωπίζει πρόβλημα σύνδεσης. Για να λυθεί αυτό το πρόβλημα συνήθως απαιτείται ενημέρωση λογισμικού από τον κατασκευαστή, το οποίο πολλές φορές απαιτεί πολύ χρόνο για να διαμορφωθεί.

Τέλος, τα πρωτόκολλα επικοινωνίας εξελίσσονται για να προσφέρουν βελτιωμένες υπηρεσίες αλλά αυτό επίσης καθιστά την αναβάθμιση των δικτυακών υποδομών πολύ κοστοβόρα για τους λόγους που προαναφέρθηκαν. Επίσης, αν μια εταιρεία θελήσει να κάνει αναβάθμιση του εξοπλισμού της δημιουργείται μεγάλη δυσκολία μεταφοράς από το παλιό δίκτυο στο καινούριο χωρίς να υπάρξει διακοπή παροχής υπηρεσιών. Τέτοια μεγάλα προβλήματα αντιμετωπίζουν κολοσσιαίες εταιρείες όπως η Google, Facebook, Amazon και λοιπές.

Αυτά τα προβλήματα προσπαθούν να λυθούν με τα SDN τα οποία διαχωρίζουν τη διαχείριση του δικτύου. Τη διαχείριση αναλαμβάνει ένας controller που βλέπει όλες τις συσκευές μέσα στο δίκτυο, είναι προγραμματιζόμενος σε γλώσσα υψηλού επιπέδου και μπορεί να γίνει εικονική προσομοίωση μια νέας εφαρμογής χωρίς να χρειάζεται να πειραχτεί το υπάρχον δομημένο δίκτυο. Ο controller λειτουργεί ως ο εγκέφαλος του δικτύου, στον οποίο διαμορφώνονται όλες οι λειτουργίες του δικτύου, ενώ οι υπόλοιπες συσκευές λειτουργούν ως πομποδέκτες δεδομένων.

2.2 Πώς φτάσαμε στα SDN δίκτυα, Ιστορική Αναδρομή

Μέχρι το 1981 τα δίκτυα λειτουργούσαν με κεντρικοποιημένο έλεγχο, δηλαδή ήταν μονοκαναλικά και όλες οι διεργασίες βασίζονταν σε συχνότητες λειτουργίας. Το 1981 η AT&T παρουσίασε το Network Point το οποίο διαχώρισε τον έλεγχο του δικτύου από τα δεδομένα που διακινούνταν σε αυτό.

Στις αρχές της δεκαετίας του 90 παρουσιάστηκαν τα Active Networks, προάγγελος των Programmable Networks, στα οποία άρχισαν να γίνονται κάποιες πρώτες διεργασίες επάνω στα πακέτα δεδομένων όπως route trace, proxy, firewall και άλλες εφαρμογές. Τα δίκτυα αυτά χρειάστηκαν περίπου μια δεκαετία για να πρωτοτυποποιηθούν, να αναπτυχθούν και να κυριαρχήσουν στη δικτυακή αγορά. Τα δίκτυα αυτά αποτελούνταν από δύο δομές, το Capsules στο οποίο κάθε μήνυμα είναι κομμάτι προγράμματος και αξιολογείται από το Node και τα Programmable Switches όπου συναρτήσεις τρέχουν στους δρομολογητές και τα πακέτα δρομολογούνται μέσω των προγραμματιζόμενων κόμβων καθώς το πρόγραμμα που τρέχει για τη δρομολόγηση του πακέτου εξαρτάται από το περιεχόμενο στο header του πακέτου.

Πέραν των πολλών πλεονεκτημάτων τους, στα Active Networks έγιναν αντιληπτές παθογένειες σε τομείς όπως η ασφάλεια, η ταχύτητα του δικτύου, το κόστος του εξοπλισμού. Λύση σε αυτά ήρθε να δώσει το OpenFlow, το οποίο θα αναλύσουμε στο κεφάλαιο 2.

Την ίδια περίπου εποχή εμφανίστηκε και άρχισε να αναπτύσσεται το Network Virtualization[07] και έγινε εφικτή η δυνατότητα αναπαράστασης περισσότερων δικτυακών τοπολογιών σε μια υπάρχουσα δικτυακή υποδομή. Τέτοιες εφαρμογές είναι το Nicira, τα VLANs, VMWare, Vini, Tempest. Πλεονεκτήματα αυτών των εφαρμογών είναι ο διαμοιρασμός των πόρων καθώς σε μια κοινή πλατφόρμα λειτουργούν πολλοί δρομολογητές χρησιμοποιώντας κοινή κεντρική μονάδα επεξεργασίας (CPU) , κοινή μνήμη, Forwarding Tables και Bandwidth. Σε αυτή την πλατφόρμα μπορούμε να έχουμε εξειδικευμένο λογισμικό βάσει των εκάστοτε αναγκών, το οποίο συγκεκριμενοποιεί τις αναγκαίες πολιτικές δρομολόγησης και προώθησης πακέτων.

Τα παραπάνω οδήγησαν στην ανάπτυξη των SDN[07], καθώς έπαψαν οι δικτυακές υπηρεσίες να άπτονται του δικτυακού εξοπλισμού, έγινε εφικτό να υπάρχουν περισσότεροι του ενός controller σε ένα switch και να έχουμε σε μια δικτυακή υποδομή περισσότερες από μια τοπολογίες.

Το 2003 δημιουργήθηκε η πρώτη εφαρμογή ελέγχου μεταγωγής πακέτων σε δίκτυα, το FORCES. Το FORCES χρησιμοποίησε πρωτόκολλα επικοινωνίας πολλαπλών ελεγκτών και πρωτόκολλα προώθησης πακέτων. Αργότερα προτάθηκε η χρήση των υπαρχόντων πρωτοκόλλων προσδιορισμού διαδρομής για τα προωθούμε να πακέτα μέσω του δικτύου, η τεχνική αυτή ονομάστηκε RCP (Routing Control Platform). Στο RCP η βέλτιστη διαδρομή βρίσκεται από ένα αυτόνομο σύστημα και προτείνεται μέσω του πρωτοκόλλου iBGP. Το 2007 παρουσιάστηκε το Ethane ως αρχιτεκτονική για εταιρικά δίκτυα. Βασίστηκε σε έναν Domain Controller που υπολογίζει τα flow tables με βάση τις υπάρχουσες policies αλλά για να εφαρμοστεί χρειάζονται τροποποιημένα switches, όπως OpenWrt- NetFPGA και Linux. Το 2008 εμφανίζεται το Openflow. Για τη χρήση του απαιτείται οι κατασκευαστές να δημιουργήσουν ένα interface ώστε να επικοινωνούν απευθείας controller και switch.

Όλα αυτά οδήγησαν στη δημιουργία των SDN. Τα SDN είναι ο ουσιαστικός διαχωρισμός του επιπέδου ελέγχου του δικτύου με το επίπεδο προώθησης πακέτων. Αποτελούν μια νέα δυναμική αρχιτεκτονική, εύκολα προσαρμόσιμη, λόγο του προγραμματισμού ενός ελεγκτή, και οικονομικά αποδοτικότερη συγκριτικά με τις προϋπάρχουσες μεθόδους.

2.3 Αρχιτεκτονική SDN δικτύων

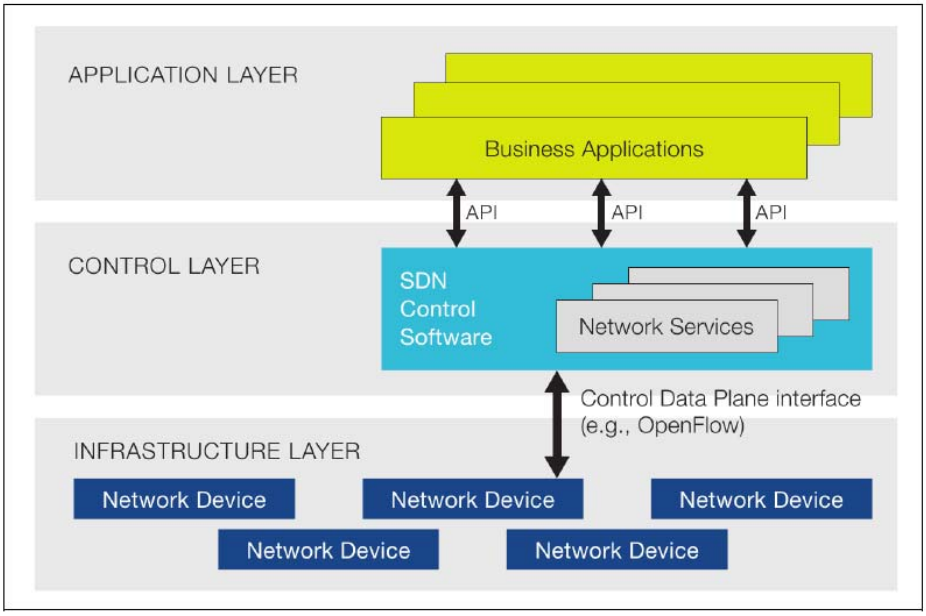
Η αρχιτεκτονική των SDN αποτελείται από 3 δομές[3]:

- Application layer
- Control Layer
- Infrastructure Layer

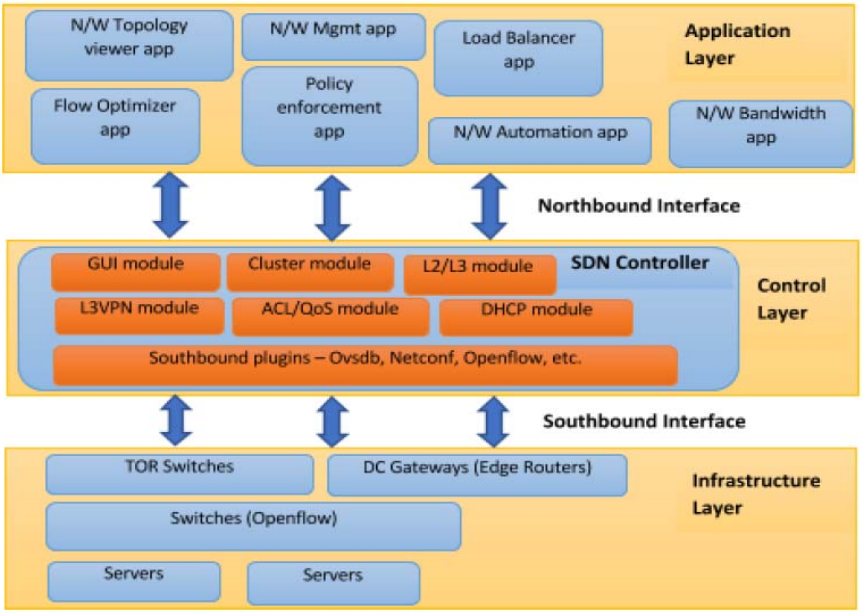
Application layer: Είναι η δομή στην οποία αναπτύσσονται ο κώδικας και οι εφαρμογές. Σε μια υψηλού επιπέδου γλώσσα προγραμματισμού αναπτύσσονται και παραμετροποιούνται εφαρμογές. Είναι επίπεδο φιλικό προς το χρήστη, γίνεται η διαμόρφωση και η διαχείριση του δικτύου, επιλύονται ζητήματα ασφάλειας, επιλύονται τα προβλήματα που προκύπτουν μέσα στο δίκτυο και αυτοματοποιούνται οι διαδικασίες. Σε αυτό το επίπεδο δομούνται και οι εφαρμογές για τις επιχειρήσεις και τους servers.

Control layer: Είναι το επίπεδο του Controller και ο εγκέφαλος του δικτύου. Βρίσκεται ενδιάμεσα του Application και του Infrastructure Layer, και βασικός του ρόλος είναι η προώθηση των εντολών που λαμβάνει από το Application Layer στις διαδικτυακές συσκευές. Ο ελεγκτής δέχεται πληροφορίες, οι οποίες προέρχονται είτε από τα APIs του δικτύου, τα προγράμματα που δίνουν τον τρόπο μεταφοράς των πακέτων, είτε τη διαχείριση των προβλημάτων που προκύπτουν στο δίκτυο, είτε από τις δικτυακές συσκευές, που παρέχουν τις απαραίτητες πληροφορίες για τη μεταφορά των πακέτων, τα προβλήματα που προκύπτουν και στατιστικά στοιχεία της κίνησης του δικτύου. Πολλοί κατασκευαστές προσπαθούν να έχουν ήδη προγραμματίσει κάποιες εφαρμογές στους ελεγκτές που παρέχουν ώστε να υπάρχει μια βέλτιστη χρήση του δικτύου, αλλά και μια απλοποίηση για το διαχειριστή του δικτύου όταν αυτός θέλει να παραμετροποιήσει το δίκτυο και να τρέξει τις προσομοιώσεις λειτουργίας του.

Infrastructure layer: Αυτό το επίπεδο αποτελείται από το δικτυακό εξοπλισμό. Όλες οι δικτυακές συσκευές ανήκουν σε αυτό το επίπεδο και αναλαμβάνουν την προώθηση των πακέτων βάσει των εντολών που δέχονται από τον controller.



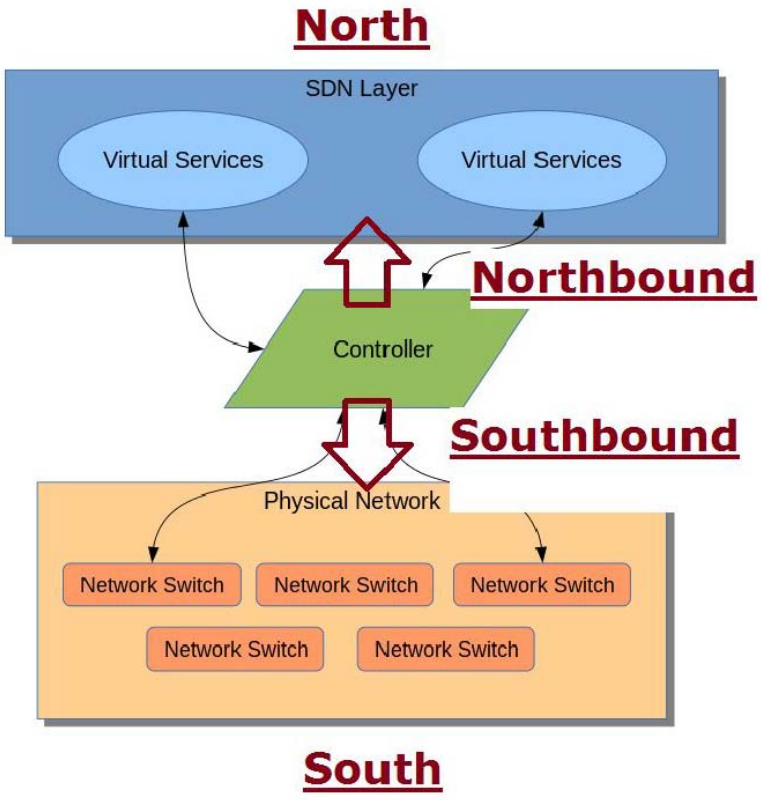
Εικόνα 2.2:Αρχιτεκτονική SDN Δικτύων



Εικόνα 2.3:Συστατικά Αρχιτεκτονικής SDN Δικτύων

NorthBound: Ως Northbound ορίζεται η επικοινωνία του ελεγκτή με τα APIs. Ονομάστηκε έτσι γιατί δείχνει την επικοινωνία με το ανώτερο επίπεδο.

SouthBound: Ως Southbound ορίζεται η επικοινωνία του ελεγκτή με το δικτυακό εξοπλισμό. Ονομάστηκε έτσι γιατί δείχνει την επικοινωνία με το κατώτερο επίπεδο.



Εικόνα 2.4:Northbound και Southbound Interfaces

2.4 Πλεονεκτήματα SDN δικτύων

Η αρχιτεκτονική των SDN προσφέρει πολλά πλεονεκτήματα έναντι των παραδοσιακών δικτύων. Τα πλεονεκτήματα αυτά αναφέρονται :

- Στην κεντρική διαχείριση του δικτύου από ένα ελεγκτή. Αυξάνεται η αξιοπιστία και η ασφάλεια του δικτύου καθώς η διαχείριση της μεταφοράς πακέτων γίνεται από τον ελεγκτή και δεν χάνονται πακέτα, η πολιτική ασφάλειας είναι ενιαία και δυσχεραίνεται η

διείσδυση απειλών στο δίκτυο.

- Μειώνονται ο χρόνος και τα λάθη στη διαμόρφωση του δικτύου, καθώς πλέον δε γίνεται διαμόρφωση κάθε συσκευής χειροκίνητα αλλά κεντρικά από τον ελεγκτή. Επίσης μέσω των εικονικών δικτύων μπορούν να τρέξουν προσομοιώσεις και να προληφθούν αστοχίες.

- Η διαμόρφωση του δικτύου καθίσταται πολύ πιο εύκολη γιατί γίνεται μέσω APIs.

- Η διαμόρφωση του δικτύου γίνεται πιο αποδοτική γιατί κάθε δίκτυο προσαρμόζεται στις ανάγκες των χρηστών του. Τα δίκτυα γίνονται εξειδικευμένα και όχι γενικής χρήσης.

- Τα δίκτυα είναι πιο εύκολα επεκτάσιμα καθότι οι όποιες αλλαγές γίνονται στο διαχειριστικό πρόγραμμα του δικτύου. Έτσι δε χρειάζεται να γίνονται αναβαθμίσεις ή αντικατάσταση του υπάρχοντος εξοπλισμού όποτε χρειάζεται να γίνει κάποια επέκταση στο δίκτυο.

- Η δυνατότητα του προγραμματισμού του δικτυακού περιβάλλοντος σε γλώσσα προγραμματισμού υψηλού επιπέδου βοηθάει στην ανάπτυξη καινοτομιών καθώς και πιο user friendly περιβάλλον για το χρήστη του δικτύου.

Κεφάλαιο 3
Μεθοδολογία

Αρχικά, θα πραγματοποιηθεί βιβλιογραφική επισκόπηση γύρω από την τεχνολογία του SDN. Θα μελετηθούν οι υπάρχουσες εφαρμογές που έχουν σχεδιαστεί για παροχή ενισχυμένης ασφάλειας. Όσον αφορά το εμπειρικό – πρακτικό κομμάτι της διατριβής, θα χρησιμοποιηθούν ποσοτικές μέθοδοι. Τα πρωτογενή δεδομένα θα συλλεγούν με τη χρήση πειραμάτων για να συγκριθεί ένα παραδοσιακό δίκτυο με ένα SDN. Αναλυτικότερα:

- Θα χρησιμοποιηθούν προκαθορισμένα εργαλεία για σχεδιασμό των δύο δικτύων (Oracle VM VirtualBox, Ubuntu, Floodlight Controller, Mininet)

- Θα ληφθούν μετρικές εύρους ζώνης με τη χρήση του εργαλείου iperf

- Θα εκτελεστεί εντολή επίθεσης στα 2 δίκτυα για να διαπιστωθεί η συμπεριφορά τους ως προς την ασφάλεια

Τέλος θα ερευνηθούν οι υπάρχουσες λύσεις και θα προταθούν οδηγίες ανάπτυξης για ασφαλή χρήση των SDN δικτύων.

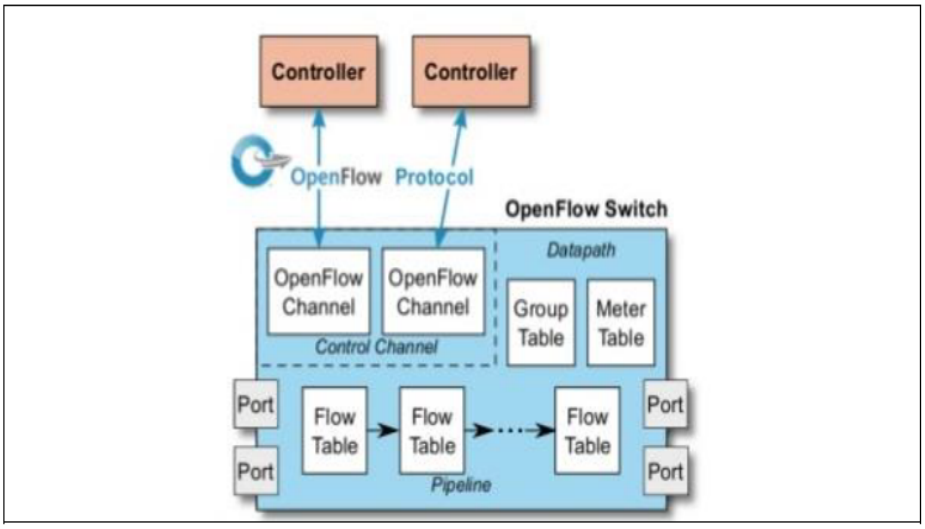
Κεφάλαιο 4
Το Πρωτόκολλο OpenFlow

Το OpenFlow[03] είναι το γνωστότερο και πιο χρησιμοποιούμενο πρωτόκολλο επικοινωνίας μεταξύ Control Layer και Infrastructure Layer. Πολλοί το μπερδεύουν με τα ίδια τα SDN αλλά στην πραγματικότητα αποτελεί κομμάτι τους. Το OpenFlow χρησιμοποιείται ώστε ο έλεγχος του δικτυακού εξοπλισμού να περάσει στον Controller του SDN, αποτελεί ουσιαστικά το southbound του δικτύου.

4.1 Αρχιτεκτονική OpenFlow

Το OpenFlow αποτελείται από δύο δομικά στοιχεία:

- Τον Ελεγκτή (Controller) ο οποίος είναι υπεύθυνος για τον έλεγχο του δικτύου
- Τους μεταγωγείς πακέτων οι οποίοι αποτελούνται από τις θύρες, το ασφαλές κανάλι OpenFlow και τους πίνακες ροών.



Εικόνα 4.1:Αρχιτεκτονική του OpenFlow

Το OpenFlow αποτελεί το μέσο επικοινωνίας μεταξύ του ελεγκτή και των μεταγωγών πακέτων του δικτύου. Η επικοινωνία αυτή γίνεται μέσα από ένα ασφαλές κανάλι, μέσα από το οποίο ο ελεγκτής μπορεί να στέλνει μηνύματα στις δικτυακές συσκευές καθώς και να λαμβάνει μηνύματα από αυτές. Το κανάλι αυτό δημιουργείται μέσω TCP σύνδεσης και συνήθως η επικοινωνία κρυπτογραφείται μέσω του πρωτοκόλλου TLS. Ο μεταγωγέας είναι η συσκευή που λαμβάνει τα μηνύματα-οδηγίες του ελεγκτή και με βάση αυτές τις οδηγίες δρομολογεί τα πακέτα. Η δρομολόγηση των πακέτων βασίζεται σε ένα σύνολο πινάκων ροής (flow tables), η συμπλήρωση των οποίων γίνεται μέσα από τα μηνύματα που στέλνει ο controller. Από τη στιγμή που φτάσουν τα μηνύματα αναλαμβάνει ρόλο ο μεταγωγέας.

Ο μεταγωγέας αποτελείται από κάποια επιμέρους στοιχεία. Τα στοιχεία αυτά είναι τρία: οι φυσικές πύλες, οι λογικές πύλες και οι κλειστές πύλες. Οι φυσικές πύλες είναι αυτές στις οποίες συνδέονται τα καλώδια με τα οποία ο κάθε μεταγωγέας επικοινωνεί με άλλους μεταγωγείς είτε με τερματικές συσκευές του δικτύου. Οι λογικές πύλες αναφέρονται στα κυκλώματα του μεταγωγέα και πως αυτά δημιουργούν το κύκλωμα του. Υπάρχουν και οι κλειστές πύλες που χρησιμοποιούνται για την εσωτερική διαχείριση των πακέτων σε κάθε μεταγωγέα. Οι κλειστές πύλες έχουν 5 κατηγορίες:

- Τις πύλες ALL, οι οποίες είναι οι πύλες στις οποίες μπορούν να προωθηθούν τα πακέτα

- Την πύλη CONTROLLER, η οποία είναι αυτή από την οποία περνάνε τα μηνύματα επικοινωνίας του ελεγκτή με το μεταγωγέα μέσω του ασφαλούς καναλιού.

- Την πύλη TABLE, η οποία είναι η εισαγωγική πύλη σε ένα διασωληνομένο κύκλωμα που παριστάνει τον πίνακα

- Την πύλη IN_PORT, η οποία είναι παράλληλα εισερχόμενη και εξερχόμενη και αφορά τα μηνύματα που επιστρέφουν στο μεταγωγέα.

- Η πύλη ANY, η οποία χρησιμοποιείται είτε ως εισερχόμενη, εξερχόμενη ή οποιαδήποτε πύλη. Είναι η πύλη που χρησιμοποιεί το Openflow όταν δεν έχει κατάλληλη περιγραφή χρειαζούμενης πύλης.

Ακόμη υπάρχουν κάποιες προαιρετικές πύλες:

- Οι πύλες LOCAL οι οποίες είναι εξωτερικές και εσωτερικές πύλες του δικτυακού εξοπλισμού και χρησιμεύουν στην εσωτερική διαχείριση του μεταγωγέα.

- Οι πύλες NORMAL, ώστε ο δικτυακός εξοπλισμός να δουλέψει με τον παραδοσιακό τρόπο και όχι βασισμένος στον ελεγκτή. Αφορά μεταγωγείς οι οποίοι έχουν υβριδική λειτουργία.

- Οι πύλες FLOOD, οι οποίες αφορούν και αυτές υβριδικούς μεταγωγείς και είναι πύλες στις οποίες στέλνει, μέσω παραδοσιακής λειτουργίας, τα πακέτα σε άλλες flooded πύλες.

Σημαντικό κομμάτι της αρχιτεκτονικής του OpenFlow είναι το ασφαλές κανάλι μέσα από το οποίο επικοινωνούν ελεγκτής και μεταγωγέας. Μέσα από αυτό το κανάλι μεταφέρονται τα μηνύματα και τα πακέτα από τον ελεγκτή στο μεταγωγέα και αντίστροφα. Μέσω της TCP σύνδεσης, προσδιορίζεται και η έκδοση του openflow που θα χρησιμοποιηθεί, και αυτή που επιλέγεται είναι η νεότερη έκδοση την οποία υποστηρίζουν και οι δύο. Αν δε βρεθεί κοινή έκδοση που να υποστηρίζουν το σύστημα βγάζει μήνυμα λάθους και η σύνδεση τερματίζεται. Αν δε βρεθεί κοινή έκδοση ο μεταγωγέας μπαίνει σε μια εκ των τριών επόμενων καταστάσεων:

- Fail Secure Mode: όπου ο μεταγωγές σταματά να προσπαθεί να επικοινωνήσει με τον ελεγκτή και δρομολογεί τα πακέτα με τις υπάρχουσες εγγραφές.

- Fail Standalone Mode: Αν ο μεταγωγέας είναι υβριδικός μπαίνει σε παραδοσιακή λειτουργία.

Αν επιτευχθεί ξανά επικοινωνία μεταξύ ελεγκτή και μεταγωγέα μπορεί είτε να ζητηθεί από το μεταγωγέα ανανέωση των υπαρχόντων εγγραφών είτε ο ελεγκτής να κάνει εκκαθάριση εγγραφών και να στείλει καινούριες καθώς οι παλιές εγκυμονούν κινδύνους για το σύστημα.

Ακόμη γίνεται έλεγχος την ποιότητας σύνδεσης με τη μέθοδο ECHO REQUEST /REPLY.

Στόχος της ανταλλαγής μηνυμάτων μεταξύ ελεγκτή και μεταγωγέα είναι η πλήρωση των πινάκων ροής όπου και με βάση αυτές τις εγγραφές γίνεται η διαχείριση των πακέτων από το μεταγωγέα. Οι εγγραφές στον πίνακα ροής αποτελούνται από τα εξής πεδία:

- Match: ορίζει τις προϋποθέσεις για να ταιριάζει ένα πακέτο σε μια εγγραφή
- Priority: ορίζει την προτεραιότητα μια εγγραφής
- Counter: αναφέρεται σε στατιστικά στοιχεία των πακέτων που ταιριάζουν σε κάθε εγγραφή
- Instruction: ορίζει τις ενέργειες που θα εκτελέσει ο μεταγωγέας όταν ένα πακέτο ταιριάζει σε μια εγγραφή
- Timeouts: ορίζει το μέγιστο χρόνο ισχύος μιας εγγραφής
- Flags: ορίζει την αλλαγή τρόπου διαχείρισης των εγγραφών

Αν κάποιο πακέτο ταιριάζει σε παραπάνω από μια εγγραφές τα instructions προσδιορίζουν σε ποιο match θα καταταχθεί το πακέτο.

Επιπλέον είναι σύνηθες να μην υπάρχει μόνο ένας πίνακας ροής αλλά περισσότεροι οι οποίοι συνδέονται μεταξύ τους. Οι πίνακες κατατάσσονται με αύξοντα αριθμό ξεκινώντας από το μηδέν. Κάθε πακέτο που εισέρχεται στο μεταγωγέα ελέγχει τις εγγραφές σε κάθε πίνακα ξεκινώντας από τον πρώτο κινούμενο σε αύξουσα αρίθμηση. Στο τέλος υπάρχει ένας πίνακας table miss για πακέτα που δεν βρίσκουν υπάρχουσα εγγραφή στην οποία ταιριάζουν. Αν δεν υπάρχει table miss πίνακας απορρίπτεται το πακέτο.

Πέραν από τους πίνακες ροής υπάρχουν και οι group πίνακες. Αυτοί οι πίνακες υπάρχουν για τη διαχείριση ενός συνόλου όμοιων πακέτων τα οποία αντιμετωπίζονται με τον ίδιο τρόπο, ως group. Οι group πίνακες αποτελούνται από τις εξής στήλες:

Το group identifier που είναι ένας αριθμός 32 bit και είναι χαρακτηριστικός για την αναγνώριση του group.

Το group type που παίρνει τιμές All και εκτελούνται όλες οι ενέργειες επάνω στα πακέτα, Select που με βάση κάποιο αλγόριθμο εκτελείται ένα υποσύνολο ενεργειών στα πακέτα, Indirect στο οποίο εκτελείται μόνο μια ενέργεια επάνω στα πακέτα και Fast Failover και αφορά ενέργειες επί συγκεκριμένης πύλης όταν σε αυτή την πύλη αποτύχουν οι ενέργειες που είχαν προσχεδιαστεί.

4.2 Επικοινωνία και μηνύματα ελεγκτή-μεταγωγέα

Όπως αναφέρθηκε για τη συμπλήρωση των πινάκων ροής γίνεται ανταλλαγή μηνυμάτων μεταξύ ελεγκτή και μεταγωγέα. Τα μηνύματα αυτά ανήκουν σε 3 διαφορετικές κατηγορίες. Επίσης τα μηνύματα περιλαμβάνουν κάποια δομικά στοιχεία, όπου κάθε δομικό στοιχείο περιλαμβάνει πληροφορίες για τη διαχείριση του πακέτου.

Ξεκινώντας από τις κατηγορίες των μηνυμάτων έχουμε controller-to-switch, asynchronous και symmetric.

Τα controller-to-switch μηνύματα χρησιμοποιούνται για τη διαχείριση του δικτυακού εξοπλισμού. Είναι τα μηνύματα που στέλνει ο ελεγκτής στις δικτυακές συσκευές για τη διαχείριση των πακέτων.

Τα ασύγχρονα μηνύματα στέλνονται από τους μεταγωγείς στον ελεγκτή και αφορούν είτε κάποιο πακέτο που ο μεταγωγέας δε γνωρίζει πως να διαχειριστεί είτε κάποια ενημέρωση που έγινε σε κάποιο πίνακα ροής του.

Τα συμμετρικά μηνύματα είναι μηνύματα που στέλνονται και από τους μεταγωγείς και από τον ελεγκτή και είναι hellos, requests, replies και echo. Είναι μηνύματα που ελέγχουν την επικοινωνία μεταξύ ελεγκτή και μεταγωγέα.

Εν συνεχεία, τα μηνύματα αυτά έχουν μια δομή. Αναλυτικότερα η δομή των μηνυμάτων περιλαμβάνει τα εξής δομικά στοιχεία: version, type, length και transaction id.

Το version αναφέρεται στην έκδοση του Openflow που θα χρησιμοποιηθεί.

Το type δείχνει το είδος του μηνύματος.

Το length δείχνει το μήκος του μηνύματος.

Το transaction id (XID) ξεχωρίζει κάθε μήνυμα από ένα άλλο όμοιο με αυτό.

4.3 Διαχείριση πακέτων

Τα μηνύματα, όπως έχει αναφερθεί, τα στέλνει ο ελεγκτής στο μεταγωγέα ώστε να συμπληρωθούν οι πίνακες ροής και να γίνει η διαχείριση των πακέτων. Το κομμάτι του πίνακα που είναι υπεύθυνο για να ορίσει σε ποια κατηγορία ανήκει ένα πακέτο είναι η στήλη match του πίνακα ροής. Σε αυτή τη στήλη είναι δυνατό να παραχωρηθούν οι εξής 4 τιμές:

Flow match: αναφέρεται σε έναν συνδυασμό παραμέτρων όπως οι διευθύνσεις layer 2 και layer 3, τα QoS bits και οι πύλες του TCP.

Header match: αναφέρεται σε πεδία που αντιστοιχούν με τους headers των Layer 2 και Layer 3 πακέτων.

Pipeline match: αναφέρεται σε πεδία που προστίθενται στα πακέτα για την προσπέλαση τους σε περίπτωση πολλαπλών πινάκων.

Experimenter Flow match: ένα προαιρετικό πεδίο που μπορεί να χρησιμοποιηθεί σε περιπτώσεις ερευνών και δοκιμών και γι' αυτό τον λόγο δεν διαθέτει καθορισμένες επιλογές.

Όταν επιλεχθεί η κατάλληλη εγγραφή για το κάθε πακέτο, ορίζεται ένα σετ ενεργειών για την διαχείριση του. Το σετ των ενεργειών που θα ακολουθηθεί αποτελείται από 6 δομικά στοιχεία. Τα 6 αυτά στοιχεία είναι τα instructions, instruction sets, actions, actions sets, action lists, action bucket. Αναλυτικότερα :

Τα instructions έχουν 6 κατηγορίες και αφορούν αλλαγές σε πακέτα, σε εγγραφές, προσπέλαση πινάκων και κάποιες αφορούν actions.

Τα instruction sets που αποτελούν ένα σύνολο instructions, μέχρι 6 και από διαφορετική κατηγορία.

Τα actions που είναι οι προς εκτέλεση ενέργειες.

Οι action lists που κάθε μία μπορεί να περιλαμβάνει ενέργειες, μία ή περισσότερες, που σχετίζονται με την Apply-Actions instruction, όπου οι ενέργειες εκτελούνται με τη σειρά που είναι στη λίστα, ή με την Write-Actions instructions, όπου οι ενέργειες μεταφέρονται στα action set και δεν εκτελούνται, ή με τα πακέτα PACKET-OUT, τα οποία είναι πακέτα που στέλνει ο ελεγκτής για την τροποποίηση ή τη μεταφορά κάποιου πακέτου. .

Τα action sets χρησιμοποιούνται κατά την προσπέλαση πολλαπλών πινάκων. Καθώς ένα πακέτο συγκρίνει τις εγγραφές όλων των πινάκων σε περίπτωση που βρει εγγραφή που ταιριάζει προσθέτει τις action list των εγγραφών με write-instructions στο action set του. Με το τέλος των πινάκων, εκτελούνται οι ενέργειες που περιέχονται στο action set του. Κάθε action set μπορεί να περιέχει μόνο ένα είδος ενέργειας.

Τα action buckets που είναι ένα σύνολο από action sets και χρησιμοποιούνται σε περιπτώσεις group πινάκων.

Κεφάλαιο 5

Εφαρμογές SDN για ενίσχυση της ασφάλειας δικτύωσης

Στο κεφάλαιο αυτό, θα παρουσιαστούν οι σημαντικότερες εφαρμογές που σχεδιάστηκαν για ενίσχυση της ασφάλειας σε διάφορους τομείς δικτύωσης. Ειδικότερα θα γίνει αναφορά στις εφαρμογές των δικτύων SDN σε ασύρματα δίκτυα (WLAN), σε δίκτυα κινητής τηλεφωνίας, σε δίκτυα που χρησιμοποιούνται σε κέντρα δεδομένων (Data Centers) , καθώς και σε δίκτυα εκπαιδευτικών ιδρυμάτων (Campus -πανεπιστημίων).

5.1 To WLAN Enviroment

Το OpenRoads[25], είναι από τις πιο αποτελεσματικές εφαρμογές των δικτύων SDN που χρησιμοποιούνται σε ασύρματα τοπικά δίκτυα. Το OpenRoads, χρησιμοποιεί το OpenFlow και αξιοποιεί την κινητικότητα από το φυσικό δίκτυο, ώστε να επιτρέψει σε πολλούς παρόχους να ελέγχουν και να διαμορφώνουν ταυτόχρονα την υποδομή ενός δικτύου. Η πλατφόρμα OpenRoads στοχεύει στο να επιτρέψει την πειραματική έρευνα χρησιμοποιώντας ελεγκτή ανοιχτού κώδικα και να την επεκτείνει ώστε να ελέγχει και να εντοπίζει ασύρματα συμβάντα, όπως η σύνδεση host-AP. Ένα σημαντικό πλεονέκτημα του OpenRoads είναι το γεγονός ότι είναι ανοιχτού κώδικα (open source) , και όλα τα εργαλεία που χρησιμοποιούνται, αναπτύσσονται και εφαρμόζονται από τον χρήστη, ελεύθερα, με άδειες ανοιχτού κώδικα. Συνεπώς, ο καθένας μπορεί να συνεισφέρει και να βελτιώσει τον κώδικα και τις λειτουργίες του και να ενθαρρύνει στην βελτίωση τους[06].

Για τα ασύρματα εταιρικά δίκτυα, υπάρχει και η εφαρμογή Odin[19], η οποία προσφέρει μια πλατφόρμα SDN που δίνει σημαντικές δυνατότητες διαχείρισης της ασφάλειας των δικτύων. Το Odin, προσφέρει ένα εικονικό σημείο πρόσβασης (LVAP), και έτσι υπάρχει διαχωρισμός του φυσικού σημείου πρόσβασης του δικτύου από το εικονικό, και το γεγονός αυτό, απλοποιεί την διαχείριση του δικτύου για τον χρήστη. Ο σχεδιασμός του LVAP της εφαρμογής Odin, επιτρέπει στους χειριστές και τους προγραμματιστές να προγραμματίζουν και να αναπτύσσουν τυπικές υπηρεσίες WLAN ως εφαρμογές δικτύου. Για παράδειγμα, η Odin υποστηρίζει αποτελεσματική μεταβίβαση χρησιμοποιώντας το LVAP για να αποφευχθεί η ανταλλαγή μηνυμάτων στον πελάτη. Ο διαχειριστής κινητικότητας Odin μπορεί να παρακολουθεί την ισχύ του σήματος του δέκτη μέσω τοπικών παραγόντων για να καθοδηγήσει την επιλογή του AP handoff target. Τα βασικά συστατικά του Odin είναι χτισμένα πάνω από τον ελεγκτή ανοιχτού κώδικα OpenFlow Floodlight. Σήμερα, το Odin, συνεχίζει να εξελίσσεται ενεργά από την ερευνητική κοινότητα, με σκοπό την βελτίωση στον εμπλουτισμό της πλατφόρμας του, δημιουργώντας περισσότερα δυνατότητες, πέρα αυτού του LVAP[06].

Για την πρόσβαση στο άκρο, το OpenAPI[20], αναπτύσσει μια αρχιτεκτονική συστήματος που επιτρέπει τον αποτελεσματικό έλεγχο και την κοινή χρήση πόρων WLAN, εικονοποιώντας την υποδομή πρόσβασης τελευταίου μιλίου. Η αρχιτεκτονική καθορίζει τις διεπαφές μεταξύ του παρόχου διαδικτύου (Internet Service Provider), του παρόχου περιεχομένου και του τελικού χρήστη για να επιτρέψει μια ανοιχτή και ευέλικτη διαχείριση ποιότητας υπηρεσιών. Τα προτεινόμενα ανοιχτά API ενθαρρύνουν όλα τα μέρη να συμμετάσχουν και να συνεργαστούν, στα οποία ο πάροχος διαδικτύου, μπορεί να βελτιώσει τη δημιουργία εσόδων των πόρων υποδομής

τους σε ροή βάση χωρίς να αποκαλύπτει εσωτερικά το δίκτυο. Ο πάροχος περιεχομένου μπορεί να βελτιώσει επιχειρηματικά μοντέλα ρυθμίζοντας επιλεκτικά την ποιότητα της υπηρεσίας για διαφορετικούς τύπους ροών και οι τελικοί χρήστες μπορούν να προσαρμόσουν το βαθμό εικονοποίησης (virtualization) για να καλύψουν τις ειδικές ανάγκες. Ένας αλγόριθμος εικονικοποίησης αναπτύσσεται χρησιμοποιώντας την ελαστικότητα χρόνου των εφαρμογών μαζικής μεταφοράς και τη χωρική επικάλυψη κάλυψης WiFi για την επίτευξη αποτελεσματικής χρήσης πόρων.

Τέλος, η εφαρμογή OpenRadio, υποστηρίζει αποτελεσματικά την ασφάλεια και την διαχείριση των ασυρμάτων τοπικών δικτύων (Wireless Local Area Network) καθιστώντας την διαχείριση δικτύου ευέλικτη για τον χρήστη[02].

5.2 Κέντρα Δεδομένων και Υπολογιστικό Νέφος (Cloud and Data Center)

Αναφορικά με τα κέντρα δεδομένων (Data Centers), είναι γνωστό ότι σήμερα, χρησιμοποιείται κατά κύριο λόγο η τεχνολογία υπολογιστικού νέφους (cloud). Μία από τις πιο αποτελεσματικές εφαρμογές SDN που στοχεύουν στην βελτιστοποίηση της ασφάλειας των δικτύων στα κέντρα δεδομένων, είναι το NetFuse[24]. Το NetFuse είναι μια νέα πρόταση για περιβάλλον cloud και data center για την προστασία του δικτύου από αυξημένη τάση του ρεύματος και παρακολουθεί την κίνηση των δεδομένων στο δίκτυο, για τον εντοπισμό επιθέσεων ασφαλείας, αλλά και πιθανά σφάλματα του χειριστή, που δημιουργούνται από εσφαλμένη διαμόρφωση δρομολόγησης. Το NetFuse, χρησιμοποιεί τόσο παθητική ακρόαση όσο και προσαρμοστικά ενεργά ερωτήματα, για την αποτελεσματική παρακολούθηση της κατάστασης του δικτύου. Χρησιμοποιεί μια πολυδιάστατη συγκέντρωση για να βρει τις ύποπτες ομάδες ροής δεδομένων. Για τη βελτίωση της απόδοσης και της απόκρισης, το NetFuse χρησιμοποιεί έναν επιπλέον μηχανισμό εντοπισμού σφαλμάτων και προτεινόμενων λύσεων αντιμετώπισης, για να διαμορφώσει προσαρμοστικά τον ρυθμό ροής σύμφωνα με τις απαιτήσεις κάθε εφαρμογής. Ο σχεδιασμός αυτός, υλοποιείται με την βοήθεια ενός διακομιστή μεσολάβησης μεταξύ του ελεγκτή OpenFlow και του δρομολογητή. Το NetFuse ακολουθεί το πρότυπο OpenFlow αλλά δεν τροποποιεί το επίπεδο ελέγχου και δεδομένων. Παρέχει τοπική βελτιστοποίηση, διευκολύνοντας το βαρύ φορτίο από τον ελεγκτή, όπως ανακατεύθυνση ροής, καθυστέρηση έγχυσης ή μπλοκάρισμα.

Ακόμη μια εφαρμογή SDN για την βελτίωση της ασφάλειας των κέντρων δεδομένων και του υπολογιστικού νέφους είναι το CloudWatcher. Το CloudWatcher χρησιμοποιεί τα οφέλη και τις δυνατότητες της τεχνολογίας SDN, ώστε να δημιουργήσει ένα πλαίσιο που μπορεί να παρακολουθεί αποτελεσματικά τις υπηρεσίες σε μεγάλα και δυναμικά δίκτυα cloud. Η προτεινόμενη γλώσσα δέσμης ενεργειών επιτρέπει στους διαχειριστές του δικτύου, να παρακολουθούν και να ρυθμίζουν τις παραμέτρους ασφάλειας, με γρήγορο και βολικό τρόπο. Το CloudWatcher περιλαμβάνει τέσσερις αλγόριθμους δρομολόγησης για τον επαναπροσανατολισμό της κυκλοφορίας σε έναν κόμβο παρακολούθησης ασφαλείας. Το πλαίσιο αποτελείται από τρία βασικά στοιχεία:

Α) συσκευή και διαχειριστή πολιτικής

Β) γεννήτρια κανόνων δρομολόγησης

Γ) εφαρμογή επιβολής κανόνα ροής

Το CloudWatcher δεν απαιτεί αλλαγές στο επίπεδο ελέγχου ή δεδομένων και χρησιμοποιεί τους αλγόριθμους δρομολόγησης για τη βελτιστοποίηση της παρακολούθησης ασφάλειας.

5.3 Δίκτυα Κινητής Τηλεφωνίας

Καθώς τα ασύρματα δίκτυα κινητής τηλεφωνίας χρησιμοποιούνται από μεγάλο ποσοστό χρηστών για την πρόσβαση σε υπηρεσίες διαδικτύου, υπάρχει αυξημένη ανάγκη για την δημιουργία μιας υποδομής δικτύου που θα είναι σε θέση να διαχειριστεί, τον αυξανόμενο αριθμό χρηστών αλλά και την αποτελεσματική διασφάλιση με τον ρυθμό αύξησης των χρηστών και την κλίμακα των υπηρεσιών. Για παράδειγμα, η πρόσφατη ζήτηση χωρητικότητας δικτύου για κίνηση δεδομένων κινητής τηλεφωνίας υπερβαίνει κατά πολύ την προσφορά των υφιστάμενων δικτύων. Ταυτόχρονα, οι υπηρεσίες εξελίσσονται επίσης τόσο στην ποικιλία όσο και στην πολυπλοκότητα. Δεδομένου ότι οι φορείς εκμετάλλευσης περιορίζονται από τον εμπορικό προϋπολογισμό και το κόστος λειτουργίας, είναι εξαιρετικά δύσκολο, αν όχι αδύνατο, να συμβαδίζει με αυτήν την ταχύτητα, ενώ ταυτόχρονα αναβαθμίζει την υποδομή με αποδοτικό

κόστος, παρέχει ενημερώσεις υπηρεσιών και βελτιώνει την εμπειρία του τελικού χρήστη με την υπάρχουσα υποδομή.

Η υπάρχουσα υποδομή κινητής τηλεφωνίας έχει χαρακτηριστεί ως δαπανηρή και άκαμπτη, και εφαρμόζονται πολύπλοκα πρωτόκολλα επιπέδου ελέγχου και πολύπλοκες διεπαφές διαμόρφωσης, που καθιστούν δύσκολο το έργο των παρόχων τηλεπικοινωνιών και δικτύων. Προκειμένου να απλοποιηθεί η διαχείριση των κυψελοειδών δικτύων δεδομένων, η πρωτοποριακή εφαρμογή CellSDN προτείνει ένα σχεδιασμό SDN για την υποδομή του κυψελοειδούς πυρήνα. Επειδή η εφαρμογή SDN σε δίκτυα κινητής τηλεφωνίας, πρέπει να αντιμετωπίσει πολλές προκλήσεις, συμπεριλαμβανομένης της κινητικότητας των χρηστών και της προσαρμογής σε πραγματικό χρόνο, εντοπίζεται ένα σύνολο απαραίτητων επεκτάσεων για τα βασικά στοιχεία της αρχιτεκτονικής CellSDN. Στην προτεινόμενη επέκταση ελεγκτή, οι πολιτικές των χαρακτηριστικών των συνδρομητών μεταφράζονται σε κανόνες εναλλαγής που ταιριάζουν στις κεφαλίδες πακέτων. Ένας τοπικός παράγοντας ελέγχου εισάγεται στο διακόπτη για την αποσυμφόρηση και την κλιμάκωση του κεντρικού ελέγχου εκτελώντας τοπικές ενέργειες καθοδηγούμενες από την πλατφόρμα ελέγχου[12].

Με την προώθηση του υψηλού επιπέδου σχεδιασμού CellSDN, το SoftCell παρουσιάζει μια λεπτομερή επεκτάσιμη αρχιτεκτονική σχεδίαση για την υποστήριξη λεπτομερών πολιτικών σε κυψελοειδή δίκτυα πυρήνα. Με τον ελεγκτή να χειρίζεται λεπτομέρειες χαμηλού επιπέδου, όπως θέση εναλλαγής και αναγνωριστικό δικτύου, η SoftCell υιοθετεί ένα σύνολο πολιτικών υπηρεσιών ως υψηλού επιπέδου αφαίρεσης με βάση χαρακτηριστικά και εφαρμογές συνδρομητών. Οι πολιτικές υπηρεσιών περιλαμβάνουν προτεραιότητα, δράση υπηρεσίας και προδιαγραφές. Για να χειριστεί τη δυναμική του δικτύου και να ενεργοποιήσει τις λεπτομερείς πολιτικές σε κλίμακα, το SoftCell επιτυγχάνει επεκτασιμότητα επεκτείνοντας τόσο το επίπεδο ελέγχου όσο και το επίπεδο δεδομένων[10].

Στο επίπεδο ελέγχου, η SoftCell χρησιμοποιεί τοπικούς πράκτορες λογισμικού για την προσωρινή αποθήκευση των ταξινομητών πακέτων και των ετικετών πολιτικής προκειμένου να μειώσει το φορτίο του κύριου ελεγκτή. Στο επίπεδο δεδομένων, το SoftCell ωθεί την ταξινόμηση πακέτων στους διακόπτες πρόσβασης και εφαρμόζει την πολυδιάστατη συσσώρευση κανόνων προώθησης για να ελαχιστοποιήσει την κατάσταση στο κεντρικό δίκτυο.

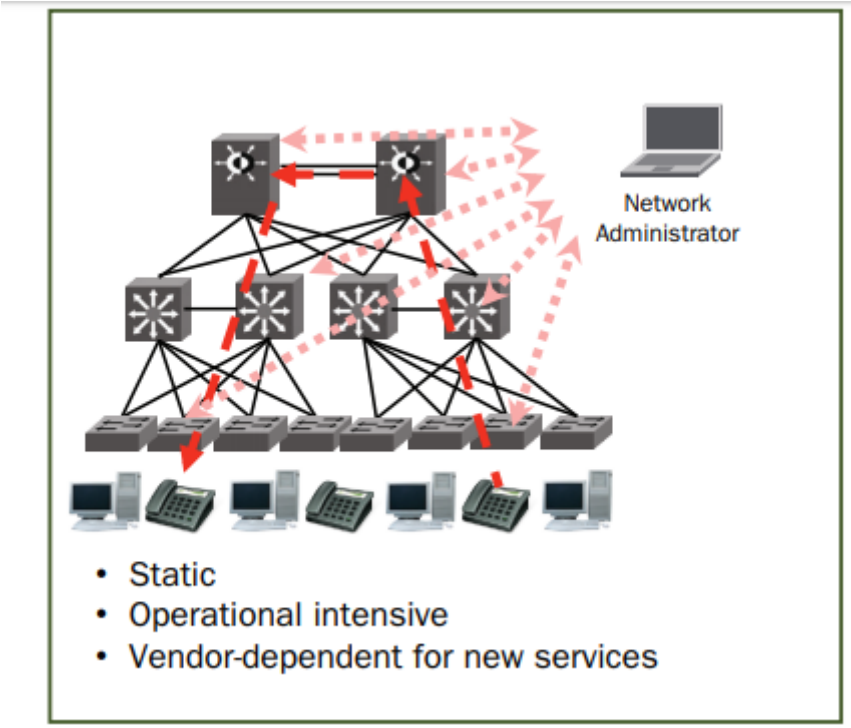
Για την πρόσβαση στο κινητό, το SoftRAN και το OpenRadio είναι οι πιο πρόσφατες προτάσεις που αποσκοπούν στο να φέρουν τη δύναμη του SDN για καινοτομία στον τομέα της ασύρματης πρόσβασης. Το SoftRAN επικεντρώνεται στη σχεδίαση επιπέδου ελέγχου αφαιρώντας πολλούς σταθμούς βάσης σε έναν εικονικό μεγάλο σταθμό βάσης. Ένα τρισδιάστατο πλέγμα πόρων ορίζεται από το SoftRAN για να επιτρέπει στους χειριστές να διαχειρίζονται τους πόρους ραδιοφώνου σε μια γεωγραφική περιοχή μέσω τριών διαστάσεων - χρόνου, συχνότητας και ευρετηρίου σταθμού βάσης. Ο ελεγκτής SoftRAN διατηρεί μια βάση πληροφοριών RAN (RIB) στην οποία επιτρέπεται η πρόσβαση μέσω διαφόρων μονάδων ελέγχου για διαχείριση πόρων ραδιοφώνου. Το RIB αποτελείται από βασικές πληροφορίες που πρέπει να ενημερώνονται από τον ελεγκτή, όπως ο χάρτης παρεμβολών, η εγγραφή ροής και η προτίμηση του χειριστή δικτύου. Καθώς το στοιχείο ραδιοφώνου έχει πιο έγκαιρη προβολή της τοπικής κατάστασης από το τηλεχειριστήριο, το SoftRAN βελτιστοποιεί περαιτέρω την απόφαση ελέγχου διαχωρίζοντας τη λειτουργικότητα ελέγχου μεταξύ του κεντρικού ελεγκτή και των στοιχείων ραδιοφώνου[06].

Το OpenRadio προτείνει μια λύση επιπέδου δεδομένων που επιτρέπει την προγραμματιζόμενη δυνατότητα μέσω διεπαφών αρθρωτού και δηλωτικού προγραμματισμού σε όλη την ασύρματη στοίβα. Καθώς η υπάρχουσα ασύρματη υποδομή πάσχει από το στενά συνδεδεμένο υλικό, το OpenRadio στοχεύει στην αποσύνδεση του ορισμού του πρωτοκόλλου από το υλικό και την παροχή ενός επιπέδου αφαίρεσης λογισμικού για να επιτρέψει τον προγραμματισμό του MAC και του φυσικού επιπέδου. Η κύρια ιδέα είναι η αποσύνθεση των ασύρματων πρωτοκόλλων σε επίπεδο επεξεργασίας και επίπεδο απόφασης όπου το επίπεδο επεξεργασίας περιλαμβάνει ενέργειες και το επίπεδο απόφασης περιλαμβάνει κανόνες. Λόγω της γενικότερης σχεδίασης, το OpenRadio μπορεί να εφαρμοστεί τόσο στο κινητά δίκτυα όσο και σε ασύρματα περιβάλλοντα[02].

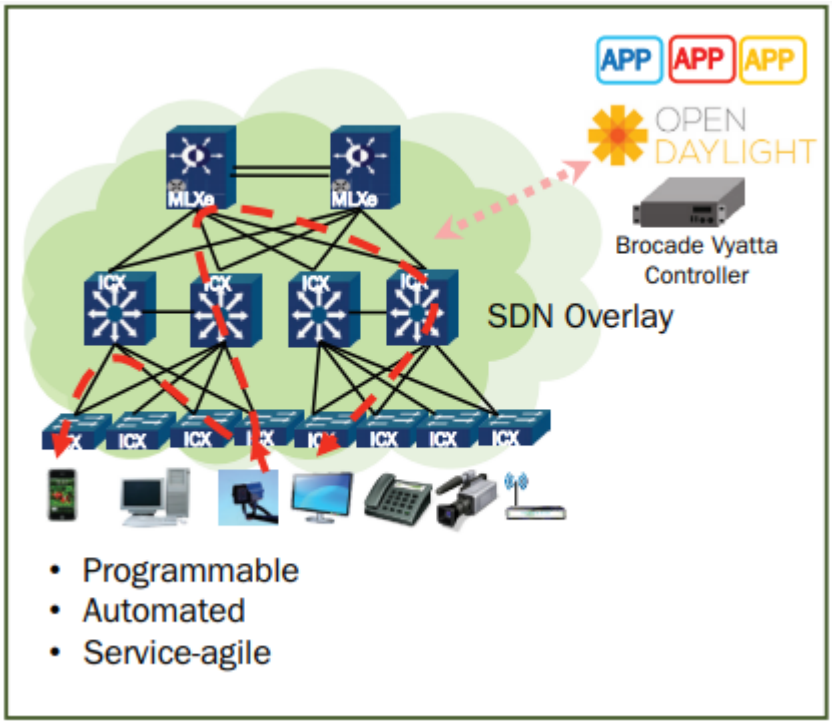
5.4 Δίκτυα Πανεπιστημίων (Campus)

Τα Παραδοσιακά δίκτυα, απαιτούν συγκεκριμένες πολιτικές εφαρμογής, όπως ασφάλεια και έλεγχος πρόσβασης, απομόνωση κίνησης εικονικού τοπικού δικτύου (VLAN), παροχή ποιότητας υπηρεσιών (Quality of Service). Όμως, αυτό καταναλώνει σημαντικό αριθμό πόρων του δικτύου και οδηγεί σε ένα στατικό δίκτυο που δεν μπορεί να ενημερωθεί εύκολα καθώς εξελίσσονται οι επιχειρηματικές απαιτήσεις ή εμφανίζονται και αναπτύσσονται νέες εφαρμογές.

Αντίθετα, τα δίκτυα SDN, υποστηρίζουν δυναμική κατανομή πόρων για τις εφαρμογές, και έτσι, μπορούν δυναμικά να εκχωρήσουν πόρους δικτύου σε πραγματικό χρόνο για να καλύψουν τις ανάγκες εκτέλεσης των εφαρμογών. Οι προσαρμοσμένες εφαρμογές SDN που εκτελούνται πάνω από τον ελεγκτή OpenFlow μπορούν να χρησιμοποιούν πολλές εισόδους, από διάφορες πηγές, συμπεριλαμβανομένων απαιτήσεων ασφάλειας και της υπηρεσίας QoS για συγκεκριμένες εφαρμογές, φυσικών στατιστικών δικτύου, δραστηριότητας χρήστη, ανάλυσης απειλών ασφαλείας και ούτω καθεξής για την κατανομή και προστασία πόρων του δικτύου, και την ρύθμιση ελέγχου πρόσβασης κανόνες. Με αυτό τον τρόπο, τα δίκτυα SDN επιτρέπουν την μετάδοση των δεδομένων σε πραγματικό χρόνο, με πλήρως δυναμικό τρόπο.



Εικόνα 5.1: Παραδοσιακό Δίκτυο Πανεπιστημίου



Εικόνα 5.2: SDN Δίκτυο Πανεπιστημίου

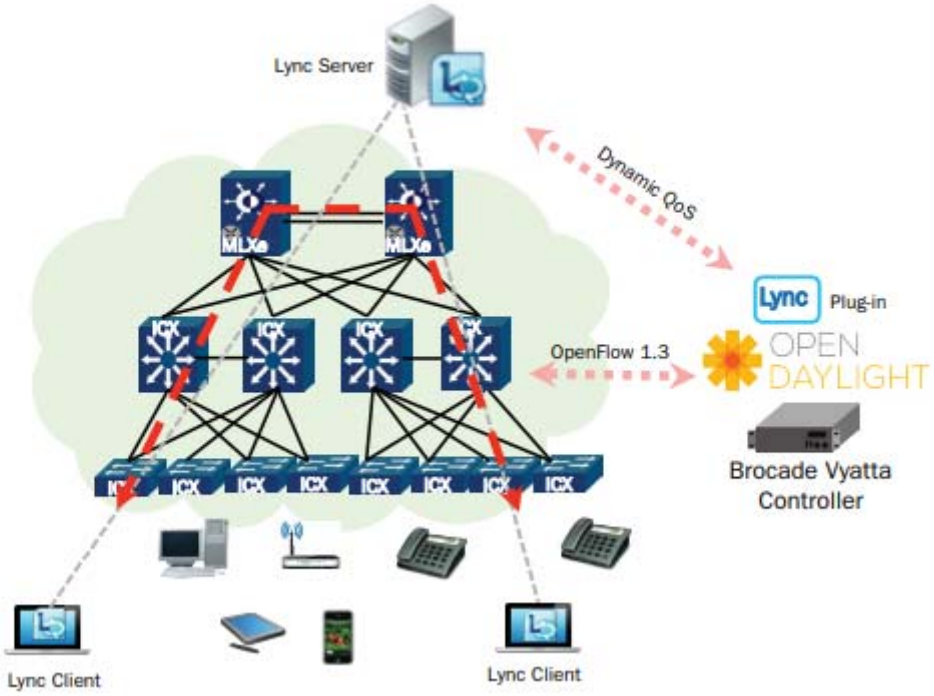
Η διαχείριση της ροής πληροφοριών στα δίκτυα των πανεπιστημίων είναι ζωτικής σημασίας. Η συνεχής ροή πληροφορίας, θα πρέπει να πραγματοποιείται ανενόχλητα και σε πραγματικό χρόνο, ενώ ταυτόχρονα θα πρέπει να παρακολουθείται η μετάδοση και η κίνηση των δεδομένων, ώστε να διασφαλίζεται η ακεραιότητα τους και να υπάρχει αποτελεσματική προστασία, από ενδεχόμενες απειλές και επιθέσεις. Οι εφαρμογές χρηστών έχουν εξελιχθεί από e-mail, εκτύπωση και μεταφορά αρχείων σε ευαίσθητες στο χρόνο επικοινωνίες βίντεο και ήχου, απεικόνιση σε πραγματικό χρόνο και μεταφορές μεγάλης κλίμακας Big Data. Οι παλαιότερες αρχιτεκτονικές δικτύου, και τα προηγούμενα πρωτόκολλα δικτύου, δεν μπορούν πλέον να ικανοποιήσουν τις αυξημένες απαιτήσεις των σύγχρονων εφαρμογών, όπως επίσης αδυνατούν να παρέχουν ένα ευέλικτο περιβάλλον διαχείρισης δικτύου.

Εφαρμογές των δικτύων SDN, είναι σε θέση να ικανοποιήσουν τι νέες ανάγκες των χρηστών και τις αυξημένες απαιτήσεις των εφαρμογών στα πανεπιστημιακά δίκτυα. Οι νέες αρχιτεκτονικές και νέα πρωτόκολλα που στηρίζονται στην τεχνολογία SDN, εξασφαλίζουν ασφαλή και ελεύθερη ροή πληροφοριών στα δίκτυα των εκπαιδευτικών ιδρυμάτων.

Για παράδειγμα, η αρχιτεκτονική Brocade HyperEdge[04], επιτρέπει μια νέα τοπολογία δικτύωσης για την κάλυψη των φυσικών απαιτήσεων της παράδοσης δεδομένων. Το SDN έχει

γίνει βασική τεχνολογία που επιτρέπει την αρχιτεκτονική HyperEdge. Το OpenFlow, που λειτουργεί σε Brocade switches , μπορεί είτε να επηρεάσει όλη την κίνηση σε έναν δεδομένο σύνδεσμο είτε να λειτουργήσει σε συνδυασμό με παραδοσιακά πρωτόκολλα που χρησιμοποιούν τη λειτουργία υβριδικής ανά ροή Brocade. Αυτό επιτρέπει τον χειρισμό συγκεκριμένων ροών σε έναν σύνδεσμο, ενώ αφήνει άλλες ροές να χρησιμοποιούν τον κανονικό αγωγό επεξεργασίας πακέτων. Το SDN δίνει τη δυνατότητα προσαρμογής της κυκλοφορία δικτύου με νέο τρόπο. Η εφαρμογή SDN μπορεί να λάβει εισροές από πολλές πηγές: φυσικά στατιστικά στοιχεία δικτύου, χρήστες που συνδέονται ή αποσυνδέονται από το δίκτυο, πού ξεκίνησαν και σταμάτησαν οι εφαρμογές χρηστών υψηλής προτεραιότητας, αναμενόμενη κυκλοφορία λόγω ιστορικών τάσεων, ανάλυση απειλών ασφαλείας κ.ο.κ. Αυτές οι πληροφορίες μπορούν στη συνέχεια να χρησιμοποιηθούν για τη λήψη αποφάσεων σχετικά με τον καλύτερο τρόπο απόκρισης. Ο ελεγκτής SDN, με βάση τον χάρτη δικτύου που δημιουργεί, λαμβάνει την απόφαση για το πού βρίσκεται στο δίκτυο να προωθήσει αυτές τις αλλαγές. Αυτό μπορεί να είναι τόσο απλό όσο μια αύξηση στην προτεραιότητα μιας συγκεκριμένης ροής εφαρμογών σε πλήρη έλεγχο πρόσβασης δικτύου με κατανομή πόρων βάσει ρόλου. Όλα αυτά λειτουργούν με κάθε επίπεδο ανεξάρτητο το ένα από το άλλο, μια καθορισμένη διεπαφή προγραμματισμού εφαρμογών (API) μεταξύ των επιπέδων και ένα προκαθορισμένο σύνολο μηνυμάτων. Αυτό επιτρέπει ένα ισχυρό σύνολο λειτουργιών που κλιμακώνονται με τις δυνατότητες που κάθε στρώμα αναφέρει το ένα στο άλλο.

Σε αντίθεση με το παρελθόν, μια ενημέρωση σε ένα επίπεδο δεν διακόπτει τη λειτουργία ενός άλλου επιπέδου. Το Brocade τυποποιεί την έκδοση 1.3 του OpenFlow - με τη σχετική αυξημένη λειτουργικότητα, υψηλή διαθεσιμότητα και δυνατότητες ασφάλειας σε σχέση με την έκδοση 1.0 για μια ισχυρή εταιρική λύση. Ορισμένοι προμηθευτές έχουν αποφασίσει να εφαρμόσουν το OpenFlow χρησιμοποιώντας επεξεργασμένο λογισμικό CPU και προώθηση ροών κίνησης. Προκειμένου να εξασφαλιστεί το υψηλότερο δυνατό επίπεδο απόδοσης, το Brocade εφαρμόζει την επεξεργασία ροής σε όλο το υλικό.



Εικόνα 5.3: Εφαρμογή SDN με χρήση αυτοματοποιημένης παροχής ποιότητας υπηρεσιών

Κεφάλαιο 6
Προσομοίωση προκαθοριζόμενου και μη-προκαθοριζόμενου από λογισμικό δικτύου (SDN/non-SDN)

6.1 Εισαγωγή

Στο εμπειρικό-πειραματικό κομμάτι αυτής της εργασίας, αντικείμενο θα είναι η προσομοίωση ενός δικτύου τύπου SDN, η προσομοίωση ενός δικτύου μη-καθοριζόμενου από λογισμικό (το ονομάζουμε non-SDN), καθώς και μερικά ακόμη στοιχεία τα οποία σχετίζονται με αυτά τα δίκτυα. Τα στοιχεία αυτά είναι:

- η εκτέλεση εντολών λήψης μετρικών έκαστου δικτύου

- η εκτέλεση μιας εντολής επίθεσης σε καθένα από αυτά τα δίκτυα

- ανίχνευση και εντοπισμός του διαφορισμού του ενός δικτύου από το άλλο

Ειδικότερα, θα πραγματοποιηθεί ένα είδος Επίθεσης Άρνησης Εξυπηρέτησης (Denial of Service Attack- DoS) και στη συνέχεια θα διακριβωθεί η συμπεριφορά του κάθε δικτύου. Ακριβέστερα, η επίθεση που υλοποιείται είναι τύπου Ping flooding. Αυτό που αναμένεται, προφανώς, θα είναι η καλύτερη συμπεριφορά του καθοριζόμενου-από-λογισμικό (SDN) δικτύου, με την έννοια ότι θα εμφανίσει σημάδια καλύτερης ασφάλειας έναντι μιας τέτοιας επίθεσης.

6.2 Λογισμικό προσομοίωσης

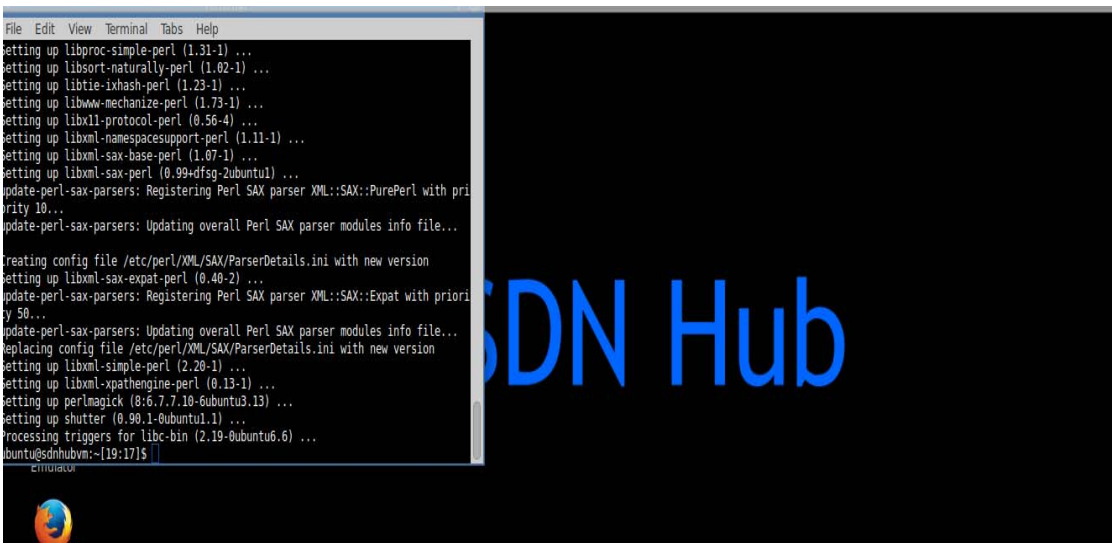
Στην παράγραφο αυτή, θα πραγματοποιηθεί μια αναφορά στα λογισμικά των οποίων γίνεται χρήση σε αυτό το τμήμα, προκειμένου δηλαδή να εκτελεστούν όλα τα επιμέρους στοιχεία που αναφέρθηκαν παραπάνω.

Καταρχάς, πρέπει να αναφερθεί ότι το περιβάλλον προσομοίωσης θα είναι το Ubuntu Linux και μάλιστα στο πλαίσιο του Oracle Virtual Box. Δεύτερον, γίνεται χρήση μιας προδημιουργημένης εικονικής συσκευής (pre-built image), του τύπου SDN Hub Tutorial VM 64-bit with Docker. Ένα πρώτο στιγμιότυπο οθόνης από αυτή την εικονική συσκευή φαίνεται παρακάτω.

Εικόνα 6.1:SDN Hub Tutorial VM 64bit with Docker

Η συγκεκριμένη προδημιουργημένη εικονική μηχανή παρέχει σειρά από εφαρμογές που έχουν να κάνουν με τα προκαθοριζόμενα από λογισμικό δίκτυα. Ορισμένα από τα σημαντικότερα εργαλεία, μαζί με τα υπόλοιπα που χρησιμοποιούνται στα πλαίσια αυτού του μέρους είναι τα ακόλουθα:

- Oracle VM VirtualBox
- 64-bit Ubuntu 14.04
- Ελεγκτές δικτύου SDN: OpenDaylight, Floodlight, RYU, POX, ONOS
- Mininet



Εικόνα 6.2:Εγκατάσταση λογισμικών της προδημιουργημένης εικονικής μηχανής

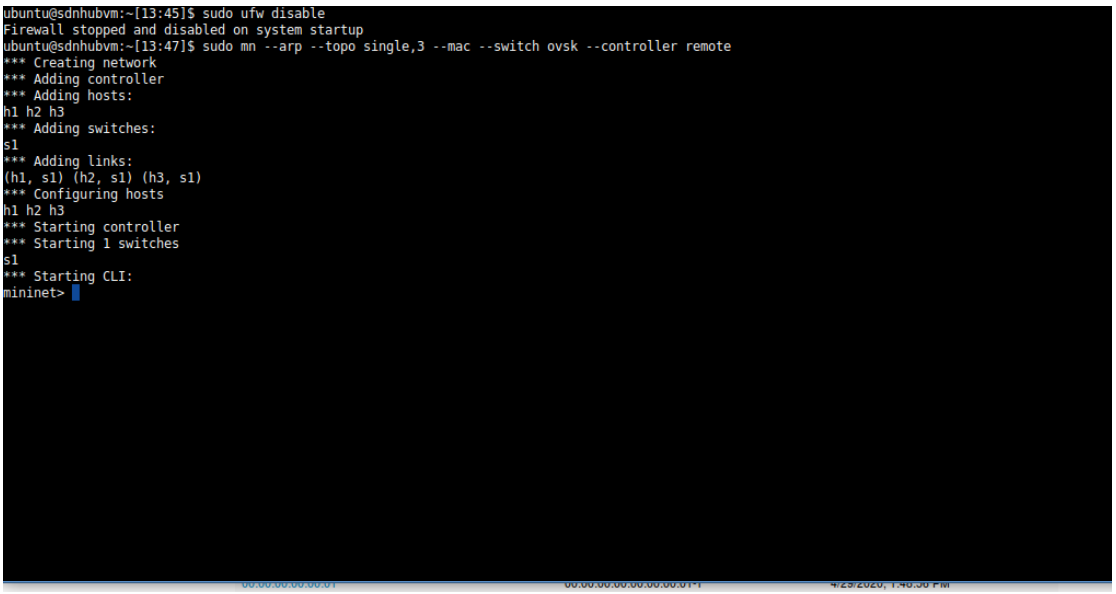
Τα κυριότερα εργαλεία επομένως για το συγκεκριμένο μέρος είναι ο προσομοιωτής Mininet, όπως εκτελείται μέσα στην εικονική μηχανή του VirtualBox, με όλα τα ενσωματωμένα εργαλεία με έμφαση σε αυτά της απόδοσης δικτύου, καθώς και το Floodlight, που χρησιμοποιείται για την ανασκόπηση τοπολογιών.

Καταληκτικά, επισημαίνεται πως απαιτούνται σε προκαταρκτικό επίπεδο δύο προσαρμογείς δικτύου (network adapters) για την εικονική μηχανή. Οι δύο αυτοί προσαρμογείς είναι οι εξής:

- Προσαρμογέας τύπου NAT (Network Address Translation)
- Προσαρμογέας τύπου Host-only

6.3 Δημιουργία δικτύου SDN και Ethernet και λήψη μετρικών

Το πρώτο δίκτυο που δημιουργείται είναι το προκαθορισμένο από λογισμικό δίκτυο, όπως φαίνεται παρακάτω.



Εικόνα 6.3: Εκτέλεση απλής τοπολογίας SDN δικτύου

Παρατηρείται ότι εκτελείται μέσω της γραμμής εντολών του Ubuntu Linux μία πολύ απλή τοπολογία, η οποία αποτελείται από τρεις υπολογιστές υποδοχής (hosts), ενώ γίνεται χρήση ενός –όπως συμβατικά αποκαλείται- «απομακρυσμένου» ελεγκτή δικτύου (remote controller). Στην Εικόνα 3, παρατηρείται ότι μετά την επιτυχή εκτέλεση της εντολής mn, που είναι η εντολή δημιουργίας δικτύου με το mininet, φτάνουμε στο CLI (Command-Line Interface), από όπου είναι εφικτή η εκτέλεση διαφόρων εντολών.

Στη συνέχεια, ακολουθείται μια σειρά από βήματα, όπως παρατίθενται παρακάτω:

1. Εμφάνιση συνόλου πληροφορίας για τους κόμβους του δικτύου από τη μνήμη (information dump) [SDN δίκτυο]

2. Άνοιγμα τερματικών για τους δύο πρώτους από τους υπολογιστές υποδοχής (με την εντολή xterm) [SDN δίκτυο]

3. Δοκιμή ενσωματωμένου εργαλείου Mininet για υπολογισμό απόδοσης δικτύου (iperf) [SDN δίκτυο]

4. Εύρος ζώνης TCP [SDN δίκτυο]

5. Δημιουργία παραδοσιακού (non-SDN) δικτύου

6. Επίδειξη αντιστοίχισης κόμβων σε αριθμούς OpenFlow [non-SDN δίκτυο]

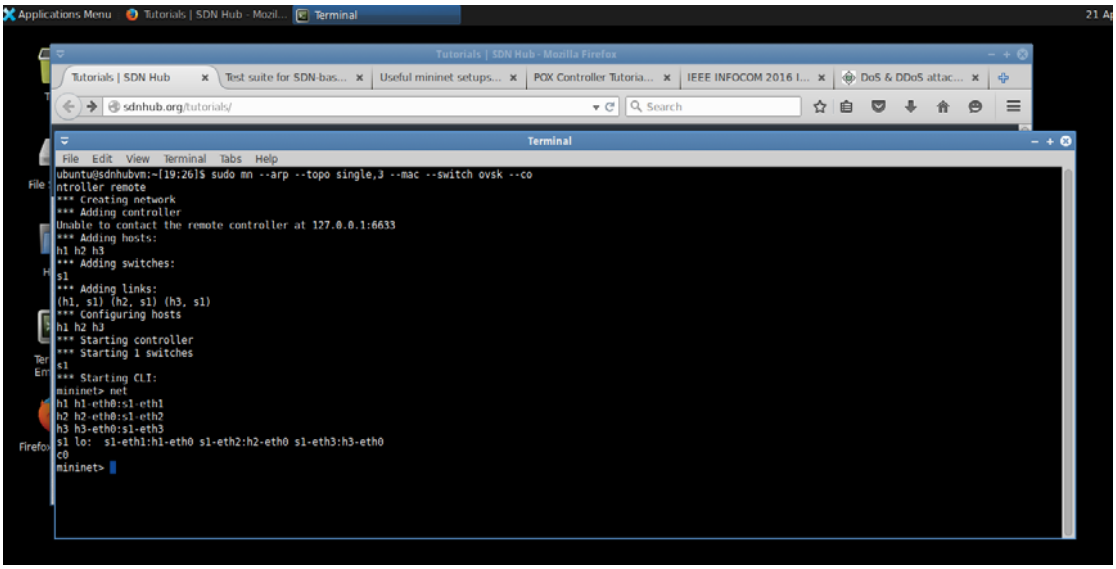
7. Πειραματισμός λειτουργίας των δημιουργημένων ροών κυκλοφορίας με ping [non-SDN δίκτυο]

8. Πειραματισμός λειτουργίας των δημιουργημένων ροών κυκλοφορίας με Pingall [non-SDN δίκτυο]

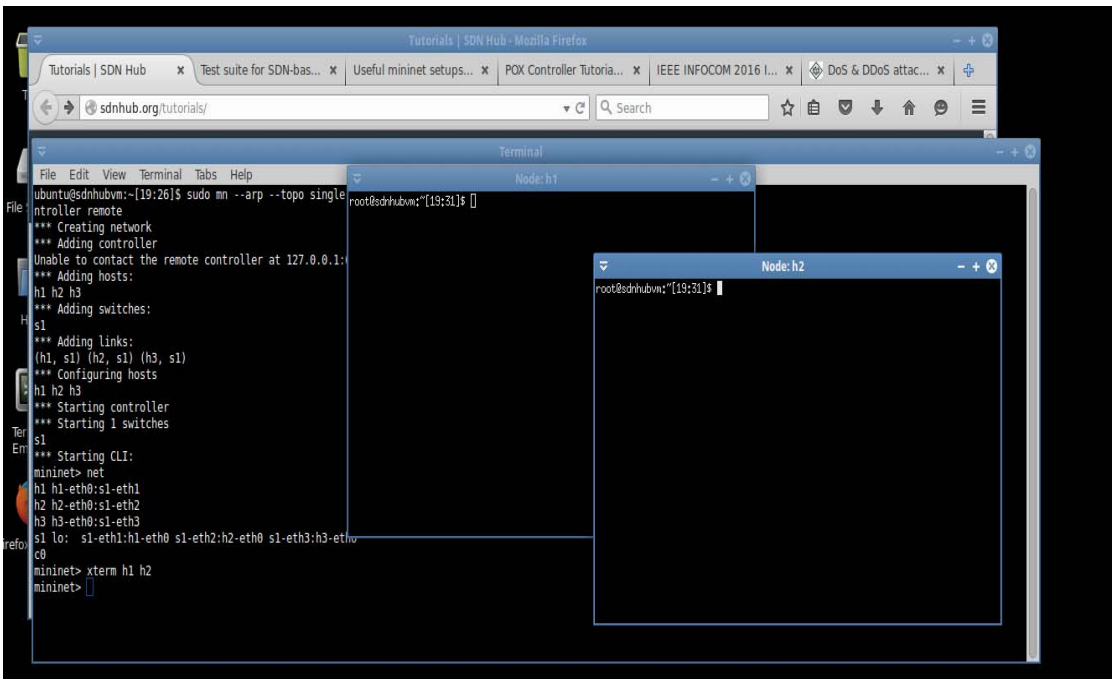
9. Προσθήκη κανόνα προώθησης ροών στον h3 [non-SDN δίκτυο]

10. Εύρος ζώνης TCP [non-SDN δίκτυο]

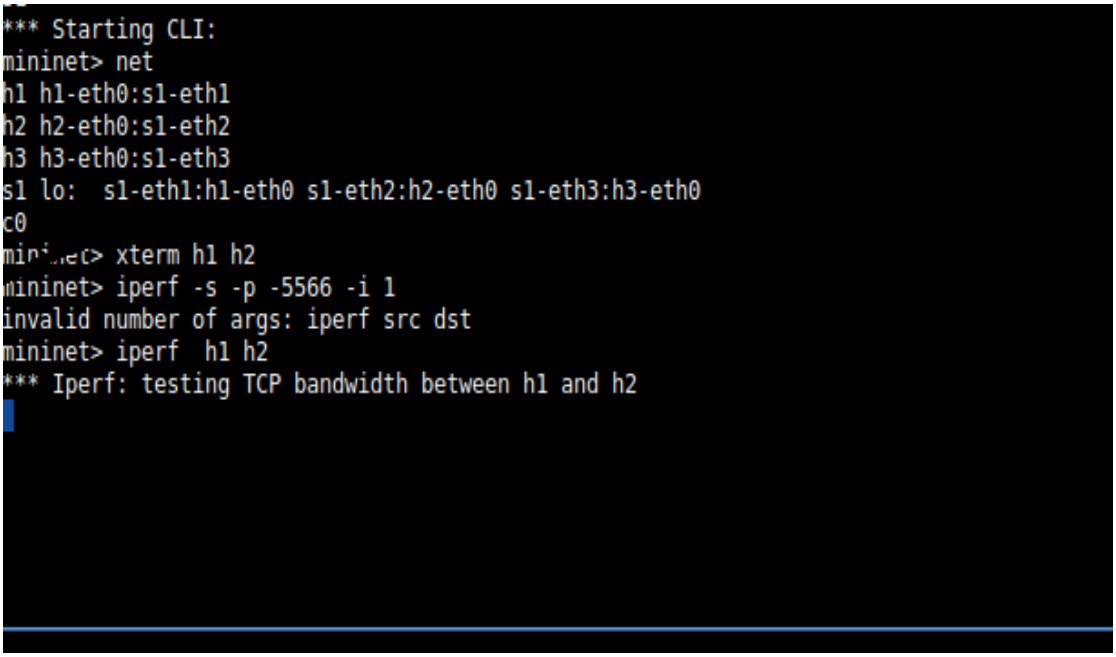
Στη συνέχεια παρατίθενται τα σχετικά στιγμιότυπα οθόνης από τα βήματα αυτά.



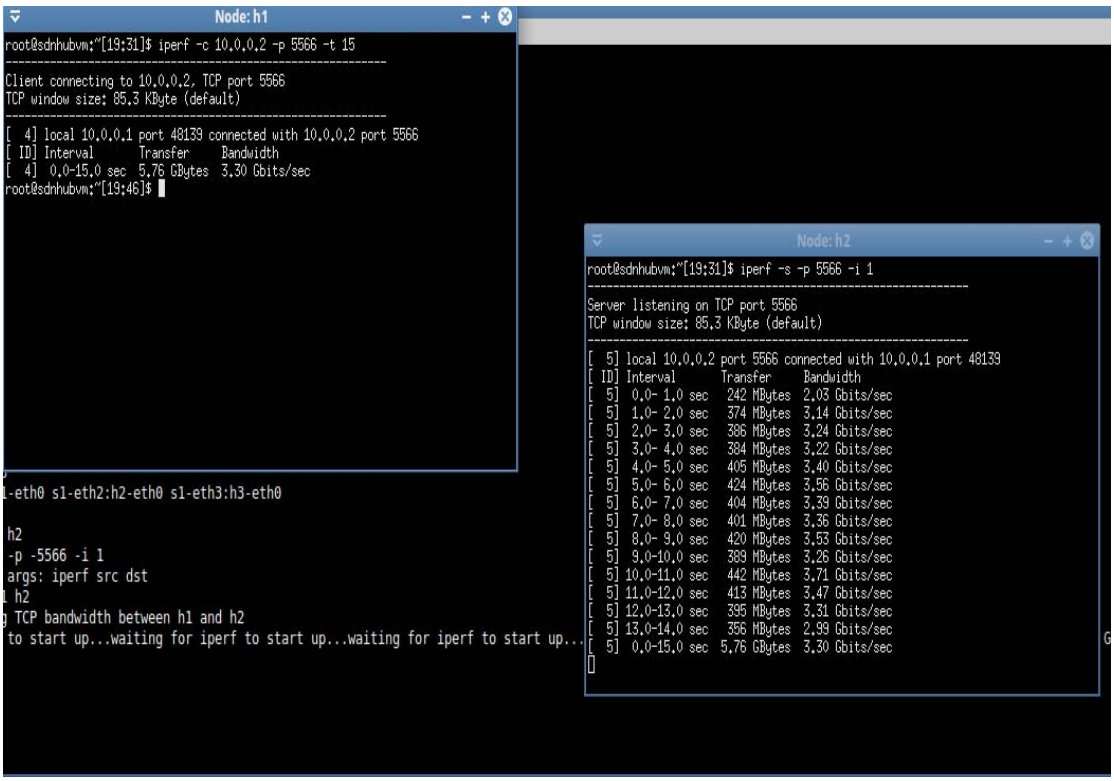
Εικόνα 6.4: Εμφάνιση πληροφοριών κόμβου SDN δικτύου



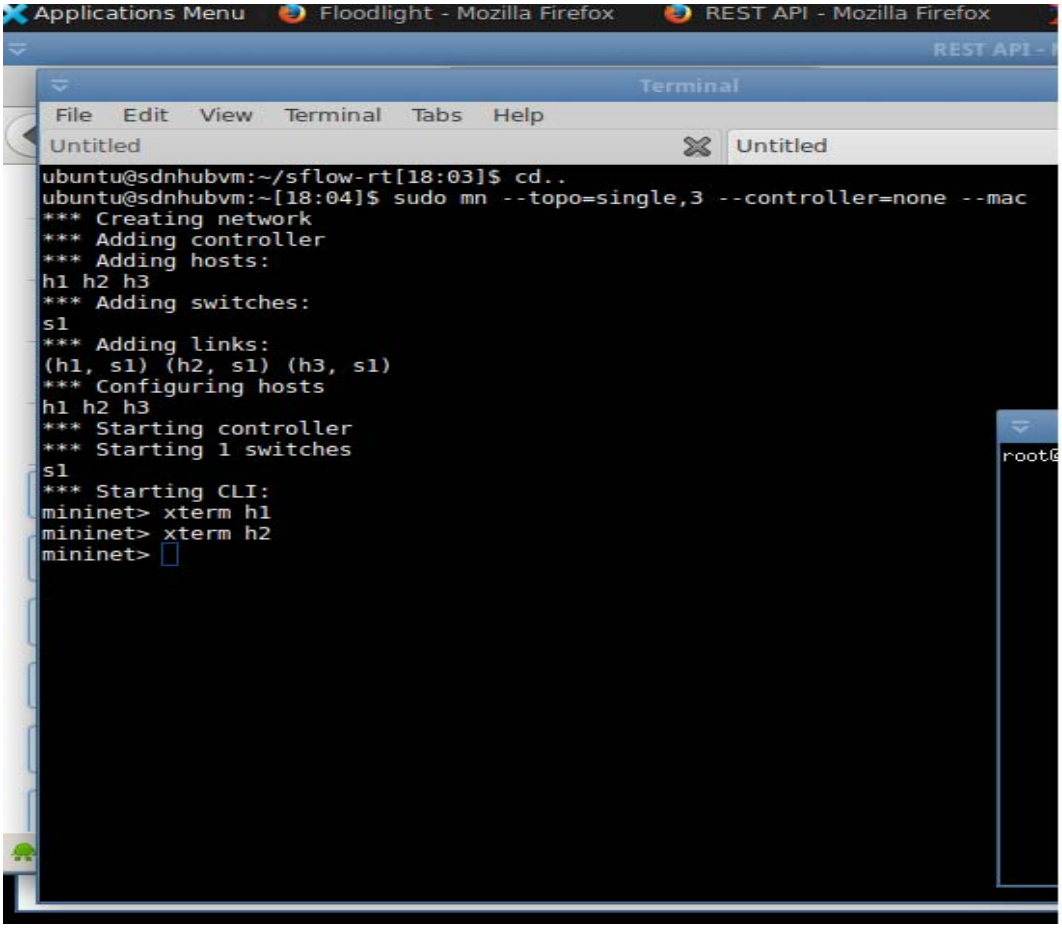
Εικόνα 6.5: Άνοιγμα τερματικών για υπολογιστές υποδοχής h1 και h2 SDN δικτύου



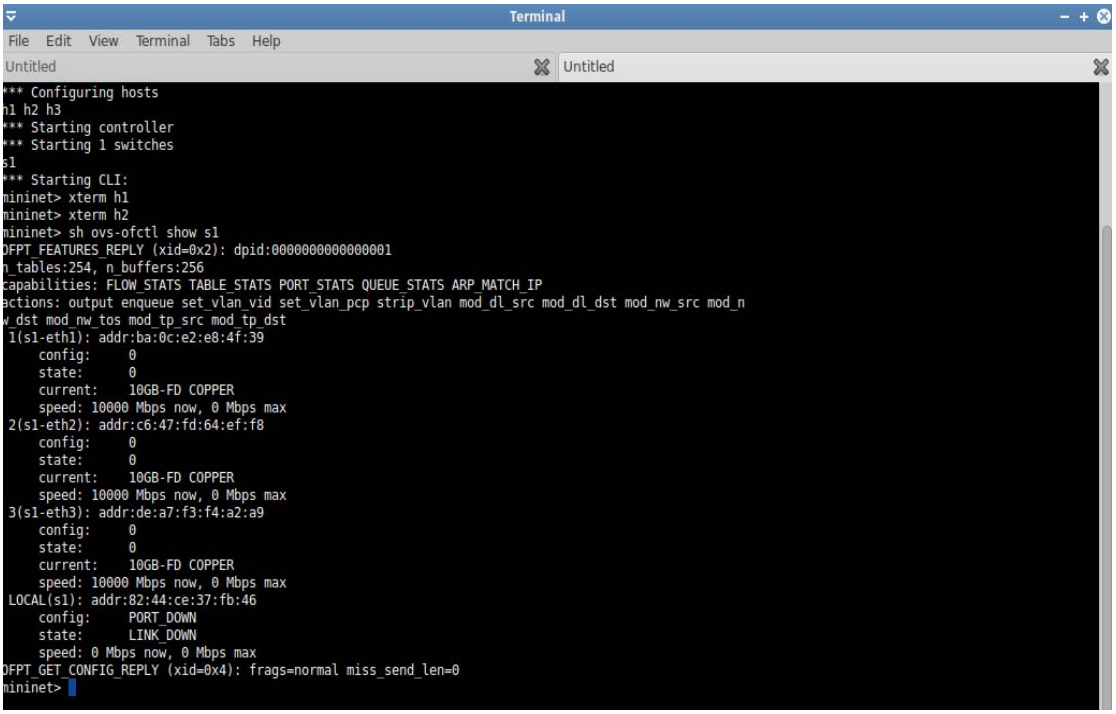
Εικόνα 6.6: Δοκιμή λήψης μετρικών για υπολογιστές υποδοχής h1 και h2 SDN δικτύου



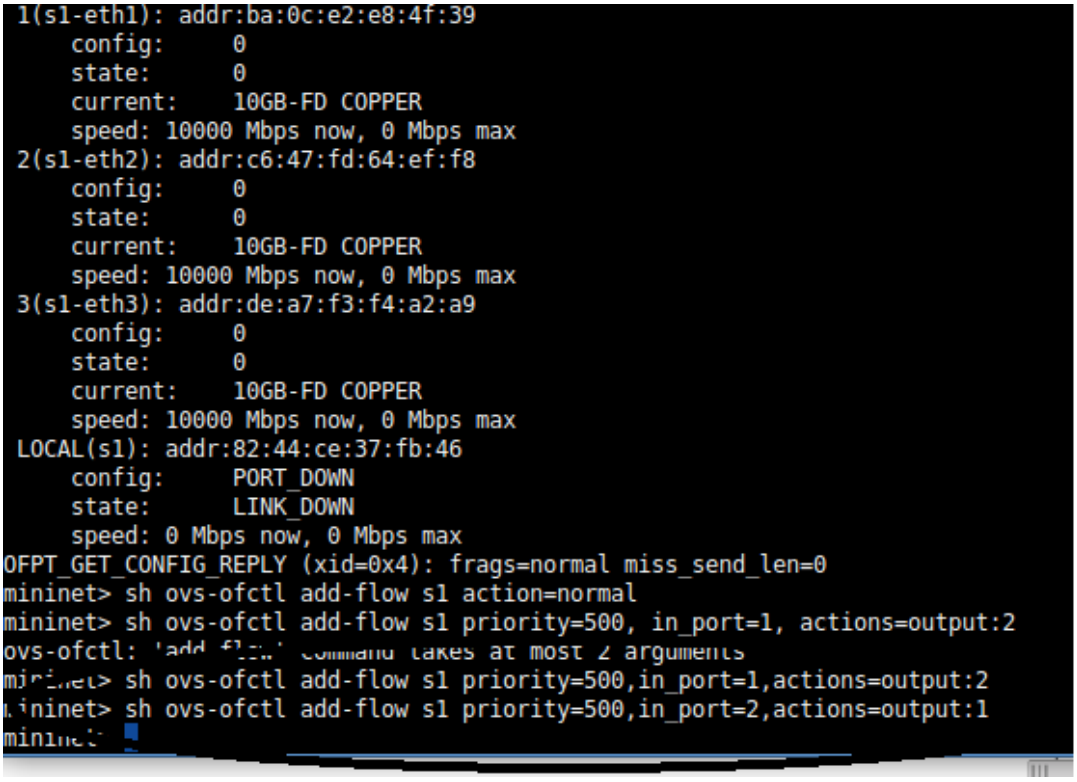
Εικόνα 6.7: Λήψη μετρικών για υπολογιστές υποδοχής h1 και h2 SDN δικτύου



Εικόνα 6.8: Δημιουργία παραδοσιακού δικτύου



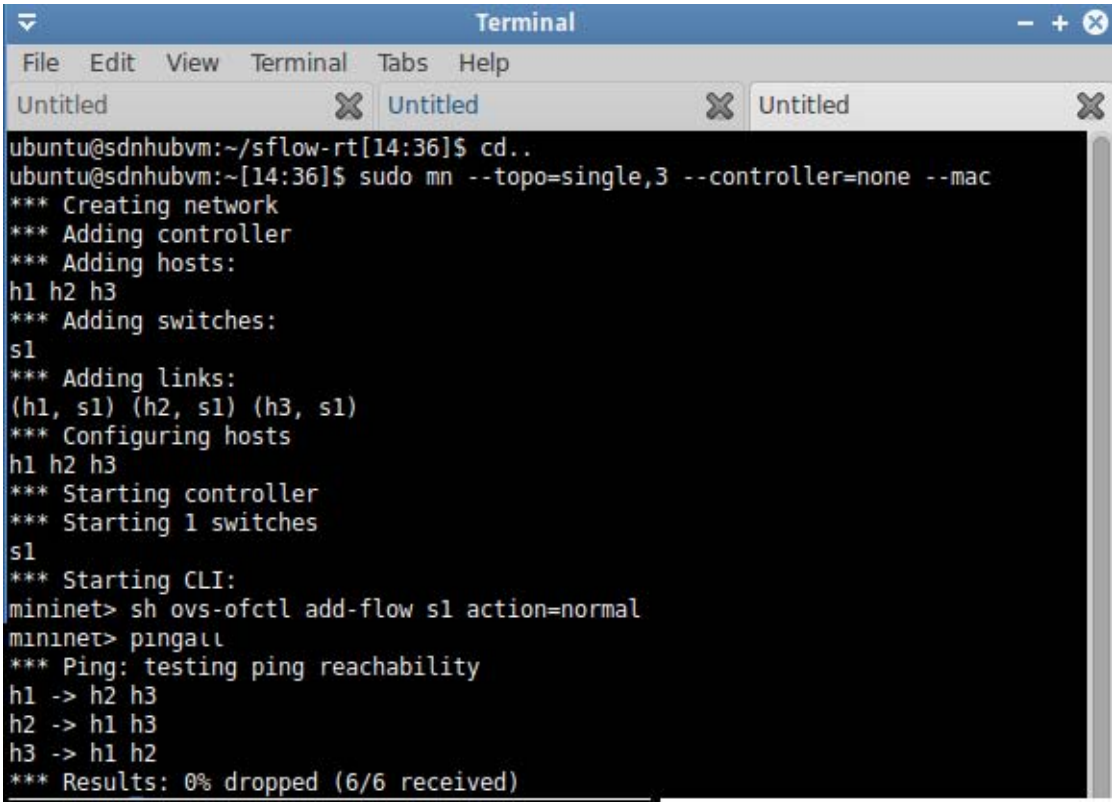
Εικόνα 6.9: Επίδειξη αντιστοίχισης κόμβων σε αριθμούς OpenFlow



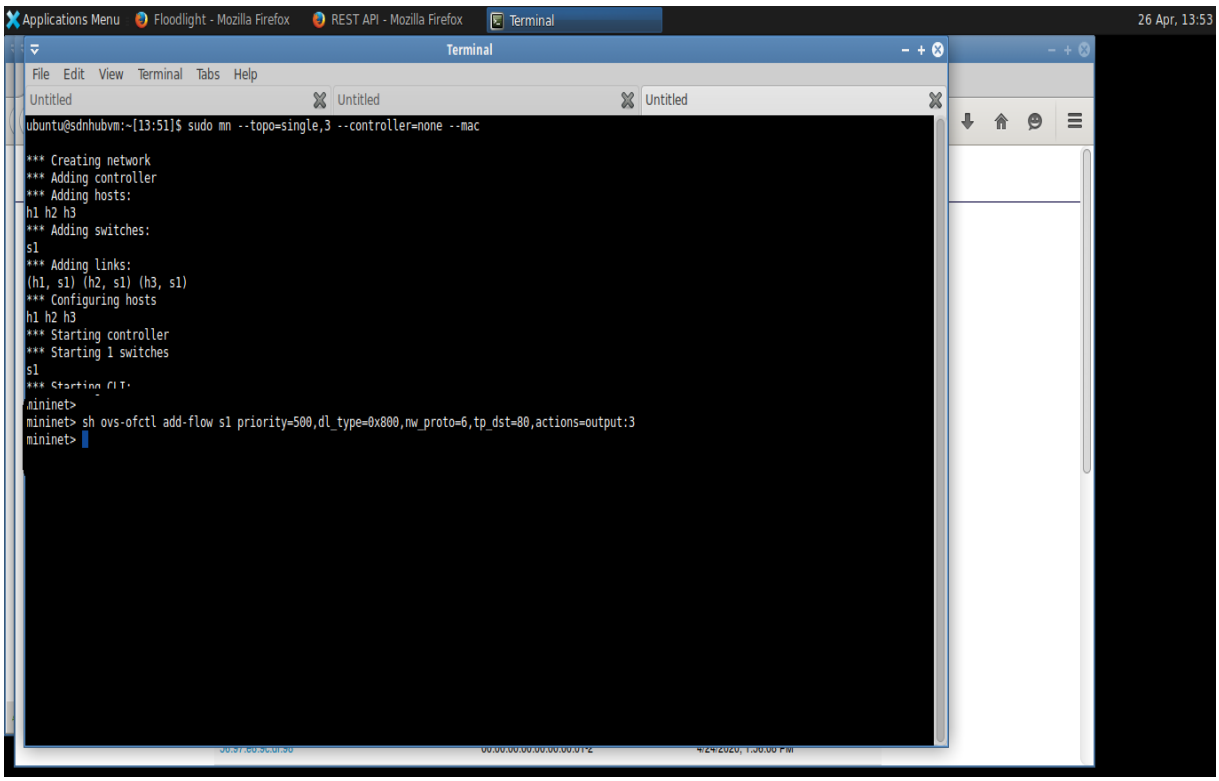
Εικόνα 6.10: Δημιουργία ροών κυκλοφορίας(δοκιμαστική)

```
OFPT_GET_CONFIG_REPLY (xid=0x4): frags=normal miss_send_len=0
mininet> sh ovs-ofctl add-flow s1 action=normal
mininet> sh ovs-ofctl add-flow s1 priority=500, in_port=1, actions=output:2
ovs-ofctl: 'add-flow' command takes at most 2 arguments
mininet> sh ovs-ofctl add-flow s1 priority=500,in_port=1,actions=output:2
mininet> sh ovs-ofctl add-flow s1 priority=500,in_port=2,actions=output:1
mininet> h1 ping -c2 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=2.70 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.159 ms

--- 10.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.159/1.431/2.704/1.273 ms
mininet> h3 ping -c2 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=2.56 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.149 ms

--- 10.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.149/1.355/2.561/1.206 ms
mininet>
```

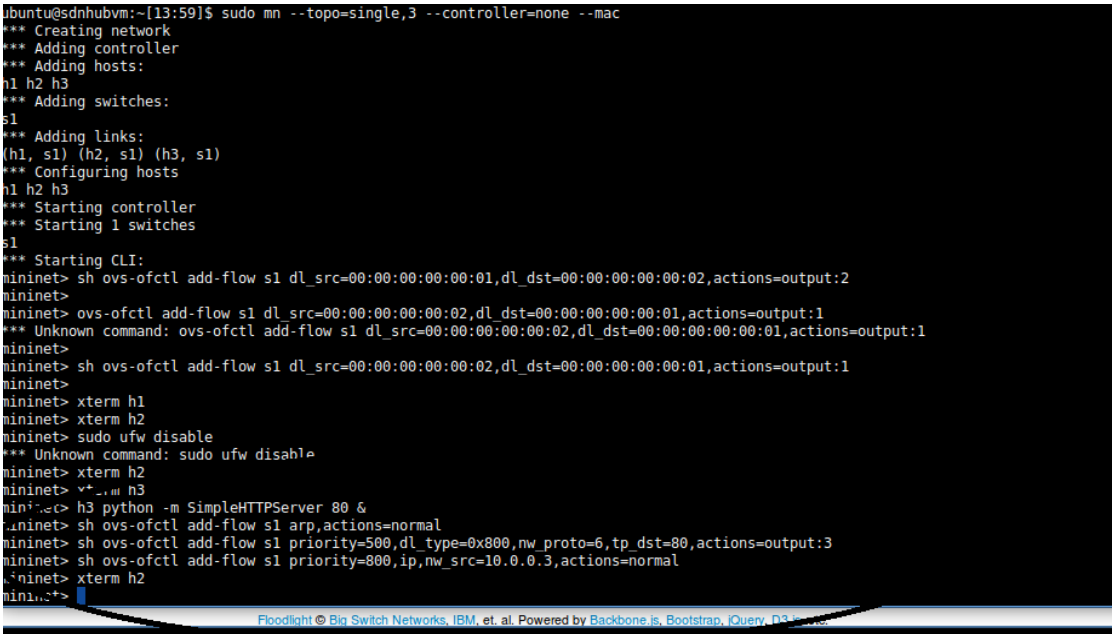
Εικόνα 6.11:Πειραματισμός λειτουργίας των δημιουργημένων ροών κυκλοφορίας



Εικόνα 6.12:Πειραματισμός λειτουργίας των δημιουργημένων ροών με pingall

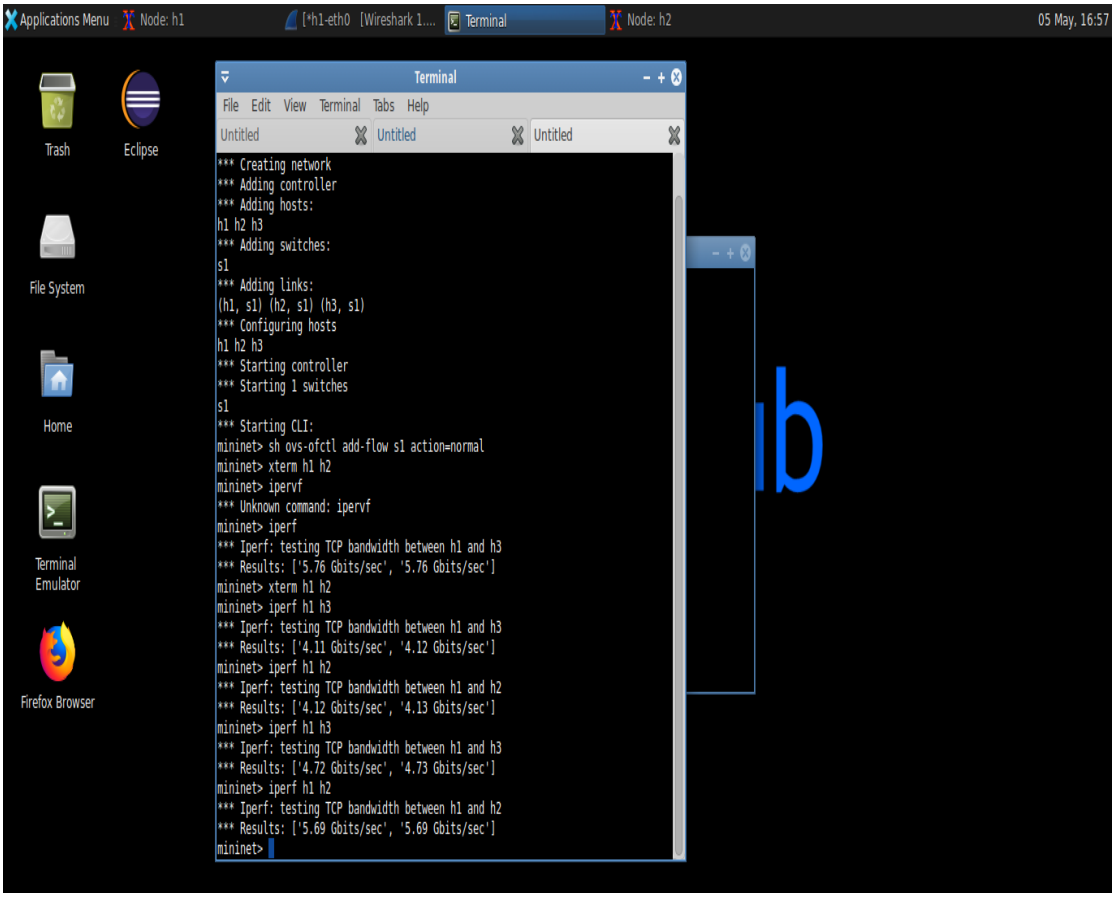


Εικόνα 6.13:Προσθήκη κανόνα προώθησης ροών στον h3



Εικόνα 6.14: Αναίρεση κανόνα προώθησης όλων των ροών κυκλοφορίας στον h3

[1] Για τα βήματα αυτά, αξιοποιείται η μεθοδολογία που περιγράφεται στον ακόλουθο Σύνδεσμο: https://hackmd.io/@pmanzoni/SyWm3n0HH



Εικόνα 6.15:Εύρος ζώνης TCP παραδοσιακού δικτύου

6.4 Ασφάλεια Δικτύων

Στο σημείο αυτό, θα πραγματοποιηθεί έλεγχος της ασφάλειας των μη-προκαθοριζόμενων από λογισμικό και των προκαθοριζόμενων από λογισμικό δικτύων. Αρχικά, θα πραγματοποιηθεί η σχετική διεργασία για το SDN δίκτυο και στη συνέχεια η αντίστοιχη διαδικασία για το μη-προκαθοριζόμενο από λογισμικό δίκτυο. Η ασφάλεια θα αξιολογηθεί με την εξαπόλυση μιας επίθεσης άρνησης εξυπηρέτησης (DoS), έτσι ώστε να συγκριθούν τα δύο δίκτυα σε ό,τι αφορά τις δυνατότητες ασφάλειας τις οποίες διαθέτουν.

Τα βήματα τα οποία ακολουθούνται είναι τα ακόλουθα:

1. Εκτέλεση Floodlight

2. Επισκόπηση δημιουργημένων κόμβων στο Floodlight

3. Επισκόπηση τοπολογίας στο Floodlight

4. Εκτέλεση Επίθεσης Άρνησης Εξυπηρέτησης (Δημιουργία απλού Εξυπηρετητή HTTP, εκτέλεση Ping flooding attack)

5. Δοκιμή λήψης μετρικών απόδοσης (SDN)

6. Διάγραμμα εισόδου εξόδου για h1 (Wireshark)

7. Δημιουργία επίθεσης DDoS Attack στον h1

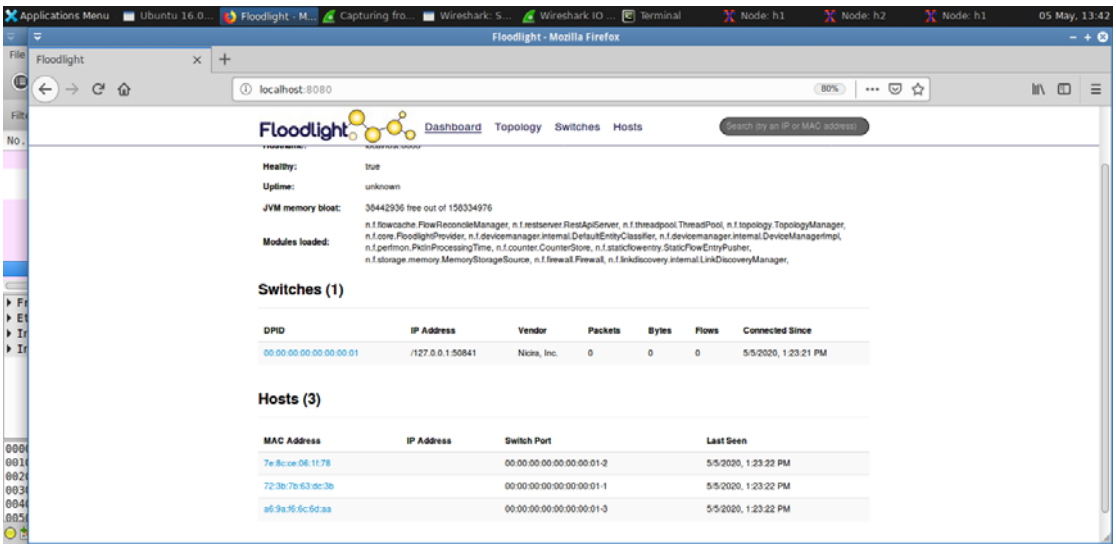
8. Προσπάθεια λήψης εύρους ζώνης μεταξύ h3, h2 με τον h1

9. Λήψη μετρικών μη-SDN μετά το DDoS attack

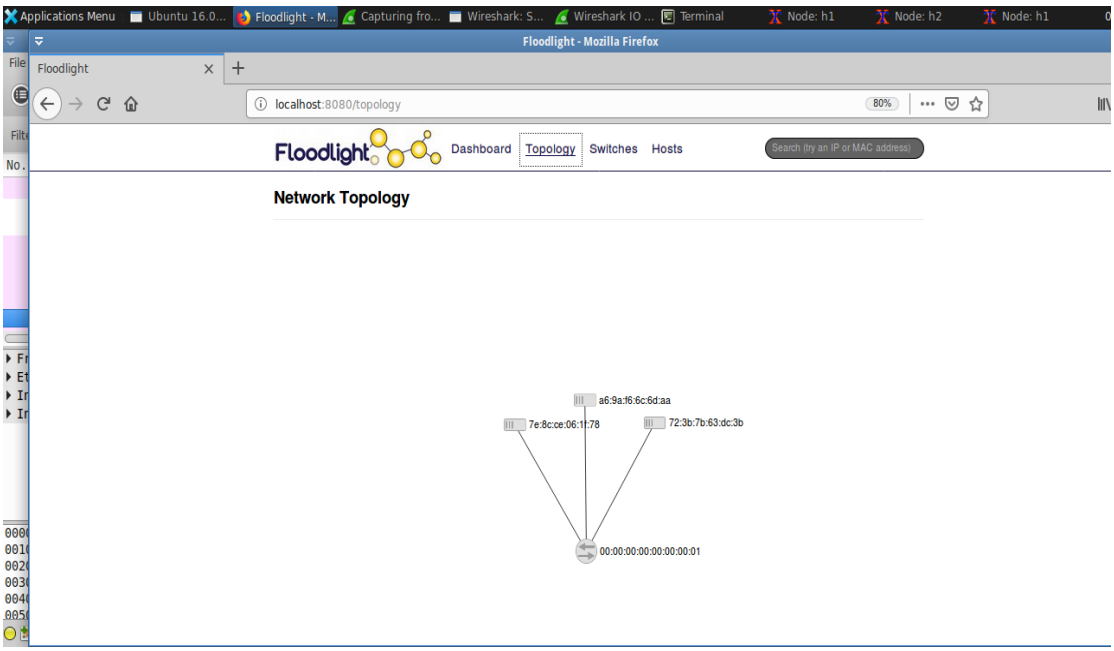
10. Διάγραμμα με DDoS Attack μεταξύ 8 hosts

11. Απεικόνιση δείγματος πακέτων Ping (ICMP) που δεν έλαβαν απάντηση (Wireshark)

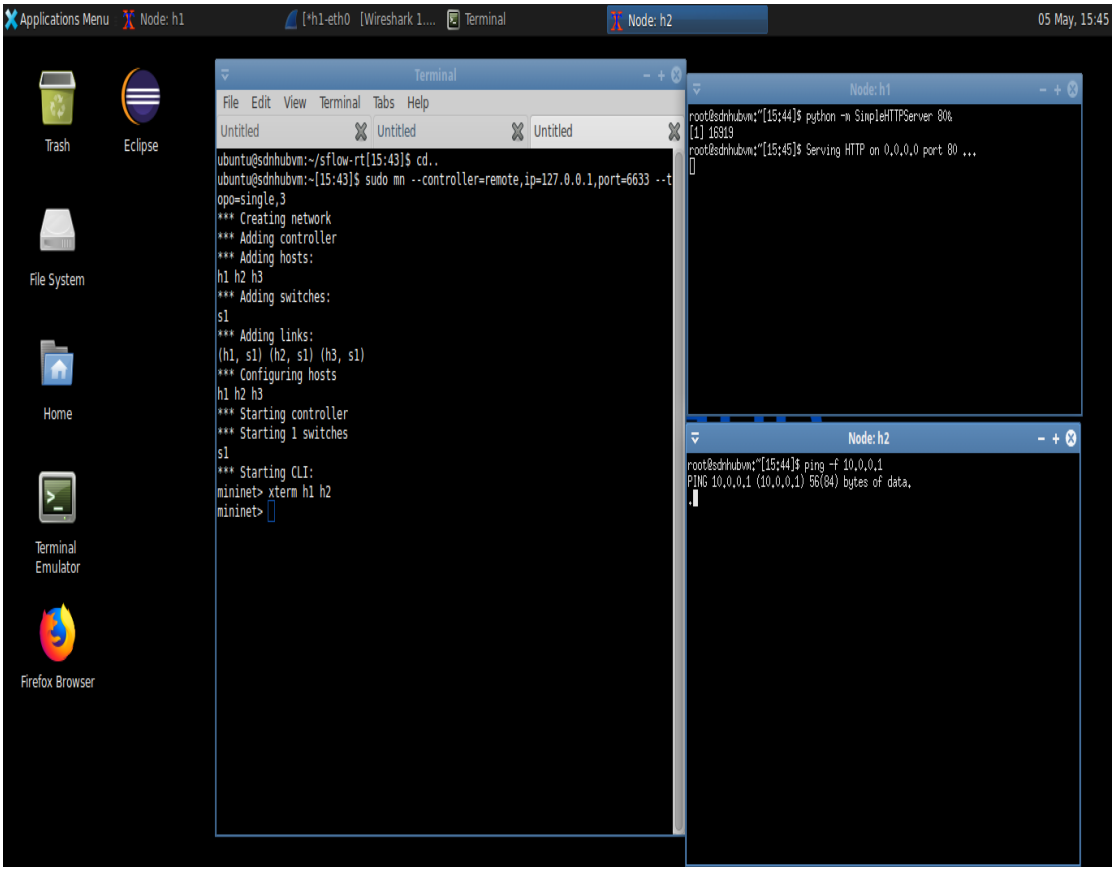
Ακολούθως, η διαδικασία παρακολουθείται μέσω των στιγμιότυπων οθόνης, που παρατίθενται παρακάτω.



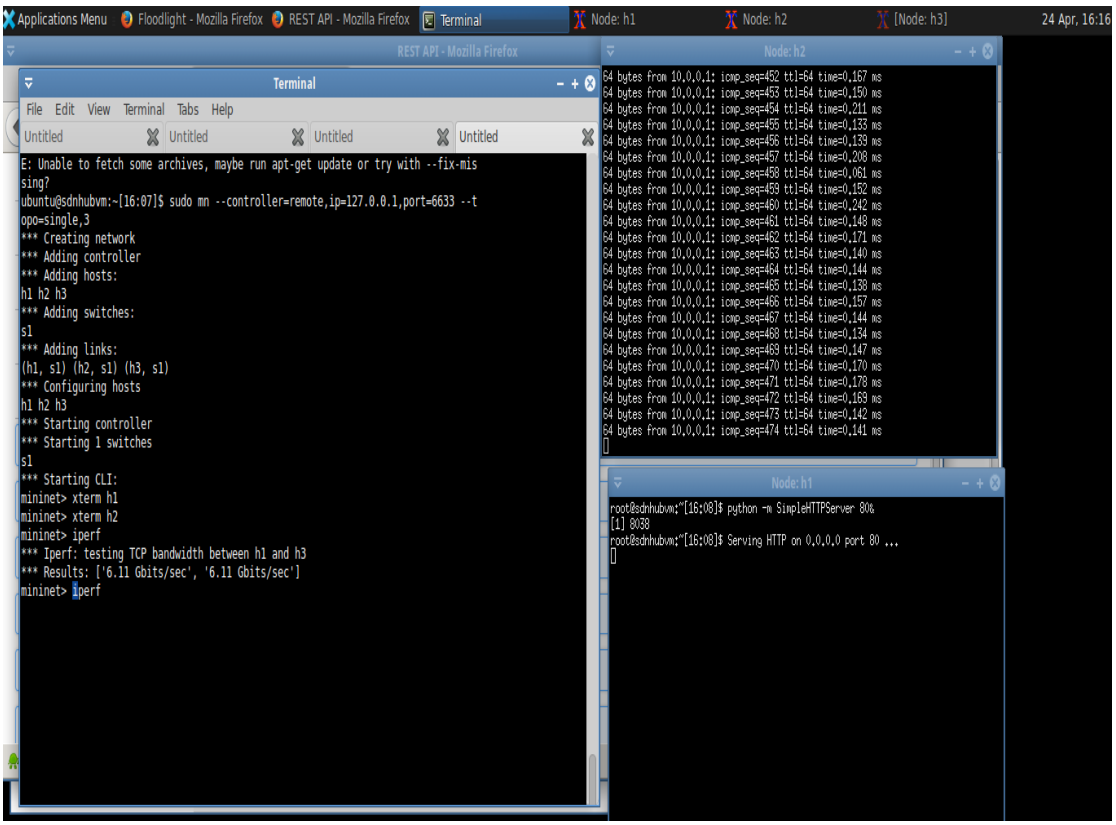
Εικόνα 6.16: Άνοιγμα λογισμικού ελεγκτή Floodlight



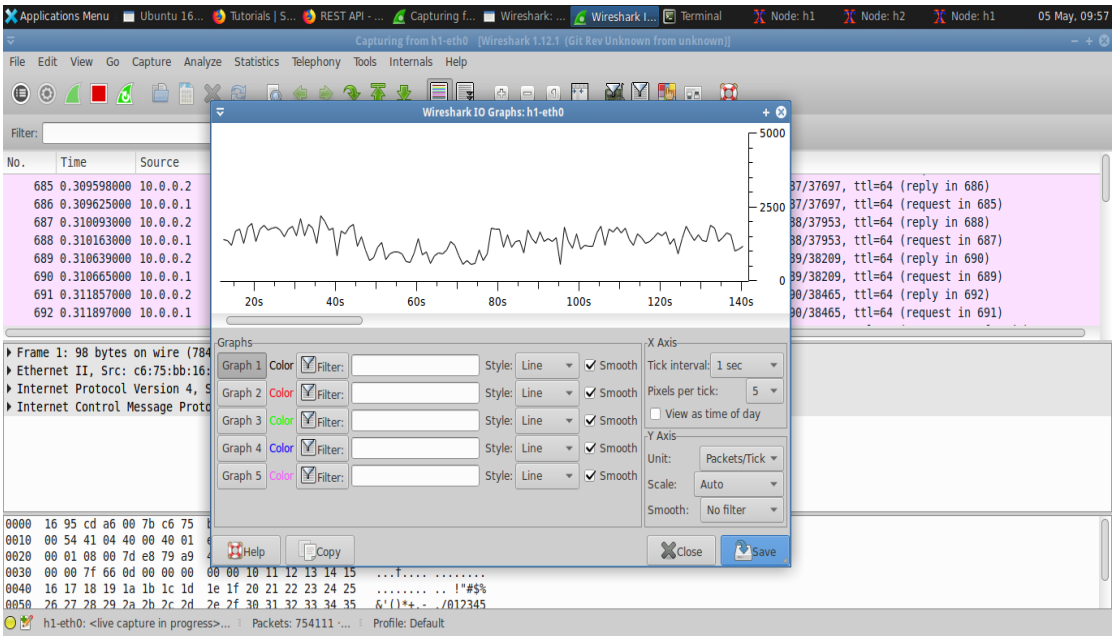
Εικόνα 6.17: Άνοιγμα τοπολογίας δικτύου SDN στο Floodlight



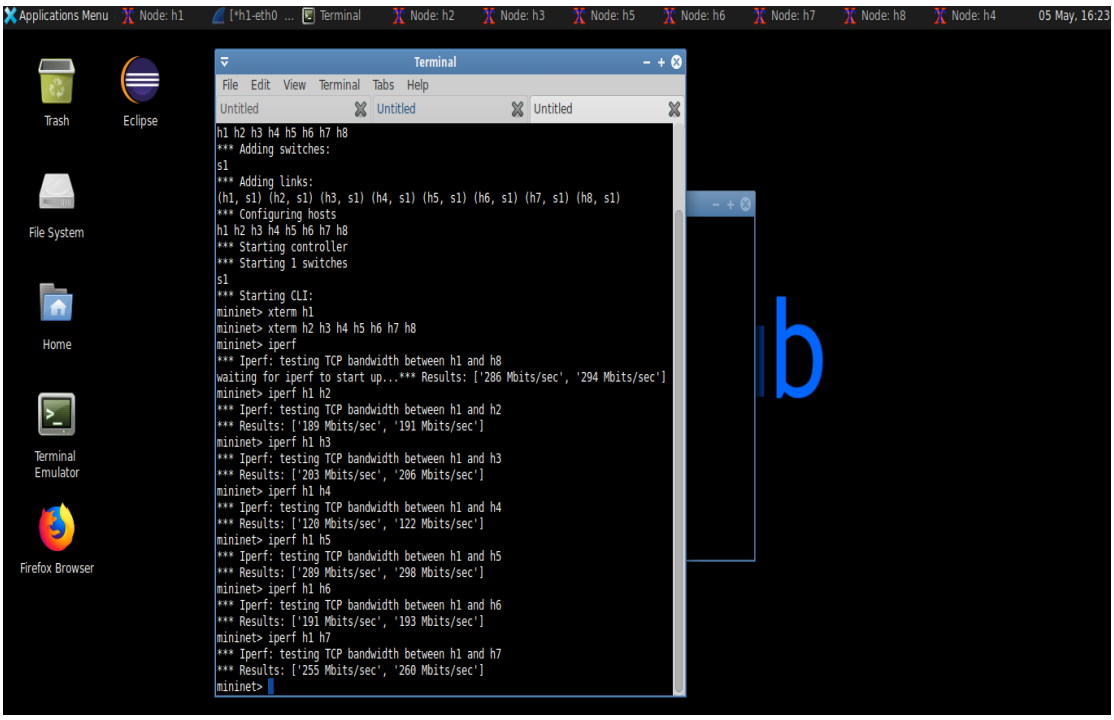
Εικόνα 6.18: Εκτέλεση επίθεσης Ddos από τον h2 στον h1 στο SDN δίκτυο



Εικόνα 6.19:Λήψη μετρικών απόδοσης μεταξύ δικτύου h1 και h3 στο SDN δίκτυο



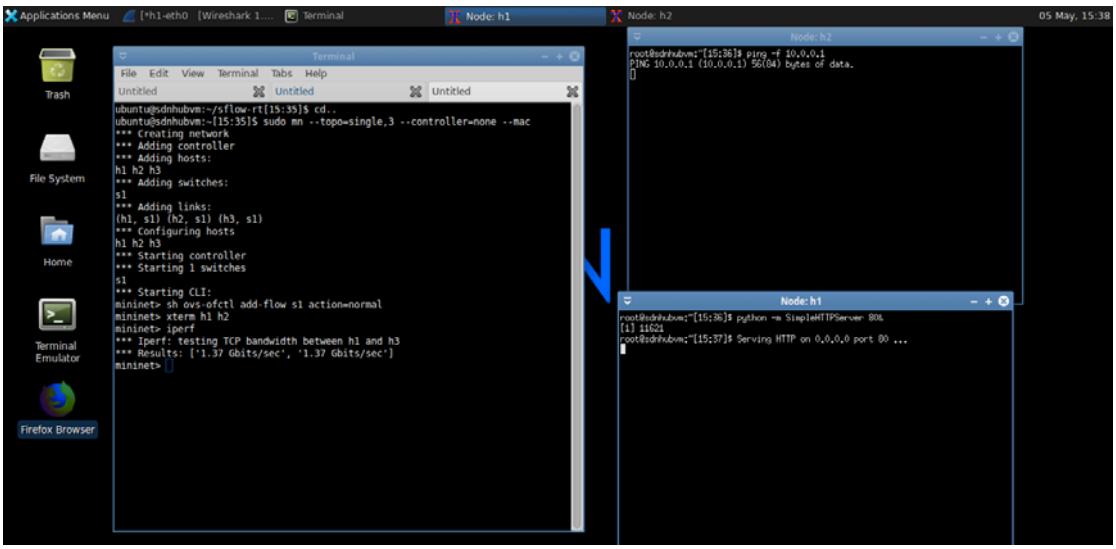
Εικόνα 6.20: Διάγραμμα εισόδου-εξόδου για h1(Wireshark)



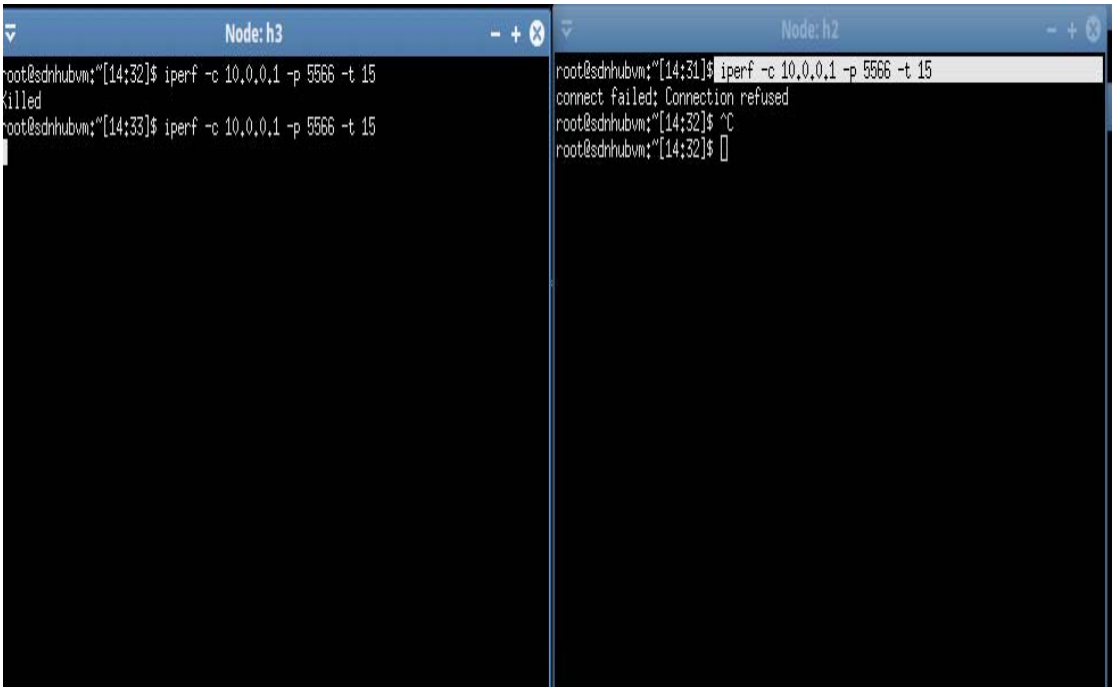
Εικόνα 6.21:Διάγραμμα με Ddos attack μεταξύ 8 hosts στο SDN δίκτυο

Από την εκτέλεση όλων των παραπάνω βημάτων, συμπεραίνουμε ότι η Επίθεση Άρνησης Εξυπηρέτησης που εξαπολύεται μεταξύ των υπολογιστών εξυπηρέτησης, είτε αυτοί είναι 2 είτε είναι 8, επιδρά μεν στο ύψος του εύρους ζώνης, χωρίς όμως να είναι τελικά αποτελεσματική, δηλαδή ώστε να επιφέρει αποτελέσματα άρνησης εξυπηρέτησης (απώλειας αιτημάτων στον εξυπηρετητή του h1). Μπορούμε να αποδώσουμε μια τέτοια δυνατότητα στην ύπαρξη του ελεγκτή δικτύου, ο οποίος, όπως ήδη έχει αναλυθεί, παίζει ρυθμιστικό και αντισταθμιστικό ρόλο.

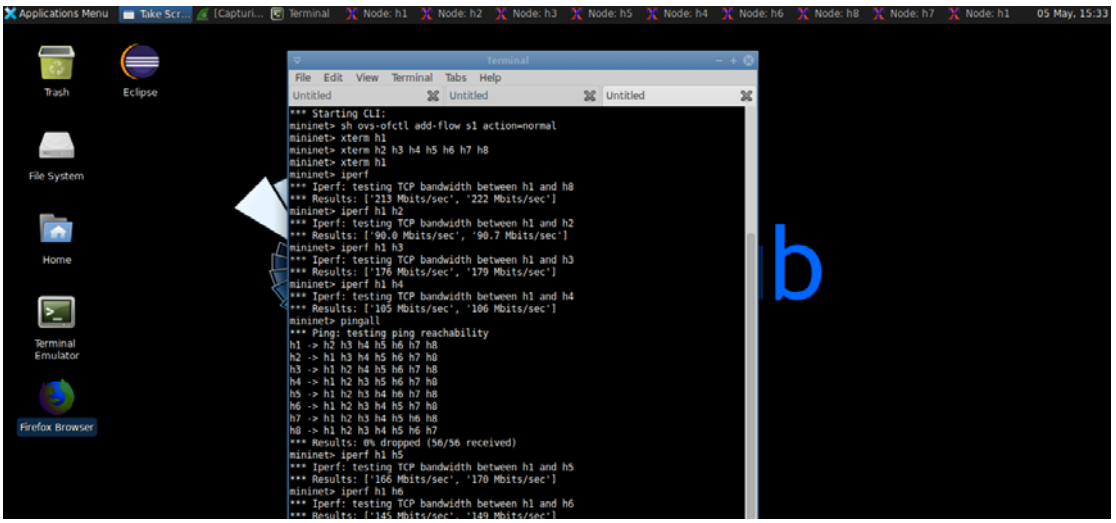
Στη συνέχεια, θα πραγματοποιηθούν τα αντίστοιχα βήματα και για το απλό δίκτυο, χωρίς την ύπαρξη ελεγκτή δικτύου τύπου SDN.



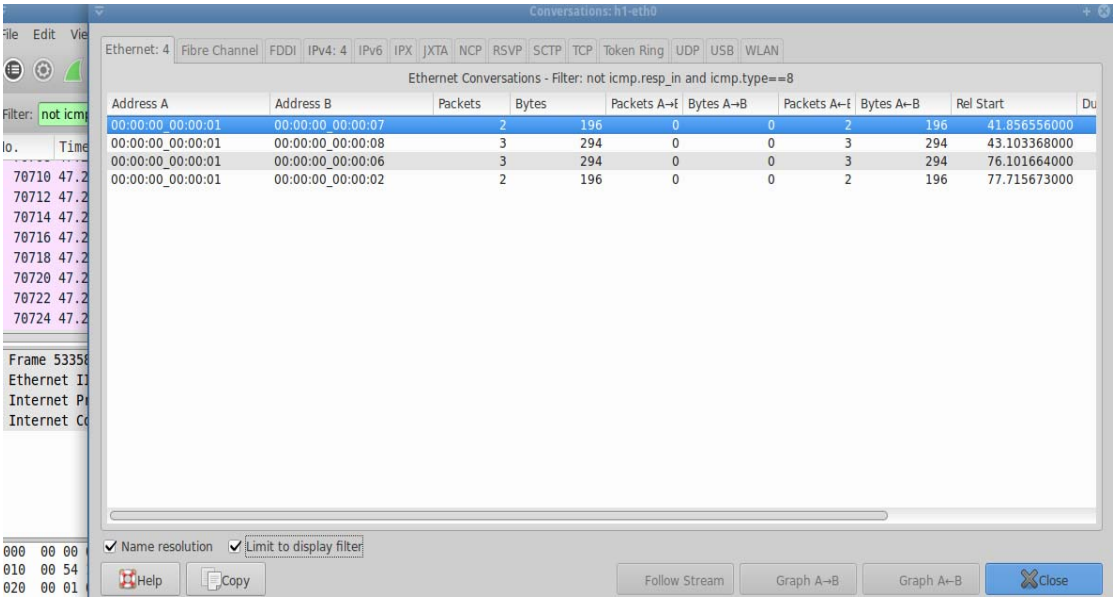
Εικόνα 6.22: Εκτέλεση επίθεσης Ddos από τον h2 στον h1 στο παραδοσιακό δίκτυο



Εικόνα 6.23: Προσπάθεια λήψης εύρους ζώνης μεταξύ h3, h2 με τον h1 στο παραδοσιακό δίκτυο



Εικόνα 6.24: Διάγραμμα με Ddos attack μεταξύ 8 hosts στο παραδοσιακό δίκτυο



Εικόνα 6.25: Απεικόνιση δείγματος πακέτων PING(ICMP) στο παραδοσιακό δίκτυο που δεν έλαβαν απάντηση(Wireshark)

6.5 Συμπεράσματα

Στην καταληκτική παράγραφο αυτή, συνοψίζουμε τα συμπεράσματα από τους δύο πειραματισμούς που πραγματοποιήθηκαν σε παραδοσιακά (μη-καθοριζόμενα από λογισμικό) αλλά και καθοριζόμενα από λογισμικό δίκτυα σε ό,τι αφορά τις επιθέσεις DDoS. Παρατηρήθηκε

ότι και στα δύο δίκτυα αρχικά έγινε σειρά επιτυχών πειραματισμών. Στο μη-SDN, με προσθήκη διάφορων ροών κυκλοφορίας (όπως απαιτείται σε παραδοσιακό δίκτυο), με δημιουργία ελεγκτή κυκλοφορίας και λήψη αντίστοιχων μετρικών.

Όμως, όταν πραγματοποιήθηκε η Επίθεση Άρνησης Εξυπηρέτησης, παρατηρήθηκαν δύο διαφορετικές συμπεριφορές:

- Στο SDN δίκτυο, το λογισμικό το οποίο καθορίζει τη λειτουργία και την κυκλοφορία μέσω του ελεγκτή (controller) στάθηκε δυνατό να «ρυθμίσει» την κυκλοφορία στον «βομβαρδιζόμενο» από πακέτα υπολογιστή υποδοχής h1, με αποτέλεσμα τη μη-διακοπή της κυκλοφορίας από και προς αυτό τον κόμβο αλλά και τη διατήρηση του Εύρους Ζώνης σε ικανοποιητικά επίπεδα χωρίς απώλειες πακέτων

- Στο παραδοσιακό δίκτυο, όπου τέτοιο λογισμικό απουσιάζει, δεν ήταν εφικτή η ρύθμιση των πρόσθετων ροών σε ανάλογο βαθμό, με αποτέλεσμα ένα πολύ μειωμένο Εύρος Ζώνης, δύο προσπάθειες σύνδεσης από τους δύο κόμβους h1 και h2 να αποτύχουν και να υπάρξουν πακέτα ping που δεν έλαβαν απαντήσεις (Εικόνα 19)

Το συμπέρασμα που προκύπτει από το σύνολο της διαδικασίας αυτής είναι η ανθεκτικότητα την οποία προσδίδει το λογισμικό στο δίκτυο SDN, σε αντίθεση με την ευπάθεια σε παρόμοιες επιθέσεις από την οποία διακρίνεται το μη-καθοριζόμενο από λογισμικό δίκτυο. Πράγματι, τα συμπεράσματα αυτά είναι συμβατά με αντίστοιχες έρευνες[14] και [18],όπου επισημαίνεται μεν η ευαλωτότητα μόνο του κεντρικού ελεγκτή σε ορισμένα είδη επιθέσεων, αλλά αναδεικνύεται η βελτιωμένη ασφάλεια των εν λόγω δικτύων, σε σύγκριση με τα παραδοσιακά δίκτυα.

Κεφάλαιο 7
Υπάρχουσες λύσεις για την ασφάλεια SDN

Όπως προκύπτει από την μελέτη της ανασκόπησης της βιβλιογραφίας, η ερευνητική κοινότητα, φαίνεται να δείχνει έντονο ενδιαφέρον γύρω από την μελέτη της βελτίωσης της ασφάλειας των δικτύων SDN. Όπως έχει ήδη αναφερθεί, σε προηγούμενο κεφάλαιο, είναι κοινώς αποδεκτό, ότι τα δίκτυα SDN μπορεί να αποφέρουν σημαντικά οφέλη στο ζήτημα της ασφάλειας των δικτύων. Όμως, εξακολουθεί να υπάρχει περιθώριο βελτίωσης των προτεινόμενων εφαρμογών SDN στου διάφορους τύπους δικτύων.

Στο κεφάλαιο αυτό, θα εξεταστούν και θα παρουσιαστούν αρχικά τα ζητήματα και οι προκλήσεις που καλούνται να αντιμετωπίσουν τα δίκτυα SDN. Επίσης, θα μελετηθούν οι ευπάθειες, οι απειλές και οι διάφοροι τύποι επιθέσεων που σχετίζονται με τα δίκτυα SDN. Στην συνέχεια, παρουσιάζονται διάφορες προτεινόμενες λύσεις για την αποτελεσματική ασφάλεια των δικτύων SDN.

7.1 Ευπάθειες των SDN δικτύων

Το γεγονός ότι η τεχνολογία SDN αλλάζει τον τρόπο με τον οποίο λειτουργούν τα δίκτυα, είναι πιθανό να δημιουργήσει νέες μεθόδους επίθεσης, οι οποίοι μπορούν να χρησιμοποιηθούν για την εκμετάλλευση των μεμονωμένων στοιχείων μιας αρχιτεκτονικής SDN. Οι νέοι τρόποι επικοινωνίας και αλληλεπίδρασης της τεχνολογίας SDN (π.χ. συσκευές-προς-ελεγκτές, ελεγκτής σε ελεγκτή και ελεγκτής σε εφαρμογή), μπορεί να θέσει ένα δίκτυο SDN σε κίνδυνο και να προκαλέσει την συνολική αποτυχία λειτουργίας ενός δικτύου[23].

Επίσης, όπως έχει αναφερθεί, τα δίκτυα SDN συγκεντρώνουν σε ένα κεντρικό σημείο ελέγχου την διαχείριση του δικτύου, και όλα τα άλλα επίπεδα δικτύου πρέπει να διατηρούν μια διεπαφή στην οποία μπορούν να ανταλλάσσουν σημαντικές πληροφορίες με το κεντρικό σημείο ελέγχου[09]. Συνήθως, η διεπαφή που χρησιμοποιείται από το επίπεδο δεδομένων και το data plane για την επικοινωνία. Αυτή η διεπαφή είναι γνωστή ως διεπαφή ελέγχου-δεδομένων-επιπέδου, ή απλά ως διασύνδεση Southbound. Οι Εφαρμογές SDN βρίσκονται επίσης σε ένα εννοιολογικό επίπεδο εφαρμογών και επικοινωνούν με τον ελεγκτή μέσω της διεπαφής «Northbound Interface» ή Control-Application-Plane. Οι εφαρμογές που βρίσκονται σε αυτό το επίπεδο έχουν τη δυνατότητα να αιτούνται πληροφορίες απευθείας από τον ελεγκτή και να λαμβάνουν χρήσιμες πληροφορίες σχετικά με τη λογική / φυσική κατάσταση των δικτύων. Αυτό είναι επωφελές για τους προγραμματιστές που δημιουργούν και αναπτύσσουν εφαρμογές SDN, καθώς τα προγράμματά τους μπορούν να έχουν πρόσβαση σε μεγάλες ποσότητες σημαντικών δεδομένων σε πραγματικό χρόνο[22].

Ωστόσο, το γεγονός αυτό δημιουργεί σημαντικό κίνδυνο, καθώς κακόβουλοι χρήστες ενδέχεται να είναι σε θέση να προγραμματίσουν τις εφαρμογές τους για να χρησιμοποιήσουν αυτές τις χρήσιμες πληροφορίες για να προκαλέσουν επιθέσεις, καθιστώντας το δίκτυο ευπαθή όσο αναφορά την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, τα οποία μεταδίδονται μέσα σε ένα δίκτυο. Συνεπώς, από τη μία πλευρά, οι αλλαγές στην αρχιτεκτονική του δικτύου μέσω της τεχνολογίας SDN δημιουργούν ευελιξία και καινοτομία στην διαχείριση των εφαρμογών και την ασφάλεια των δεδομένων και δίνει στους προγραμματιστές τη δυνατότητα να προστατεύουν αποτελεσματικότερα τα δίκτυο από ενδεχόμενες απειλές και επιθέσεις. Από την άλλη πλευρά, οι σύνδεσμοι μεταξύ του data plane, του επιπέδου δεδομένων και του επιπέδου εφαρμογής δημιουργούν νέες ευκαιρίες επίθεσης στους κακόβουλους χρήστες.

Στην επόμενη ενότητα, θα παρουσιαστούν οι διάφοροι τύποι επιθέσεων, που πραγματοποιούνται λόγω της αλλαγής της αρχιτεκτονικής ενός δικτύου, δηλαδή επιθέσεις που πραγματοποιούνται σε ένα δίκτυο SDN. Οι λύσεις που θα εξεταστούν, εστιάζουν στην προσπάθεια αντιμετώπισης των επιθέσεων αυτών και εξασφαλίζουν ότι ακόμα και στην αλλαγή της αρχιτεκτονικής δικτύου από παραδοσιακό δίκτυο σε δίκτυο SDN, τα δεδομένα θα παραμείνουν ασφαλή κατά την μετάδοσή τους[01].

7.2 Επιθέσεις των SDN δικτύων

Τα δίκτυα που λειτουργούν με την τεχνολογία και την αρχιτεκτονική SDN εξακολουθούν να έχουν τις ίδιες απαιτήσεις ασφαλείας με τις παραδοσιακές ρυθμίσεις δικτύου, καθώς είναι πιθανό ότι θα μεταφέρουν συχνά εμπιστευτικές πληροφορίες. Επειδή, δημιουργούνται νέες ευκαιρίες από την αλλαγή της αρχιτεκτονικής, δημιουργείται επίσης η ανάγκη για την δημιουργία επιπέδων ασφάλειας, όπως συμβαίνει με τα παραδοσιακά δίκτυα, αλλά δημιουργείται και η ανάγκη για νέους μηχανισμούς ασφάλειας, ώστε να προστατεύονται τα νέα επίπεδα αλληλεπίδρασης που απαρτίζουν τα δίκτυα SDN[21].

7.2.1 Επιθέσεις άρνησης υπηρεσιών (Ddos – Flow requests)

Πολλοί τύποι συμβατικών επιθέσεων άρνησης υπηρεσιών (DDoS- Denial of Service attack) μπορούν να πραγματοποιηθούν σε ένα περιβάλλον δικτύου SDN, αλλά επίσης, υπάρχουν και νέου τύπου επιθέσεις DDos, στις οποίες οι κακόβουλοι χρήστες χρησιμοποιούν καταχωρήσεις ροής (Data flows) οι οποίες στοχεύουν σε κάποιον ελεγκτή, με κίνδυνο να τεθεί εκτός λειτουργίας. Οι κακόβουλοι χρήστες, «πλημμυρίζουν» κάποιον ελεγκτή με πολλαπλά αιτήματα ροής. Στην συνέχεια, οι ελεγκτές υπολογίζουν τους διαθέσιμους πόρους για την ικανοποίηση των αιτημάτων. Όμως, ο ελεγκτής μπορεί να καταστεί αδύνατον να αντιμετωπίσει τυχόν νόμιμα αιτήματα που λαμβάνει. Στοχεύοντας το κεντρικό σημείο ελέγχου (δηλαδή τον ελεγκτή) καθιστά το σύνολο του δικτύου σε μεγάλο βαθμό αχρησιμοποίητο. Ενώ οι διαδρομές δεδομένων που βρίσκονται επί του παρόντος στο δίκτυο ενδέχεται να είναι σε θέση να λειτουργούν προσωρινά με έναν ελεγμένο χειριστή, όταν έχει παρέλθει ένα μεγάλο χρονικό όριο των κανόνων (που αποθηκεύεται στον πίνακα τους), θα πρέπει να αιτηθούν ξανά τον ελεγκτή, ο οποίος δεν θα είναι σε θέση να

αντιμετωπίσει τα αιτήματα. Τελικά, αν η επίθεση κατακλύσει με πολλαπλά αιτήματα για αρκετό χρονικό διάστημα το δίκτυο, είναι πιθανόν να τεθεί εκτός λειτουργίας[22].

7.2.2 Επιθέσεις άρνησης υπηρεσιών (Dos-Switching-flow table entry flooding)

Στο επίπεδο του επιπέδου δεδομένων, οι ψευδώς δημιουργημένες καταχωρήσεις ροής μπορούν να δημιουργήσουν προβλήματα αδυναμίας επεξεργασίας, από τις συσκευές του δικτύου SDN, και έτσι να καταναλώσουν το χώρο στους πίνακες εισόδου ροής. Κατ' επέκταση, αυτό σημαίνει ότι οι δρομολογητές του δικτύου SDN δεν θα μπορούν στην συνέχεια να προσθέσουν νέες καταχωρήσεις ροής στους πίνακες τους και έχει ως αποτέλεσμα οι συσκευές να μην μπορούν να ενσωματώσουν επακόλουθες ενημερώσεις ροής, δημιουργώντας συμφόρηση στο δίκτυο. Η αδυναμία των συσκευών Data plane να διακρίνουν νόμιμα και παράνομα αιτήματα, μπορεί να δημιουργήσει υπερχείλιση στον flowbuffer[22].

7.2.3. Παραβίαση Ελεγκτή (Hijacked/Rogue Controller)

Ο ελεγκτής μπορεί να θεωρηθεί ως ο κεντρικός «εγκέφαλος» ενός SDN. Ελέγχει ολόκληρο το δίκτυο από ένα σημείο, καθιστώντας το αναμφισβήτητα το πιο ζωτικό στοιχείο της αρχιτεκτονικής SDN. Ένας εισβολέας που καταφέρνει να θέσει σε κίνδυνο τον ελεγκτή έχει ουσιαστικά έλεγχο σε ολόκληρο το δίκτυο[11]. Η ικανότητα ελέγχου των ενεργειών του ελεγκτή θα επέτρεπε στον κακόβουλο χρήστη, να χειριστεί τις καταχωρήσεις ροής με οποιονδήποτε τρόπο όπως να επιλέξει, π.χ. διακοπή ορισμένων τύπων πακέτων που φθάνουν στον προορισμό τους, ανακατεύθυνση πακέτων σε κακόβουλους κόμβους στην υποδομή του δικτύου. Σε συνδυασμό με αυτό, ο κακόβουλος χρήστης θα μπορούσε να θέσει σε κίνδυνο μια συγκεκριμένη συσκευή προώθησης (δρομολογητή) στο δίκτυο και να της επιτρέψει να λειτουργεί ως κόμβος «man-in-the-middle» ή blackhole. Συνεπώς, αυτή η επίθεση μπορεί να έχει ως αποτέλεσμα, την αλλοίωση των δεδομένων και των πακέτων που μεταδίδονται προ το δίκτυο. Επίσης, σε ένα χειρότερο σενάριο, ο έλεγχος του ελεγκτή από τον κακόβουλο χρήστη, μπορεί να επηρεάσει / ή ακόμα και να διακόψει τη διαθεσιμότητα άλλων ελεγκτών, να αλλάξει κανόνες εγκατεστημένους σε κρυφές μνήμες διαδρομών δεδομένων, ή να διακόψει κρίσιμες εφαρμογές στο αντίστοιχο επίπεδο δικτύου.

7.2.4 Κακόβουλες εφαρμογές

Λόγω του επιτρεπόμενου πλαισίου SDN για ενσωμάτωση εφαρμογών τρίτων, προκύπτει το ζήτημα των κακόβουλων εφαρμογών. Οι εφαρμογές που παρουσιάζουν κακόβουλη συμπεριφορά σε ένα περιβάλλον SDN μπορεί να έχουν καταστροφικές συνέπειες, παρόμοιες με εκείνες ενός ελεγχόμενου ελεγκτή[2]. Είναι δύσκολο να επιβληθεί ο έλεγχος ταυτότητας και η εξουσιοδότηση μιας εφαρμογής για λειτουργία σε περιβάλλον SDN. Οι εφαρμογές που βασίζονται σε τεχνικές βαθιάς επιθεώρησης πακέτων για λειτουργία μπορούν να δημιουργήσουν δυνητικούς κινδύνους για το δίκτυο - μπορεί να είναι σε θέση να ελέγχουν έμμεσα ολόκληρο το δίκτυο μέσω των πληροφοριών που έχουν συλλέξει κατά την επιθεώρηση πακέτων[08].Η αυξημένη ποσότητα δεδομένων και ο τρόπος με τον οποίο βρίσκεται σε κεντρική τοποθεσία, είναι αυτό που δίνει σε κακόβουλες εφαρμογές τη δυνατότητα να απειλήσει την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών χρήστη / δικτύου στις οποίες έχουν πρόσβαση. Η εξασφάλιση της διεπαφής είναι μια δύσκολη εργασία, καθώς κάθε εφαρμογή που την χρησιμοποιεί μπορεί να απαιτεί πρόσβαση σε ένα μοναδικό υποσύνολο πληροφοριών από τον ελεγκτή. Για την επιτυχή παρακολούθηση αυτού, πρέπει να εφαρμοστεί κάποιο είδος αυστηρής πολιτικής πρόσβασης στις πληροφορίες. Αυτό διασφαλίζει ότι μια εφαρμογή δηλώνει ποιες πληροφορίες θα χρειαστεί και μπορεί να έχει πρόσβαση μόνο σε αυτές. Αυτό θα μπορούσε να διασφαλίσει ότι οι εφαρμογές δεν κλέβουν κρυφά ή χρησιμοποιούν πληροφορίες από άλλες εφαρμογές. Πρέπει επίσης να διασφαλίζεται η αυθεντικότητα, προτού μια εφαρμογή μπορεί να επικοινωνήσει με τον ελεγκτή.

7.2.5 Επιθέσεις συνδέσμου ελέγχου-δεδομένων Data Plane

Μια άλλη βασική περιοχή στα SDN που εκμεταλλεύεται ως ευκαιρία για επίθεση από τους κακόβουλους χρήστες, είναι η σύνδεση μεταξύ του επιπέδου ελέγχου και του επιπέδου δεδομένων. Η προδιαγραφή OpenFlow ορίζει τη χρήση του TLS (Transport Layer Security) ως προαιρετικό, καθιστώντας αυτό ένα αδύνατο σημείο και είναι ευάλωτα σε διάφορες επιθέσεις, δηλαδή επιθέσεις man in-the-middle και επιθέσεις black-hole[23].

- Επίθεση Man-in-the-Middle: Μια επίθεση τύπου man-in-the-middle λαμβάνει χώρα όταν ένας κακόβουλος κόμβος εγκαθίσταται μεταξύ του ελεγκτή και των διαδρομών δεδομένων που βρίσκονται στο επίπεδο δεδομένων. Αντί να προωθεί άμεσα τα μηνύματα

απευθείας στον ελεγκτή (ή το αντίστροφο), ο κόμβος «man-in-the-middle» είναι σε θέση να χειριστεί / ή να ελέγξει το περιεχόμενο των πακέτων.

- Επίθεση μαύρης τρύπας: Θα μπορούσε επίσης να πραγματοποιηθεί επίθεση τύπου μαύρης τρύπας, στην οποία ένας κόμβος εγκαθίσταται μεταξύ μιας στοχευμένης συσκευής και του ελεγκτή και απλώς ρίχνει τα πακέτα που λαμβάνει χωρίς να τα προωθήσει στον ελεγκτή. Αυτό οδηγεί σε ανάλυση των επικοινωνιών δικτύου και καθιστά τις υπηρεσίες μη διαθέσιμες σε νόμιμους χρήστες . Εάν ένας εισβολέας καταφέρει να εδραιωθεί ως ενδιάμεσος μεταξύ του επιπέδου ελέγχου και του επιπέδου δεδομένων, μπορεί ενδεχομένως να είναι καταστροφικό για ολόκληρο το δίκτυο.

Η επίθεση τύπου man-in-the-middle είναι μια άμεση επίθεση στην ακεραιότητα των μηνυμάτων ελέγχου μεταξύ συσκευών δικτύου στο επίπεδο δεδομένων και του ελεγκτή. Ένας αντίπαλος μπορεί να ανταλλάξει τα μηνύματα ελέγχου και να διαμορφώσει τον τρόπο με τον οποίο σχηματίζεται το δίκτυο με τρόπο που να τους ωφελεί. Από την άλλη πλευρά, η επίθεση τύπου black-hole είναι μια άμεση επίθεση στη διαθεσιμότητα των υπηρεσιών δικτύων. Εάν όλα τα μηνύματα μεταξύ συσκευών δικτύου και ελεγκτή δεν προωθούνται από τον κακόβουλο κόμβο, θα οδηγήσει αναπόφευκτα σε διακοπή της επικοινωνίας, και οι συσκευές στο επίπεδο δεδομένων να μην μπορούν να ζητήσουν τον ελεγκτή όταν είναι απαραίτητο.

7.3 Προτεινόμενες λύσεις για την ασφάλεια των SDN δικτύων

Το SDN / OpenFlow παρέχει δυνατότητα προγραμματισμού, δυναμικότητας, ευελιξίας και ευφυίας σε τρέχουσες αρχιτεκτονικές δικτύου και τα οφέλη της μπορούν να παραδοθούν από τέσσερα κύρια χαρακτηριστικά:

(i) δυναμικός έλεγχος ροής

(ii) ορατότητα σε όλο το δίκτυο με κεντρικό έλεγχο

(iii) Δυνατότητα προγραμματισμού δικτύου

(iv) Απλοποιημένο επίπεδο δεδομένων.

Στο SDN, όλα τα επίπεδα δεδομένων συνδέονται με ένα κεντρικό επίπεδο ελέγχου για τη λήψη μηνυμάτων ελέγχου (π.χ. εισαγωγή κανόνα ροής και διαμόρφωση επιπέδου δεδομένων). Επιπλέον, το επίπεδο ελέγχου συλλέγει πληροφορίες κατάστασης δικτύου από κάθε επίπεδο δεδομένων στέλνοντας ένα μήνυμα ερωτήματος στατιστικών στοιχείων. Επομένως, μια εφαρμογή δικτύου που εκτελείται στο επίπεδο ελέγχου έχει φυσικά μια άποψη όλων των συνδεδεμένων επιπέδων δεδομένων και μπορεί να ελέγχει όλα τα επίπεδα δεδομένων με κεντρικό τρόπο. Πολλές εφαρμογές παρακολούθησης σε ολόκληρο το δίκτυο με SDN (π.χ. BigTap και μια εφαρμογή διαχείρισης δικτύου) είναι καλά παραδείγματα που επωφελούνται από αυτήν τη δυνατότητα.

Δεδομένου ότι όλα τα επίπεδα δεδομένων σε ένα δίκτυο SDN μπορούν να ελεγχθούν από ένα πρόγραμμα εφαρμογής δικτύου, το SDN παρέχει μια ισχυρή ικανότητα προγραμματισμού που επιτρέπει νέες λειτουργίες δικτύου. Αυτό είναι παρόμοιο με τον προγραμματισμό μιας εφαρμογής smartphone (π.χ. Android) για την ενεργοποίηση απεριόριστης δημιουργικότητας λειτουργιών. Για την ενίσχυση αυτής της δυνατότητας, έχουν προταθεί αρκετές γλώσσες προγραμματισμού δικτύου έως τώρα, και μας βοηθούν να προγραμματίζουμε τις λειτουργίες δικτύου εύκολα. Απλοποιημένο επίπεδο δεδομένων: Βασικά, η αρχιτεκτονική SDN διαχωρίζει το επίπεδο δεδομένων από το επίπεδο ελέγχου, και έτσι το επίπεδο δεδομένων έχει σχετικά απλή λογική. Αυτό το απλοποιημένο επίπεδο δεδομένων μας δίνει πιθανότητες να προσθέσουμε μερικές νέες δυνατότητες Το NetFPGA, το DevoFlow αποτελούν καλά παραδείγματα του απλοποιημένου επιπέδου δεδομένων και της τροποποίησής του.

7.3.1 Ευκαιρίες και νέες δυνατότητες για την βελτίωση της ασφάλειας των SDN

Η δυνατότητα προγραμματισμού μέσω ανοιχτών διεπαφών προγραμματισμού εφαρμογών και ο έλεγχος των πολιτικών μέσω ενός κεντρικού ελεγκτή οντοτήτων παρέχει διάφορους τρόπους για την ενίσχυση της ασφάλειας και τον μετριασμό των απειλών. Το SDN ανοίγει μια νέα πλατφόρμα για τη δημιουργία προσαρμοσμένων αλγορίθμων ασφαλείας. Το υποστηριζόμενο από το SDN

δίκτυο προσφέρει ένα κεντρικό μέρος για τη συλλογή δεδομένων από συσκευές δικτύου και οι νέες προσεγγίσεις ασφαλείας προϋποθέτουν ένα συγκεντρωτικό μοντέλο δεδομένων που δεν ήταν δυνατό σε συμβατικά δίκτυα. Πρόκειται για έναν ακραίο μετασχηματισμό, ο οποίος έχει θετική επιρροή για διάφορους αλγόριθμους που σχετίζονται με την παρακολούθηση δικτύου και μεθοδολογίες τείχους προστασίας[17].

7.3.2 Παρακολούθηση δικτύου

Η παρακολούθηση δικτύου είναι το θεμελιώδες μέρος για την ασφάλεια του δικτύου. Στην πραγματικότητα, υπάρχουν ύποπτα μοτίβα κυκλοφορίας συλλέγοντας δεδομένα σε πραγματικό χρόνο από το δίκτυο και δοκιμάζοντάς το για παραβίαση ασφαλείας μέσω διαφόρων αλγορίθμων ανίχνευσης ανωμαλιών. Για παράδειγμα, ένας εισβολέας μπορεί να χρησιμοποιήσει εργαλεία σάρωσης για να γνωρίζει τη συμπεριφορά του δικτύου πριν κάνει τη λειτουργία επίθεσης. Σε αυτήν την περίπτωση η παρακολούθηση του δικτύου γίνεται πιο σημαντική. Η παρακολούθηση δικτύου σε SDN, με βάση την ανοικτή ροή αποτελείται από τη συλλογή δεδομένων με βάση τη ροή στην πλευρά του ελεγκτή, η οποία είναι μια φυσική διαδικασία ανοιχτής ροής στο SDN. Αυτό μπορεί να επιτευχθεί με δύο τρόπους. Ένα μέσω της λειτουργίας ώθησης, όταν ένας δρομολογητής ενημερώνει τον ελεγκτή για τη ροή που έχει λήξει (μήνυμα FlowRemoved). Ένας άλλος τρόπος είναι η λειτουργία έλξης όταν ο ελεγκτής ζητά από τις συσκευές προώθησης να γνωρίζουν την κατάσταση των ροών μέσω των μηνυμάτων FlowStatisticsRequest και FlowStatisticsReply. Το FlowSense, είναι ένα παράδειγμα λειτουργίας push[17].

7.3.3 Επαλήθευση δικτύου και αυτοματοποίηση

Η μη αυτόματη διαμόρφωση πολιτικής είναι πάντα επιρρεπής σε σφάλματα και πρέπει να υπάρχουν κάποιες τεχνικές αυτοματοποίησης για την επαλήθευση και τη συνέπεια της διαμόρφωσης. Μια έρευνα από τον Gartner, επισημαίνει ότι σε ένα πέρασμα του έτους 2010 έως 2015, το μεγαλύτερο μέρος των διακοπών δικτύου που επηρεάζουν ζωτικές διοικήσεις οφείλονται σε μη αυτόματες διαμορφώσεις και σχετικές με τη διαδικασία και πάνω από το ήμισυ προέρχονται από αλλαγές πολιτικής, δηλαδή ζητήματα αναδιαμόρφωσης και ενημερώσεων.

Στο SDN, όταν υπάρχουν περισσότεροι από ένας ελεγκτές, πολλές εφαρμογές και πολλοί χρήστες εκτελούνται ταυτόχρονα στον ίδιο τομέα, αυτό μπορεί να οδηγήσει σε προβλήματα ασυνέπειας και παραβίασης πολιτικής. Αυτό μπορεί να προκαλέσει πολλά σφάλματα δικτύου, όπως βρόχους, blackholes και προβλήματα ελέγχου πρόσβασης. Επιπλέον, σε μεγάλα δίκτυα όπου υπάρχουν πολλοί διακόπτες, οι ελεγκτές πρέπει να εγκαταστήσουν χιλιάδες ροές που ασχολούνται με πολλούς πίνακες ροής, ο ελεγκτής μπορεί να εγκαταστήσει περίπου 50000 νέες ροές κάθε δευτερόλεπτο, θα πρέπει να υπάρχει μια γρήγορη, αποτελεσματική προσέγγιση για να διασφαλιστεί η συνέπεια της ασφάλειας, προσαρμογή σε μη κρίσιμη αποτυχία και γρήγορη ανακατεύθυνση. Το FlowChecker, αποτελεί μία καλή λύση, καθώς προσφέρει μια σειρά από εργαλεία επαλήθευσης βάσει ιδιοτήτων που εντοπίζουν διαφορετικές εσφαλμένες ρυθμίσεις στο δίκτυο. Το FlowChecker χρησιμοποιεί διαγράμματα δυαδικών αποφάσεων και κωδικοποιεί τη διαμόρφωση πίνακα ροής για να δημιουργήσει μια μηχανή κατάστασης που απεικονίζει τα στατιστικά στοιχεία ροής των συσκευών προώθησης στο δίκτυο[17].

Το NICE[05], είναι επίσης ένα άλλο εργαλείο εύρεσης σφαλμάτων στις διαμορφώσεις SDN. Επιπλέον, εκτός από αυτές τις λύσεις που χρησιμοποιούνται πριν από την έναρξη του δικτύου ή την εγκατάσταση της εφαρμογής, το VeriFlow είναι μια ρύθμιση στο Data plane, το οποίο ελέγχει την ακρίβεια του δικτύου σε πραγματικό χρόνο καθώς το δίκτυο προχωρά προοδευτικά. Ο ελεγκτής NOX διαθέτει επίσης μια ενσωματωμένη λύση ελέγχου σφαλμάτων που ονομάζεται FORTNOX, η οποία προσδιορίζει κανόνες διένεξης σε πραγματικό χρόνο[16].

7.3.4 Βελτιωμένη ανίχνευση απειλών

Στο SDN, ο ελεγκτής παρέχει μια πλήρη εικόνα των συσκευών που είναι πολύ ευνοϊκές για τον εντοπισμό απειλών. Οι διακόπτες ανοιχτής ροής δεν έχουν από προεπιλογή πολιτική επικοινωνίας, όπως στους διακόπτες μάθησης L2, οι διακόπτες OF ακολουθούν τις οδηγίες από τον ελεγκτή και ο ελεγκτής μπορεί να επαναπρογραμματίσει τις συσκευές επιπέδου δεδομένων στο δίκτυο για να πραγματοποιήσει ανάλυση για ύποπτα δεδομένα και κακόβουλη συσκευή στο δίκτυο. Τα περισσότερα από τα παραδοσιακά συστήματα ασφαλείας παρέχουν ασφάλεια στο επίπεδο 3 και στο επίπεδο 4 και δεν μπορούν να εντοπίσουν το κακόβουλο ωφέλιμο φορτίο σε επίπεδο εφαρμογής, σε περίπτωση ασφάλειας επιπέδου εφαρμογής στο SDN, θα πρέπει να σταλούν όλα τα πακέτα σε ελεγκτές.

Για να αποφευχθεί αυτή η κατάσταση, προτείνεται ένας αλγόριθμος που βασίζεται στον αριθμό των ανεπιτυχών προσπαθειών σύνδεσης ψεύτικου αιτήματος[13]. Στέλνει μόνο αυτά τα πακέτα στους ελεγκτές που είναι ύποπτα βάσει των δεδομένων αλγορίθμων. Επίσης, η εταιρία Microsoft χρησιμοποιεί λύσεις SDN στα κέντρα δεδομένων της για κακόβουλη ανίχνευση κυκλοφορίας. Με μια πολύ μεγάλη υποδομή της συμβατικής τεχνολογίας πακέτων της Microsoft, όπως ο κατοπτρισμός θύρας και ο αναλυτής θύρας διακοπτών (SPAN), δεν είναι εφικτές, οι οποίες απαιτούν πολύ υλικές θύρες και λογιστικές ρυθμίσεις. Στο SDN αυτό μπορεί να ρυθμιστεί εύκολα μέσω του ελεγκτή, χρησιμοποιώντας τις εικονικές θύρες .

7.3.5 Δυναμική απόκριση σε απειλές

Η πλήρης προβολή δικτύου σε ολόκληρο το σύστημα SDN, ο προγραμματισμός μέσω ανοιχτών διεπαφών προγραμματισμού εφαρμογών, ο έλεγχος πολιτικών μέσω ενός κεντρικού ελεγκτή οντοτήτων, ενισχύει τους παρόχους ασφαλείας καθώς και τους ερευνητές και ανοίγει νέους τρόπους για να παρέχει δυναμική ανταπόκριση σε απειλές . Λόγω της έλλειψης κεντρικού ελέγχου στο παλιό δίκτυο, η μόνη απάντηση είναι η πτώση της κακόβουλης επισκεψιμότητας, αλλά σε περίπτωση SDN μπορούμε να ανακατευθύνουμε την κίνηση κακόβουλων επιθέσεων, με τον επαναπρογραμματισμό των διακοπτών δυναμικά μέσω του ελεγκτή. Τα FRESCO και FORTNOX είναι παραδείγματα δυναμικής απόκρισης με δυνατότητα SDN , ενάντια σε επιθέσεις[17].

7.4 Βασικές Αρχές Ασφάλειας σύμφωνα με τον ONF(Open Networking Foundation)

Ο οργανισμός ONF (Open Networking Foundation) είναι μια κοινοπραξία που σκοπό έχει να παρέχει τα πρότυπα για το πρωτόκολλο Open-flow, να προωθεί και να υποστηρίζει τα δίκτυα SDN. Ο οργανισμός ιδρύθηκε το 2011, ως ο βασικός φορέας για τα δίκτυα SDN. Ο οργανισμός υποστηρίζεται από τουλάχιστον 200 μέλη (μεγάλες διεθνείς εταιρίες) και ανάμεσα στους συνεργάτες του, είναι οι μεγαλύτερες εταιρίες πληροφορικής, δικτύων και τηλεπικοινωνιών σε όλο τον κόσμο, όπως την εταιρία AT&T, την εταιρία Unicom στην Κίνα, την εταιρία Comcast, την εταιρία Deutsche Telekom στην Γερμανία, την εταιρία Google καθώς και την εταιρία Turk Telekom

στην Τουρκία. Παρακάτω θα γίνει αναφορά στις βασικές αρχές ασφάλειας των δικτύων SDN, σύμφωνα με τον οργανισμό ONF. Με βάση τις μοναδικές προκλήσεις ασφαλείας του SDN, η Ομάδα του ONF που είναι υπεύθυνη για την ασφάλεια, προτείνει ένα σύνολο βασικών αρχών ασφαλείας που παρέχουν τα κριτήρια και τις οδηγίες για το σχεδιασμό και την ανάπτυξη προδιαγραφών, σύμφωνα με τα οποία μπορεί να καθοριστεί υψηλό επίπεδο ασφαλείας στα συστήματα που χρησιμοποιούν την τεχνολογία SDN. Οι βασικές αρχές που θα παρουσιαστούν παρακάτω, ενδέχεται να καλύπτουν διαφορετικά ζητήματα ασφαλείας ανάλογα με το περιβάλλον, π.χ. περίπτωση στην οποία παρέχεται ασφάλεια σε ένα πρωτόκολλο SDN, ή περίπτωση που παρέχεται ασφάλεια σε ένα στοιχείο SDN ή σε μια διεπαφή SDN[15].

7.4.1. Βασική Αρχή 1: Καθορισμός εξαρτήσεων ασφαλείας και ορίων εμπιστοσύνης

Θα πρέπει να οριστούν με σαφήνεια, εξαρτήσεις ασφαλείας και τα όρια εμπιστοσύνης, σε ένα μηχανισμό ασφαλείας για ένα δίκτυο SDN. Οι κυκλικές εξαρτήσεις στα στοιχεία που απαρτίζουν το σύστημα SDN θα πρέπει να αποφεύγονται. Ο σαφής ορισμός των ορίων εμπιστοσύνης επιτρέπει στοχευμένη ανάλυση κινδύνου και αξιολόγηση ελέγχου ασφάλειας. Τα όρια εμπιστοσύνης θα πρέπει να καθορίζονται με βάση τους τομείς αλλαγής προνομίων, την ροή πληροφοριών μεταξύ τομέων και την εξάρτηση από δεδομένα όπου δεν μπορεί να επαληθευτεί η εμπιστευτικότητα και η ακεραιότητα.

Η διασύνδεση ενός δικτύου SDN, με συστήματα που ανήκουν σε εξωτερικά περιβάλλοντα, θα πρέπει να παρέχει επαρκή λειτουργικότητα ασφαλείας για την πρόληψη και την μείωση επιθέσεων προς το εσωτερικό περιβάλλον του συστήματος SDN που έχουν ξεκινήσει εξωτερικά. Τα εξωτερικά συστήματα θα πρέπει να έχουν περιορισμένη πρόσβαση μέσω μιας μεθόδου με ελάχιστο προνόμιο για τη μείωση του κινδύνου για το σύστημα.

7.4.2. Βασική Αρχή 2: Διασφάλιση ισχυρής ταυτότητας

Η βάση για την δημιουργία μιας αποτελεσματικής ασφάλειας σε ένα υπολογιστικό σύστημα, προϋποθέτει τον εντοπισμό και τον έλεγχο ασφαλείας των επιμέρους στοιχείων του συστήματος SDN, την αποτελεσματική δυνατότητα μοναδικής αναγνώρισης όλων των στοιχείων και των

χρηστών ενός συστήματος καθώς και την ασφαλή επαλήθευση ταυτότητας μιας αξιόπιστης πηγής. Χωρίς ένα ισχυρό πλαίσιο ταυτότητας, η δυνατότητα δημιουργίας αποτελεσματικών ελέγχων ταυτότητας, εξουσιοδότησης θα είναι περιορισμένη. Επομένως, ένα ισχυρό σύστημα ταυτοποίησης πρέπει να έχει τις ακόλουθες ιδιότητες:

- Δυνατότητα διάκρισης του κατόχου της από άλλες οντότητες εντός ενός προκαθορισμένου πεδίου.

- Δυνατότητα δημιουργίας, ενημέρωσης και ανάκλησης.

- Πρόληψη πλαστοπροσωπίας, μέσω ισχυρών κρυπτογραφικών μηχανισμών. Η ανάλυση της αρχιτεκτονικής SDN εντοπίζει πολλά μέσα για στοιχεία εντός του ορίου εμπιστοσύνης του συστήματος να θέσουν σε κίνδυνο τη διαθεσιμότητα του λογικά συγκεντρωτικού ελέγχου. Ο ισχυρός έλεγχος ταυτότητας που βασίζεται στην εγγυημένη ταυτότητα, είναι επομένως κρίσιμος για την ασφάλεια του συστήματος.

7.4.3. Βασική Αρχή 3: Δημιουργία ασφάλειας βάσει ανοιχτών προτύπων

Η χρήση ανοικτών προτύπων μπορεί να αποφέρει σημαντικά οφέλη τόσο στη φορητότητα όσο και στη διαλειτουργικότητα. Όπου είναι δυνατόν, πρέπει να εφαρμόζονται πιστοποιημένα πρωτόκολλα και πρακτικές που έχουν ελεγχθεί για την αποτελεσματικότητα της λειτουργίας τους. Συνεπώς, νέα πρωτόκολλα και νέοι αλγόριθμοι δημιουργούνται ως τελευταία λύση, όταν δεν μπορούν να ικανοποιηθούν οι υπάρχουσες απαιτήσεις. Για παράδειγμα, απαιτείται προστασία επιπέδου μεταφοράς για τη διασφάλιση του καναλιού επικοινωνίας OpenFlow τόσο για την κεφαλίδα κίνησης όσο και για το ωφέλιμο φορτίο Transmission Control Protocol (TCP).

7.4.4. Βασική Αρχή 4: Προστασία του «τριγώνου» Ασφάλειας Πληροφοριών

Το τρίγωνο ασφάλειας: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, θα πρέπει να διασφαλίζει ότι τυχόν νέοι έλεγχοι ασφαλείας, δεν θα επιφέρουν νέες ευπάθειες ή νέους κινδύνους επιθέσεων σε ένα σύστημα. Οποιαδήποτε μείωση της αποτελεσματικότητας των βασικών

στοιχείων του τριγώνου ασφάλειας, πρέπει να εξαλείφεται εγκαίρως. Για παράδειγμα, η εισαγωγή ενός κεντρικού διακομιστή ασφαλείας στην αρχιτεκτονική SDN πρέπει να αξιολογηθεί προσεκτικά σε περίπτωση που η πιθανή ευπάθεια του διακομιστή σε επιθέσεις άρνησης υπηρεσίας (DoS) ενδέχεται να επηρεάσει τη διαθεσιμότητα του συστήματος.

7.4.5. Βασική Αρχή 5: Προστασία δεδομένων αναφοράς λειτουργίας

Η αποτελεσματικότητα ενός ελέγχου ασφαλείας επηρεάζεται άμεσα από την ακεραιότητα των δεδομένων αναφοράς (π.χ. διαπιστευτήρια και αριθμούς ακολουθίας), η οποία αποτελεί βασική απαίτηση για τη λήψη επιχειρησιακών αποφάσεων. Οι λανθασμένες πληροφορίες μπορεί να οδηγήσουν σε απροσδόκητη συμπεριφορά συστήματος που μπορεί να οδηγήσει σε απώλεια εμπιστευτικότητας, ακεραιότητας ή/και διαθεσιμότητας. Επιπλέον, η διαρροή ορισμένων ευαίσθητων δεδομένων αναφοράς, όπως τα κρυπτογραφικά κλειδιά, θα προκαλέσει πιθανές παραβιάσεις του ελέγχου ασφαλείας. Τα επιχειρησιακά δεδομένα αναφοράς για όλους τους ελέγχους ασφαλείας πρέπει να ορίζονται σαφώς και να προστατεύονται σε επίπεδο συνοχής σύμφωνα με την πολιτική ασφάλειας και τις παραδοχές της αρχιτεκτονικής ασφαλείας.

7.4.6. Βασική Αρχή 6: Ελάχιστο επίπεδο ασφάλειας

Οι έλεγχοι ασφαλείας θα πρέπει να παρέχουν πολλαπλά επίπεδα ασφαλείας για να ικανοποιούν τις απαιτήσεις όλων των πιθανών περιπτώσεων χρήσης του συστήματος. Αυτά τα επίπεδα μπορεί να διαφέρουν από κατάσταση κατά την οποία ένα στοιχείο ελέγχου είναι απενεργοποιημένο σε κατάσταση που μπορεί να ικανοποιεί τις πιο αυστηρές απαιτήσεις ασφαλείας (π.χ. απόρριψη από προεπιλογή). Ανεξάρτητα από την προβλεπόμενη περίπτωση χρήσης, το σύστημα πρέπει να καθορίσει ένα ελάχιστο επίπεδο στο οποίο τα περισσότερα στοιχεία ελέγχου πρωτεύουσας ασφάλειας είναι ενεργοποιημένα από προεπιλογή. Εκτός από την ενεργοποίηση, αυτά τα στοιχεία ελέγχου πρέπει να διαμορφωθούν με τρόπο που να πληροί τα ελάχιστα κριτήρια για να διασφαλιστεί ότι το στοιχείο ελέγχου είναι αποτελεσματικό.

7.4.7. Βασική Αρχή 7: Παροχή λογοδοσίας και ιχνηλασιμότητας

Όλοι οι έλεγχοι ασφαλείας πρέπει να είναι ελεγχόμενοι για την κατάσταση και τις ενέργειες που είναι κρίσιμες για την ασφάλεια του συστήματος. Τα καταγεγραμμένα δεδομένα πρέπει να περιέχουν επαρκείς πληροφορίες για τους διαφόρους ελέγχους του διαχειριστή του συστήματος.

7.4.8. Βασική Αρχή 8: Ιδιότητες ελεγχόμενων ελέγχων ασφαλείας

Εκτός από τις επτά αρχές που περιγράφηκαν παραπάνω, κατά την εισαγωγή νέων στοιχείων ελέγχου σε μια αρχιτεκτονική ή ένα πρότυπο, πρέπει να λαμβάνονται υπόψη οι ακόλουθες ιδιότητες του ελέγχου:

- Πριν από το σχεδιασμό ή την εισαγωγή ενός ελέγχου ασφαλείας, το οι στόχοι και οι υποθέσεις ασφαλείας πρέπει να αποσαφηνιστούν.

- Οι έλεγχοι ασφαλείας πρέπει να δημιουργούνται με τέτοιο τρόπο, ώστε να μπορούν να είναι επεκτάσιμοι και να υποστηρίζουν εγκαταστάσεις συστημάτων μικρού μεγέθους, αλλά και μεγάλες εγκαταστάσεις, χωρίς όμως να δημιουργείται περιττή πολυπλοκότητα.

- Κατά την εισαγωγή νέων ελέγχων, θα πρέπει να εξεταστεί ο αντίκτυπος της εφαρμογής της λύσης και της διαχείρισης του κύκλου ζωής. Οι νέες λειτουργίες ασφαλείας θα πρέπει να εισάγουν ελάχιστη πολυπλοκότητα στην εφαρμογή. Μια καλή εφαρμογή πρέπει να είναι επεκτάσιμη, ώστε να μπορούν να εισαχθούν στο μέλλον πρόσθετες λειτουργίες ελέγχου ασφάλειας.

- Οι έλεγχοι ασφαλείας πρέπει να είναι εύκολο να εφαρμοστούν, να συντηρηθούν και να λειτουργήσουν.

- Θα πρέπει να διασφαλίζεται ότι τα στοιχεία ελέγχου είναι πλήρως τεκμηριωμένα και βασίζονται σε καθορισμένα πρότυπα.

- Θα πρέπει πάντα να είναι δυνατή η ανάκληση και τροποποίηση διαπιστευτηρίων ασφαλείας ως μέρος του κύκλου ζωής ενός συστήματος.

- Τέλος, η ικανότητα παρακολούθησης, αντιμετώπισης προβλημάτων και εντοπισμού σφαλμάτων οποιουδήποτε συστήματος είναι θεμελιώδης για την επιτυχή υιοθέτηση του.

Κεφάλαιο 8
Επίλογος

8.1 Σύνοψη

Δεν υπάρχει αμφιβολία ότι το SDN αποτελεί μια επαναστατική καινοτομία στον τομέα της δικτύωσης, αφού υπόσχεται να μετατρέψει τα σημερινά στατικά δίκτυα σε ευέλικτες, επεκτάσιμες και προγραμματίσιμες πλατφόρμες.

Σε αυτή τη διατριβή, παρουσιάσαμε μια ευρεία ανασκόπηση του ερευνητικού έργου σχετικά με την ασφάλεια στα SDN δίκτυα μέχρι σήμερα και αναφερθήκαμε στις βασικότερες εφαρμογές αλλά και στις υπάρχουσες λύσεις που έχουν προταθεί για ενίσχυση της ασφάλειας. Μέσα από το πειραματικό στάδιο, αναδείξαμε την καλύτερη συμπεριφορά τους απέναντι στα παραδοσιακά, αφού χάρις στις διάφορες πολιτικές αντιστάθμισης και ρύθμισης που έχουν, μπορούν να αναχαιτίσουν αποτελεσματικά διάφορες κακόβουλες επιθέσεις.

Πέραν των τεράστιων δυνατοτήτων και πλεονεκτημάτων τους, τα SDN δίκτυα αντιμετωπίζουν διάφορες προκλήσεις με αποτέλεσμα πολλές φορές να τίθενται εκτεθειμένα σε διάφορες επιθέσεις. Είναι σημαντικό να αξιοποιηθεί στο μεγαλύτερο δυνατό βαθμό η μεγάλη προγραμματιστική τους δυνατότητα αλλά και η κεντρική τους διαχείριση, αφού θα οδηγήσει στην ανάπτυξη αποτελεσματικότερων μηχανισμών ασφάλειας, περιορίζοντας την ανάπτυξη απειλών στον ελάχιστο δυνατό βαθμό. Οι οδηγίες του ONF μπορούν να αποτελέσουν ένα πολύτιμο εγχειρίδιο στην ανάπτυξη ασφαλών SDN δικτύων, τα οποία αναμφίβολα θα αποτελέσουν πολύ σύντομα το μέλλον της δικτύωσης.

8.2 Μελλοντική Εργασία

Από την άποψη της μελλοντικής έρευνας, διανοίγονται προοπτικές σε πολλά επίπεδα. Ειδικότερα, προτείνεται η μελέτη διαφορετικών τύπων επιθέσεων, που στοχεύουν σε διαφορετικά σημεία SDN και παραδοσιακών δικτύων, με σκοπό την ανακάλυψη τυχών ευπαθειών και συγκριτικών πλεονεκτημάτων των SDN δικτύων. Επίσης, προτείνεται να μελετηθούν διάφορες ευπάθειες σε θέματα ασφάλειας που αντιμετωπίζουν οι ελεγκτές, και να αναπτυχθούν εφαρμογές που θα αντιμετωπίζουν αποτελεσματικά τυχόν επιθέσεις.

Βιβλιογραφία

[01] Alsmadi, I, Xu, D.,(2015), "Security of Software Defined Networks: A survey", Computers and Security, 53, 79-108

[02] Bansal M, J. Mehlman, S. Katti, P. Levis(2012). OpenRadio: A Programmable Wireless Dataplane. In Proceedings of ACM HotSDN..

[03] Braun W.,Menth, M. (2014), "Software-defined networking using OpenFlow: Protocols, applications and architectural design choices", Future Internet, 6(2), 302-336.

[04] Brocade (2015). Software-Defined Networking in the Campus Network. Available at: http://www.aikcu.org/wp-content/uploads/2015/07/Software-Defined-Networking-SDN-in-the-Campus-Network.pdf

[05] M.Canini, D.Venzano, P.Peresini, D.Kostic, and J.Rexford (2012). A NICE way to test OpenFlow applications," in Proc. 9th USENIX Conf. Networked Systems Designand Implementation (NSDI)

[06] Ding, Aaron Yi & Crowcroft, Jon & Tarkoma, Sasu & Flinck, Hannu. (2014). Software defined networking for security enhancement in wireless mobile networks. Computer Networks. 66. 94–101. 10.1016

[07] Feamster, N., Rexford, J., and Zegura, E. (2014), "The road to SDN: An intellectual history of programmable networks", ACM SIGCOMM Computer Communication Review, 44 (2), 87-98.

[08] Hizver J. (2015). Taxonomic Modelling of Security Threats in Software Defined Networking', BlackHat Conference, pp. 1-16.

[09] Hu, Z., Wang, M. Yan, X., Yin, Y., and Luo, Z.,(2015),"A Comprehensive Security Architecture for SDN", *18th International Conference on Intelligence in Next Generation Networks, 30-37*

[10] Jin, L. E. Li, L. Vanbever, J. Rexford (2013). SoftCell: Scalable and Flexible Cellular Core Network Architecture. In Proceedings of ACM CoNEXT

[11] Li, P. Li, S. Guo, and S. Yu (2014). Byzantine-resilient secure software defined networks with multiple controllers, in Communications (ICC), 2014 IEEE International Conference on. IEEE, 2014, pp. 695–700

[12] Li L.E. , Z. M. Mao, J. Rexford(2012). Toward Software-Defined Cellular Networks. In Proceedings of IEEE EWSDN

[13] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in Recent Advances in Intrusion Detection. Springer, 2011, pp. 161-180

[14] N.D. Neykov(2017), Real-time detection and mitigation of flood attacks in SDN networks

[15] ONF(2015). Open Network Foundation, Principles and Practices for Securing Software-Defined Networks. Available at: https://www.opennetworking.org/wp-content/uploads/2014/10/Principles and Practices for Securing Software-Defined Networks applied to OFv1.3.4 V1.0.pdf

[16] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for OpenFlow networks," inProc.1st ACM Workshop Hot Topics in Software Defined Networks (HotSDN), 2012, pp. 121–126

[17] Pradeep Kumar Sharma, S. S. Tyagi (2019). Improving Security through Software Defined. Networking (SDN): AN SDN based Model, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4

[18] S. Singh, R. A. Khan, A. Agrawal,(2015)."Prevention mechanism for infrastructure based Denial-of-Service attack over software Defined Network," International Conference on Computing, Communication & Automation, Noida, pp. 348-353.

[19] Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, T. Vazao(2014). Towards Programmable Enterprise WLANs with Odin. In Proceedings of ACM Hot SDN.

[20] Sivaraman, T. Moors, H. H. Gharakheili, D. Ong, J. Matthews, C. Russell (2013). Virtualizing the Access Network via Open APIs. In Proceedings of ACM CoNEXT..

[21] Schehlmann, S. Abt and H. Baier(2014). Blessing or curse? Revisiting security aspects of Software-Defined Networking', International Conference on Network and Service Management (CNSM), pp. 382- 387.

[22] Seungwon, Shin & Xu, Lei & Hong, Sungmin & Gu, Guofei. (2016). Enhancing Network Security through Software Defined Networking (SDN). 10.1109/ICCCN.2016.7568520.

[23] Spooner, Jakob & Shao, Dr. (2016). A Review of Solutions for SDN-Exclusive Security Issues. International Journal of Advanced Computer Science and Applications. 7. 10.14569/IJACSA.2016.070817.

[24] Wang, Y. Zhang, V. Singh, C. Lumezanu, G. Jiang(2016). NetFuse: Shortcircuiting Traffic Surges in the Cloud. In Proceedings of IEEE ICC

[25] Yap, et al.(2010). Blueprint for Introducing Innovation into Wireless Mobile Networks. In Proceedings of ACM VISA