Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Investigating the effectiveness of IDS/IPS system in enhancing resilience of ONOS controller against TCP SYN flood DDoS attacks

Στέλιος Αγαπίου

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Μάιος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Investigating the effectiveness of IDS/IPS system in enhancing resilience of ONOS controller against TCP SYN flood DDoS attacks

Στέλιος Αγαπίου

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 2023

Περίληψη

Η δικτύωση που καθορίζεται από το λογισμικό (SDN) αποτελεί μια νέα προσέγγιση στην αρχιτεκτονική των δικτύων διαχωρίζοντας το επίπεδο ελέγχου από το επίπεδο δεδομένων. Ο διαχωρισμός αυτός επιτρέπει μέσω ενός ελεγκτή, που βασίζεται σε λογισμικό, τον πλήρη έλεγχο του δικτύου καθιστώντας ευκολότερη τη διαχείριση και την αυτοματοποίηση των λειτουργιών του. Ωστόσο, η οποιαδήποτε αποτυχία του ελεγκτή μπορεί να προκαλέσει την αστοχία ολόκληρου του δικτύου, καθιστώντας τον το θεμελιώδες σημείο αποτυχίας. Ο τομέας που προκαλεί την μεγαλύτερη ανησυχία όσον αφορά τη διασφάλιση της ανθεκτικότητας των δικτύων SDN είναι οι κατανεμημένες επιθέσεις άρνησης (DDoS). Οι επιθέσεις πλημμύρας TCP SYN είναι ένας τύπος επίθεσης DDoS που εκμεταλλεύεται το μηχανισμό three-way handshake που χρησιμοποιείται από το πρωτόκολλο TCP για τη δημιουργία συνδέσεων. Οι επιθέσεις αυτές έχουν ως στόχο να καταναλώσουν τους πόρους του δικτύου κατακλύζοντας το με μεγάλο όγκο κίνησης, καθιστώντας δύσκολο για τον ελεγκτή να ανταποκριθεί στις νόμιμες αιτήσεις του δικτύου.

Σκοπός της παρούσας μεταπτυχιακή διατριβής είναι να εξετάσουμε κατά πόσο τα δίκτυα SDN μπορούν να προσφέρουν την απαιτούμενη ανθεκτικότητα σε επιθέσεις τύπου DDoS αλλά και να μετρήσουμε ποσοτικά τον αντίκτυπο που έχουν οι επιθέσεις αυτές. Για το σκοπό αυτό εκτελέσαμε επιθέσεις πλημμύρας (κεφάλαιο 4) στον ελεγκτή ONOS και καταγράψαμε το χρόνο απόκρισης του δικτύου, το φορτίου του ελεγκτή, το εύρος ζώνης του δικτύου και το εύρος ζώνης του διακομιστή ιστού. Η εκτέλεση περιλάμβανε 4 σενάρια: α) μετρήσεις χωρίς την προσομοίωση επίθεση DDoS, β) μετρήσεις κατά τη διάρκεια προσομοίωσης επίθεσης DDoS, γ) μετρήσεις κατά τη διάρκεια προσομοίωσης επίθεσης DDoS αλλά με ταυτόχρονη λειτουργία συστήματος IDS/IPS, και δ) μετρήσεις κατά τη διάρκεια προσομοίωσης επίθεσης DDoS διαφορετικής ισχύς με ταυτόχρονη λειτουργία συστήματος IDS/IPS. Παρουσιάζουμε αναλυτικά τα αποτελέσματα των ελέγχων στο κεφάλαιο 5 και προτείνουμε τον κατάλληλο σχεδιασμό (κεφάλαιο 6) έτσι ώστε τα δίκτυα SDN να καταστούν ανθεκτικά και αξιόπιστα σε επιθέσεις τύπου DDoS, υποστηρίζοντας τις ανάγκες των σύγχρονων δικτυακών περιβαλλόντων.

Λέξεις κλειδιά: SDN, OpenFlow, ONOS Controller, DDoS, TCP SYN attack, IDS/IPS

Summary

The networking that is defined by software (SDN) is a new approach to network architecture that separates the control plane from the data plane. This separation allows for full control of the network through a software-based controller, making it easier to manage and automate its functions. However, any failure of the controller can cause the entire network to fail, making it the single point of failure.

The area that causes the greatest concern regarding the resilience of SDN networks is distributed denial-of-service (DDoS) attacks. TCP SYN flood attacks are a type of DDoS attack that exploits the three-way handshake mechanism used by the TCP protocol to establish connections. These attacks aim to consume network resources by flooding it with a large volume of traffic, making it difficult for the controller to respond to legitimate network requests.

The purpose of this thesis is to examine whether software-based networks can offer the required resilience to DDoS attacks and to quantify the impact that such attacks have. We conducted flood attacks (chapter 4) on the ONOS controller and recorded the network response time, controller load, network bandwidth and web server bandwidth. The execution included 4 scenarios: a) measurements without the simulated DDoS attack, b) measurements during the simulated DDoS attack, c) measurements during the simulated DDoS attack but with simultaneous IDS/IPS system operation, and d) measurements during simulated DDoS attack of different strength with simultaneous IDS/IPS system operation. We present the detailed results of the tests in Chapter 5 and propose the appropriate design (Chapter 6) so that SDN networks can become resilient and reliable to DDoS attacks, supporting the needs of modern network environments.

Based on these results, we conclude that software-based networks are particularly vulnerable to DDoS attacks and that additional measures must be taken to ensure their resilience. These measures could include implementing distributed control planes and utilizing anomaly detection systems to identify and mitigate attacks in real-time.

Keyword: SDN, OpenFlow, ONOS Controller, DDoS, TCP SYN attack, IDS/IPS

Ευχαριστίες

Για την εκπόνηση της μεταπτυχιακής διατριβής θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στην επιβλέπουσα καθηγήτρια μου κα. Αδαμαντίνη Περατικού για την καθοδήγηση, την στήριξη και τον πολύτιμο χρόνο που μου έχει αφιερώσει κατά τη διάρκεια αυτής της διαδικασίας.

Επίσης, θα ήθελα εκφράσω την ευγνωμοσύνη μου στην οικογένεια μου για την αμέριστη συμπαράσταση, την υπομονή και την κατανόηση τους καθ' όλη τη διάρκεια αυτού του ταξιδιού.

Αφιέρωση

στον πατέρα μου

και στο γιο μου

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η δικτύωση που καθορίζεται από το λογισμικό (Software Defined Networking - SDN) έχει εξελιχθεί ως μια πρωτοποριακή προσέγγιση στη δικτύωση, προσφέροντας κεντρική διαχείριση, ευέλικτη δυνατότητα προγραμματισμού και βελτιωμένο αυτοματισμό των δικτύων. Ωστόσο, η αυξανόμενη πολυπλοκότητα και η ποικιλομορφία των απειλών δικτύου, ειδικά των επιθέσεων κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service - DDoS), προσφέρουν μια ουσιαστική πρόκληση για την ανθεκτικότητα των δικτύων SDN. Ως αποτέλεσμα, υπάρχει η αυξανόμενη ανάγκη σχεδιασμού ανθεκτικών δικτύων SDN που θα έχουν τη δυνατότητα να μπορούν να ανιχνεύσουν, να αποτρέψουν και να ελαχιστοποιήσουν αποτελεσματικά τον αντίκτυπο των επιθέσεων DDoS προσφέροντας τις υπηρεσίες δικτύου στους τελικούς χρήστες.

1.1 Αναγκαιότητα για έρευνα

Η αυξανόμενη συχνότητα, η ισχύς και η πολυπλοκότητα των επιθέσεων DDoS, σε συνδυασμό με την αδυναμία των συστημάτων δικτύωσης SDN να αποτρέψουν τις επιθέσεις, αποτελούν σημαντική απειλή για την αξιοπιστία και την ασφάλεια των κρίσιμων υπηρεσιών δικτύου. Ως εκ τούτου, υπάρχει επιτακτική η ανάγκη οι ερευνητές να επικεντρωθούν στην ανάπτυξη και την

εφαρμογή ανθεκτικών λύσεων που θα μπορούν να ανιχνεύσουν και να μετριάσουν τον αντίκτυπο των επιθέσεων DDoS στα δίκτυα SDN.

Αυτό απαιτεί εκτεταμένη έρευνα για τον εντοπισμό των ειδικών χαρακτηριστικών των επιθέσεων DDoS που στοχεύουν σε δίκτυα SDN, την κατανόηση του τρόπου με τον οποίο επηρεάζονται τα επίπεδα ελέγχου και δεδομένων και την ανάπτυξη μηχανισμών ανίχνευσης και μετριασμού που θα μπορούν να αποτρέψουν ή να ελαχιστοποιήσουν τον αντίκτυπο αυτών των επιθέσεων. Με την αναποτελεσματικότητα των παραδοσιακών μηχανισμών ασφαλείας, όπως τα τείχη προστασίας (firewalls), οι γρήγοροι και αποτελεσματικοί μηχανισμοί ανίχνευσης έχουν γίνει ένα κρίσιμο στοιχείο για την εφαρμογή μιας αποτελεσματικής άμυνας DDoS. Τα κριτήρια επιτυχίας για την εξάλειψη μιας απειλής στο συντομότερο χρονικό διάστημα είναι η ταχύτητα και η ακρίβεια της ανίχνευσης.

1.2 Δομή της μεταπτυχιακής διατριβής

Στο κεφάλαιο 2 καταγράφουμε μέσα από τη βιβλιογραφική ανασκόπηση την αρχιτεκτονική των δικτύων SDN και τη βασική τους διαφορά με τα παραδοσιακά δίκτυα εστιάζοντας επίσης στα οφέλη που προσφέρει, συμπεριλαμβανομένης της κεντρικής διαχείρισης και ελέγχου, του προγραμματισμού και της βελτιωμένης ευελιξίας του δικτύου. Ακολούθως, παρουσιάζουμε το πρωτόκολλο OpenFlow, το οποίο αποτελεί αναπόσπαστο μέρος της αρχιτεκτονικής SDN. Τέλος, επισημάνουμε τις προκλήσεις σε θέματα ανθεκτικότητας των δικτύων που βασίζονται στην τεχνολογία SDN.

Στο κεφάλαιο 3 καταγράφουμε το σκοπό, το είδος της έρευνας αλλά και τη μεθοδολογία που ακολουθείτε για τον έλεγχο της ανθεκτικότητας του ελεγκτή ONOS σε επιθέσεις πλημμύρας TCP SYN. Τέλος, παρουσιάζουμε τη μεθοδολογίας κύκλου ζωής ανάπτυξης λογισμικού που έχουμε επιλέξει για τον έλεγχο της ανθεκτικότητας των δικτύων SDN.

Στο κεφάλαιο 4 παρουσιάζουμε τα βήματα που ακολουθήθηκαν για τη διαμόρφωση των εικονικών μηχανών (Virtual Machines - VMs) όπως επίσης και της τοπολογία του δικτύου που χρησιμοποιείται. Εκτελούμε τη προσομοίωση επίθεσης πλημμύρας TCP SYN για τον έλεγχο της ανθεκτικότητας του δικτύου SDN και καταγράφουμε το χρόνο απόκρισης του δικτύου, το φορτίου του ελεγκτή, το εύρος ζώνης του δικτύου και το εύρος ζώνης του διακομιστή ιστού για 4 διαφορετικά σενάρια, α) χωρίς επίθεση DDoS, β) με επίθεση DDoS, γ) με επίθεση DDoS αλλά με

ταυτόχρονη λειτουργία του συστήματος IDS/IPS και τέλος δ) με επίθεση DDoS διαφορετικής ισχύς αλλά με ταυτόχρονη λειτουργία του συστήματος IDS/IPS. Στο κεφάλαιο παρουσιάζονται επίσης τα εργαλεία που χρησιμοποιήθηκαν για την εκτέλεση της επίθεσης πλημμύρας TCP SYN, συμπεριλαμβανομένου του hping3.

Στο κεφάλαιο 5 συγκρίνουμε τις επιπτώσεις της επίθεσης πλημμύρας TCP SYN στον ελεγκτή ONOS με βάση τα αποτελέσματα των μετρήσεων. Το κεφάλαιο παρέχει λεπτομερή ανάλυση των αποτελεσμάτων της επίθεσης DDoS στον ελεγκτή ONOS, συμπεριλαμβανομένου του χρόνου απόκρισης, του φορτίου του ελεγκτή, το εύρος ζώνης του δικτύου και το εύρος ζώνης του διακομιστή ιστού.

Το κεφάλαιο 6 κλείνει με συζήτηση για τις επιπτώσεις των επιθέσεων DDoS στα δίκτυα SDN, τη μελλοντική έρευνα σχετικά με την ανθεκτικότητα των δικτύων SDN και τις δυνατότητες μετριασμού των επιπτώσεων σε επιθέσεις DDoS.

Κεφάλαιο 2
Βιβλιογραφική Επισκόπηση

Στο κεφάλαιο αυτό παρουσιάζουμε μέρος από τις πιο σημαντικές μελέτες και έρευνες που έχουν γίνει τα τελευταία χρόνια και σχετίζονται με θέματα που αφορούν την ανθεκτικότητα των δικτύων που βασίζονται στην τεχνολογία SDN. Η παρουσίαση περιλαμβάνει την περιγραφή των παραδοσιακών δικτύων, βασικές λειτουργίες δρομολογητή, αλγόριθμοι δρομολόγησης, περιγραφή της τεχνολογίας και της αρχιτεκτονικής SDN, τη σύγκριση με τα παραδοσιακά δίκτυα, το ρόλο του SDN στην εποχή του υπολογιστικού νέφους (cloud computing) αλλά και τις ανησυχίες που υπάρχουν σε θέματα που αφορούν την ασφάλεια και την ανθεκτικότητα των δικτύων.

2.1 Παραδοσιακά δίκτυα

Τα παραδοσιακά δίκτυα χωρίζονται σε τρία επίπεδα λειτουργικότητας: α) το επίπεδο δεδομένων, β) το επίπεδο ελέγχου και γ) το επίπεδο διαχείρισης. Το επίπεδο δεδομένων αντιστοιχεί στις συσκευές δικτύωσης. Το επίπεδο ελέγχου αντιπροσωπεύει τα πρωτόκολλα που χρησιμοποιούνται για τη συμπλήρωση των πινάκων προώθησης των στοιχείων του επιπέδου δεδομένων. Και τέλος, το επίπεδο διαχείρισης περιλαμβάνει τις υπηρεσίες λογισμικού, όπως εργαλεία βασισμένα στο πρωτόκολλο διαχείρισης δικτύου (Simple Network Management Protocol - SNMP), που χρησιμοποιούνται για την απομακρυσμένη παρακολούθηση και

διαμόρφωση. Η πολιτική δικτύου ορίζεται στο επίπεδο διαχείρισης, το επίπεδο ελέγχου επιβάλλει την πολιτική και το επίπεδο δεδομένων την εκτελεί προωθώντας τα δεδομένα ανάλογα.

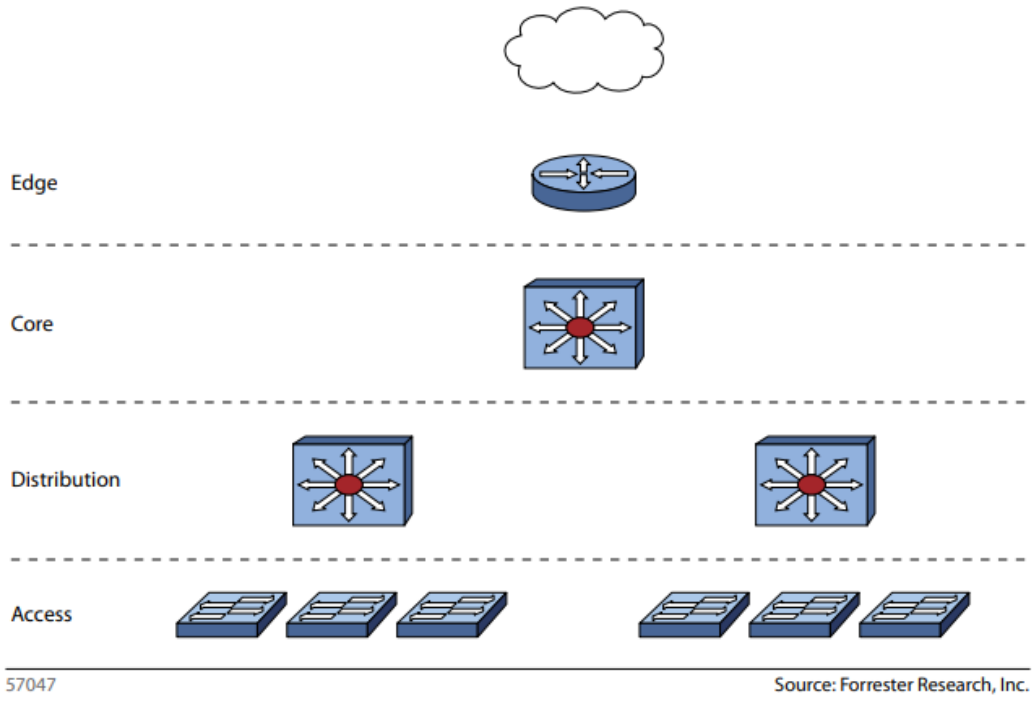
Οι παραδοσιακές λειτουργίες δικτύωσης υλοποιούνται σε αποκλειστικό υλικό, όπως ολοκληρωμένα κυκλώματα για συγκεκριμένες εφαρμογές (Application Specific Integrated Circuit - ASIC). Στα παραδοσιακά δίκτυα, τα επίπεδα ελέγχου και δεδομένων είναι ενσωματωμένα στις ίδιες τις συσκευές δικτύωσης και ολόκληρη η δομή είναι εξαιρετικά αποκεντρωμένη. Η διαδικασία δημιουργίας της τοπολογίας του δικτύου χρησιμοποιώντας ένα επίπεδο ελέγχου που εκτελείται τοπικά είναι πολύπλοκη. Αυτή η πολυπλοκότητα προκύπτει από το γεγονός ότι καμία συσκευή δεν γνωρίζει ολόκληρη την τοπολογία του δικτύου με συνέπεια η διαχείριση και η διαμόρφωση τους να γίνεται μεμονωμένα κάτι που δεν αποτελεί αποτελεσματική προσέγγιση. Το επίπεδο ελέγχου είναι υπεύθυνο για τη διαμόρφωση του κόμβου και το προγραμματισμό των διαδρομών που θα χρησιμοποιηθούν για τις ροές των δεδομένων. Μόλις καθοριστούν αυτές οι διαδρομές, ωθούνται προς τα κάτω στο επίπεδο δεδομένων. Η προώθηση των δεδομένων σε επίπεδο υλικού βασίζεται στις πληροφορίες ελέγχου. Στην παραδοσιακή δικτύωση, αφού οριστεί η διαχείριση ροής (πολιτική προώθησης), ο μόνος τρόπος για να γίνει μια προσαρμογή στην πολιτική είναι μέσω αλλαγών στη διαμόρφωση των συσκευών. Ωστόσο, η αποκεντρωμένη διαμόρφωση των συσκευών είναι επιρρεπής σε σφάλματα, καθώς αυξάνει την πιθανότητα να γίνουν λάθη. Ο σχεδιασμός αυτός θεωρήθηκε ως ο καλύτερος τρόπος για να εγγυηθεί την ανθεκτικότητα των παραδοσιακών δικτύων. Αυτή η προσέγγιση, με βάση την μελέτη των (Kreutz et al., 2015), ήταν αρκετά αποτελεσματική όσον αφορά την απόδοση των δικτύων, ωστόσο, είχε ως αποτέλεσμα μια περίπλοκη και στατική αρχιτεκτονική.

Οι (Kindervag, 2010) στο άρθρο τους αναλύουν την αρχιτεκτονική των παραδοσιακών δικτύων, αναφέροντας την ως "Three Tiered Network Architecture", τονίζοντας ότι αποτελεί ένα απαρχαιωμένο και ανασφαλές μοντέλο στο οποίο το επίπεδο ασφάλειας είτε το υποβάθμισαν είτε το απέρριψαν κατά το σχεδιασμό τους οι υπεύθυνοι των δικτύων. Τα στοιχεία (εικόνα 1) που βρίσκονται στα περισσότερα παραδοσιακά δίκτυα έχουν σχεδιαστεί έτσι ώστε:

1. Ο πυρήνας (core) αποτελεί τη ραχοκοκαλιά (backbone) του δικτύου και συνδέει το εταιρικό δίκτυο (enterprise network) με το διαδίκτυο (internet) συγκεντρώνοντας όλη την κυκλοφορία του δικτύου σε μια ενιαία υποδομή μεταγωγέα υψηλής ταχύτητας (high-speed) και χαμηλής καθυστέρησης (low latency).

2. Το επίπεδο διανομής (distribution layer) παρέχει τη συνδεσιμότητα προωθώντας τα πακέτα σε πολλαπλούς μεταγωγείς επιπέδου διανομής (distribution layer switch) και επιβάλλει την ανάλογη πολιτική προώθησης λειτουργώντας ως γέφυρα επικοινωνίας μεταξύ του επιπέδου πρόσβασης και του επιπέδου πυρήνα. Είναι υπεύθυνο για τη δρομολόγηση και την προώθηση της κυκλοφορίας μεταξύ διαφορετικών εικονικών τοπικών δικτύων (Virtual Local Area Network - VLAN), την εφαρμογή πολιτικών ποιότητας υπηρεσιών (Quality of Service - QoS) και την παροχή πλεονασμού (redundancy) και εξισορρόπησης φορτίου (load balancing).

3. Και τέλος, το επίπεδο πρόσβασης (access layer) συνδέει τους χρήστες απευθείας σε έναν μεταγωγέα επιπέδου πρόσβασης (access layer switch) προκειμένου να έχουν πρόσβαση σε εγκεκριμένους πόρους του δικτύου.



Εικόνα 1: Αρχιτεκτονική παραδοσιακών δικτύων (Πηγή: (Kindervag, 2010))

2.1.1 Βασικές λειτουργίες δρομολογητή

Ένας δρομολογητής εκτελεί δύο βασικές εργασίες: α) τη δρομολόγηση (routing) και β) την προώθηση (forwarding) των πακέτων. Οι παράμετροι υπολογισμού της διαδρομή μεταξύ του κόμβου πηγής (source host) και του προορισμού (destination) ποικίλλουν ανάλογα με τον αλγόριθμο που χρησιμοποιείται και μπορεί να σχετίζονται με τη χρήση του εύρους ζώνης

(bandwidth), τη χρονική καθυστέρηση (delay), τον αριθμό των ενδιάμεσων δρομολογητών του δικτύου (hops count), τη συμφόρηση στο δίκτυο (network congestion) ή το συνδυασμό αυτών. Το απλούστερο κριτήριο απόδοσης υπολογισμού είναι το hop count, η τιμή του οποίου βασίζεται στον αριθμό των ενδιάμεσων κόμβων που διασχίζει το πακέτο. Ωστόσο, ο αριθμός των hops αποτελεί ένα αποτελεσματικό κριτήριο απόδοσης εάν οι συνδέσεις είναι παρόμοιες ως προς το εύρος ζώνης.

Οι αλγόριθμοι δρομολόγησης σχεδιάστηκαν με βάση την προσέγγιση του ελάχιστου κόστους και οι παράμετροι κοστολόγησης ποικίλλουν ανάλογα με τον αλγόριθμο ή τις παραμέτρους του δικτύου. Οι αποφάσεις στη δρομολόγηση των δεδομένων μπορούν να διαφοροποιηθούν με βάση το χρόνο λήψης της απόφασης. Η απόφαση δρομολόγησης μπορεί να ληφθεί πριν από την έναρξη της μεταφοράς των δεδομένων μεταξύ των κόμβων ή κατά τη διάρκεια της μεταφοράς των δεδομένων. Στην περίπτωση ενός δικτύου datagram όπου λαμβάνει χώρα η μεταγωγή πακέτων, η απόφαση δρομολόγησης λαμβάνεται σε όλη τη διαδρομή στην οποία το πακέτο βρίσκεται σε μεταφορά, καθώς κάθε κόμβος αποφασίζει για τη δρομολόγηση του πακέτου στον επόμενο κόμβο hop.

Η πιο συχνά χρησιμοποιούμενη, αλλά σχετικά πολύπλοκη, στρατηγική είναι η κατανεμημένη λήψη αποφάσεων, όπου κάθε ενδιάμεσος κόμβος αποφασίζει για την επόμενη σύνδεση στην οποία θα προωθήσει το πακέτο. Κάθε κόμβος λήψης αποφάσεων πρέπει να έχει πλήρεις ή μερικές πληροφορίες για το δίκτυο. Η αποτυχία μερικών ενδιάμεσων κόμβων δεν επηρεάζει δραστικά την απόδοση του δικτύου, καθώς το πακέτο προωθείται μέσω κάποιας εναλλακτικής διαδρομής. Μια εναλλακτική λύση σε αυτό είναι η κεντρική απόφαση δρομολόγησης, στην οποία υπάρχει ένας κεντρικός κόμβος ελέγχου που λαμβάνει όλες τις αποφάσεις δρομολόγησης. Ο κόμβος ελέγχου έχει προβολή ολόκληρης της τοπολογίας του δικτύου και ελέγχει τη δρομολόγηση του πακέτου μέσω του δικτύου. Το μειονέκτημα ενός τέτοιου σχεδιασμού είναι η αποτυχία της δρομολόγησης του πακέτου σε περίπτωση αστοχίας του κόμβου ελέγχου.

2.1.2 Αλγόριθμοι δρομολόγησης

Ο αλγόριθμος δρομολόγησης καθορίζει τα περιεχόμενα των πινάκων προώθησης (forwarding tables) ενός δρομολογητή. Ο αλγόριθμος δρομολόγησης εκτελείται σε κάθε δρομολογητή και οι συναρτήσεις προώθησης και δρομολόγησης περιέχονται σε έναν δρομολογητή. Η συνάρτηση του αλγορίθμου δρομολόγησης ενός δρομολογητή επικοινωνεί με τις συναρτήσεις αλγορίθμων δρομολόγησης των άλλων δρομολογητών για να υπολογιστούν οι τιμές του πίνακα προώθησης.

Η επικοινωνία μεταξύ των δρομολογητών επιτυγχάνεται με την ανταλλαγή μηνυμάτων δρομολόγησης που περιέχουν πληροφορίες δρομολόγησης σύμφωνα με το πρωτόκολλο δρομολόγησης.

Με βάση τις πληροφορίες που ανταλλάσσουν μεταξύ τους οι γειτονικοί δρομολογητές, χρησιμοποιώντας τα πρωτόκολλα δρομολόγησης (routing protocols), δημιουργούν την τοπολογία του δικτύου. Οι καλύτερες διαδρομές (best paths) υπολογίζονται και αποθηκεύονται στον πίνακα προώθησης ο οποίος αποτελεί βασικό στοιχείο σε κάθε δρομολογητή δικτύου. Η προώθηση γίνεται με βάση την τιμή ενός ή περισσότερων πεδίων στην κεφαλίδα του πακέτου και στη συνέχεια, με βάση τις τιμές κεφαλίδας δημιουργεί το ευρετήριο στον πίνακα προώθησης. Οι τιμές που είναι αποθηκευμένες στην καταχώρηση του πίνακα προώθησης υποδεικνύουν τη διεπαφή της εξερχόμενης σύνδεσης σε αυτόν το δρομολογητή στον οποίο πρόκειται να προωθηθεί το πακέτο. Η προώθηση αποτελεί τη βασική λειτουργία που εκτελείται στο επίπεδο δεδομένων. Η διαδικασία προώθησης πακέτων μετακινεί ένα πακέτο από μια διεπαφή εισόδου (ingress) ενός δρομολογητή στην κατάλληλη διεπαφή εξόδου (egress) με βάση τις πληροφορίες που περιέχονται στον πίνακα προώθησης.

Οι (Obaidat et al., n.d.) στην έρευνα τους παρουσιάζουν τα πλεονεκτήματα ενός δικτύου SDN όσο αφορά την σύγκλιση των πρωτοκόλλων δρομολόγησης RIP, OSPF και EIGRP κατά τη διάρκεια αστοχίας των κόμβων και των συνδέσεων σε αντίθεση με τα παραδοσιακά δίκτυα. Για τα δίκτυα SDN, χρησιμοποιήθηκε ο ελεγκτής Floodlight και για την προσομοίωση του δικτύου το πρόγραμμα Mininet ενώ για τα παραδοσιακά δίκτυα το Packet Tracer το οποίο είναι εργαλείο προσομοίωσης και απεικόνισης δικτύων. Και στα δύο δίκτυα για τη μέτρηση του χρόνου σύγκλισης δρομολόγησης χρησιμοποιήθηκαν οι εντολές ping και traceroute. Στα δίκτυα SDN η μόνη συσκευή που ενημερώνεται για την αποτυχία της σύνδεσης είναι ο ελεγκτής. Επομένως ο χρόνος σύγκλισης των πρωτοκόλλων δρομολόγησης επηρεάζεται λιγότερο εν συγκρίσει με τα παραδοσιακά δίκτυα όπου γίνεται χρήση της πλημμύρας (flooding) για τη γρήγορη διανομή των ενημερώσεων των πρωτοκόλλων δρομολόγησης σε ολόκληρο το δίκτυο. Ο ελεγκτής υπολογίζει τη νέα διαδρομή και προωθεί τις πληροφορίες της επαναδρομολογημένης διαδρομής στους επηρεαζόμενους μεταγωγείς.

2.2 Σύγκριση παραδοσιακών δικτύων και SDN

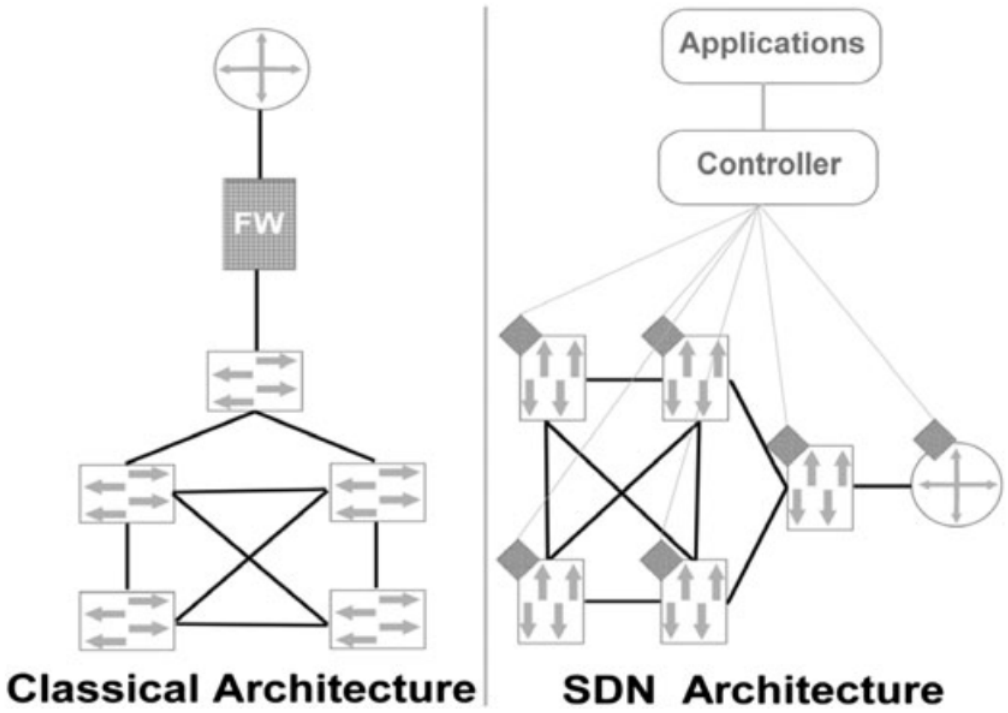
Η υποδομή των παραδοσιακών δικτύων είναι καθαρά φυσική και περιλαμβάνει μεταγωγείς και δρομολογητές, ενώ η υποδομή που βασίζεται σε λογισμικό λειτουργεί ουσιαστικά με επίπεδα ελέγχου. Τα παραδοσιακά πρωτόκολλα δικτύου IP σχεδιάστηκαν για να υιοθετήσουν μια αρχιτεκτονική κατανεμημένου ελέγχου, όπου οι συσκευές δικτύου επικοινωνούν μεταξύ τους μέσω ενός μεγάλου συνόλου πρωτοκόλλων δικτύου. Τα παραδοσιακά δίκτυα περιορίζονται από μια σειρά απαιτήσεων σε υπηρεσίες καθώς και κεντρικής διαχείρισης του δικτύου. Αυτές οι απαιτήσεις σχετίζονται με τη διαχείριση της ροής, την εφαρμογή πολιτικής, την αξιοπιστία και την εικονικοποίηση. Το επίπεδο ελέγχου στα παραδοσιακά δίκτυα υλοποιεί ένα κατανεμημένο παράδειγμα. Για κάθε συσκευή δικτύου, τα πρωτόκολλα ARP, OSPF, EIGRP, BGP λειτουργούν ανεξάρτητα χωρίς να υπάρχει μια κεντρική διαχείριση ολόκληρου του δικτύου. Το παράδειγμα αυτό συνοψίζει την πιο ουσιώδη διαφορά μεταξύ της παραδοσιακής δικτύωσης που βασίζεται στο υλικό και της τεχνολογίας SDN που βασίζεται στο λογισμικό. Κάθε φορά που απαιτείται μια νέα λειτουργία όπως, ένας εξισορροπητής φορτίου (load balancer), μια νέα συσκευή ενσωματώνεται στο δίκτυο ή μια από τις υφιστάμενες συσκευές διαμορφώνεται κατάλληλα για να εκτελέσει τη νέα λειτουργία.

Όπως επισημαίνουν μάλιστα οι (Kreutz et al., 2015) τα παραδοσιακά δίκτυα IP παρά την ευρεία υιοθέτησή τους, παραμένουν πολύπλοκα και δύσκολα στη διαχείριση τους. Για τη διαμόρφωση των παραδοσιακών συσκευών δικτύου, οι διαχειριστές πρέπει να διαμορφώσουν ξεχωριστά κάθε μεμονωμένη συσκευή χρησιμοποιώντας συνήθως τη διεπαφή γραμμής εντολών (Command Line Interface - CLI). Η διαμόρφωση πραγματοποιείτε με τη χρήση συγκεκριμένων εντολών και συχνά αυτές διαφέρουν ανά προμηθευτή. Εκτός από την πολυπλοκότητα της διαμόρφωσης, οι μηχανισμοί αυτόματης αναδιαμόρφωσης και απόκρισης είναι ουσιαστικά ανύπαρκτοι στα τρέχοντα δίκτυα. Επομένως, η επιβολή των απαιτούμενων πολιτικών σε ένα cloud περιβάλλον είναι εξαιρετικά δύσκολη.

Επίσης, οι (Nunes Astuto et al., 2014) ανέδειξαν τις αυξημένες δυσκολίες που υπάρχουν για τη διαμόρφωση των παραδοσιακών δικτύων. Οι διαχειριστές του δικτύου, οι οποίοι είναι υπεύθυνοι για τη διαμόρφωση των πολιτικών, συχνά χρειάζεται να ολοκληρώσουν περίπλοκες εργασίες με πρόσβαση σε πολύ περιορισμένα εργαλεία. Λόγω της τεράστιας ανάπτυξης του διαδικτύου και του γεγονότος ότι θεωρείται πλέον μέρος της κρίσιμης υποδομής της κοινωνίας μας, έχει γίνει εξαιρετικά δύσκολο να εξελιχθεί τόσο ως προς τη φυσική του υποδομή όσο και ως προς τα πρωτόκολλα και τις αποδόσεις του. Οι συσκευές δικτύου πωλούνται ως κλειστά κυκλώματα και οι διαχειριστές είναι σε θέση να διαμορφώνουν μόνο τις παραμέτρους των διαφόρων πρωτοκόλλων του δικτύου.

Οι (Mousa et al., 2017) στη μελέτη τους εστιάζουν στο πρόβλημα της διαμόρφωσης, της ευελιξίας και της καινοτομίας που αντιμετωπίζουν τα παραδοσιακά δίκτυα. Σε ένα κατανεμημένο δίκτυο, πολλαπλών προμηθευτών, πολλαπλών πρωτοκόλλων και εξαρτώμενο από τον ανθρώπινο παράγοντα, η διαμόρφωση και η αντιμετώπιση προβλημάτων γίνεται πολύ σύνθετη. Όπως αναφέρεται μάλιστα στη μελέτη, οι διαχειριστές των δικτύων θα πρέπει να μεταφράσουν πολιτικές υψηλού επιπέδου (high level network policies) σε σενάρια χαμηλού επιπέδου (low level scripts) που γράφονται για κάθε μεμονωμένη συσκευή, κοινώς γνωστή ως «γλώσσα διαμόρφωσης» (configuration language). Η ενσωμάτωση εξοπλισμού διαφορετικών προμηθευτών στο δίκτυο μπορεί να οδηγήσει σε προβλήματα διαλειτουργικότητας. Επίσης, το επίπεδο ελέγχου (που είναι υπεύθυνο για το χειρισμό της κυκλοφορίας δικτύου) και το επίπεδο δεδομένων το οποίο προωθεί την κυκλοφορία (σύμφωνα με τις αποφάσεις που λαμβάνονται από το επίπεδο ελέγχου) εκτελούνται από τις συσκευές δικτύωσης, εμποδίζοντας την καινοτομία και μειώνοντας την εξέλιξη και την ευελιξία της υποδομής της δικτύωσης. Όπως τονίζουν μάλιστα οι (Kreutz et al., 2015) η μετάβαση από το IPv4 στο IPv6, που ξεκίνησε πριν από μερικά χρόνια εξακολουθεί να είναι σε μεγάλο βαθμό ημιτελής, ενώ στην πραγματικότητα το IPv6 αντιπροσώπευε απλώς μια ενημέρωση πρωτοκόλλου (protocol). Η εφαρμογή ενός νέου πρωτοκόλλου δρομολόγησης, στα παραδοσιακά δίκτυα, μπορεί να χρειαστεί πέντε έως δέκα χρόνια να σχεδιαστεί, να αξιολογηθεί και να αναπτυχθεί πλήρως. Τελικά, η κατάσταση αυτή έχει διογκώσει τα λειτουργικά έξοδα λειτουργίας ενός δικτύου IP.

Επίσης, οι συγγραφείς (Benzekki et al., 2016) στην έρευνα τους εστιάζουν στα προβλήματα και στις δυσκολίες της υλοποίησης και της διαμόρφωσης των παραδοσιακών δικτύων. Όπως αναφέρουν μάλιστα η υλοποίηση, η διαμόρφωση και η αντιμετώπιση προβλημάτων σε δίκτυο πολλαπλών προμηθευτών απαιτεί καταρτισμένους τεχνικούς και αυξημένο λειτουργικό κόστος. Στην πραγματικότητα, η ποικιλία και η πολυπλοκότητα των στοιχείων που αποτελούν το δίκτυο καθιστούν τη συντήρηση του πολύ δαπανηρή και λιγότερο αξιόπιστη. Καθώς το SDN διαχωρίζει (εικόνα 2) τις αποφάσεις δρομολόγησης και προώθησης των στοιχείων δικτύωσης από το επίπεδο δεδομένων, η υλοποίηση και η διαχείριση του δικτύου γίνεται απλούστερη. Το επίπεδο ελέγχου είναι υπεύθυνο μόνο για τις πληροφορίες που σχετίζονται με τη τοπολογία του δικτύου και τη δρομολόγηση της κυκλοφορίας. Αντίθετα, το επίπεδο δεδομένων ενορχηστρώνει την κυκλοφορία του δικτύου σύμφωνα με την καθιερωμένη διαμόρφωση στο επίπεδο ελέγχου. Στα δίκτυα SDN οι λειτουργίες ελέγχου συγκεντρώνονται στον ελεγκτή που υπαγορεύει τις πολιτικές του δικτύου.



Εικόνα 2: Παραδοσιακή δικτύωση (Πηγή: (Benzekki et al., 2016))

Οι (Haji et al., 2021) στη μελέτη τους εστιάζουν στις δυνατότητες της εικονικοποίησης που μπορούν να προσφέρουν τα δίκτυα SDN επιτρέποντας τον κεντρικό έλεγχο και τη διαχείριση των εικονικών πόρων. Η εικονικοποίηση του δικτύου επιτρέπει την ευέλικτη χρήση κοινών φυσικών πόρων δικτύωσης από πολλούς χρήστες (ενοικιαστές), προσφέροντας τους τη δυνατότητα να αξιοποιήσουν τα συνδυασμένα οφέλη της δικτύωσης SDN και της εικονικοποίησης του δικτύου. Επιπλέον, η εικονικοποίηση σε επίπεδο δικτύου, με τις εικονικές συσκευές δικτύου (Virtual Network Functions - VNFs) να εξομοιώνουν λειτουργίες δρομολογητών, μεταγωγέων και τείχη προστασίας, παρέχουν υψηλότερο επίπεδο αφαίρεσης και μεγαλύτερη ευελιξία στο σχεδιασμό και τη διαχείριση του δικτύου.

Επίσης, οι (Blenk et al., 2016) ανέδειξαν τις αυξημένες δυνατότητες που προσφέρει η εικονικοποίηση του δικτύου. Οι προγραμματιζόμενες διεπαφές επιτρέπουν τις αλληλεπιδράσεις μεταξύ των εφαρμογών δικτύωσης και του φυσικού δικτύου (δηλαδή, του επιπέδου δεδομένων) που χρησιμοποιείται για την παροχή υπηρεσιών δικτύωσης στις εφαρμογές. Συγκεκριμένα, το πρωτόκολλο OpenFlow παρέχει μια τυποποιημένη διεπαφή μεταξύ του επιπέδου ελέγχου και του επιπέδου των δεδομένων. Χρησιμοποιώντας το πρωτόκολλο OpenFlow, ένας υπερ-επόπτης (hypervisor) μπορεί να δημιουργήσει πολλαπλά εικονικά δίκτυα SDN (virtual SDN - vSDN) έχοντας ως βάση ένα φυσικό δίκτυο. Η εικονικοποίηση της φυσικής υποδομής του δικτύου SDN μέσω ενός hypervisor επιτρέπει σε πολλαπλούς ενοικιαστές να μοιράζονται την ίδια υποδομή.

Κάθε μισθωτής μπορεί να λειτουργεί το δικό του εικονικό δίκτυο SDN, δηλαδή το δικό του λειτουργικό σύστημα δικτύου, ανεξάρτητα από τους άλλους ενοικιαστές.

Οι (Lara et al., 2014) στη μελέτη τους καταγράφουν την αποτυχία δρομολόγησης και αποκατάστασης των παραδοσιακών δικτύων και προτείνουν την χρήση ενός ελεγκτής που θα έχει γνώση του ολόκληρου του δικτύου. Οι συγγραφείς σημειώνουν ότι οι παραδοσιακές προσεγγίσεις συχνά βασίζονται σε στατικές αρχιτεκτονικές και κεντρικούς μηχανισμούς ελέγχου, οι οποίοι μπορούν να περιορίσουν την επεκτασιμότητα, την ευελιξία και την ανθεκτικότητα. Η βασική ιδέα είναι η δημιουργία μιας κεντρικής πολιτικής την οποία θα διαχειρίζεται ο ελεγκτής. Σε ένα παραδοσιακό δίκτυο, κάθε μεταγωγέας έχει περιορισμένη γνώση του δικτύου. Όταν μια σύνδεση αποτύχει, τότε οι διαδρομές αναπροσαρμόζονται σε κάθε μεταγωγέα μέχρι να βρεθούν νέες διαδρομές. Σε ένα δίκτυο OpenFlow, ένας κεντρικός ελεγκτής μπορεί να υπολογίσει τις νέες διαδρομές με πολύ ταχύτερο και ευκολότερο τρόπο. Ο υπολογισμός των διαδρομών σε μεγάλα και πολύπλοκα δίκτυα μπορεί να απαιτεί τη συνεργασία μεταξύ διαφορετικών τομέων. Τα δίκτυα που βασίζονται στο πρωτόκολλο OpenFlow, ο ελεγκτής συνήθως έχει ευρύτερη γνώση του δικτύου και επομένως ο έλεγχος είναι συγκεντρωτικός. Η ανάλυση της κίνησης βάσει λογισμικού αποτελεί ένα σημαντικό πλεονέκτημα των δικτύων SDN. Αυτή η δυνατότητα επιτρέπει σε μεγάλο βαθμό την καινοτομία, καθώς η ανάλυση της κυκλοφορίας μπορεί να πραγματοποιηθεί σε πραγματικό χρόνο με τη χρήση αλγορίθμων μηχανικής μάθησης (machine learning - ML), βάσεων δεδομένων και οποιουδήποτε άλλου εργαλείου λογισμικού.

Οι συγγραφείς (Rifai et al., 2017) εστιάζουν στις προκλήσεις και στους περιορισμούς της χρήσης των CAM και TCAM στο SDN, όπως το υψηλό κόστος, η περιορισμένη χωρητικότητα και η κατανάλωση ενέργειας. Με τη χρήση των CAM και TCAM, οι μεταγωγείς SDN μπορούν να επιταχύνουν την επεξεργασία πακέτων και να βελτιώσουν την απόδοση του δικτύου. Ωστόσο, επισημαίνουν την περιορισμένη χωρητικότητα των CAM και TCAM, η οποία μπορεί να αποτελέσει το σημείο συμφόρησης σε μεγάλης κλίμακας δίκτυα SDN. Οι συγγραφείς προσπαθούν να συμπιέσουν τους κανόνες ροής μειώνοντας τον αριθμό των bits που περιγράφουν τη ροή εντός του μεταγωγέα, εισάγοντας μια μικρή ετικέτα στην επικεφαλίδα του πακέτου. Αυτή η λύση απαιτεί αλλαγή: α) στις επικεφαλίδες των πακέτων και β) στον τρόπο με τον οποίο συμπληρώνονται οι πίνακες SDN. Η προσθήκη του αναγνωριστικού σε κάθε εισερχόμενο πακέτο είναι δύσκολο να πραγματοποιηθεί στα κλειστά κυκλώματα ASICs των παραδοσιακών συσκευών δικτύωση, δεδομένου ότι αυτή δεν είναι μια τυπική λειτουργία, με αποτέλεσμα τα πακέτα να υποβάλλονται σε επεξεργασία από την κεντρική CPU του δρομολογητή επιβαρύνοντας επιπρόσθετα την απόδοση και τον ρυθμό κίνησης.

2.3 Περιγραφή της τεχνολογίας SDN

2.3.1 Ορισμός SDN

Σύμφωνα με τον ορισμό που δίνεται από το ONF (Software-Defined Networking (SDN) Definition - Open Networking Foundation, n.d.) το SDN αναφέρεται στην αρχιτεκτονική δικτύου στην οποία η διαχείριση της προώθησης στο επίπεδο δεδομένων πραγματοποιείται μέσω ενός απομακρυσμένου επίπεδου αποσυνδεδεμένου από το πρώτο. Η αρχιτεκτονική SDN αποσυνδέει τις λειτουργίες ελέγχου και προώθησης δικτύου επιτρέποντας στον έλεγχο δικτύου να γίνει απευθείας προγραμματιζόμενος και η υποκείμενη υποδομή να αφαιρεθεί από την υλοποίηση των εφαρμογών και των υπηρεσιών δικτύου. Με βάση τον ορισμό, το SDN ορίζεται από δύο χαρακτηριστικά, την αποσύνδεση των επιπέδων ελέγχου και δεδομένων και τη δυνατότητα προγραμματισμού στο επίπεδο ελέγχου.

Σύμφωνα με τους (Xia et al., 2015) το SDN αποτελεί μια αναδυόμενη αρχιτεκτονική δικτύου όπου ο έλεγχος δικτύου (network control) αποσυνδέεται από την προώθηση (forwarding) και είναι απευθείας προγραμματιζόμενος. Η αρχιτεκτονική SDN είναι δυναμική, διαχειρίσιμη, οικονομικά αποδοτική και προσαρμόσιμη, καθιστώντας την ιδανική για τη δυναμική φύση των σημερινών εφαρμογών και του υπολογιστικού νέφους. Η μοναδικότητα της τεχνολογίας SDN έγκειται στο γεγονός ότι προσφέρει απλές προγραμματιζόμενες συσκευές δικτύου, αντί να κάνει τις συσκευές δικτύωσης πιο περίπλοκες όπως ισχύει στην περίπτωση της παραδοσιακής δικτύωσης. Επιπλέον, προτείνεται ο διαχωρισμός των επιπέδων ελέγχου και δεδομένων στον αρχιτεκτονικό σχεδιασμό του δικτύου SDN. Με βάση το σχεδιασμό, ο έλεγχος δικτύου πραγματοποιείται στο επίπεδο ελέγχου χωρίς να επηρεάζονται οι ροές των δεδομένων. Ως εκ τούτου, η ευφυΐα του δικτύου μπορεί να αφαιρεθεί από τις συσκευές μεταγωγής και να τοποθετηθεί σε ελεγκτές. Ταυτόχρονα, οι συσκευές μεταγωγής μπορούν να ελέγχονται εξωτερικά από λογισμικό χωρίς ενσωματωμένη νοημοσύνη. Η αποσύνδεση του επιπέδου ελέγχου από το επίπεδο δεδομένων προσφέρει, όχι μόνο ένα απλούστερο προγραμματιζόμενο περιβάλλον αλλά και μεγαλύτερη ελευθερία στο λογισμικό να ορίζει τη συμπεριφορά ενός δικτύου.

2.3.2 Πρωτόκολλο OpenFlow

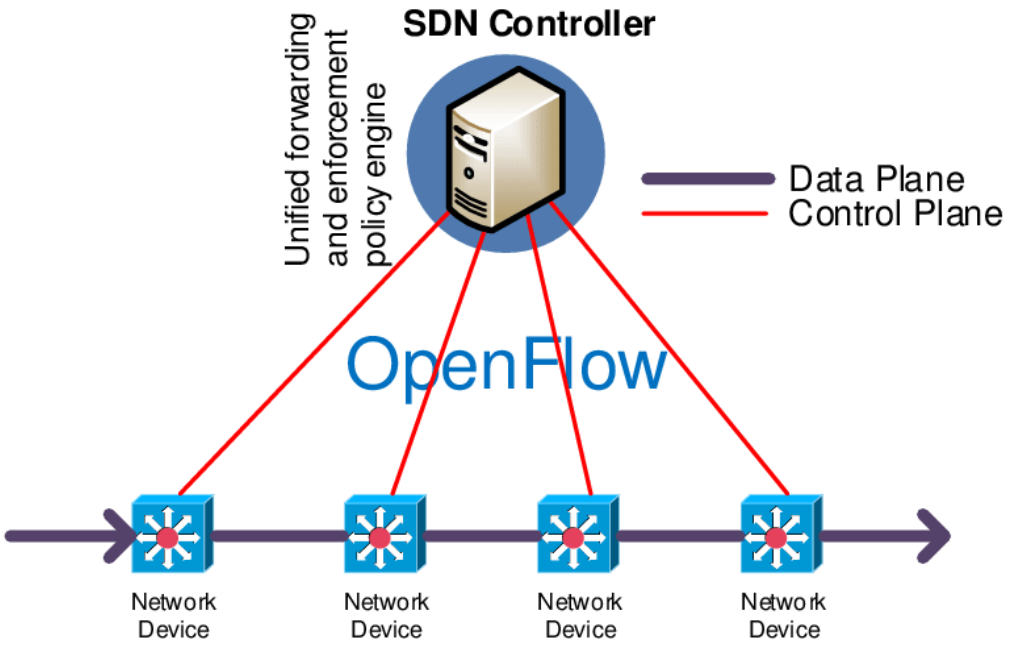
Το Open Networking Foundation (ONF) αποτελεί μη κερδοσκοπική κοινοπραξία του κλάδου που ηγείται τις εξελίξεις σε θέματα που σχετίζονται με την τεχνολογία SDN και της τυποποίησης των

στοιχείων της αρχιτεκτονικής SDN, όπως το πρωτόκολλο OpenFlow. Το πρωτόκολλο OpenFlow δομεί την επικοινωνία μεταξύ των επιπέδων ελέγχου και δεδομένων των υποστηριζόμενων συσκευών δικτύου (Software-Defined Networking: The New Norm for Networks - Open Networking Foundation, n.d.). Αν και το SDN και το OpenFlow ξεκίνησαν ως ακαδημαϊκά πειράματα, έχουν κερδίσει σημαντική έλξη στον επιχειρηματικό τομέα τα τελευταία χρόνια. Η πλειοψηφία των κατασκευαστών μεταγωγέων προσφέρουν πλέον υποστήριξη στο πρωτόκολλο OpenFlow API (Application Programming Interface) στα προϊόντα τους. Οι Google, Facebook, Yahoo, Microsoft, Verizon και Deutsche Telekom χρηματοδότησαν την κοινοπραξία ONF με πρωταρχικό στόχο την προώθηση και τη διευκόλυνση της υιοθέτησης του SDN μέσω της δημιουργίας ανοιχτών προτύπων.

Οι συγγραφείς (Mckeown et al., n.d.) εστιάζουν στην ανάγκη για την ανάπτυξη προγραμματιζόμενων δικτύων. Τα δίκτυα απαιτούν προγραμματιζόμενους μεταγωγείς και δρομολογητές που θα μπορούν ταυτόχρονα να επεξεργάζονται πακέτα για πολλαπλά απομονωμένα πειραματικά εικονικά δίκτυα. Όπως αναφέρουν στην μελέτη τους, τα εικονικά προγραμματιζόμενα δίκτυα μπορούν να προσφέρουν νέες ιδέες για καινοτομία στην υποδομή των δικτύων. Το πρωτόκολλο OpenFlow παρέχει έναν τυποποιημένο τρόπο διαχείρισης της κυκλοφορίας και δομεί τον τρόπο επικοινωνίας ενός ελεγκτή με τις συσκευές δικτύου, όπως μεταγωγείς και δρομολογητές. Οι συσκευές που υποστηρίζουν το πρωτόκολλο OpenFlow αποτελούνται από δύο λογικά στοιχεία: α) έναν πίνακα ροής που ορίζει τον τρόπο επεξεργασίας και προώθησης πακέτων εντός του δικτύου και β) μια διεπαφή προγραμματισμού εφαρμογών OpenFlow (Application Programming Interface - API) που χειρίζεται την επικοινωνία μεταξύ του μεταγωγέα και του ελεγκτή. Το ανοικτό πρωτόκολλο OpenFlow επιτρέπει σε εφαρμογές λογισμικού να προγραμματίζουν τον πίνακα ροής των μεταγωγέων μέσω της διεπαφής προγραμματισμού εφαρμογών (API).

Η αρχιτεκτονική OpenFlow όπως φαίνεται στην εικόνα 3 αποτελείται από τρία κύρια στοιχεία: α) έναν μεταγωγέα συμβατό με το OpenFlow, β) ένα ασφαλές κανάλι και γ) έναν ελεγκτή. Οι μεταγωγείς χρησιμοποιούν τους πίνακες ροής για την προώθηση των πακέτων. Ένας πίνακας ροής είναι ένας κατάλογος καταχωρήσεων ροής (flow table) στον οποίο κάθε καταχώρηση περιλαμβάνει πεδία αντιστοίχισης όπως, μετρητές (counters) και οδηγίες (instructions). Ο ελεγκτής είναι υπεύθυνος για το χειρισμό του πίνακα ροής του μεταγωγέα, χρησιμοποιώντας το πρωτόκολλο OpenFlow. Ένας συμβατός με το OpenFlow μεταγωγέας προωθεί τα πακέτα σύμφωνα με τους κανόνες που ορίζονται στον πίνακα ροής. Εσωτερικά, ένας μεταγωγέας χρησιμοποιεί την τριαδική διευθυνσιοδοτούμενη μνήμη (Ternary Content Addressable Memory -

TCAM) και τη μνήμη τυχαίας προσπέλασης (Random Access Memory - RAM) για την επεξεργασία του κάθε πακέτου.



Εικόνα 3: Διάγραμμα OpenFlow (Πηγή: https://www.researchgate.net/figure/A-schematic-overview-of-SDN-implemented-with-OpenFlow_fig1_288890479)

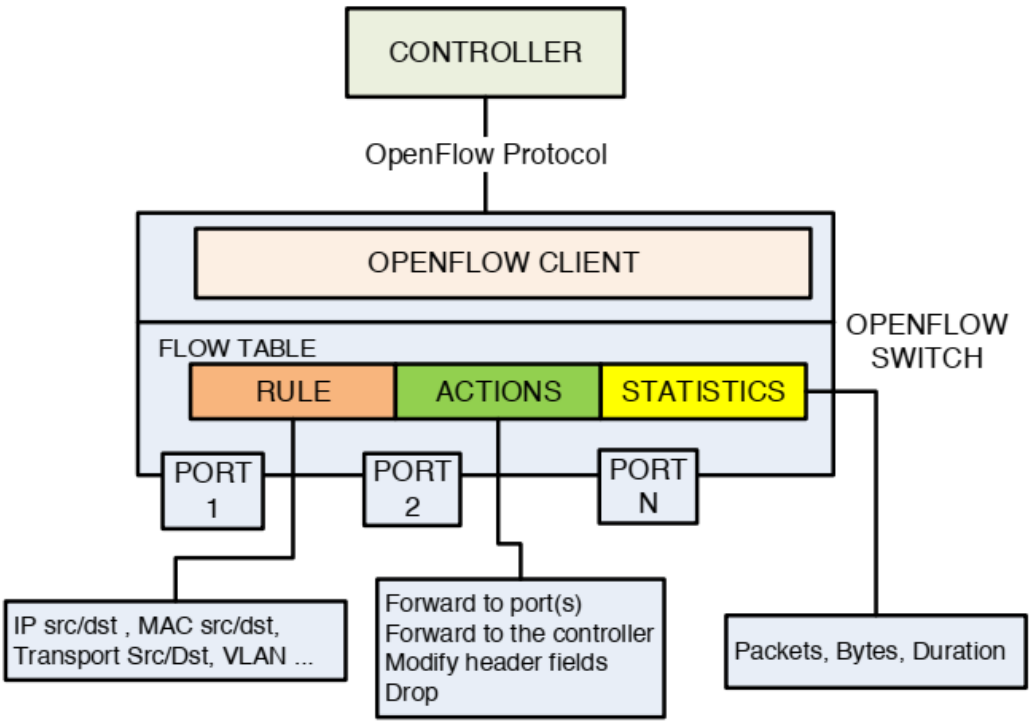
Στην αρχιτεκτονική OpenFlow, όπως απεικονίζεται στο πιο κάτω διάγραμμα (εικόνα 4), η συσκευή προώθησης περιέχει ένα ή περισσότερους πίνακες ροής και ένα επίπεδο αφαίρεσης που επικοινωνεί με ασφάλεια μέσω του πρωτοκόλλου OpenFlow με έναν ελεγκτή. Οι πίνακες ροής αποτελούνται από εγγραφές ροής, και καθορίζουν τον τρόπο με τον οποίο θα επεξεργαστούν και θα προωθηθούν τα πακέτα που αντιστοιχούν σε μια ροή. Οι καταχωρήσεις ροής αποτελούνται συνήθως από:

1. Τους κανόνες αντιστοίχισης, που χρησιμοποιούνται για την αντιστοίχιση των εισερχόμενων πακέτων. Οι κανόνες αντιστοίχισης βασίζονται σε πεδία στην κεφαλίδα (header) του πακέτου και μπορούν να χρησιμοποιηθούν για την αντιστοίχιση συγκεκριμένων τιμών παρέχοντας έναν ευέλικτο τρόπο επεξεργασίας και προώθησης των πακέτων σε περιβάλλοντα SDN. Τα πιο κοινά πεδία που χρησιμοποιούνται στους κανόνες αντιστοίχισης OpenFlow περιλαμβάνουν τις διευθύνσεις πηγής και προορισμού (IP source, IP destination), τις διευθύνσεις MAC του αποστολέα και του παραλήπτη και το αναγνωριστικό VLAN (VLAN ID).

2. Τους μετρητές (counters), που χρησιμοποιούνται για τη συλλογή στατιστικών στοιχείων για τη συγκεκριμένη ροή, όπως ο αριθμός των ληφθέντων πακέτων, ο αριθμός των bytes και η διάρκεια της ροής.

3. Ένα σύνολο ενεργειών που πρέπει να εφαρμοστούν μετά από μια αντιστοίχιση. Κατά την άφιξη ενός πακέτου σε έναν μεταγωγέα OpenFlow, τα πεδία της επικεφαλίδας του πακέτου εξάγονται και συγκρίνονται με το τμήμα πεδίων αντιστοίχισης των καταχωρίσεων του πίνακα ροής.

Εάν βρεθεί μια αντίστοιχη καταχώρηση, ο μεταγωγέας εφαρμόζει το κατάλληλο σύνολο ενεργειών που σχετίζεται με την αντιστοίχιση αυτή. Εάν η διαδικασία αναζήτησης του πίνακα ροής δεν καταλήξει σε ταύτιση, η ενέργεια που αναλαμβάνει ο μεταγωγέας εξαρτάται από τις οδηγίες που ορίζονται από την καταχώρηση ροής που σχετίζεται με τις εγγραφές που δεν υπάρχουν στον πίνακα (Nunes Astuto et al., 2014).



Εικόνα 4: Αρχιτεκτονική OpenFlow (Πηγή: (Nunes Astuto et al., 2014))

Οι (Lara et al., 2014) στην ερευνά τους αναλύουν το πρωτόκολλο OpenFlow και εστιάζουν στις δυνατότητες που μπορούν να αξιοποιηθούν από ερευνητές για να πειραματιστούν με νέες ιδέες και νέες εφαρμογές για τρείς, κυρίως, λόγους:

1. Οι αρχιτεκτονικές OpenFlow επιτρέπουν τον κεντρικό έλεγχο του δικτύου, την ανάλυση της κίνησης βάσει λογισμικού, τη δυναμική ενημέρωση των κανόνων προώθησης και τον έλεγχο της ροής.

2. Η ανάλυση της κίνησης βάσει λογισμικού επιτρέπει σε μεγάλο βαθμό την καινοτομία, καθώς είναι δυνατό να βελτιωθούν οι δυνατότητες ενός μεταγωγέα χρησιμοποιώντας οποιαδήποτε τεχνική που βασίζεται σε λογισμικό.

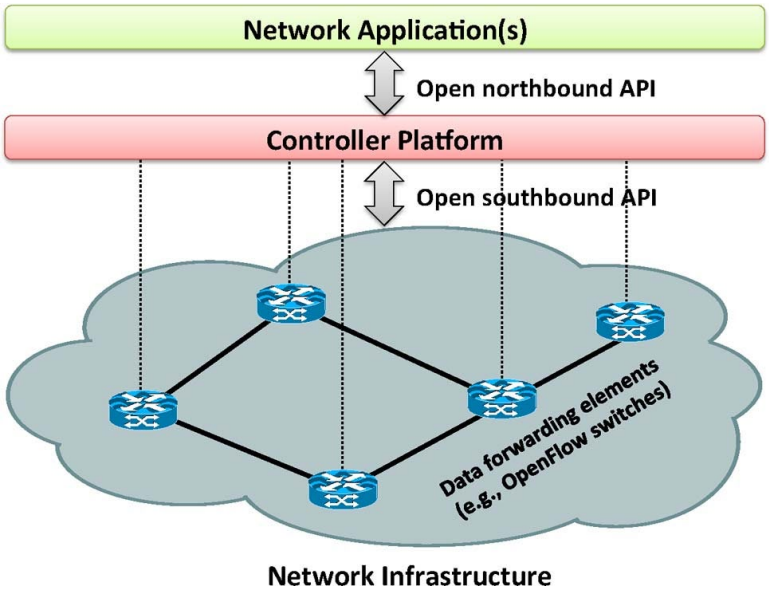
3. Και τέλος, επιτρέπουν τις δυναμικές ενημερώσεις των κανόνων προώθησης.

Στην έκδοση 1.4 το OpenFlow εισήγαγε νέα χαρακτηριστικά ασφαλείας με στόχο το μετριασμό των ευπαθειών που θα μπορούσαν να αξιοποιηθούν από τους επιτιθέμενους. Τα νέα χαρακτηριστικά περιλαμβάνουν τη δυνατότητα ελέγχου ταυτότητας και κρυπτογράφηση των μηνυμάτων OpenFlow, καθώς και τη δυνατότητα περιορισμού του ρυθμού αποστολής μηνυμάτων στον ελεγκτή για την αποτροπή επιθέσεων άρνησης παροχής υπηρεσιών (Kreutz et al., 2015). Επιπλέον, ο μεταγωγέας μπορεί να ρυθμιστεί ώστε να περιορίζει το μέγιστο μέγεθος του πίνακα ροής, το οποίο μπορεί να βοηθήσει στην αποτροπή επιθέσεων υπερχείλισης. Επίσης, υπάρχει η δυνατότητα να περιοριστεί ο ρυθμός με τον οποίο προστίθενται οι νέες εγγραφές ροής στον πίνακα ροής, γεγονός που μπορεί να βοηθήσει στην αποτροπή της υπερφόρτωσης του μεταγωγέα από μια πλημμύρα νέων ροών (*OpenFlow Switch Specification*, 2015). Ενώ στην έκδοση 1.4 εισήχθησαν νέα χαρακτηριστικά ασφαλείας, η διασφάλιση ενός δικτύου OpenFlow απαιτεί μια ολιστική προσέγγιση που θα περιλαμβάνει όχι μόνο την εξασφάλιση του επιπέδου ελέγχου αλλά και του επιπέδου δεδομένων, του επιπέδου διαχείρισης και της φυσικής υποδομής (*OpenFlow Switch Specification*, 2015).

2.3.3 Αρχιτεκτονική SDN

Οι επερχόμενες τάσεις των τελευταίων ετών, όπως η τεχνολογία cloud, τα μεγάλα δεδομένα (big data), και το διαδίκτυο των πραγμάτων (Internet of Things - IoT) ανάγκασαν τους παρόχους δικτύων να επαναξιολογήσουν τις προσεγγίσεις τους όσο αφορά την αρχιτεκτονική των δικτύων. Η ανάγκη για ταχύτητα και αυτοματισμό καθιστά το SDN στρατηγική λύση για τους οργανισμούς που επιδιώκουν να επωφεληθούν από μια τεχνολογία ανοιχτού δικτύου που προσφέρει μεγαλύτερη ευελιξία, περισσότερες ευκαιρίες για τεχνολογικές καινοτομίες, βελτιωμένη διαλειτουργικότητα και εξοικονόμηση κόστους. Το SDN, με βάση την εργασία των (Kreutz et al., 2015) αποτελεί μια σχετικά καινοτόμο προσέγγιση στο σχεδιασμό, υλοποίηση και διαχείριση

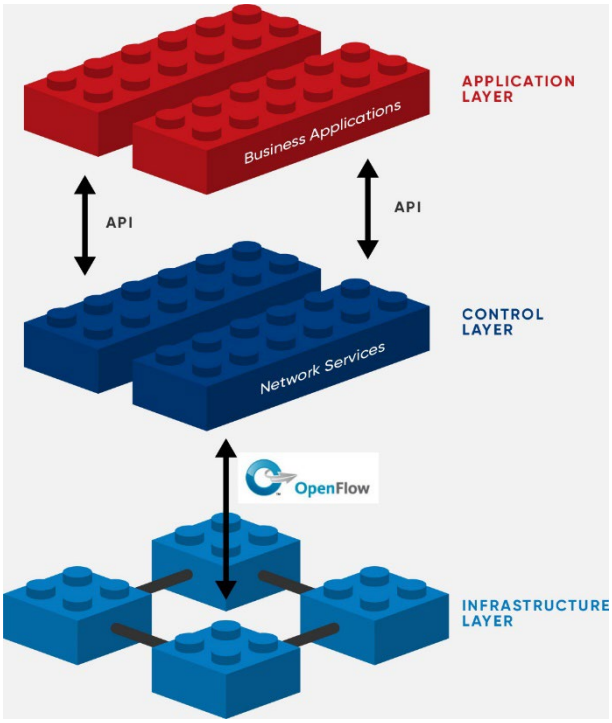
πολύπλοκων δικτύων, τα οποία ενδέχεται να απαιτούν αναδιαμόρφωση και διαχείριση σε τακτά χρονικά διαστήματα. Η τεχνολογία SDN διαχωρίζει τον έλεγχο δικτύου και τη διαδικασία προώθησης προσφέροντας καλύτερη διαχείριση. Ένα απλοποιημένο διάγραμμα απεικόνισης της αρχιτεκτονικής SDN παρουσιάζεται στην εικόνα 5. Η τμηματοποίηση του δικτύου προσφέρει πολυάριθμα οφέλη όσον αφορά την ευελιξία, τη διαχείριση και τον έλεγχο του δικτύου. Αφενός, επιτρέπει το συνδυασμό των πλεονεκτημάτων της εικονικοποίησης (virtualization) και αφετέρου, την εύκολη διαχείριση και συντήρηση του δικτύου.



Εικόνα 5: Απλοποιημένο διάγραμμα της αρχιτεκτονικής SDN (Πηγή: (Kreutz et al., 2015))

Όπως τονίζεται μάλιστα από τους συγγραφείς (Kreutz et al., 2015) ο διαχωρισμός είναι ζωτικής σημασίας για την επίτευξη της απαραίτητης ευελιξίας του δικτυού, καθώς απλοποιεί την διαχείριση, την εισαγωγή νέων στοιχείων και προάγει την ανάπτυξη και την καινοτομία του δικτύου. Ως αποτέλεσμα, οι επιχειρήσεις και οι παρόχοι αποκτούν αυτοματισμό και έλεγχο του δικτύου μέσω προγραμματισμού δίνοντας τους τη δυνατότητα να δημιουργήσουν επεκτάσιμα και ευέλικτα δίκτυα που προσαρμόζονται εύκολα στις μεταβαλλόμενες επιχειρηματικές ανάγκες. Ο ελεγκτής SDN επικοινωνεί με τις εφαρμογές δικτύου μέσω της διεπαφής Northbound (Control - Application Plane Interface), ενώ η διασύνδεση του επιπέδου ελέγχου με το επίπεδο των δεδομένων γίνεται μέσω της διεπαφής Southbound. Το πιο δημοφιλές πρωτόκολλο που χρησιμοποιείται σήμερα για την επικοινωνία μεταξύ του ελεγκτή SDN και του επιπέδου δεδομένων είναι το πρωτόκολλο OpenFlow.

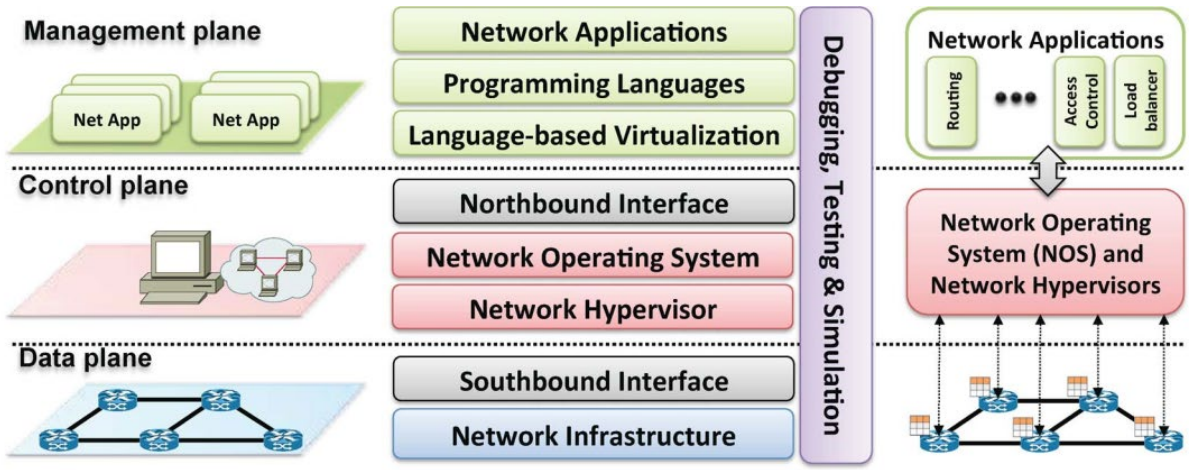
Η δομή του SDN αποτελείται από τρία διαφορετικά επίπεδα όπως παρουσιάζεται στην εικόνα 6: α) το επίπεδο εφαρμογής (application plane), β) το επίπεδο ελέγχου (control plane) και γ) το επίπεδο υποδομής (infrastructure plane) ή αλλιώς επίπεδο δεδομένων (data plane).



Εικόνα 6: Βασική δομή SDN (Πηγή: (Software-Defined Networking (SDN) Definition - Open Networking Foundation, n.d.))

2.3.4 Επίπεδο εφαρμογής (Application Plane)

Στη δικτύωση, ένα επίπεδο είναι μια αφηρημένη αντίληψη του τόπου όπου λαμβάνουν χώρα ορισμένες διεργασίες. Στην εικόνα 7 μπορούμε να διακρίνουμε πως τα τρία επίπεδα, το επίπεδο εφαρμογών, το επίπεδο ελέγχου και το επίπεδο δεδομένων συνδέονται μεταξύ τους μέσω των διεπαφών Southbound και Northbound. Το επίπεδο εφαρμογών είναι υπεύθυνο για την εκτέλεση των υπηρεσιών και των εφαρμογών ασφαλείας του δικτύου που εύκολα μπορούν να διαμορφωθούν, να αναπτυχθούν και να διαχειριστούν μέσω του ελεγκτή SDN. Η εικονικοποίηση του δικτύου, τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS), τα συστήματα πρόληψης εισβολών (Intrusion Prevention Systems - IPS), η υλοποίηση τείχους προστασίας, η εξισορρόπηση του φορτίου, ο ορισμός και η επιβολή πολιτικών δικτύου είναι μερικά παραδείγματα που χειρίζεται αυτό το επίπεδο. Το επίπεδο εφαρμογής αλληλοεπιδρά με το επίπεδο ελέγχου χρησιμοποιώντας τη διεπαφή επιπέδου ελέγχου εφαρμογών (Application Control Plane Interface - A-CPI) που ονομάζεται επίσης και διεπαφή εφαρμογών Northbound.



Εικόνα 7: Επίπεδα αρχιτεκτονικής SDN (Πηγή: (Kreutz et al., 2015))

Με αυτόν τον τρόπο, οι εφαρμογές SDN κοινοποιούν τις απαιτήσεις δικτύου τους στον ελεγκτή SDN, ο οποίος τις μεταφράζει σε εντολές και κανόνες προώθησης για τη διεπαφή Southbound. Η διεπαφή Southbound με τη σειρά της τις υπαγορεύει στις επιμέρους συσκευές επιπέδου δεδομένων οι οποίες είναι υπεύθυνες για τη προώθηση των πακέτων.

2.3.5 Επίπεδο ελέγχου (Control Plane)

Το επίπεδο ελέγχου στην αρχιτεκτονική SDN αποτελείται συνήθως από δύο στοιχεία: α) τον ελεγκτή SDN και β) το πρωτόκολλο OpenFlow. Το επίπεδο λειτουργεί ως διαμεσολαβητής για το επίπεδο δεδομένων και το επίπεδο εφαρμογής. Ο ελεγκτής SDN περιέχει τη λογική ελέγχου του δικτύου και είναι υπεύθυνος για τη διαχείριση της ροής της κυκλοφορίας λαμβάνοντας αποκλειστικά αποφάσεις σχετικά με τη δρομολόγηση, την προώθηση και την απόρριψη των πακέτων μέσω προγραμματισμού, την εφαρμογή πολιτικών δικτύου και την παροχή μιας κεντρικής διεπαφής για τη διαχείριση του δικτύου. Οι ελεγκτές σε ένα κατανεμημένο περιβάλλον επικοινωνούν μεταξύ τους μέσω των διεπαφών Eastbound και Westbound. Το επίπεδο ελέγχου και το επίπεδο δεδομένων επικοινωνούν μεταξύ τους μέσω της διεπαφής Southbound με τη χρήση των πρωτοκόλλων OpenFlow ή NetConf. Το επίπεδο ελέγχου καθορίζει το σύνολο των δεδομένων που χρησιμοποιείται για τη δημιουργία των καταχωρήσεων του πίνακα προώθησης, οι οποίες με τη σειρά τους χρησιμοποιούνται από το επίπεδο δεδομένων για την προώθηση της κυκλοφορίας μεταξύ των θυρών εισόδου και εξόδου μιας συσκευής. Το σύνολο των δεδομένων που χρησιμοποιείται για την αποθήκευση της τοπολογίας του δικτύου ονομάζεται βάση πληροφοριών δρομολόγησης (Routing Information Base - RIB). Η RIB ενημερώνεται συχνά μέσω της ανταλλαγής πληροφοριών μεταξύ άλλων επιπέδων ελέγχου εντός του δικτύου. Οι καταχωρήσεις του πίνακα

προώθησης ονομάζονται βάση πληροφοριών προώθησης (Forwarding Information Base - FIB) και συχνά αντικατοπτρίζονται μεταξύ των επιπέδων ελέγχου και δεδομένων μιας συσκευής δικτύου. Η FIB προγραμματίζεται μόλις η RIB θεωρηθεί συνεπής και σταθερή.

2.3.6 Επίπεδο δεδομένων (Data Plane)

Το επίπεδο δεδομένων περιλαμβάνει τις συσκευές δικτύου, όπως δρομολογητές και μεταγωγείς. Σε αυτό το στρώμα συνυπάρχουν τόσο εικονικοί μεταγωγείς όπως οι Open vSwitch και Indigo, όσο και φυσικοί μεταγωγείς. Η κύρια λειτουργία του επιπέδου δεδομένων μιας συσκευής μεταγωγής SDN είναι η προώθηση των πακέτων. Το επίπεδο δεδομένων εφαρμόζεται συνήθως σε υλικό, το οποίο παρέχει γρήγορη και αποτελεσματική επεξεργασία της κίνησης του δικτύου. Είναι υπεύθυνο για τη διαχείριση και τον έλεγχο της ροής της κυκλοφορίας του δικτύου, καθώς και για την παροχή υπηρεσιών δικτύου, όπως δρομολόγηση, προώθηση και εξισορρόπηση φορτίου. Τα πακέτα δικτύου υποβάλλονται σε επεξεργασία και προωθούνται με βάση τις οδηγίες που παρέχονται από τον ελεγκτή SDN. Συγκεκριμένα, κατά τη λήψη ενός πακέτου, η συσκευή μεταγωγής προσδιορίζει πρώτα τον κανόνα προώθησης που αντιστοιχεί στο πακέτο και στη συνέχεια προωθεί το πακέτο στο αμέσως επόμενο hop. Η προώθηση των πακέτων στα παραδοσιακά δίκτυα βασίζεται σε διευθύνσεις IP ή MAC, ενώ η προώθηση των πακέτων σε δίκτυα SDN βασίζεται σε επιπρόσθετες παραμέτρους όπως η θύρα TCP ή UDP, στην ετικέτα εικονικού τοπικού δικτύου ή και στη θύρα εισόδου του μεταγωγέα.

Οι βασικές αρμοδιότητες του στρώματος υποδομής περιλαμβάνουν:

1. Τη διατήρηση της συνδεσιμότητας μεταξύ των συσκευών δικτύου.

2. Τη δημιουργία εικονικών πόρων δικτύου, οι οποίοι επιτρέπουν την ανάπτυξη υπηρεσιών και εφαρμογών δικτύου χωρίς να απαιτείται η φυσική αναδιαμόρφωση της υποδομής.

3. Μηχανισμούς ασφαλείας όπως ο έλεγχος πρόσβασης, η κρυπτογράφηση και η ανίχνευση και πρόληψη εισβολών για την προστασία του δικτύου.

4. Μηχανισμούς για τη διασφάλιση της δυνατότητας κλιμάκωσης του δικτύου όπως την προσθήκη και αφαίρεση πόρων δικτύου ανάλογα με τις ανάγκες, καθώς και εξισορρόπηση φορτίου και μηχανική της κυκλοφορίας.

2.3.7 Διεπαφές

Η επικοινωνία μεταξύ των τριών επιπέδων επιτυγχάνεται μέσω των Southbound και Northbound APIs. Το Southbound API χρησιμοποιείται για την επικοινωνία μεταξύ του ελεγκτή και του επιπέδου δεδομένων, ενώ το Northbound API χρησιμοποιείται για την επικοινωνία μεταξύ του ελεγκτή και των εφαρμογών. Τα δυο APIs είναι σημαντικά για την ορθή λειτουργία της αρχιτεκτονικής SDN, καθώς επιτρέπουν στον ελεγκτή να αλληλοεπιδρά με τα διάφορα στοιχεία του δικτύου.

2.3.8 Διεπαφή Southbound

Η διεπαφή Southbound συνδέει τα επίπεδα ελέγχου και προώθησης, αποτελώντας έτσι το κρίσιμο μέσο για το σαφή διαχωρισμό των λειτουργιών του επιπέδου ελέγχου και των δεδομένων. Επιτρέπει στον ελεγκτή να στέλνει οδηγίες στους μεταγωγείς ή στους δρομολογητές σχετικά με τον τρόπο διαχείρισης της κυκλοφορίας του δικτύου. Το πρωτόκολλο OpenFlow αποτελεί το πιο ευρέως αποδεκτό και διαδεδομένο ανοικτό Southbound πρότυπο για το SDN. Παρέχει την κοινή προδιαγραφή για την υλοποίηση συσκευών προώθησης με δυνατότητα OpenFlow, καθώς και το κανάλι επικοινωνίας μεταξύ των συσκευών του επιπέδου δεδομένων και ελέγχου. Το OpenFlow επιτρέπει στους διαχειριστές δικτύου να προγραμματίζουν τη ροή της κυκλοφορίας δίνοντάς τους περισσότερο έλεγχο στον τρόπο λειτουργίας του δικτύου. Άλλα διαθέσιμα Southbound APIs είναι τα NETCONF, RESTCONF και OVSDB, το καθένα με τα δικά του πλεονεκτήματα και περιπτώσεις χρήσης. Στην έκδοση OpenFlow 1.3.0 παρέχεται πλέον η υποστήριξη κρυπτογραφημένης επικοινωνίας Transport Layer Security (TLS) και ανταλλαγής πιστοποιητικών μεταξύ των μεταγωγέων και του ελεγκτή.

2.3.9 Διεπαφή Northbound

Η διεπαφή Northbound αποτελεί κρίσιμο μέρος στην αρχιτεκτονική του ελεγκτή SDN επιτρέποντας την επικοινωνία μεταξύ του επιπέδου ελέγχου και του επιπέδου εφαρμογής. Επιτρέπει στις εφαρμογές να αλληλοεπιδρούν με το δίκτυο και να έχουν πρόσβαση στις υπηρεσίες δικτύου που παρέχονται από τον ελεγκτή. Το πολυτιμότερο όφελος του SDN προκύπτει από την ικανότητά του να υποστηρίζει και να επιτρέπει καινοτόμες εφαρμογές. Τα Northbound APIs υποστηρίζουν μεγάλη ποικιλία εφαρμογών και επιτρέπουν τη σύνδεση με αυτοματοποιημένες στοίβες όπως το OpenStack ή το CloudStack που χρησιμοποιούνται για τη διαχείριση του Cloud. Υπάρχουν πολλά διαθέσιμα Northbound APIs, όπως το REST API, το Java API και το Python API,

το καθένα με τα δικά του πλεονεκτήματα και περιορισμούς. Επί του παρόντος, το πρωτόκολλο Representational State Transfer (REST) είναι η πιο χρησιμοποιούμενη διεπαφή Northbound και υλοποιείται στους περισσότερους ελεγκτές (Salman et al., 2016). Για να αξιοποιηθεί το πλεονεκτήματα και τα οφέλη που προσφέρει το πρωτόκολλο REST, πρέπει να τηρείται μια σειρά από αρχές κατά το σχεδιασμό του. Οι παραβιάσεις των αρχών σχεδιασμού REST έχουν ως αποτέλεσμα μη επεκτάσιμα και διαλειτουργικά APIs (Zhou et al., 2014).

2.3.10 Datapath

Το datapath αποτελεί τμήμα του επιπέδου δεδομένων που υλοποιεί τους κανόνες προώθησης. Τυπικά υλοποιείται στο μεταγωγέα ή στο δρομολογητή και είναι υπεύθυνο για τη διακίνηση των πακέτων μέσω του δικτύου. Το datapath ελέγχεται από τον ελεγκτή SDN, ο οποίος στέλνει εγγραφές ροής στο datapath, καθορίζοντας τον τρόπο προώθησης των πακέτων. Αυτές οι καταχωρήσεις ροής χρησιμοποιούνται για την ενημέρωση των πινάκων προώθησης στο datapath και τα πακέτα προωθούνται στη συνέχεια με βάση τις πληροφορίες που περιέχονται σε αυτούς τους πίνακες. Στο OpenFlow, το datapath αντιπροσωπεύεται από τον μεταγωγέα OpenFlow, ο οποίος είναι ένας μεταγωγέας λογισμικού ή υλικού που υλοποιεί το πρωτόκολλο OpenFlow και επικοινωνεί με τον ελεγκτή OpenFlow. Ο ελεγκτής OpenFlow στέλνει τις καταχωρήσεις ροής στο μεταγωγέα, καθορίζοντας τις ενέργειες που πρέπει να γίνουν στα πακέτα, όπως η προώθησή τους σε μια συγκεκριμένη θύρα ή η εφαρμογή μιας συγκεκριμένης πολιτικής ποιότητας υπηρεσίας (Quality of Services - QoS).

2.4 Προκλήσεις Ασφάλειας

Το δίκτυο βασισμένο στην τεχνολογία SDN παρέχει ένα κεντρικό έλεγχο στο δίκτυο, αν και αυτό απλοποιεί τη διαχείριση του δικτύου κάνοντας αποτελεσματική τη χρήση των πόρων, εισάγει νέες προκλήσεις για την αξιοπιστία και την ανθεκτικότητα του. Στην πραγματικότητα, ένας κεντρικός ελεγκτής αποτελεί το μοναδικό σημείο αστοχίας. Οι κατανεμημένες πλατφόρμες ελεγκτών SDN βελτιώνουν την αξιοπιστία και την επεκτασιμότητα σε κάποιο βαθμό, ωστόσο παραμένουν ευάλωτες σε επιθέσεις DDoS, ειδικά σε επίπεδο ελέγχου. Η επίτευξη ανθεκτικών δικτύων βασισμένα στην τεχνολογία SDN αποτελεί κορυφαίο σκοπό της δικτύωσης. Η αρχιτεκτονική SDN είναι ανθεκτική όταν έχει τη δυνατότητα να λειτουργεί υπό φορτίο, αστοχίες και επιθέσεις. Γενικά, η ανθεκτικότητα βασίζεται τόσο σε έννοιες αξιοπιστίας, όσο και σε έννοιες ασφάλειας. Όσον αφορά το SDN, η ανθεκτικότητα είναι η ικανότητα ενός ή περισσοτέρων στοιχείων της

αρχιτεκτονικής SDN, είτε στο επίπεδο ελέγχου, είτε στο επίπεδο δεδομένων, να ανακάμπτει γρήγορα και να συνεχίζει να λειτουργεί ακόμη και όταν υπάρχει βλάβη εξοπλισμού, διακοπή ρεύματος ή άλλη διαταραχή στο δίκτυο. Καθώς το δίκτυο SDN μπορεί να είναι επιρρεπές σε αστοχίες, η ανάπτυξη του πρωτοκόλλου OpenFlow στην έκδοση 1.2 συμπεριέλαβε τη δυνατότητα εφαρμογής διαμόρφωσης πρωτεύων (master) και εφεδρικού (slave) ελεγκτή για την αντιμετώπιση ελαττωματικών ελεγκτών OpenFlow και την αύξηση της ανθεκτικότητας του δικτύου.

Στην έρευνα τους οι (van Asten et al., 2014) εστιάζουν στο πρόβλημα αποτυχίας του ελεγκτή και προτείνουν τη χρήση εφεδρικού ελεγκτή για να μπορέσει να αναλάβει τον έλεγχο των εκχωρημένων μεταγωγέων. Η αποτυχία ενός μόνο ελεγκτή θα έχει ως αποτέλεσμα μόνο ένα ανεξέλεγκτο τμήμα του δικτύου. Για τη δημιουργία ενός ανθεκτικού δικτύου, η τοπολογία του δικτύου πρέπει να περιλαμβάνει πλεονάζουσες διαδρομές. Για ένα ανθεκτικό επίπεδο ελέγχου, η κατάσταση του δικτύου πρέπει να είναι συγχρονισμένη και πανομοιότυπη μεταξύ κύριου και εφεδρικού ελεγκτή. Οι πρόσθετες μονάδες και τα συστήματα συγχρονισμού πρέπει να πληρούν αυτές τις απαιτήσεις χωρίς να διακυβεύεται η απόδοση και να προστίθεται ανεπιθύμητη καθυστέρηση. Οι δυνατότητες για master-slave ελεγκτή του πρωτοκόλλου OpenFlow χρησιμοποιούνται για να παρέχουν ανθεκτικότητα στο δίκτυο. Αυτό υποδηλώνει ότι ένας πρωτεύων ελεγκτής έχει τον έλεγχο όλων των μεταγωγέων και σε περίπτωση αποτυχίας του, ένας εφεδρικός ελεγκτής μπορεί να αναλάβει τον έλεγχο των εκχωρημένων μεταγωγέων.

Οι (Yao et al., 2011) προτείνουν τον έλεγχο της διεύθυνσης πηγής (source address) κάθε νέας ροής για εντοπισμό και μετριασμό των επιθέσεων τύπου IP SYN flooding. Το υπάρχον σύστημα δρομολόγησης του διαδικτύου σχεδιάστηκε χωρίς να λαμβάνει υπόψη την εγκυρότητα της διεύθυνσης πηγής IP και αυτό το μειονέκτημα καθιστά δυνατές τις επιθέσεις με πλαστογραφημένη διεύθυνση πηγής (source IP address), όπως IP SYN flooding, Smurf και DNS amplification. Όταν προστίθεται μια νέα καταχώρηση ροής σε έναν μεταγωγέα SDN, ο μεταγωγέας στέλνει μήνυμα στον ελεγκτή SDN για να ζητήσει την έγκριση για τη νέα καταχώριση. Στη συνέχεια, ο ελεγκτής SDN επαληθεύει τη νέα καταχώρηση για να διασφαλιστεί η συμμόρφωση με τις πολιτικές και τους κανόνες δικτύου, συμπεριλαμβανομένου του ελέγχου για νέες διευθύνσεις πηγής IP. Η μεθοδολογία VAVE μπορεί να χρησιμοποιηθεί για τη βελτιστοποίηση της διαδικασίας ελέγχου νέων εισαγωγών ροής για νέες διευθύνσεις πηγής IP βελτιώνοντας τη χρήσης των πόρων στο δίκτυο. Αυτό μπορεί να επιτευχθεί με το μηχανισμό επικύρωσης διευθύνσεων πηγής VAVE μέσω της ανάλυση των προτύπων ροής του δικτύου χρησιμοποιώντας τεχνικές μάθησης βελτιστοποιώντας ταυτόχρονα τη χρήση των πόρων στο δίκτυο.

Οι (Rohrer et al., 2009) εξετάζουν έναν νέο μηχανισμό διαφοροποίησης της διαδρομής (Path Diversification - PD) που μπορεί να χρησιμοποιηθεί για την επιλογή πολλαπλών διαδρομών μεταξύ ζεύγους κόμβων για την επίτευξη της μέγιστης αξιοπιστίας της ροής. Ο μηχανισμός αποσκοπεί στη βελτίωση της ανθεκτικότητας του δικτύου παρέχοντας πολλαπλά μονοπάτια για τις ροές, αυξάνοντας έτσι την ικανότητα του δικτύου να αντέχει σε αστοχίες και επιθέσεις. Ο μηχανισμός PD λειτουργεί επιλέγοντας και διαφοροποιώντας δυναμικά τα μονοπάτια για κάθε ροή κυκλοφορίας με βάση ένα σύνολο μετρικών, όπως η συμφόρηση του δικτύου, η ποιότητα των συνδέσεων και η διαθεσιμότητα. Αυτό επιτυγχάνεται με το συνδυασμού του κεντρικού ελέγχου και των κατανεμημένων αλγορίθμων στην αρχιτεκτονική SDN. Ο κεντρικός ελεγκτής παρακολουθεί την κατάσταση του δικτύου και λαμβάνει αποφάσεις σχετικά με τη διαφοροποίηση των μονοπατιών με βάση τον τρέχοντα φόρτο κυκλοφορίας και τις συνθήκες του δικτύου, ενώ οι κατανεμημένοι αλγόριθμοι υλοποιούν τον μηχανισμό διαφοροποίησης μονοπατιών στους επιμέρους μεταγωγείς και δρομολογητές.

Οι συγγραφείς (Deng et al., 2019) εστιάζουν στην ανίχνευση των επιθέσεων DoS με βάσει στατιστικών ταξινομώντας την κυκλοφορίας ως κανονική ή κακόβουλη. Ο έλεγχος πραγματοποιείται καταγράφοντας τον αριθμό των θυρών που χρησιμοποιούνται από τις ενεργές συνδέσεις του κεντρικού υπολογιστή στο δίκτυο κατά την προηγούμενη χρονική περίοδο και εάν υπερβαίνει το ιστορικό μέγιστο, ο κεντρικός υπολογιστής θεωρείται ύποπτος. Στις μετρήσεις, χρησιμοποιείται το εργαλείο netstat του λειτουργικού συστήματος Linux για τη μέτρηση του αριθμού των ενεργών συνδέσεων του κεντρικού υπολογιστή. Για το μετριασμό τέτοιων επιθέσεων γίνεται η χρήση του λογισμικού DosDefender που έχει σχεδιαστεί να αμύνεται σε επιθέσεις DoS παρακολουθώντας την εισερχόμενη κυκλοφορία και εντοπίζοντας μοτίβα που υποδεικνύουν ότι μια επίθεση βρίσκεται σε εξέλιξη αποκλείοντας την κακόβουλη κίνηση και μετριάζοντας την επίθεση σε πραγματικό χρόνο.

Οι συγγραφείς (Li et al., 2016) προτείνουν ένα νέο πλαίσιο με την ονομασία FLOWGUARD για την προστασία των συστημάτων δικτύου από επιθέσεις DDoS χαμηλού ρυθμού. Το πλαίσιο FLOWGUARD έχει σχεδιαστεί για την ανίχνευση και το μετριασμό των επιθέσεων DDoS χαμηλού ρυθμού μέσω της δυναμικής προσαρμογής των τιμών κατωφλίου (threshold) για μηχανισμούς ανίχνευσης και απόκρισης βάσει ρυθμού. Το πλαίσιο FLOWGUARD αποτελείται από τρία κύρια στοιχεία: α) ένα μηχανισμό καθορισμού κατωφλίου, β) έναν μηχανισμό φιλτραρίσματος της κίνησης και γ) έναν μηχανισμό ανακατεύθυνσης της κίνησης. Ο μηχανισμός καθορισμού κατωφλίου προσαρμόζει δυναμικά τις τιμές κατωφλίου με βάση τα τρέχοντα μοτίβα κυκλοφορίας και τα χαρακτηριστικά των επιθέσεων επιτρέποντας στο πλαίσιο να ανιχνεύει

επιθέσεις DDoS χαμηλού ρυθμού που βρίσκονται κάτω από τις τιμές κατωφλίου. Ο μηχανισμός φιλτραρίσματος της κυκλοφορίας φιλτράρει την κυκλοφορία των επιθέσεων με βάση το μέγεθος των πακέτων, τον τύπο του πρωτοκόλλου και τον όγκο της κυκλοφορίας. Ο μηχανισμός ανακατεύθυνσης της κυκλοφορίας ανακατευθύνει τη νόμιμη κυκλοφορία σε καθορισμένους διακομιστές, ενώ εμποδίζει ταυτόχρονα την κυκλοφορία των επιθέσεων. Συνδυάζοντας αυτούς τους μηχανισμούς, το πλαίσιο FLOWGUARD είναι σε θέση να ανιχνεύσει και να μετριάσει αποτελεσματικά τις επιθέσεις DDoS χαμηλού ρυθμού χωρίς να επηρεάσει τη νόμιμη κυκλοφορία.

Στην εργασία τους οι (Kotani and Okabe, 2014) προτείνουν έναν νέο μηχανισμό με την ονομασία Packet-In Filter που μειώνει τον αριθμό των μηνυμάτων Packet-In που δημιουργούνται από τον ελεγκτή OpenFlow ως απόκριση σε συμβάντα δικτύου, όπως ροές κυκλοφορίας που δεν ταιριάζουν με κανέναν προϋπάρχοντα κανόνα. Με τη μείωση του αριθμού των μηνυμάτων Packet-In, οι συγγραφείς στοχεύουν στη μείωση του φόρτου στον ελεγκτή και στη βελτίωση της συνολικής απόδοσης και επεκτασιμότητας του δικτύου OpenFlow. Όταν ο ελεγκτής λαμβάνει μηνύματα Packet-In, εγκαθιστά νέες καταχωρήσεις ροής στους μεταγωγείς το συντομότερο δυνατό και προωθεί τα πακέτα που περιλαμβάνονται στα μηνύματα Packet-In. Παρόλο που συνιστάται η εγκατάσταση των περισσότερων καταχωρήσεων ροής πριν από τη λήψη των πακέτων, ο ελεγκτής χρειάζεται ορισμένα μηνύματα Packet-In για να μάθει τις καταστάσεις δικτύου από τα πακέτα, όπως η εκμάθηση διευθύνσεων MAC και η ανίχνευση της πηγής. Με τον προτεινόμενο μηχανισμό, ελέγχονται τα πακέτα που δεν ταιριάζουν με καμία καταχώρηση στους πίνακες ροής, ώστε να διατηρείται χαμηλό φορτίο στους μεταγωγείς.

Στην μελέτη τους οι (Sezer et al., 2013) εστιάζουν στην επεκτασιμότητα του ελεγκτή, όπου εντοπίζουν τρεις κύριες προκλήσεις. Η πρώτη αφορά την καθυστέρηση που εισάγεται από την ανταλλαγή πληροφοριών δικτύου μεταξύ πολλαπλών κόμβων και ενός μόνο ελεγκτή. Η δεύτερη αφορά τον τρόπο με τον οποίο οι ελεγκτές SDN επικοινωνούν με άλλους ελεγκτές χρησιμοποιώντας τα Eastbound και Westbound APIs και η τρίτη πρόκληση σχετίζεται με το μέγεθος και τη λειτουργία της back-end βάσης δεδομένων του ελεγκτή. Όσο αφορά το ζήτημα της καθυστέρησης, συστήνεται μια κατανεμημένη υποδομή ελεγκτών οι οποίοι θα διαμοιράζονται την επικοινωνία μεταξύ των πολλαπλών κόμβων. Ωστόσο, η προσέγγιση αυτή δεν εξαλείφει τη δεύτερη πρόκληση των αλληλεπιδράσεων μεταξύ των ελεγκτών, για την οποία απαιτείται συνολική θεώρηση του δικτύου. Για να δημιουργηθούν ανθεκτικά δίκτυα, απαιτούνται εναλλακτικές διαδρομές και δευτερεύων εξοπλισμός. Σε ένα αμιγώς SDN περιβάλλον, ένας μόνο ελεγκτής ή μια ομάδα ελεγκτών θα παρέχει υπηρεσίες επιπέδου ελέγχου για έναν ευρύτερο αριθμό κόμβων προώθησης δεδομένων, επιτρέποντας έτσι μια συστημική άποψη των πόρων του

δικτύου. Οι προσεγγίσεις που εξετάστηκαν περιλαμβάνουν την προσθήκη ενός επιπέδου ενορχήστρωσης μέσω API στο οποίο μπορούν να χρησιμοποιήσουν τα στοιχεία εφαρμογών για να ζητήσουν την επιθυμητή απόδοση από το επίπεδο μεταφοράς. Από διάφορους οργανισμούς έχει προταθεί μια επέκταση του μοντέλου δεδομένων βελτιστοποίησης της κυκλοφορίας σε επίπεδο εφαρμογής (Application Layer Traffic Optimization - ALTO), στο οποίο ο διακομιστής ALTO φιλοξενεί συγκεντρωτικές πληροφορίες με τις οποίες κάθε ελεγκτής έχει σύνδεση.

Οι (Oktian et al., 2015) ανέδειξαν τα προβλήματα ασφάλειας που σχετίζονται με τις ευπάθειες των εφαρμογών που αφορούν το Northbound API. Το SDN επιτρέπει την αξιοποίηση του ελέγχου του δικτύου από εφαρμογές τρίτων μέσω του Northbound API Interface (NBI). Σήμερα, υπάρχουν διάφορα NBIs, ειδικά για τους ελεγκτές όπως τα REST API και Java API. Ωστόσο, οι περισσότερες από τις τρέχουσες υλοποιήσεις του Northbound API δεν συμπεριλαμβάνουν την πτυχή της ασφάλειας. Ως εκ τούτου, το ONF δημιούργησε ομάδα εργασίας για την τυποποίησή τους. Το REST API παρέχει απλή ενσωμάτωση και επιτρέπει την αλληλεπίδραση με ελάχιστη επιβάρυνση μεταξύ πελατών και διακομιστών. Για το λόγο αυτό πολλές εταιρείες όπως το Facebook και η Google χρησιμοποιούν το REST API για την παροχή των υπηρεσιών τους. Οι περισσότεροι ελεγκτές SDN σήμερα χρησιμοποιούν τη διεπαφή REST NBI για την παροχή πληροφοριών δικτύου στις περιπτώσεις τρίτων. Στην παρούσα εργασία, οι συγγραφείς σχεδιάζουν REST NBI για ελεγκτές SDN, υλοποιώντας διαδικασίες ελέγχου ταυτότητας και εξουσιοδότησης με token χρησιμοποιώντας το πρωτόκολλο OAuth 2.0. Ο σχεδιασμός αυτός παρέχει τα τέσσερα βασικά χαρακτηριστικά της ασφαλείας: α) πιστοποίηση ταυτότητας, β) εξουσιοδότηση, γ) κρυπτογράφηση και δ) ακεραιότητα. Η αυθεντικοποίηση και η εξουσιοδότηση διασφαλίζονται με εφαρμογή του πρωτοκόλλου OAuth 2.0. Η κρυπτογράφηση πραγματοποιείται με τη χρήση του TLS και η ακεραιότητα των μηνυμάτων REST NBI παρέχετε χρησιμοποιώντας JSON Web Token (JWT).

2.5 Πεδία Εφαρμογών

Τα πανεπιστημιακά δίκτυα, που μπορούν να θεωρηθούν ως μια ειδική περίπτωση δικτύων με αυστηρές απαιτήσεις όσο αφορά την ασφάλεια και την απόδοση, πολλές από τις συσκευές σύνδεσης είναι προσωρινές και δεν βρίσκονται υπό τον έλεγχο του πανεπιστημίου, θέτοντας πρόσθετες προκλήσεις ασφάλειας και κατανομής πόρων. Επιπλέον, απαιτείται συχνά η υποστήριξη σε ερευνητικά testbeds και πειραματικά πρωτόκολλα. Η επαρκής διαχείριση είναι εξαιρετικά σημαντική για τα πανεπιστήμια και το SDN μπορεί να χρησιμοποιηθεί για την

προγραμματιστική προσαρμογή πολιτικών δικτύου, καθώς και για τη βοήθεια στην παρακολούθηση της δραστηριότητας και τη ρύθμιση της απόδοσης του δικτύου. Τα SDN testbeds έχουν παρακινήσει αρκετούς ερευνητές δικτύων να εκτελέσουν τα πρωτότυπα και τα πειράματά τους, καθώς και να δημιουργήσουν νέες αρχιτεκτονικές για το διαδίκτυο. Όπως αναφέρουν οι συγγραφείς (Huang et al., 2017) στην έρευνα τους, στα testbeds χωρίς SDN, οι διαχειριστές των testbeds πρέπει να ρυθμίσουν πολλές συσκευές δικτύου ξεχωριστά για να εγκαταστήσουν ένα πειραματικό περιβάλλον, το οποίο είναι χρονοβόρο και επιρρεπές σε σφάλματα. Ωστόσο, τα δοκιμαστικά περιβάλλοντα δικτύου που βασίζονται στο SDN θα μπορούν να ολοκληρώσουν τις περισσότερες διαδικασίες εγκατάστασης αυτόματα μέσω των προγραμματιστικών APIs.

Τα μεγάλα κέντρα δεδομένων (data centers) έχουν εξελιχθεί τα τελευταία χρόνια, προσπαθώντας διαρκώς να ανταποκριθούν στην ολοένα υψηλότερη και ταχέως μεταβαλλόμενη ζήτηση. Η διαχείριση της κίνησης και η επιβολή πολιτικών είναι μείζονος σημασίας κατά τη λειτουργία σε τόσο μεγάλες κλίμακες, ειδικά όταν υπάρχει διακοπή της υπηρεσίας ή πρόσθετη καθυστέρηση που μπορεί να οδηγήσει σε μαζική απώλεια παραγωγικότητας και κέρδους. Οι (Heller et al., n.d.) αναφέρουν ότι μεγάλο μέρος της έρευνας έχει επικεντρωθεί στη βελτίωση των διακομιστών και της ψύξης (70% της συνολικής ενέργειας) μέσω καλύτερης διαχείρισης υλικού ή λογισμικού. Στην έρευνα τους προτείνουν το ElasticTree, έναν διαχειριστή ενέργειας για όλο το δίκτυο που χρησιμοποιεί το SDN για να βρίσκει το υποσύνολο του δικτύου με την ελάχιστη ισχύ που ικανοποιεί τις τρέχουσες συνθήκες κίνησης και απενεργοποιεί τους διακόπτες που δεν χρειάζονται. Ως αποτέλεσμα, παρουσιάζουν εξοικονόμηση ενέργειας μεταξύ 25-62% υπό διαφορετικές συνθήκες κυκλοφορίας.

Σύμφωνα με τους (Mehdi et al., n.d.), η ανάπτυξη ενός συστήματος ανίχνευσης ανωμαλιών στο παραδοσιακό δικτύου είναι δύσκολη κυρίως λόγω του ότι τα συστήματα παρέχουν περιορισμένες πληροφορίες. Στο SDN ωστόσο, το επίπεδο ελέγχου έχει μια ολοκληρωμένη προβολή του δικτύου, γεγονός που διευκολύνει την εφαρμογή μηχανισμών ανίχνευσης. Οι συγγραφείς παρουσιάζουν τις δυνατότητες ανίχνευσης επιθέσεων με χρήση SDN. Η μελέτη τους δείχνει ότι το SDN είναι κατάλληλο για τον μετριασμό των επιθέσεων DDoS, κυρίως λόγω της χρήσης τυποποιημένων πρωτοκόλλων, υπηρεσιών και διεπαφών, διευκολύνοντας έτσι την ανάπτυξη νέων λύσεων. Μπορούν να χρησιμοποιηθούν διάφορες στρατηγικές για την ανίχνευση και τον μετριασμό των επιθέσεων DDoS όπως ταξινόμηση των ενεργειών με βάση τη χρήση μηχανικής μάθησης για την ανίχνευση ή σε λύσεις εξισορρόπησης φορτίου. Καθώς η εξισορρόπηση φορτίου δεν είναι αποτελεσματική κατά τη διάρκεια μιας επίθεσης DDoS, μπορεί να είναι αναγκαίος ένας διαχωρισμός των ροών όταν το δίκτυο είναι υπερφορτωμένο. Αυτό μπορεί να αυξήσει τις

πιθανότητες ανοχής μιας επίθεσης DDoS. Στην μελέτη τους παρουσιάζουν έναν μηχανισμό για την προστασία του μονοπατιού ελέγχου (control path) από επιθέσεις DDoS μέσω της κλιμάκωσης της χωρητικότητας του καναλιού ελέγχου. Αυτό επιτρέπει στο δίκτυο να διαχειρίζεται μεγάλο αριθμό ροών καθιστώντας το επίπεδο ελέγχου πιο ανθεκτικό.

2.6 Ο ρόλος του SDN στην cloud εποχή

Η δικτύωση που καθορίζεται από το λογισμικό έχει αναδειχθεί σε βασική τεχνολογία στην εποχή του υπολογιστικού νέφους, των μεγάλων δεδομένων και του IoT. Η συγκεντρωτική διαχείριση που παρέχει το SDN, προσφέρει καλύτερη ορατότητα και έλεγχο του δικτύου, γεγονός που οδηγεί σε βελτιωμένη απόδοση, επεκτασιμότητα και ασφάλεια του. Το SDN συμβάλει καθοριστικά στην παροχή μιας ευέλικτης και επεκτάσιμης υποδομής που μπορεί να υποστηρίξει τις αναδυόμενες τάσεις και τεχνολογίες, όπως την υπολογιστική των άκρων (edge computing) και το IoT. Με την αυξανόμενη υιοθέτηση των υπηρεσιών που βασίζονται στο cloud, το SDN προσφέρει κεντρική διαχείριση των πόρων του δικτύου, η οποία μειώνει την πολυπλοκότητα της διαχείρισης των κατανεμημένων δικτύων. Επιτρέπει την εικονικοποίηση των δικτυακών πόρων και τη δημιουργία πολλαπλών εικονικών δικτύων σε μια ενιαία φυσική δικτυακή υποδομή παρέχοντας απομόνωση και ασφάλεια για διαφορετικούς μισθωτές και εφαρμογές. Η δυναμική κατανομή των πόρων του δικτύου με βάση τις απαιτήσεις των εφαρμογών μπορεί να παρέχει βελτιωμένη απόδοση και μειωμένη καθυστέρηση. Η δυναμική κατανομή των πόρων είναι ιδιαίτερα σημαντική καθώς επιτρέπει στους οργανισμούς να επεξεργάζονται και να αναλύουν μεγάλο όγκο δεδομένων σε πραγματικό χρόνο και σε διαφορετικά περιβάλλοντα cloud. Η ικανότητά του να βελτιώνει τη διαθεσιμότητα του δικτύου, προσφέρει αποτελεσματικότερη διαχείριση των πόρων, η οποία μπορεί να συμβάλει στη μείωση του χρόνου διακοπής της λειτουργίας των υπηρεσιών, διασφαλίζοντας ότι τα κρίσιμα δεδομένα και οι εφαρμογές είναι πάντα προσβάσιμα.

Η εποχή του διαδικτύου των πραγμάτων χαρακτηρίζεται από τον πολλαπλασιασμό των συνδεδεμένων συσκευών, οι οποίες παράγουν μεγάλο όγκο δεδομένων οδηγώντας στην ανάγκη για πιο ευέλικτη και επεκτάσιμη δικτυακή υποδομή. Ένα από τα βασικά οφέλη που προσφέρει το SDN είναι η ικανότητα διαχείρισης και η δυναμική παροχή πόρων στο δίκτυο. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας έναν κεντρικό ελεγκτή για την παρακολούθηση της κυκλοφορίας και της χρήσης των πόρων των συσκευών IoT. Η λήψη αποφάσεων σχετικά με τον τρόπο κατανομής των πόρων μπορεί να συμβάλει στη βελτίωση της απόδοση του δικτύου. Η εικονικοποίηση SDN μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός εικονικού δικτύου, με

συγκεκριμένες πολιτικές και απαιτήσεις QoS για διαφορετικούς τύπους συσκευών IoT. Η χρήση των εικονικών δικτύων θα βελτιώσει την απόδοση και την ασφάλεια του δικτύου, διασφαλίζοντας ότι οι πόροι του δικτύου προορίζονται για συγκεκριμένες εφαρμογές ή υπηρεσίες.

Καθοριστικός είναι ρόλο που μπορεί να διαδραματίσει η τεχνολογία SDN στο edge computing καθώς συμβάλει στη βελτιστοποίηση της χρήσης των πόρων, μειώνοντας τη συμφόρηση του δικτύου και βελτιώνοντας της συνολικής απόδοσης του σε κατανεμημένα περιβάλλοντα. Το SDN μπορεί να συμβάλει στη γεφύρωση του χάσματος μεταξύ του edge computing και των παραδοσιακών περιβαλλόντων υπολογιστικού νέφους καθορίζοντας το τόπο που πρέπει να διεκπεραιωθούν συγκεκριμένες εργασίες. Η χρήση του SDN για τη λήψη αυτών των αποφάσεων μπορεί να βοηθήσει στη βελτιστοποίηση της χρήσης των πόρων, στη μείωση της συμφόρησης δικτύου και στη βελτίωση της συνολικής απόδοσης. Χρησιμοποιώντας τεχνολογία SDN, οι οργανισμοί μπορούν να επωφεληθούν πλήρως από τα πλεονεκτήματα του edge computing, διατηρώντας παράλληλα την ευελιξία και την επεκτασιμότητα των παραδοσιακών περιβαλλόντων υπολογιστικού νέφους.

Κεφάλαιο 3
Μεθοδολογία

3.1 Σκοπός

Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι να εξετάσουμε κατά πόσο τα δίκτυα βασισμένα στην τεχνολογία SDN μπορούν να προσφέρουν την απαιτούμενη ανθεκτικότητα σε επιθέσεις DDoS. Μέσω της βιβλιογραφικής ανασκόπησης μελετήσαμε την τεχνολογία SDN, τις υφιστάμενες λύσεις και προτάσεις για τη βελτίωση της ασφάλειας τους, ωστόσο εστιάσαμε και στις ανησυχίες που εγείρουν οι ερευνητές σε θέματα που αφορούν το σχεδιασμό και την ανθεκτικότητα τους. Για τις μετρήσεις της ανθεκτικότητας χρησιμοποιήσαμε εικονικό εργαστηριακό περιβάλλον χρησιμοποιώντας τα προγράμματα VirtualBox, ONOS και Mininet. Το εικονικό περιβάλλον μας επέτρεψε στη δημιουργία μιας ελεγχόμενης και επαναλαμβανόμενης προσομοίωσης δικτύου, η οποία ήταν απαραίτητη για τη δοκιμή και τη βελτίωση της ανθεκτικότητας ενός δικτύου SDN. Το πρώτο βήμα αφορούσε την εγκατάσταση και διαμόρφωση του ελεγκτή ONOS, το οποίο μας παρέχει ένα κεντρικό σημείο ελέγχου για το δίκτυο επιτρέποντας μας την εύκολη διαμόρφωση και διαχείριση των συσκευών του δικτύου. Διαθέτει επίσης χαρακτηριστικά όπως οι κανόνες ροής και η τοπολογία δικτύου, τα οποία είναι απαραίτητα συστατικά για τα δίκτυα SDN.

Ακολούθως, για τη δημιουργία της εικονικής τοπολογίας δικτύου εντός του εργαστηριακού περιβάλλοντος χρησιμοποιήσαμε τον εξομοιωτή δικτύων Mininet. Ο σχεδιασμός της τοπολογίας περιλάμβανε μεταγωγείς, υπολογιστές και διακομιστές με σκοπό τον έλεγχο της ανθεκτικότητας του δικτύου SDN να διαχειρίζεται τις επιθέσεις DDoS. Το Mininet προσφέρει επίσης εργαλεία όπως το iPerf για τη μέτρηση της καθυστέρησης (latency) και της ταχύτητα (bandwidth) του δικτύου. Χρησιμοποιώντας το πρόγραμμα iPerf καθορίσαμε το σημείο αναφοράς (baseline) για τον εντοπισμό των αποκλίσεων που μπορεί να υποδηλώνουν μη φυσιολογική ή κακόβουλη δραστηριότητα. Στη συνέχεια, προσομοιώσαμε τις επιθέσεις DDoS με τη δημιουργία κίνησης χρησιμοποιώντας το εργαλείο hping3. Η απόδοση του δικτύου μετρήθηκε με τη χρήση του εργαλείου iPerf κατά τη διάρκεια της επίθεσης για να προσδιοριστεί ο αντίκτυπος της επίθεσης στην απόδοση του δικτύου. Αναλύσαμε τα αποτελέσματα των δοκιμών για να προσδιοριστεί η ανθεκτικότητα του δικτύου SDN όσον αφορά τον μετριασμό της επίθεσης. Ο αντίκτυπος της επίθεσης μετρήθηκε ποσοτικά με βάση την καθυστέρηση, το εύρος ζώνης, το φορτίο του ελεγκτή και την ταχύτητα λήψης αρχείου από διακομιστή ιστού του δικτύου. Η ανάλυση μας παρείχε πολύτιμες πληροφορίες σχετικά με την απόδοση και την ανθεκτικότητα του δικτύου, οι οποίες μπορούν να χρησιμοποιηθούν για τη βελτίωση και τη διαμόρφωση του.

3.2 Είδος έρευνας

Η χρήση της ποσοτικής έρευνας έχει ως στόχο τη μέτρηση ή την ποσοτικοποίηση ενός φαινομένου ή μιας συμπεριφοράς. Στην προκειμένη περίπτωση, ο στόχος μας ήταν να μετρηθεί η απόδοση της ανθεκτικότητας του δικτύου SDN κατά την προσομοίωση επίθεσης DDoS. Ο σκοπός ήταν να ποσοτικοποιηθεί ο αντίκτυπος της επίθεσης για να εντοπίσουμε τις συσχετίσεις και τις αιτιώδεις σχέσεις μεταξύ των μεταβλητών (καθυστέρηση / ταχύτητα). Χρησιμοποιώντας ποσοτικά μέτρα όπως τα πακέτα ανά δευτερόλεπτο, η απόδοση και ο χρόνος απόκρισης, μπορέσαμε να αξιολογήσουμε την απόδοση του δικτύου SDN. Στο πλαίσιο του ελέγχου της ανθεκτικότητας του δικτύου η ποσοτική έρευνα ήταν ιδιαίτερα αποτελεσματική, διότι μας επέτρεψε να συλλέξουμε και να αναλύσουμε τα δεδομένα με συστηματικό και αντικειμενικό τρόπο. Σε αντίθεση με την ποσοτική έρευνα, η ποιοτική έρευνα περιλαμβάνει τη συλλογή δεδομένων μέσω συνεντεύξεων ανοικτού τύπου, ομάδων ή παρατήρησης και βασίζεται σε υποκειμενικές ερμηνείες των δεδομένων αυτών. Η προσέγγιση αυτή δεν θα μας παρείχε το επίπεδο της λεπτομέρειας και της ακρίβειας που απαιτείται για την αξιολόγηση της απόδοσης της ανθεκτικότητας ενός δίκτυού SDN με αντικειμενικό τρόπο. Τα δεδομένα που συλλέξαμε στη συνέχεια αναλυθήκαν στατιστικά για να προσδιοριστεί η αποτελεσματικότητα του δικτύου SDN στην αντιμετώπιση της επίθεσης.

3.3 Ερευνητικά ερωτήματα

Τα ερευνητικά ερωτήματα επικεντρώνονται στην ποσοτικοποίηση συγκεκριμένων πτυχών των επιδόσεων και της ανθεκτικότητάς του δικτύου SDN σε επιθέσεις DDoS. Με τη συλλογή και την ανάλυση των δεδομένων που σχετίζονται με αυτά τα ερωτήματα, είναι δυνατόν να αποκτηθούν γνώσεις σχετικά με την αποτελεσματικότητα των δικτύων SDN όσον αφορά την αντιμετώπιση των επιθέσεων DDoS αλλά και να εντοπιστούν τομείς για τη βελτίωση του. Ορισμένα πιθανά ερευνητικά ερωτήματα θα μπορούσαν να προκύψουν είναι τα εξής:

- Ποιες είναι οι βέλτιστες πρακτικές για την υλοποίηση ανθεκτικών δικτύων SDN και πώς μπορούν να βελτιστοποιηθούν αυτές οι πρακτικές ώστε να βελτιωθεί η συνολική ανθεκτικότητα του δικτύου SDN;

- Ποια είναι η αποτελεσματικότητα του συστήματος IDS/IPS στην ενίσχυση της ανθεκτικότητας του ελεγκτή ONOS έναντι επιθέσεων TCP SYN flood DDoS;

- Πόσο αποτελεσματικό είναι το δίκτυο SDN στο μετριασμό μιας επίθεσης DDoS και πώς μεταβάλλεται η αποτελεσματικότητά του με διαφορετικές εντάσεις επίθεσης;

- Ποια είναι η σχέση μεταξύ της καθυστέρησης, του εύρους ζώνης και της ικανότητας του δικτύου SDN να αντιμετωπίζει μια επίθεση DDoS;

3.4 Μεθοδολογίας κύκλου ζωής ανάπτυξης λογισμικού

Στο πλαίσιο της ανάπτυξης ενός δικτύου SDN και στον έλεγχο της ανθεκτικότητάς του σε ένα εικονικό εργαστηριακό περιβάλλον, η επιλογή της σωστής μεθοδολογίας κύκλου ζωής ανάπτυξης λογισμικού (Software Development Life Cycle - SDLC) είναι ζωτικής σημασίας. Δύο δημοφιλείς μεθοδολογίες SDLC είναι η ευέλικτη (agile) και η μεθοδολογία καταρράκτη (waterfall). Η ευέλικτη μοντελοποίηση είναι η μεθοδολογία που έχουμε επιλέξει για τις δοκιμές μας. Είναι βασισμένη στην πρακτική για τη μοντελοποίηση και την τεκμηρίωση συστημάτων που βασίζονται σε λογισμικό. Σκοπός της είναι να αποτελέσει μια συλλογή αξιών, αρχών και πρακτικών για τη μοντελοποίηση λογισμικού που μπορούν να εφαρμοστούν σε ένα έργο ανάπτυξης λογισμικού με πιο ευέλικτο τρόπο από τις παραδοσιακές μεθόδους μοντελοποίηση (Murugaiyan, 2012). Δίνει έμφαση στη συνεργασία, τις συχνές δοκιμές, την ανατροφοδότηση και την σταδιακή παράδοση λειτουργικού

λογισμικού. Είναι κατάλληλη για πολύπλοκα και εξελισσόμενα έργα όπως τα δίκτυα SDN που απαιτούν ευελιξία και προσαρμοστικότητα. Παραδίδοντας λειτουργικό λογισμικό σε μικρά βήματα, μπορούμε να δοκιμάσουμε και να βελτιώσουμε τα χαρακτηριστικά ασφαλείας του συστήματος σε διάφορους τύπους επιθέσεων. Η επαναληπτική προσέγγιση μας επιτρέπει να εντοπίσουμε και να διορθώσουμε τα τρωτά σημεία ασφαλείας καθώς προκύπτουν, διασφαλίζοντας ότι το σύστημα είναι ασφαλές και ανθεκτικό. Το μοντέλο καταρράκτη είναι μια διαδοχική διαδικασία σχεδιασμού, που χρησιμοποιείται συχνά σε διαδικασίες ανάπτυξης λογισμικού, στην οποία η πρόοδος θεωρείται ότι ρέει σταθερά προς τα κάτω (σαν καταρράκτης) μέσω των φάσεων (Murugaiyan, 2012). Αποτελεί μια γραμμική διαδοχική μεθοδολογία SDLC που περιλαμβάνει την ολοκλήρωση κάθε φάσης της διαδικασίας ανάπτυξης πριν προχωρήσει στην επόμενη. Ο καταρράκτης είναι πιο άκαμπτος και δεν είναι κατάλληλος για πολύπλοκα ή εξελισσόμενα έργα όπως τα δίκτυα SDN. Ωστόσο, ο καταρράκτης είναι χρήσιμος για έργα όπου οι απαιτήσεις είναι σαφώς καθορισμένες και είναι απίθανο να αλλάξουν.

Κεφάλαιο 4
Υλοποίηση

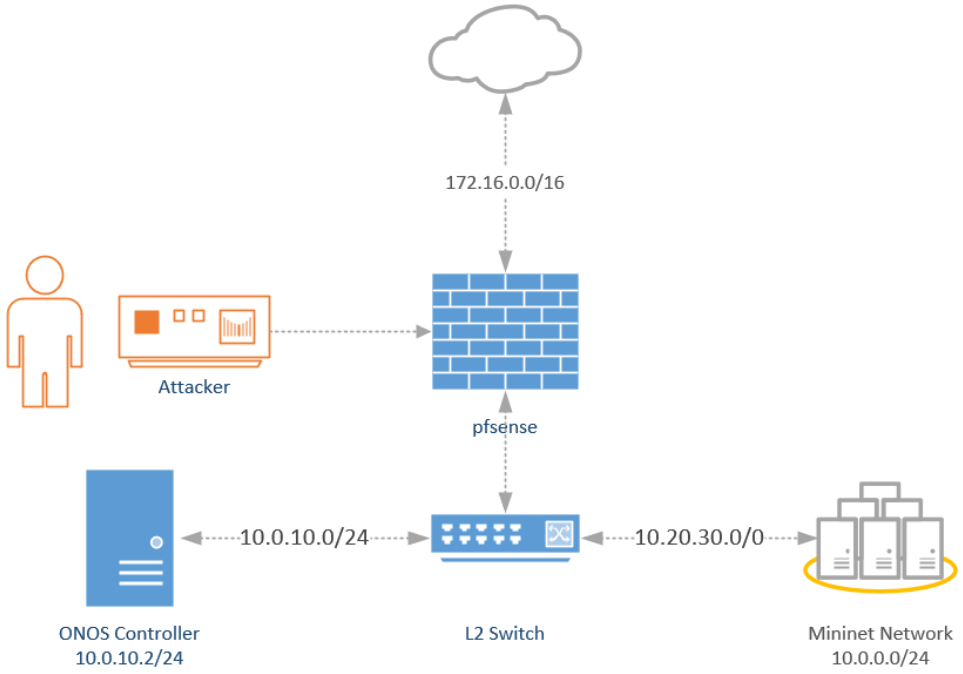
4.1 Προσομοίωση περιβάλλοντος δικτύου SDN

Για την υλοποίηση της προσομοίωσης του περιβάλλοντος δικτύου SDN χρησιμοποιήσαμε εικονικά μηχανικά (Virtual Machines - VMs) με λειτουργικά συστήματα (Operating System) Ubuntu 18.04 LTS και FreeBSD 12.3. Για την δημιουργία των VMs κάναμε χρήση το λογισμικό εικονικοποίησης ανοιχτού κώδικα Oracle VirtualBox. v6.1.30. Τα πιο πάνω εικονικά μηχανήματα φιλοξενούνται (host) σε μηχάνημα με λειτουργικό σύστημα Windows 10 Pro 64bits, 16G RAM και επεξεργαστή Intel Core i7. Το πρώτο εικονικό μηχάνημα έχει χρησιμοποιηθεί για την εγκατάσταση του ελεγκτή ONOS, ενώ το δεύτερο μηχάνημα για τη εγκατάσταση του εξομοιωτή δικτύων Mininet και του πρότυπου για την παρακολούθηση της κυκλοφορίας του δικτύου sFlow-RT. Η μηχανή ONOS έγινε κλώνος (clone) έτσι ώστε να υπάρχει η δυνατότητα για δημιουργία τοπολογίας δικτύου με δυο ελεγκτές. Η διευθυνσιοδότηση IPv4 των μηχανημάτων γίνεται μέσω μια τρίτης εικονικής μηχανικής στην οποία έχουμε εγκαταστήσει το ανοικτού κώδικα pfSense (εικόνα 8) για τη υλοποίηση του τείχους προστασίας και δρομολόγησης των δικτύων. Όλες οι VMs είναι συνδεδεμένες στο ίδιο εικονικό switch χωρίς όμως αυτό να κρίνεται απαραίτητο. Αναλυτικά

οι IPv4 διευθύνσεις των μηχανημάτων παρουσιάζονται στον πίνακα 1 ενώ το σχεδιάγραμμα της τοπολογίας του δικτύου στην εικόνα 8:

Virtual Machine	Hostname	Network	IP address	Gateway
ONOS Controller	onos	10.0.10.0/24	10.010.11 - DHCP Client	10.0.10.1
Mininet	mininet	10.0.10.0/24	10.0.10.3	10.0.10.1
pfSense (WAN)	pfsense	172.16.0.0/16	172.16.255.242 - DHCP Client	172.16.0.1
pfSense (LAN)	pfsense	10.010.0/24	10.010.1	10.010.1

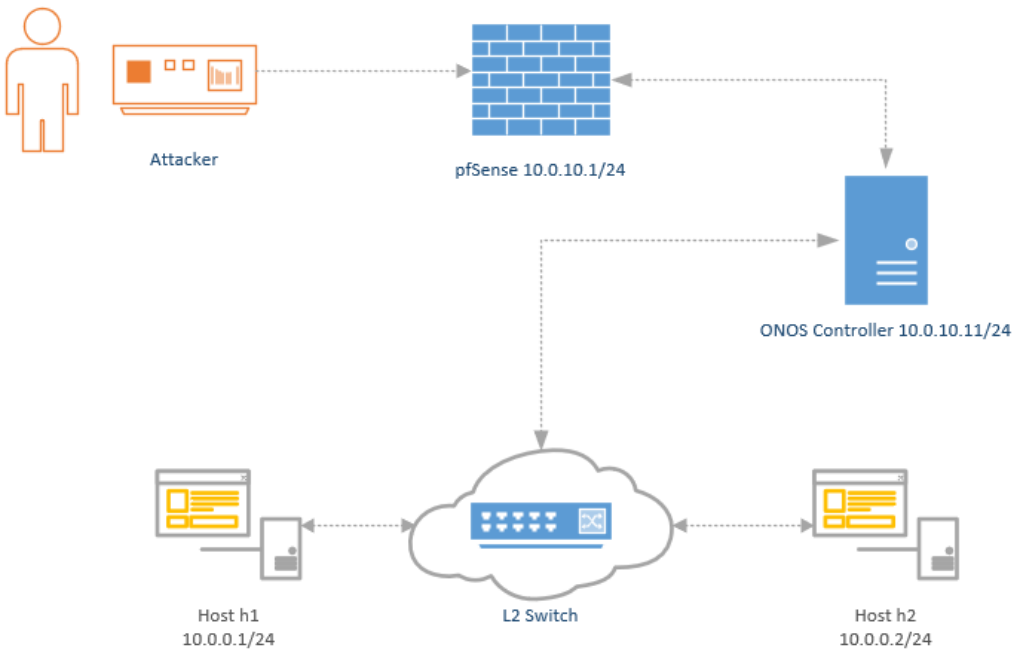
Πίνακας 1: IP διευθύνσεις



Εικόνα 8: Διάγραμμα υλοποίηση προσομοίωσης περιβάλλοντος δικτύου SDN

Χρησιμοποιώντας το διαχειριστή πακέτων Ubuntu, εγκαταστήσαμε τα απαραίτητα πακέτα για τον ελεγκτή ONOS, το Mininet και το sFlow-RT, συμπεριλαμβανομένων των Java, Git, curl και άλλων εξαρτήσεων (dependencies) που απαιτούνται για τη δημιουργία και την εκτέλεση του ONOS. Για την εκτέλεση της προσομοίωσης ξεκινήσαμε τον ελεγκτή ONOS (εκκίνηση της

υπηρεσίας -services- ONOS) και στη συνέχεια, τρέξαμε το Mininet συνδέοντας το με τον απομακρυσμένο ελεγκτή για τη δημιουργία της τοπολογία του εικονικού δικτύου (εικόνα 9).



Εικόνα 9: Τοπολογία Mininet

Χρησιμοποιώντας την εντολή «*pingall*» ελέγξαμε τη συνδεσιμότητα μεταξύ όλων των κεντρικών υπολογιστών (hosts) στην τοπολογία και διασφαλίσαμε ότι ο ελεγκτής ONOS λειτουργεί σωστά. Τρέχοντας παράλληλα το sFlow-RT συλλέξαμε στατιστικά στοιχεία σχετικά με την κίνηση που διέρχεται από την τοπολογία Mininet για να αναλυθούν στη συνέχεια και να εντοπιστούν τυχόν πιθανά προβλήματα σχετικά με την ανθεκτικότητα του δικτύου.

4.2 Εργαλεία προσομοίωσης

4.2.1 Mininet

Το Mininet αποτελεί εξομοιωτή δικτύου ανοιχτού κώδικα που επιτρέπει στους χρήστες να δημιουργούν εικονικά δίκτυα που καθορίζονται από το λογισμικό. Το Mininet υποστηρίζει μια μεγάλη ποικιλία συσκευών δικτύου, συμπεριλαμβανομένων μεταγωγέων OpenFlow και κεντρικών υπολογιστών. Παρέχει επίσης διεπαφή γραμμής εντολών (CLI) και Python API που επιτρέπει στους χρήστες να δημιουργούν και να χειρίζονται εικονικά δίκτυα, καθώς και να αλληλοεπιδρούν με τις συσκευές του δικτύου. Αυτό επιτρέπει στους χρήστες να δοκιμάζουν

εύκολα τοπολογίες δικτύου, πρωτόκολλα και ελεγκτές χωρίς την ανάγκη φυσικού υλικού. Προσφέρει μια σειρά από ενσωματωμένα παραδείγματα και σεμινάρια και μπορεί να χρησιμοποιηθούν σε συνδυασμό με άλλα εργαλεία ανοιχτού κώδικα όπως το Wireshark, το tshark και το tcpdump για την καταγραφή και την ανάλυση της κυκλοφορίας του δικτύου. Ενσωματώνει επίσης την εξομοίωση παραδοσιακών δικτύων, χρησιμοποιώντας Linux bridges και Open vSwitch (OVS) αντί για τους μεταγωγείς OpenFlow.

4.2.2 ONOS

Το ONOS (Open Network Operating System) αποτελεί πλατφόρμα ελεγκτή δικτύων ανοιχτού κώδικα, καθορισμένη από λογισμικό. Έχει σχεδιαστεί για να είναι επεκτάσιμο, ανεκτικό σε σφάλματα και μπορεί να χρησιμοποιηθεί για τον έλεγχο και τη διαχείριση μιας μεγάλης ποικιλίας συσκευών δικτύου, συμπεριλαμβανομένων μεταγωγέων OpenFlow και δρομολογητών. Το ONOS διαθέτει παραλλαγές σε γραφικό περιβάλλον χρήστη (Graphical User Interface - GUI) και CLI και είναι χτισμένο σε μια αρθρωτή αρχιτεκτονική που επιτρέπει την εύκολη προσθήκη νέων χαρακτηριστικών και πρωτοκόλλων προσφέροντας υψηλή διαθεσιμότητα (high availability), καθώς και απόδοση. Είναι γραμμένο σε πλατφόρμα που βασίζεται σε Java και περιλαμβάνει πακέτα του ελεγκτή Karaf OSGi που εκτελείται σε εικονική μηχανή Java (Java Virtual Machine - JVM). Παρέχει ένα σύνολο northbound APIs που επιτρέπουν την ενοποίηση του ONOS με άλλες εφαρμογές και συστήματα, όπως πλατφόρμες ενορχήστρωσης (orchestration) και διαχείρισης. Το ONOS διαθέτει ενσωματωμένη αρχιτεκτονική που βασίζεται σε υπηρεσίες που επιτρέπουν τη δημιουργία προσαρμοσμένων εφαρμογών και υπηρεσιών που εκτελούνται πάνω από τον ελεγκτή. Ένα από τα βασικά χαρακτηριστικά του ONOS είναι η ικανότητά του να χειρίζεται μεγάλο αριθμό συσκευών και συνδέσμων. Μπορεί να διαχειριστεί δίκτυα με δεκάδες χιλιάδες συσκευές και συνδέσμους, καθιστώντας το κατάλληλο για μεγάλης κλίμακας δίκτυα παρόχων υπηρεσιών και κέντρων δεδομένων. Υποστηρίζει μεγάλη ποικιλία πρωτοκόλλων δικτύου, συμπεριλαμβανομένων των OpenFlow, IPv4, IPv6 και MPLS και μπορεί να χρησιμοποιηθεί για τον έλεγχο τόσο των παραδοσιακών όσο και των δικτύων που καθορίζονται από λογισμικό. Προσφέρει επίσης μια σειρά από ενσωματωμένες δυνατότητες και υπηρεσίες, όπως διαχείριση κανόνων ροής, διαχείριση τοπολογίας και παροχή συσκευών. Επιπλέον, περιλαμβάνει εφαρμογές που μπορούν να χρησιμοποιηθούν για την επέκταση της λειτουργικότητας του ελεγκτή, όπως η μηχανική κυκλοφορίας, ο διαχωρισμός δικτύου και η ασφάλεια.

4.2.3 sFlow-RT

Το sFlow-RT αποτελεί πρότυπο για την παρακολούθηση της κυκλοφορίας του δικτύου. Το sFlow-RT χρησιμοποιεί την τεχνική της «δειγματοληψία» για τη συλλογή στατιστικών στοιχείων σχετικά με την κυκλοφορία δικτύου, συμπεριλαμβανομένων πληροφοριών σχετικά με τον αριθμό και το μέγεθος των πακέτων, την πηγή και τον προορισμό της κίνησης και τους τύπους εφαρμογών και πρωτοκόλλων που χρησιμοποιούνται. Το sFlow-RT επιλέγει τυχαία ένα υποσύνολο πακέτων και συλλέγει πληροφορίες σχετικά με αυτά χωρίς να απαιτείτε ο έλεγχος όλης της κίνησης του δικτύου. Αυτό επιτρέπει στο sFlow-RT να συγκεντρώνει ένα αντιπροσωπευτικό δείγμα της κίνησης του δικτύου, ελαχιστοποιώντας ταυτόχρονα τον αντίκτυπο της απόδοσης του δικτύου. Περιλαμβάνει επίσης τη δυνατότητα εξαγωγής των συλλεγόμενων στατιστικών επιτρέποντας στους διαχειριστές να χρησιμοποιούν τα δεδομένα για παρακολούθηση της χρήσης του δικτύου, την αντιμετώπιση προβλημάτων απόδοσης και τον εντοπισμό πιθανών απειλών ασφαλείας. Υποστηρίζει επίσης εργαλεία διαχείρισης και παρακολούθησης δικτύου, συμπεριλαμβανομένων λύσεων που βασίζονται σε SNMP, αναλυτών ροής και συστημάτων ασφαλείας.

4.2.4 pfSense

Το pfSense είναι λογισμικό τείχους προστασίας και δρομολόγησης ανοικτού κώδικα που βασίζεται στη διανομή Linux FreeBSD. Παρέχει διαδικτυακή κονσόλα (Web console) που επιτρέπει στους διαχειριστές να ρυθμίζουν και να διαχειρίζονται τις λειτουργίες του τείχους προστασίας και του δρομολογητή, συμπεριλαμβανομένων της μετάφρασης διευθύνσεων δικτύου (Network Address Translation - NAT), της προώθησης θυρών (tunneling), της ανίχνευσης και πρόληψης εισβολών (IDS/IPS) και της διαμόρφωσης της κυκλοφορίας. Επιπλέον, μπορεί εύκολα να προσαρμοστεί και να επεκταθεί με πρόσθετα πακέτα για να καλύψει συγκεκριμένες απαιτήσεις δικτύου.

4.2.5 Snort

Το Snort είναι σύστημα ανίχνευσης και πρόληψης εισβολών (Intrusion Detection System/Prevention - IDS/IPS) που αναλύει την κυκλοφορία του δικτύου σε πραγματικό χρόνο, ανιχνεύοντας και αποκλείοντας πιθανές απειλές ασφαλείας. Χρησιμοποιεί βάση δεδομένων με υπογραφές (signature based database) για τον εντοπισμό και την αποτροπή απειλών ασφαλείας. Παρακολουθώντας την κυκλοφορία του δικτύου που διέρχεται από μια καθορισμένη διασύνδεση, το Snort εκτελεί μια σειρά διεργασιών, συμπεριλαμβανομένης της ανάλυσης των πρωτοκόλλων

και περιεχομένου, καθώς και της παρακολούθησης εισερχόμενης και εξερχόμενης κυκλοφορίας σε πραγματικό χρόνο. Επιτρέπει επίσης στους διαχειριστές τη δημιουργία προσαρμοσμένων κανόνων για την ανίχνευση συγκεκριμένων τύπων απειλών ασφαλείας. Η διαχείριση του γίνεται μέσω κεντρικής κονσόλας, καθιστώντας εύκολη την παρακολούθηση του συστήματος.

4.2.6 Wireshark

Το Wireshark είναι λογισμικό ανοικτού κώδικα ανάλυσης πακέτων που χρησιμοποιείται για την αντιμετώπιση προβλημάτων δικτύου, την ανάλυση και την ανάπτυξη πρωτοκόλλων επικοινωνίας. Υποστηρίζει διάφορα πρωτόκολλα δικτύου, όπως TCP, UDP, HTTP, DNS επιτρέποντας στους διαχειριστές των δικτύων την καταγραφή των πακέτων σε πραγματικό χρόνο για την εύκολη διάγνωση και αντιμετώπιση των προβλημάτων.

4.2.7 iPerf

Το iPerf είναι εργαλείο μετρήσεων του μέγιστου επιτεύξιμου εύρους ζώνης (bandwidth) μεταξύ δύο τερματικών σημείων σε ένα δίκτυο IP. Υποστηρίζει τα πρωτόκολλα TCP και UDP και μπορεί να μετρήσει την απόδοση και την απώλεια πακέτων μιας σύνδεσης δικτύου. Το iPerf λειτουργεί με την αποστολή μιας ροής δεδομένων από τον πελάτη (client) στον διακομιστή (server) και τη μέτρηση του χρόνου που απαιτείται για τη μετάδοση και τη λήψη των δεδομένων, καθώς και του αριθμού των μεταδιδόμενων bytes. Το iPerf αποτελεί δημοφιλές εργαλείο για τη δοκιμή και τη βελτιστοποίηση της απόδοσης του δικτύου και χρησιμοποιείται συνήθως για τη διάγνωση και την αντιμετώπιση προβλημάτων του δικτύου, καθώς και για την αξιολόγηση της απόδοσης διαφορετικών διαμορφώσεων, συσκευών και εφαρμογών δικτύου.

4.2.8 Kali Linux

Το Kali Linux είναι διανομή Linux βασισμένη στο Debian που έχει σχεδιαστεί για ψηφιακή εγκληματολογία, δοκιμές διείσδυσης και ελέγχους ασφαλείας. Χρησιμοποιείται για εργασίες που σχετίζονται με την ασφάλεια, όπως σάρωση δικτύων, δοκιμές ευπάθειας, σπάσιμο συνθηματικών πρόσβασης και εκμετάλλευση. Έρχεται προεγκατεστημένο με ένα ευρύ φάσμα εργαλείων ασφαλείας, συμπεριλαμβανομένων πλαισίων δοκιμών διείσδυσης, ανάλυση δικτύου και σπάσιμο συνθηματικών πρόσβασης αποτελώντας ένα πολύτιμο εργαλείο για τον εντοπισμό και τον μετριασμό των τρωτών σημείων και των απειλών ασφαλείας. Συντηρείται από την Offensive

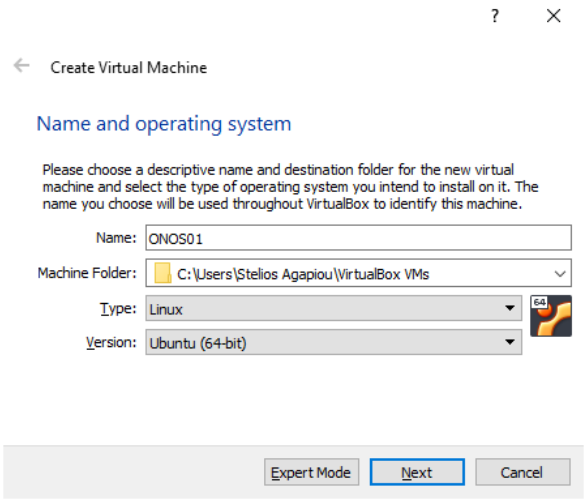
Security και είναι διαθέσιμο για δωρεάν λήψη και χρήση ενώ ο πηγαίος κώδικάς του είναι ανοιχτός και ελεύθερα διαθέσιμος στο κοινό.

4.3 Δημιουργία εικονικών μηχανών

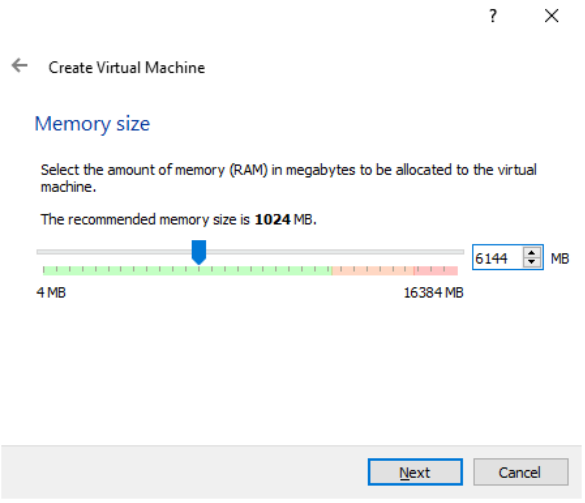
4.3.1 Ubuntu Virtual Machine

Για τη δημιουργία της εικονικής μηχανής με λειτουργικό σύστημα Ubuntu 18.04 LTS χρησιμοποιήσαμε το λογισμικό εικονικοποίησης VirtualBox. Επιλέξαμε τη δημιουργία μιας νέας εικονικής μηχανής από το μενού του λογισμικού και ακολούθως καθορίσαμε τον τύπο του λειτουργικού συστήματος, το μέγεθος της RAM, το μέγεθος του εικονικού δίσκου και τον αριθμό των vCPU που θα εκχωρήσουμε στην εικονική μηχανή όπως παρουσιάζονται στα στιγμιότυπα των εικόνων 10-21. Εκκινήσαμε την εικονική μηχανή από το αρχείο ISO και ξεκινήσαμε τη διαδικασία εγκατάστασης του λειτουργικού συστήματος Ubuntu 18.04 LTS. Στα επόμενα στάδια επιλέξαμε τη γλώσσα του λειτουργικού, διαμορφώσαμε το δίσκο και ρυθμίσαμε το λογαριασμό του χρήστη. Κατά την ολοκλήρωση της εγκατάσταση, μας ζητήθηκε η επανεκκίνηση της εικονική μηχανή.

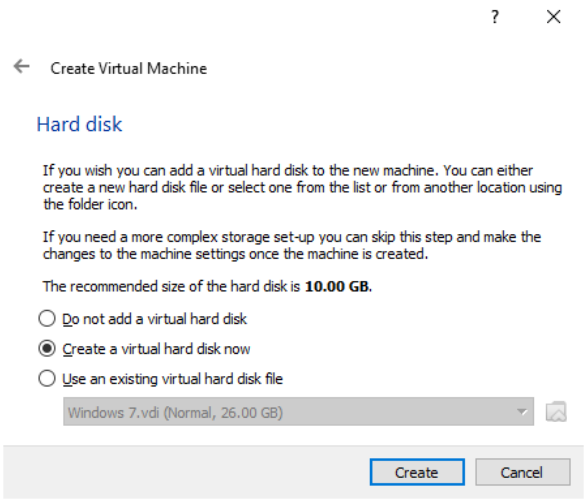
Αναλυτικά τα βήματα της δημιουργίας της εικονικής μηχανής παρουσιάζονται στα στιγμιότυπα εικόνων 10-21 που ακολουθούν.



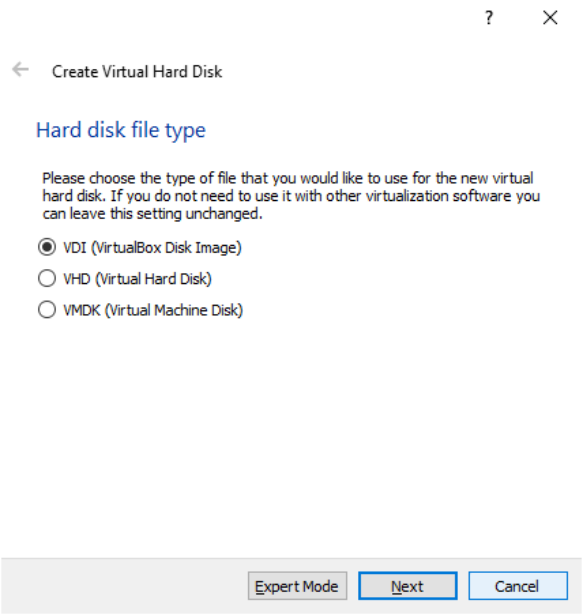
Εικόνα 10: Όνομα εικονικής μηχανής και επιλογή λειτουργικού συστήματος



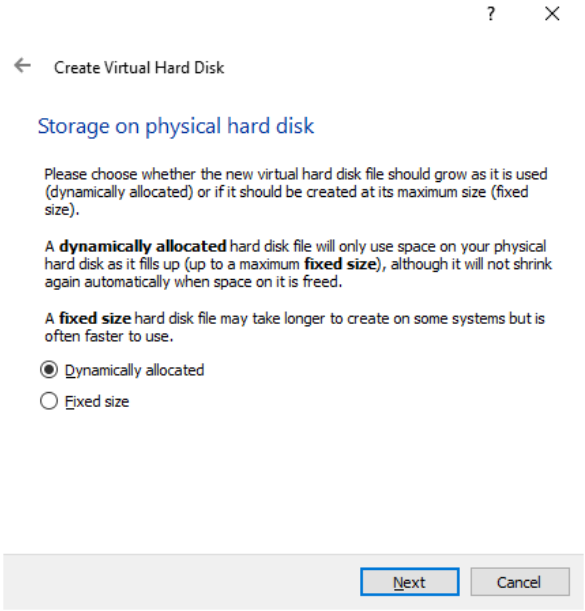
Εικόνα 11: Ρύθμιση μεγέθους RAM



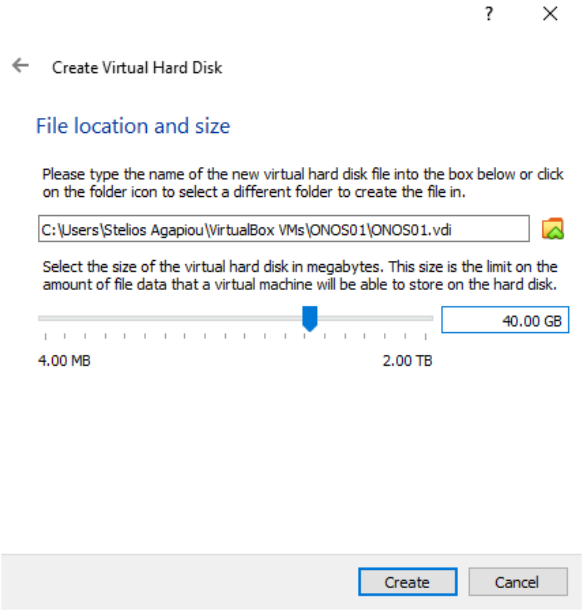
Εικόνα 12: Δημιουργία εικονικού δίσκου



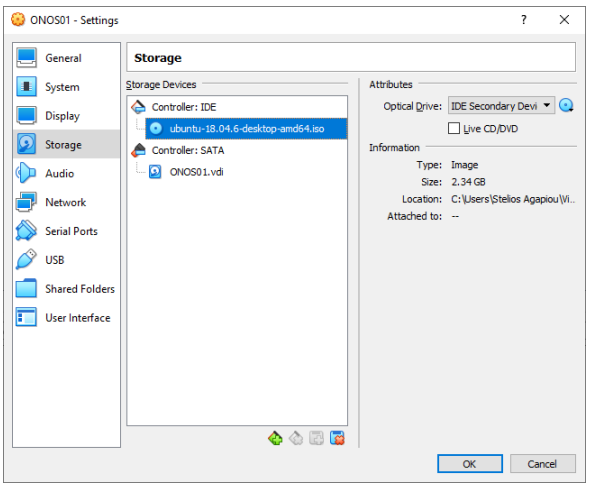
Εικόνα 13: Επιλογή τύπου δίσκου



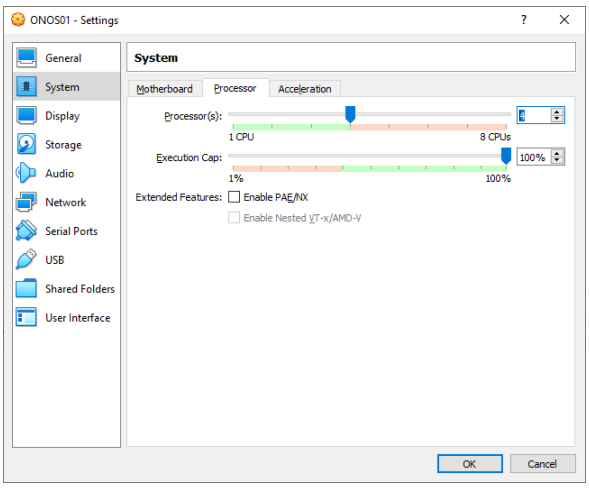
Εικόνα 14: Επιλογή δυναμικά εκχωρημένου δίσκου



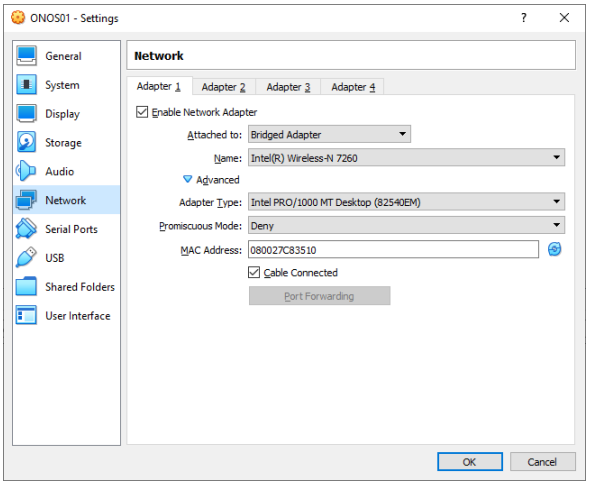
Εικόνα 15: Ρύθμιση χωρητικότητας του εικονικού δίσκου



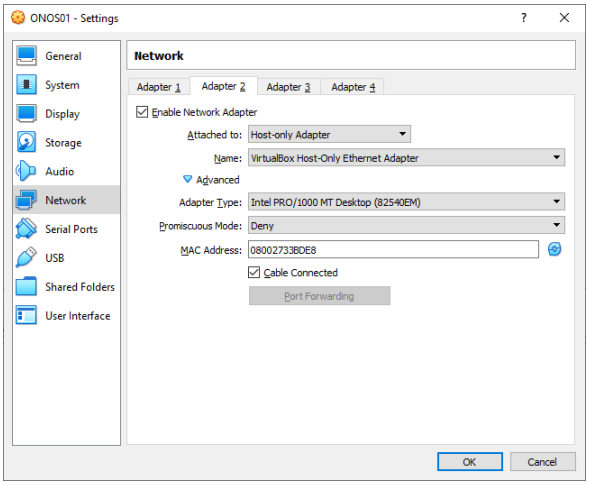
Εικόνα 16: Επιλογή Ubuntu ISO Image



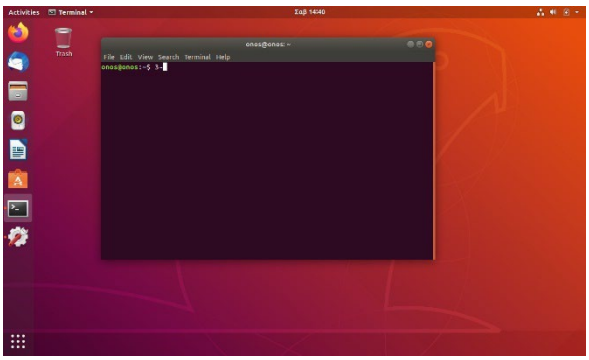
Εικόνα 17: Επιλογή vCPU Core



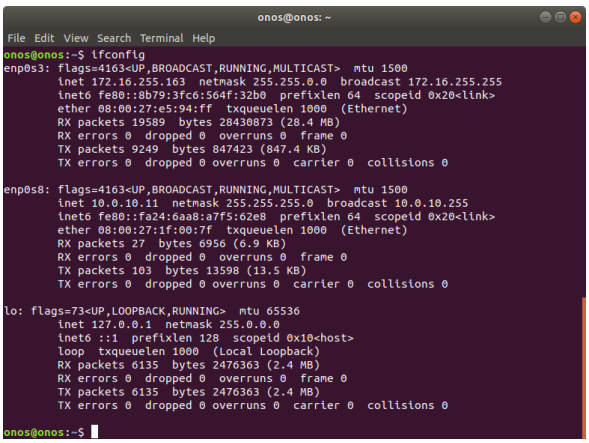
Εικόνα 18: Ρύθμιση του network adapter type για την 1η κάρτα δικτύου



Εικόνα 19: Ρύθμιση του network adapter type για την 2η κάρτα δικτύου



Εικόνα 20: Λειτουργικό σύστημα Ubuntu



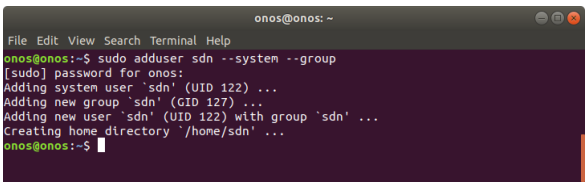
Εικόνα 21: Ρυθμίσεις κάρτας δικτύου - ONOS Controller VM

4.3.2 Εγκατάσταση του ελεγκτή ONOS

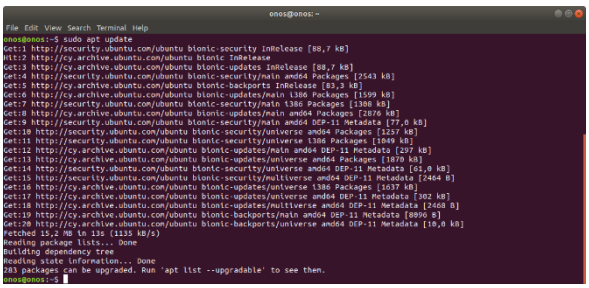
Για την εγκατάσταση του ελεγκτή ONOS στην VM με λειτουργικό σύστημα Ubuntu δημιουργήσαμε αρχικά ένα νέο χρήστη συστήματος με το όνομα «sdn» που θα χρησιμοποιήσουμε στη συνέχεια για την εκτέλεση της υπηρεσίας ONOS. Αυτό μας διασφαλίζει ότι η υπηρεσία ONOS θα εκτελείται με τα λιγότερα δυνατά προνόμια και τα αρχεία ONOS θα είναι προσβάσιμα μόνο από την ίδια την υπηρεσία. Στη συνέχεια, ενημερώσαμε τη λίστα πακέτων και προχωρήσαμε στην εγκατάσταση των απαραίτητων εξαρτήσεων για το ONOS, συμπεριλαμβανομένου του περιβάλλοντος java 11, git, zip, curl, unzip και Python. Αυτές οι εξαρτήσεις είναι απαραίτητες για να λειτουργήσει σωστά το ONOS. Ακολούθως κατεβάσαμε το πακέτο (package) ONOS για Ubuntu από τον ιστότοπο της ONOS, αποσυμπιέσαμε τα περιεχόμενα του πακέτου στον κατάλογο /opt του συστήματός και αλλάξαμε την ιδιοκτησία (ownership) του καταλόγου «onos» στο χρήστη (user) και στην ομάδα (group) «sdn». Επιπρόσθετα, στο αρχείο options ορίσαμε τις επιλογές εκκίνησης για της υπηρεσίας ONOS. Το ONOS_USER και το ONOS_APPS έχουν οριστεί σε sdn με προγράμματα οδήγησης τα OpenFlow και gui2 αντίστοιχα. Με την επιλογή ONOS_USER ορίσαμε το χρήστη που θα εκτελεί το ONOS και με την επιλογή ONOS_APPS καθορίσαμε τις εφαρμογές που θα πρέπει να είναι ενεργές από προεπιλογή. Ακολούθως, αντιγράψαμε το αρχείο υπηρεσίας ONOS στους κατάλληλους καταλόγους για να ενεργοποιήσουμε την εκτέλεση της υπηρεσίας ONOS κατά την εκκίνηση του λειτουργικού. Μετά την εγκατάσταση, μπορέσαμε να αποκτήσουμε πρόσβαση στη διαδικτυακή κονσόλα του ONOS μεταβαίνοντας στη διεύθυνση «*http://onos:8181/onos/ui/login.html*» χρησιμοποιώντας πρόγραμμα περιήγησης ιστού (Web browser). Το προεπιλεγμένο όνομα χρήστη και ο κωδικός πρόσβασης για τη διαδικτυακή κονσόλα

ONOS είναι «onos» και «rocks», αντίστοιχα. Η πρόσβαση μέσω CLI επιτυγχάνεται με τη χρήση της εντολής «*ssh -p 8101 onos@10.0.10.11*».

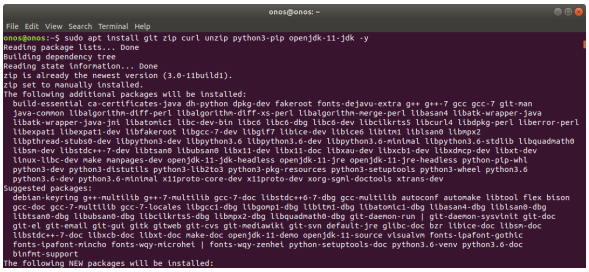
Στα στιγμιότυπα (εικόνες 22-30) που ακολουθούν παρουσιάζονται αναλυτικά τα βήματα που ακολουθήσαμε για την εγκατάσταση του ελεγκτή ONOS στο σύστημα.



Εικόνα 22: Δημιουργία του χρήστη sdn

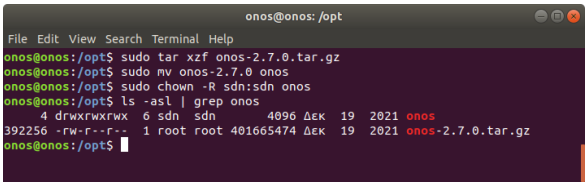


Εικόνα 23: Ενημέρωση των πακέτων

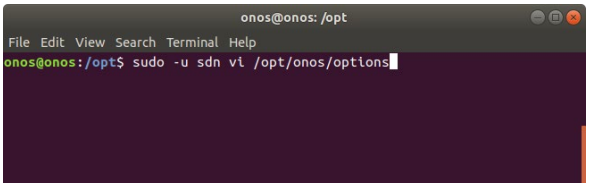


Εικόνα 24: Εγκατάσταση απαραίτητων προγραμμάτων

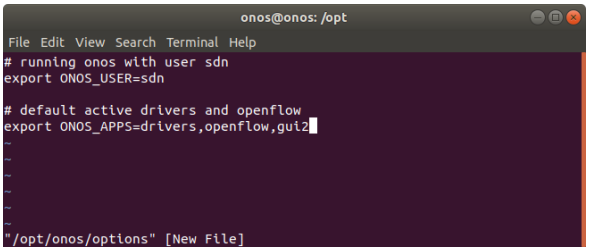
Εικόνα 25: Λήψη του ONOS



Εικόνα 26: Αποσυμπίεση του πακέτου ONOS

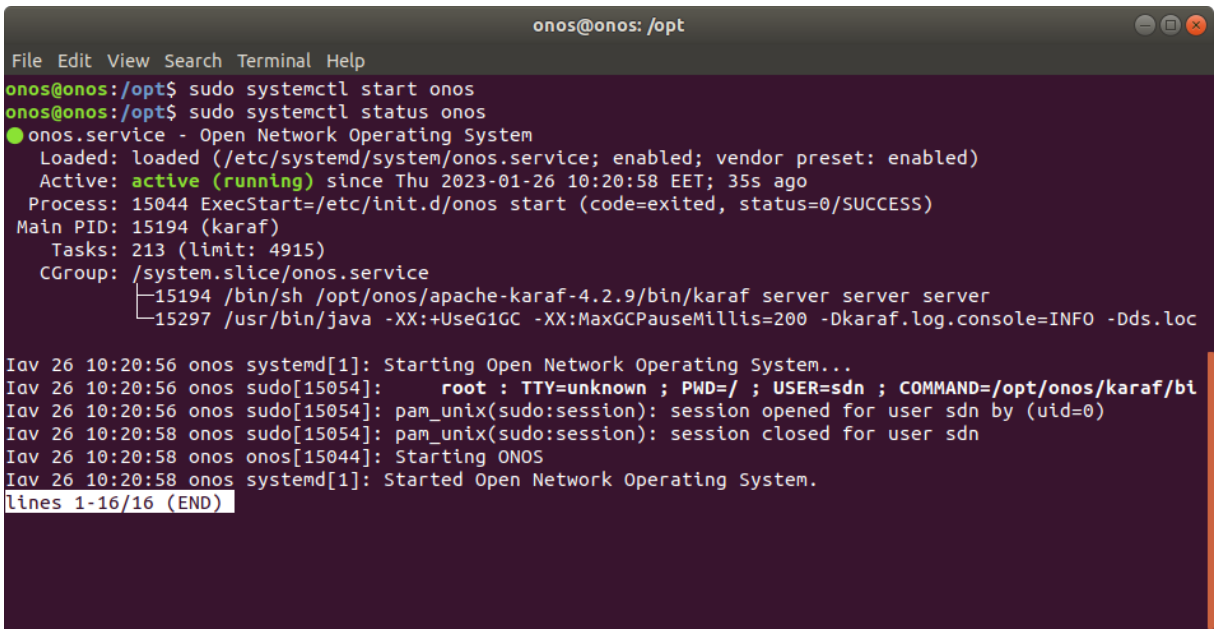


Εικόνα 27: Επεξεργασία του αρχείου options



Εικόνα 28: Καθορισμός των ONOS_USER και ONOS_APPS

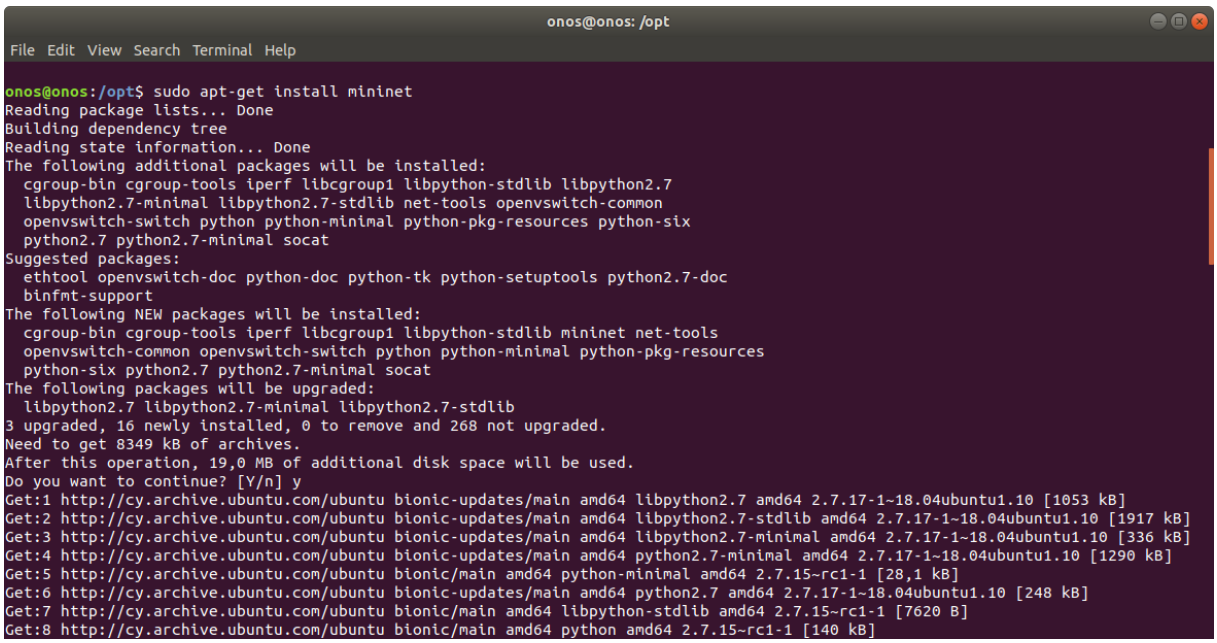
Εικόνα 29: Ενεργοποίηση της εκτέλεση της υπηρεσίας ONOS κατά την εκκίνηση του OS



Εικόνα 30: Εκκίνηση της υπηρεσία ONOS

4.3.3 Εγκατάσταση Mininet

Για την εγκατάσταση του εξομοιωτή δικτύου Mininet δημιουργήσαμε κλώνο της εικονικής μηχανής που μόλις έχουμε διαμορφώσει για τον ελεγκτή ONOS και εκτελέσαμε την εντολή «*sudo apt-get install mininet*» (εικόνα 31) με δικαιώματα χρήστη root.

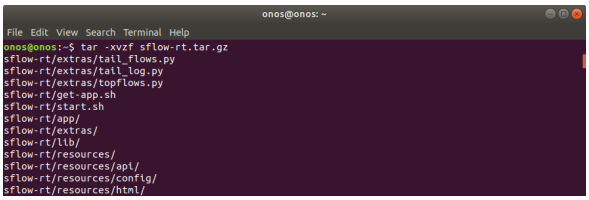


Εικόνα 31: Εγκατάσταση Mininet

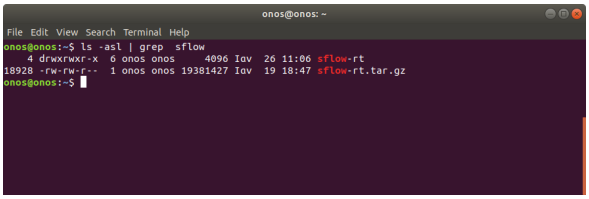
4.3.4 Εγκατάσταση του sFlow-RT

Για την εγκατάσταση του sFlow-RT κατεβάσαμε το πακέτο sFlow-RT από τη διεύθυνση «*https://inmon.com/products/sFlow-RT/sflow-rt.tar.gz*» (εικόνα 32) και εξαγάγαμε το περιεχόμενο του (εικόνες 33-34) χρησιμοποιώντας τις εντολές wget και tar αντίστοιχα. Ακολούθως, εκκινήσαμε την υπηρεσία sFlow-RT με την εντολή «*./sflow-rt/start.sh*» (εικόνα 35). Τα βήματα που ακολουθήσαμε για την εγκατάσταση του sFlow-RT και την εκτέλεση του Mininet παρουσιάζονται στα στιγμιότυπα των εικόνων πιο κάτω.

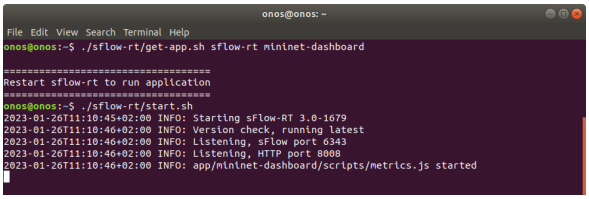
Εικόνα 32: Λήψη του sFlow-RT



Εικόνα 33: Αποσυμπίεση του αρχείου sFlow-RT

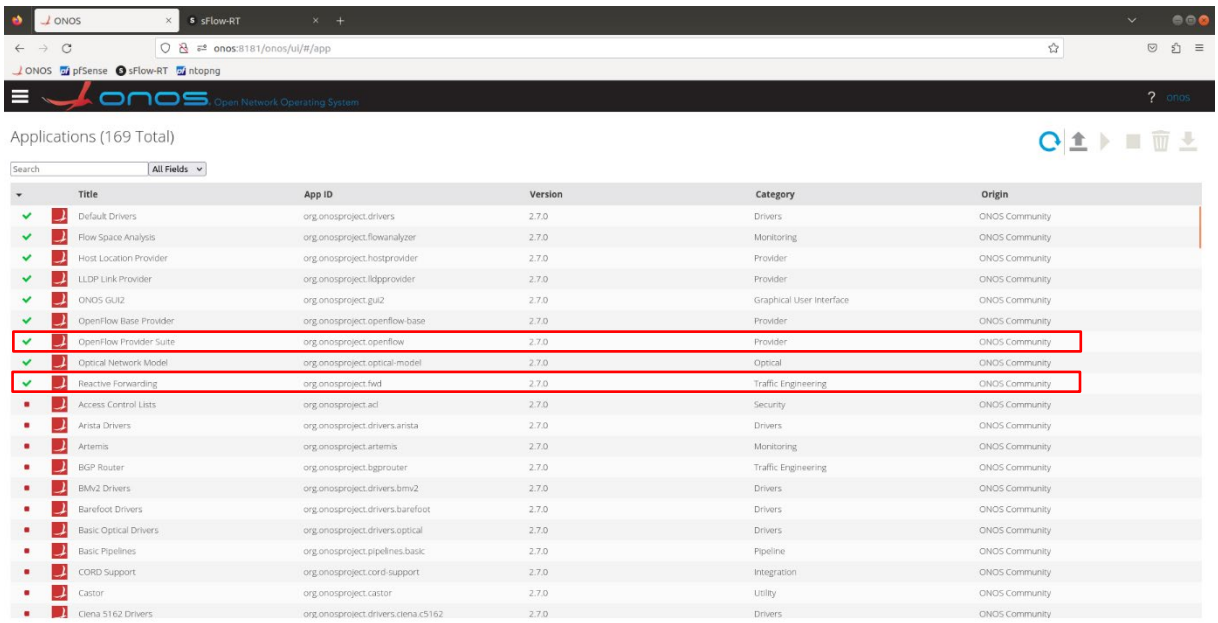


Εικόνα 34: Φάκελος προγράμματος sFlow-RT



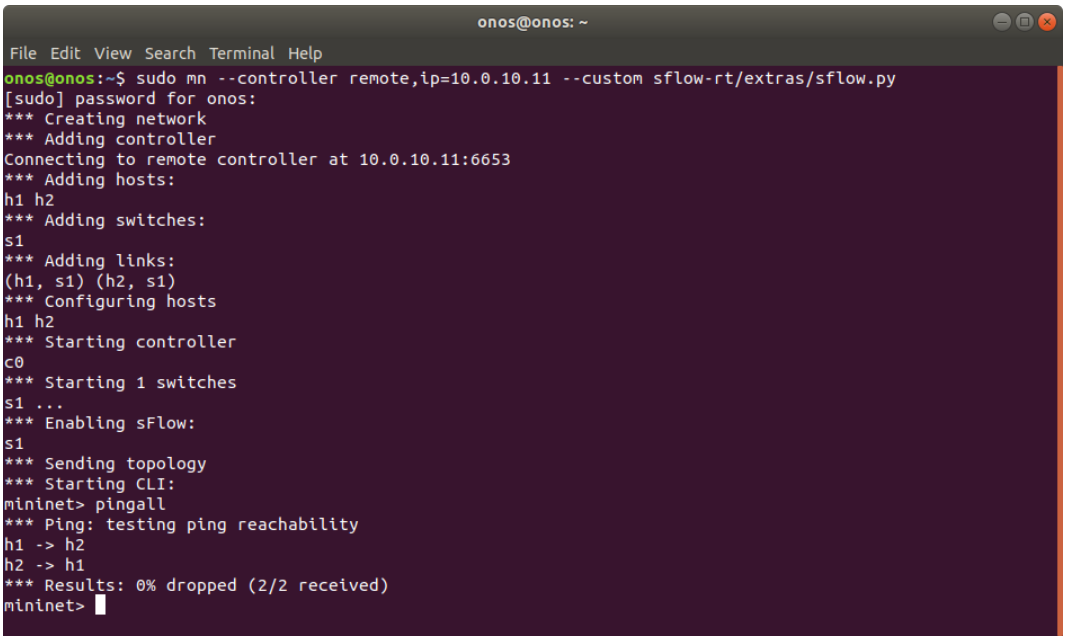
Εικόνα 35: Εκκίνηση του sFlow-RT

Από το ONOS ενεργοποιήσαμε τις εφαρμογές (applications) org.onosproject.openflow και org.onosproject.fwd (εικόνα 36). Η εφαρμογή org.onosproject.openflow αποτελεί υλοποίηση του πρωτοκόλλου OpenFlow και παρέχει υποστήριξη για μεταγωγείς και συσκευές δικτύου που βασίζονται σε OpenFlow. Η εφαρμογή επιτρέπει στον ελεγκτή ONOS να επικοινωνεί με μεταγωγείς με δυνατότητα OpenFlow και να ρυθμίζει τη συμπεριφορά προώθησής τους. Η εφαρμογή org.onosproject.fwd είναι εφαρμογή προώθησης πακέτων και παρέχει βασικές δυνατότητες προώθησης επιπέδου 2 (layer 2) στον ελεγκτή ONOS. Η εφαρμογή επιτρέπει στον ελεγκτή να προωθεί πακέτα μεταξύ διαφορετικών θυρών του μεταγωγέα με βάση τις MAC διευθύνσεις προορισμού τους.



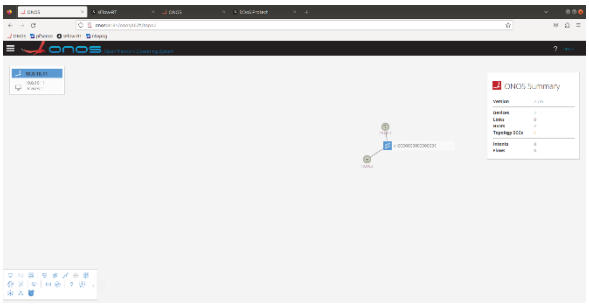
Εικόνα 36: Ενεργοποίηση εφαρμογών ONOS

Στη συνέχεια, εκκινήσαμε ένα εικονικό δίκτυο Mininet συνδέοντας το με τον απομακρυσμένο ελεγκτή στη διεύθυνση IP 10.0.10.11 και θύρα 6653 ενεργοποιώντας ταυτόχρονα την παρακολούθηση της δικτυακής κίνησης μέσω του sFlow-RT (εικόνα 37). Με την ολοκλήρωση της διαδικασίας, η τοπολογία εμφανίστηκε στη διαδικτυακή κονσόλα του ONOS (εικόνα 38).

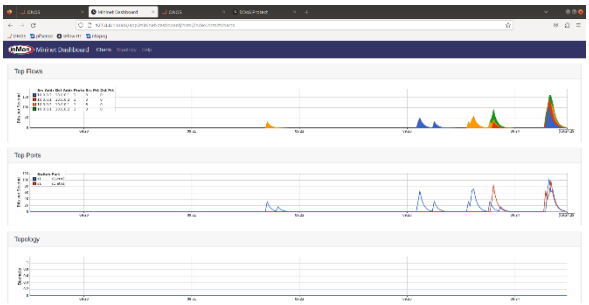


Εικόνα 37: Δημιουργία τοπολογίας δικτύου μέσω του Mininet

Η υπηρεσία sFlow-RT συνέλλεξε και ανάλυσε τα δεδομένα κίνησης του δικτύου σε πραγματικό χρόνο (εικόνα 39). Το Mininet Dashboard ήταν επίσης διαθέσιμο και μας παρείχε μια διαδικτυακή διεπαφή για την παρακολούθηση και τον έλεγχο του δικτύου Mininet.

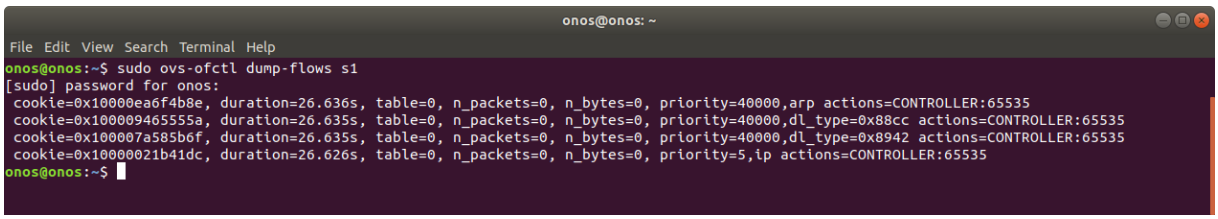


Εικόνα 38: Πρόσβαση στο Web UI του ONOS

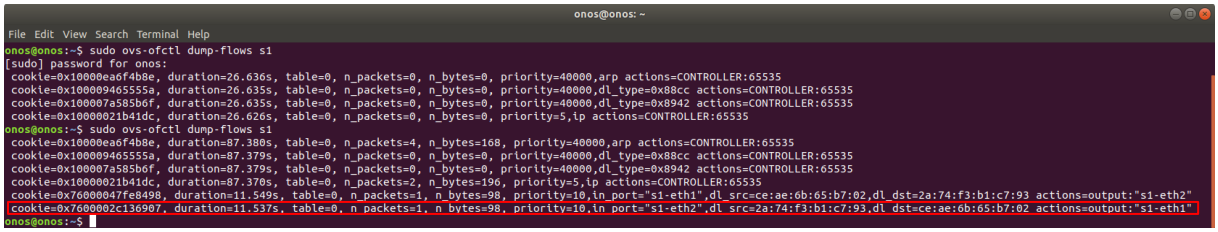


Εικόνα 39: Web UI του sFlow-RT

Για την εμφάνιση των περιεχομένων του τρέχοντος πίνακα ροής του μεταγωγέα OpenFlow «s1» εκτελέσαμε την εντολή «*sudo ovs-ofctl dump-flows s1*». Στο στιγμιότυπο της εικόνας 40 καταγράφονται οι καταχωρήσεις ροής του μεταγωγέα «s1» που ελέγχεται από τον ελεγκτή ONOS. Οι καταχωρήσεις ροής όπως καταγράφονται στην εικόνα 40 ήταν πριν την εκτέλεση της εντολής «*ping*all» και χωρίς να υπάρχει οποιαδήποτε κίνηση στο δίκτυο. Το δεύτερο στιγμιότυπο (εικόνας 41) καταγράφονται οι καταχωρήσεις ροής μετά την εκτέλεση της εντολής «*ping*all». Κάθε καταχώρηση ροής αναγνωρίζεται από την τιμή «cookie» που χρησιμοποιείται από τον ελεγκτή για τη διαχείριση της καταχώρησης ροής. Το πεδίο «duration» αντιστοιχεί στο χρονικό διάστημα που η καταχώρηση ροής ήταν ενεργή. Το πεδίο «table» υποδεικνύει τον πίνακα στον οποίο είναι εγκατεστημένη η καταχώρηση ροής ενώ τα πεδία «n_packets» και «n_bytes» εμφανίζουν των αριθμό των πακέτων και bytes που έχουν αντιστοιχηθεί στην καταχώρηση ροής, αντίστοιχα. Το πεδίο «priority» καθορίζει τη σειρά με την οποία αξιολογούνται οι καταχωρήσεις ροής ενώ το πεδίο «actions» καθορίζει την ενέργεια που πρέπει να γίνει στα πακέτα (στην προκειμένη περίπτωση, προώθησή τους στον ελεγκτή ONOS με ID 65535). Τα πεδία «dl_src» και «dl_dst» (εικόνα 41) αντιστοιχούν στις διευθύνσεις MAC προέλευσης και προορισμού των Ethernet frames που φθάνουν στο μεταγωγέα «s1». Οι διευθύνσεις MAC στις καταχωρήσεις ροής μπορούν να χρησιμοποιηθούν για την αναγνώριση των συσκευών που επικοινωνούν μέσω του δικτύου. Στην τελευταία καταχώρηση ροής (εικόνα 41) με τιμή cookie «0x7600002c136907» αντιστοιχεί σε εισερχόμενα πακέτα με διεύθυνση MAC πηγής «2a:74:f3:b1:c7:93» και διεύθυνση MAC προορισμού «ce:ae:6b:65:b7:02».



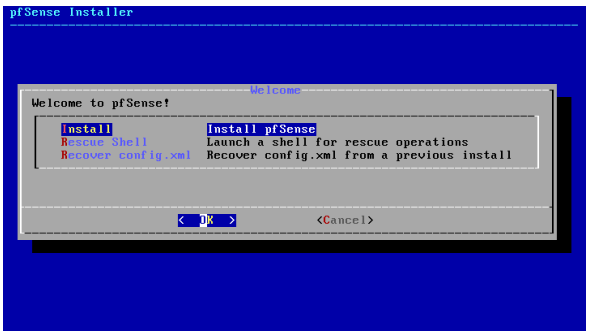
Εικόνα 40: Καταχωρήσεις ροής μεταγωγέα S1



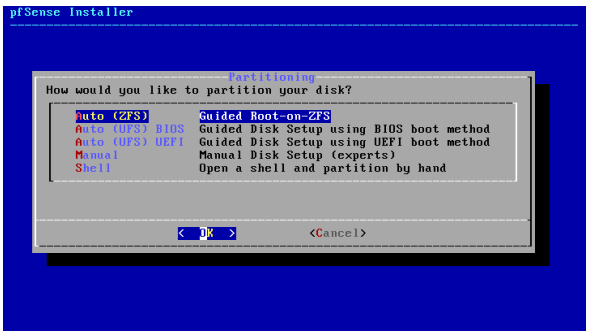
Εικόνα 41: Καταχωρήσεις ροής μεταγωγέα S1 μετά τη δημιουργία κίνησης

4.3.5 Εγκατάσταση του pfSense και διαμόρφωση του Snort

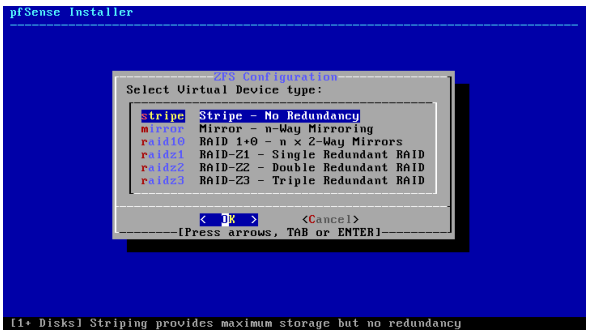
Δημιουργήσαμε μια νέα εικονική μηχανή στο VirtualBox και επιλέξαμε το ISO αρχείο του pfSense ως αρχείο εικονικού οπτικού δίσκου. Εκκινήσαμε τη VM ακολουθώντας τα βήματα για την εγκατάσταση του pfSense όπως φαίνονται στα στιγμιότυπα των εικόνων 42-45.



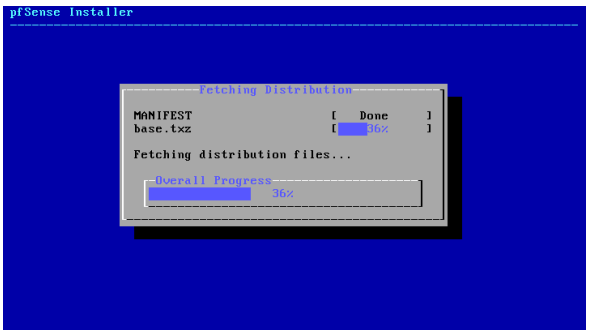
Εικόνα 42: Εγκατάσταση pfSense



Εικόνα 43: Διαμερίσματα δίσκου pfSense

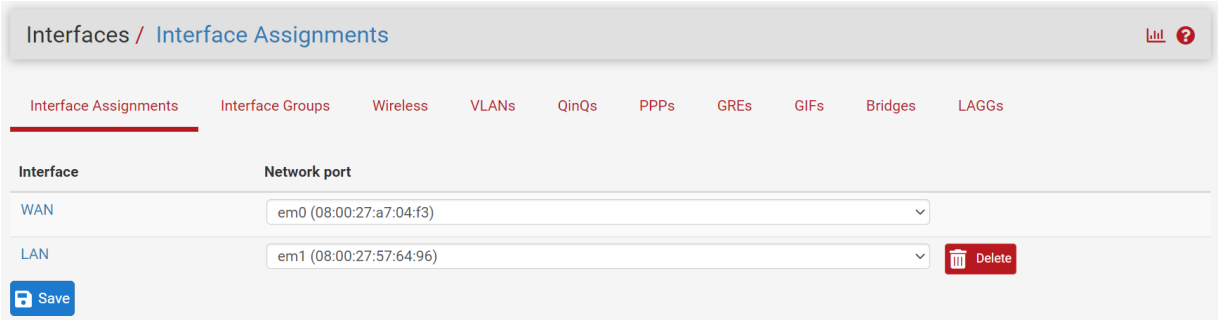


Εικόνα 44: Διαμόρφωση αποθήκευσης

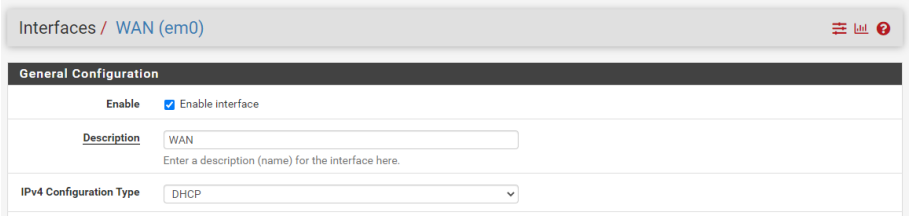


Εικόνα 45: Λήψη του λογισμικού pfSense

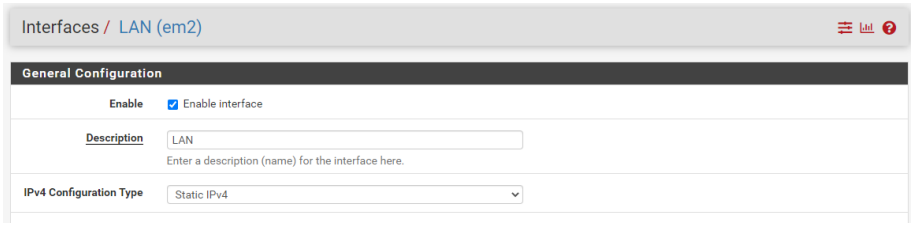
Μετά την ολοκλήρωση της εγκατάστασης και μέσω της διαδικτυακής κονσόλας του pfSense ρυθμίσαμε τις διεπαφές (interfaces) em0 και em1 (εικόνα 46). Το πρώτο interface το οποίο θα είναι και το WAN interface το ρυθμίσαμε ως DHCP client (προσωρινή διεύθυνση IPv4 172.16.255.242 με μάσκα δικτύου 255.255.0.0.), (εικόνα 47) ενώ το δεύτερο interface το οποίο θα είναι το LAN interface το ρυθμίσαμε με στατική διεύθυνση IPv4 10.0.10.1 και μάσκα δικτύου 255.255.255.0 (εικόνα 48). Ακολούθως, ενεργοποιήσαμε το DHCP server στο LAN interface του pfSense διαμορφώνοντας το DHCP pool σε 10.0.10.10-10.0.10.200 (εικόνα 49). Ο DCHP server θα διευθυνσιοδοτήσει τα υπόλοιπα εικονικά μηχανήματα του δικτύου μας.



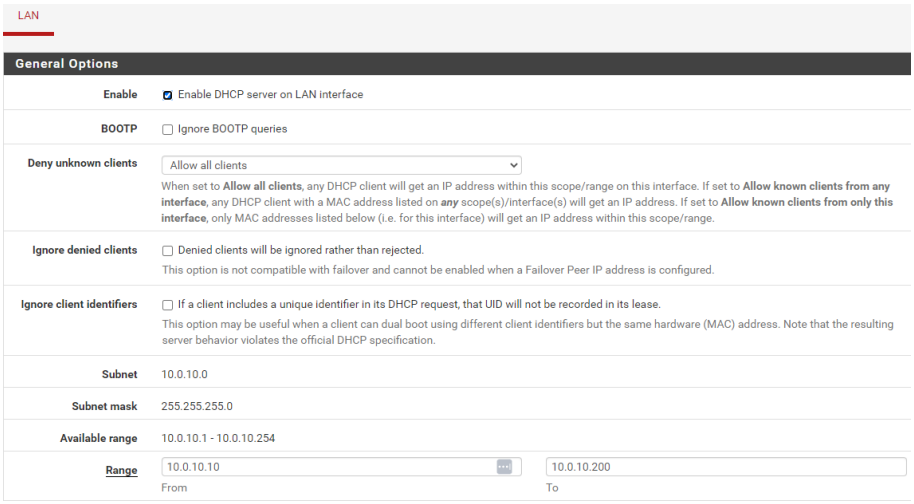
Εικόνα 46: pfSense interfaces



Εικόνα 47: pfSense WAN interface

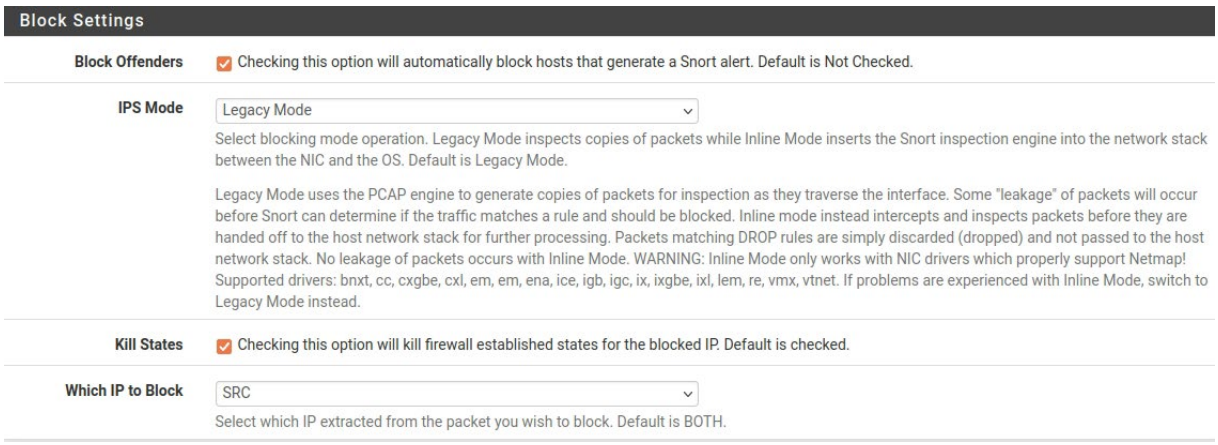


Εικόνα 48: pfSense LAN interfaces



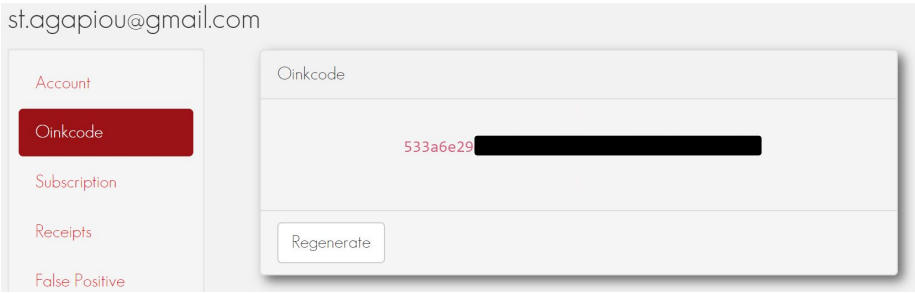
Εικόνα 49: DHCP Pool

Από τον Package Manager εγκαταστήσαμε το πακέτο του Snort και ακολούθως προχωρήσαμε στη διαμόρφωση του. Το Snort θα αποτελέσει το σύστημα ανίχνευσης και πρόληψης εισβολών του εικονικού δικτύου SDN που μόλις δημιουργήσαμε. Στο Snort, ενεργοποιήσαμε τη λειτουργία IDS/IPS (εικόνα 50) για να αποκλείσουμε την κακόβουλη κυκλοφορία που προέρχεται από την IP διεύθυνση πηγής (source – SRC) και ταιριάζει σε έναν κανόνα, να φτάσει στον προορισμό της. Η λειτουργία IDS/IPS θα μας αποτρέψει από πιθανές επιθέσεις και θα μας παρέχει ένα πρόσθετο επίπεδο ασφάλειας εμποδίζοντας ενεργά την κακόβουλη κυκλοφορία.

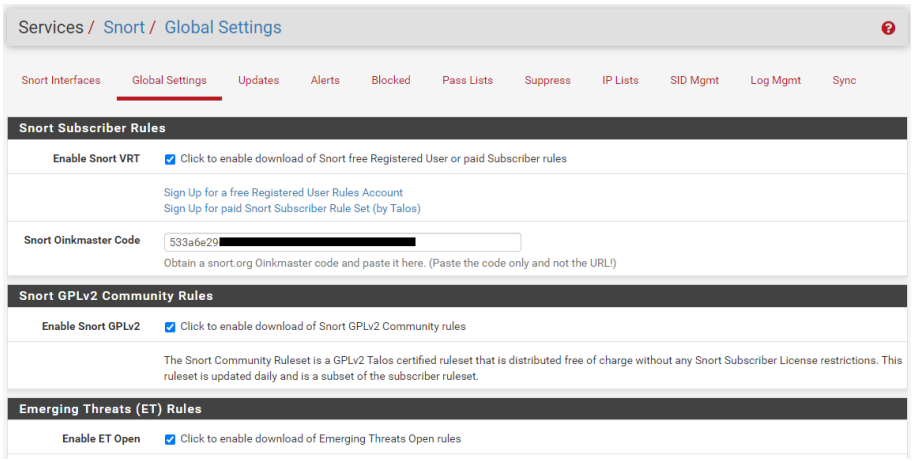


Εικόνα 50: Intrusion Prevention System

Για να χρησιμοποιήσουμε τις πλήρεις δυνατότητες του Snort, δημιουργήσαμε Oinkcode, (εικόνες 51-52) το οποίο αποτελεί ένα μοναδικό αναγνωριστικό που χρησιμοποιείται για τη λήψη των πιο πρόσφατων κανόνων του Snort μέσω του snort.org.



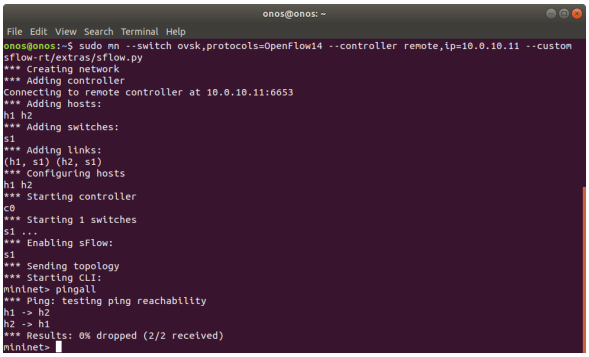
Εικόνα 51: Λήψη Oinkcode από το snort.org



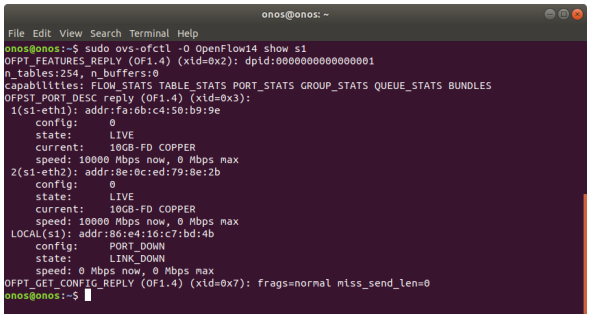
Εικόνα 52: Διαμόρφωση του snort

4.4 Αξιολόγηση SDN χωρίς την προσομοίωση επιθέσεων DDoS

Εκκινήσαμε το δίκτυο Mininet συνδέοντας το με τον απομακρυσμένο ελεγκτή στη διεύθυνση IP 10.0.10.11 και θύρα 6653 (εικόνα 53). Η τοπολογία του δικτύου αποτελείται από έναν ενιαίο μεταγωγέα Open vSwitch (OVS), δύο εικονικούς κεντρικούς υπολογιστές (virtual hosts) και μια σύνδεση με τον απομακρυσμένο ελεγκτή χρησιμοποιώντας το πρωτόκολλο OpenFlow. Ο μεταγωγέας OVS χρησιμοποιήθηκε για την προώθηση των πακέτων και ο ελεγκτής για τη δυναμική διαμόρφωση και διαχείριση της κυκλοφορίας του δικτύου. Η έκδοση του OpenFlow που χρησιμοποιείται είναι η 1.4 (εικόνα 54).



Εικόνα 53: Δημιουργία τοπολογίας δικτύου για αξιολόγηση του SDN



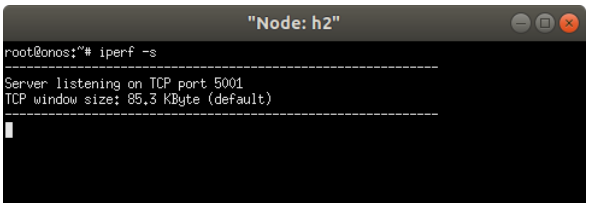
Εικόνα 54: Έκδοση OpenFlow

Αρχικά, η καταγραφή των μετρήσεων έγινε χωρίς την προσομοίωση επίθεσης πλημμύρας TCP SYN στον ελεγκτή. Ακολούθως, καταγράψαμε τις αντίστοιχες μετρήσεις εκτελώντας επίθεση πλημμύρας TCP SYN στον ελεγκτή και ακολούθως, καταγράψαμε τις ίδιες μετρήσεις έχοντας ενεργοποιημένο το σύστημα ανίχνευσης και πρόληψης εισβολών.

4.4.1 Μέτρηση του χρόνου απόκρισης

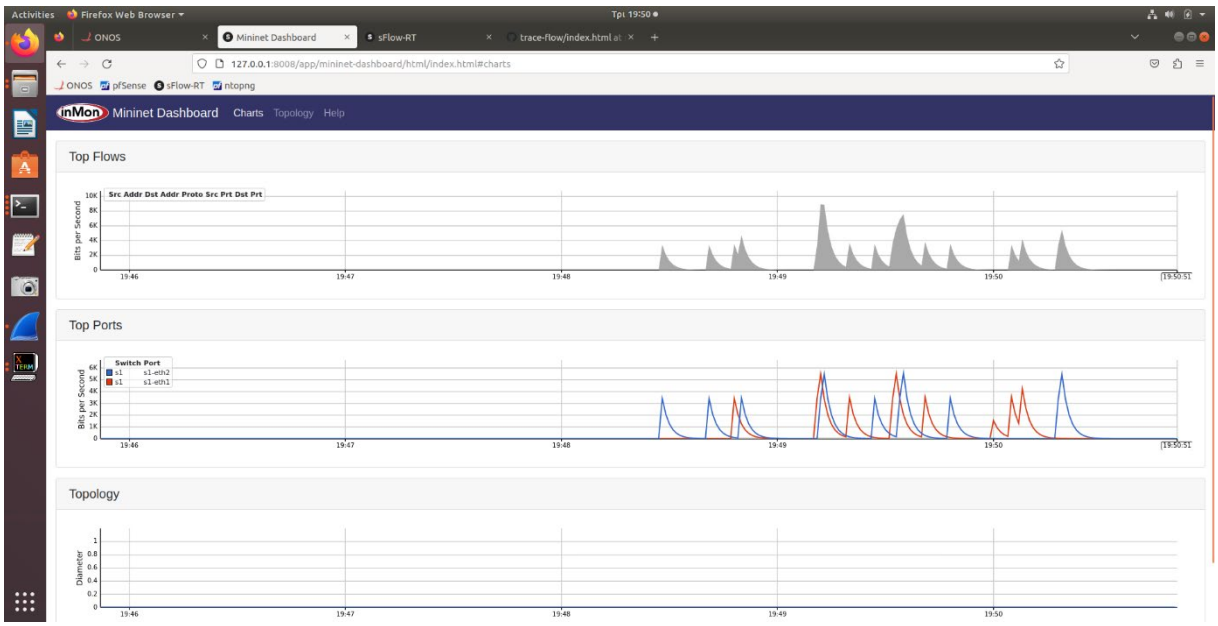
Χρησιμοποιώντας τα εργαλεία iPerf και ping μετρήσαμε το χρόνο απόκρισης μεταξύ των δυο hosts h1 και h2 στην ανταλλαγή πακέτων (εικόνες 55-56). Ο χρόνος απόκρισης αναφέρεται στο χρόνο που χρειάζεται ένα πακέτο ICMP (Internet Control Message Protocol) για να ταξιδέψει από την πηγή στον προορισμό και πάλι πίσω. Με την εκτέλεση της εντολής ping, στείλαμε αιτήσεις ICMP echo στην IP διεύθυνση προορισμού του h2 και μετρήσαμε το χρόνο διαδρομής (Round Trip Time - RTT) για κάθε αίτηση. Η ροή της κίνησης μεταξύ των δυο hosts παρουσιάζεται στο στιγμιότυπο

της εικόνας 57. Επαναλάβαμε τις μετρήσεις μας για να λάβουμε έναν ακριβέστερο μέσο όρο απόκρισης και να εντοπίσουμε τυχόν διακυμάνσεις που μπορεί να υποδεικνύουν προβλήματα στο δίκτυο, όπως συμφόρηση, προβλήματα δρομολόγησης ή και φορτίο στον host. Με τον τρόπο αυτό διασφαλίσαμε ότι τα αποτελέσματα δεν επηρεάζονται από παροδικές συνθήκες ή ακραίες τιμές. Καταγράψαμε το χρόνο απόκρισης στο αρχείο ping-h2.



Εικόνα 55: Μέτρηση χρόνου απόκρισης

Εικόνα 56: Μέτρηση χρόνου απόκρισης

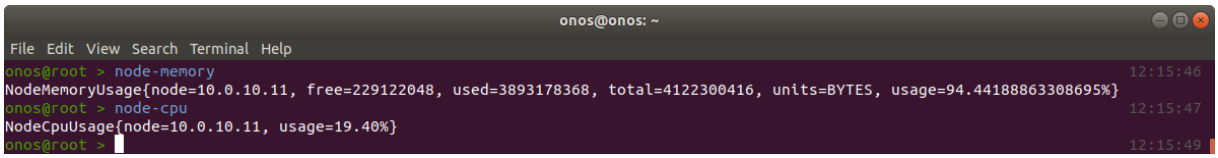


Εικόνα 57: Ροή κίνησης μεταξύ h1 και h2

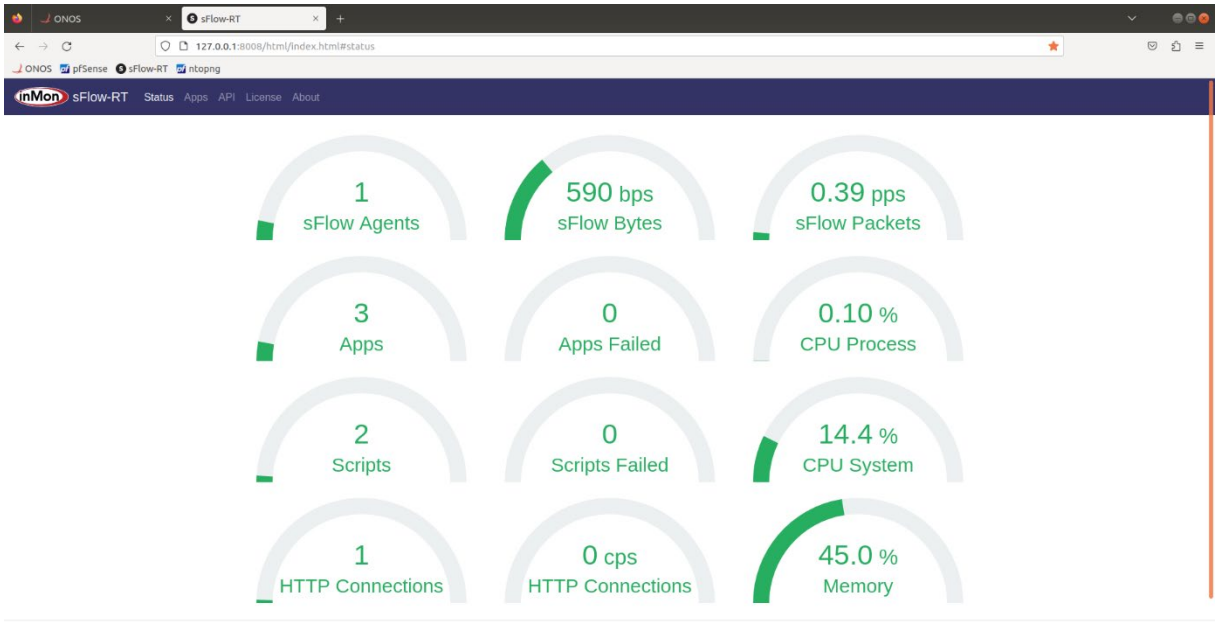
4.4.2 Μέτρηση φορτίου ελεγκτή

Κατά την ανταλλαγή των πακέτων μεταξύ των hosts καταγράψαμε τις μετρήσεις του φορτίου της μνήμης (memory) και του επεξεργαστή (CPU) με τη χρήση των εντολών του ONOS «*node-cpu*» και «*node-memory*» (εικόνα 58). Μέσω του προγράμματος sFlow-RT, εμφανίσαμε το φορτίο του ελεγκτή σε πραγματικό χρόνο (εικόνα 59). Η εντολή «*node-cpu*» μας εμφάνισε τη χρήση της CPU του απομακρυσμένου ελεγκτή ONOS στον οποίο είμαστε συνδεδεμένοι τη δεδομένη χρονική στιγμή ενώ η εντολή «*node-memory*» μας εμφάνισε την τρέχουσα χρήση της μνήμης του απομακρυσμένου ελεγκτή ONOS. Η χρήση του επεξεργαστή και της μνήμης εκφράζονται ως

ποσοστό της συνολικής χωρητικότητας του επεξεργαστή και της μνήμης του κόμβου αντίστοιχα. Με την παρακολούθηση της χρήσης του φορτίου του επεξεργαστή και της μνήμης των κόμβων μπορούμε να εντοπίσουμε και να επιλύσουμε προβλήματα επιδόσεων προτού αυτά επηρεάσουν το δίκτυο. Η ψηλή χρήση της CPU μπορεί να αποτελέσει ένδειξη προβλήματος απόδοσης του κόμβου, ενώ η ψηλή χρήση της μνήμη μπορεί να προκαλέσει ακόμη και αστοχία του κόμβου.



Εικόνα 58: ONOS φορτίο επεξεργαστή και μνήμης

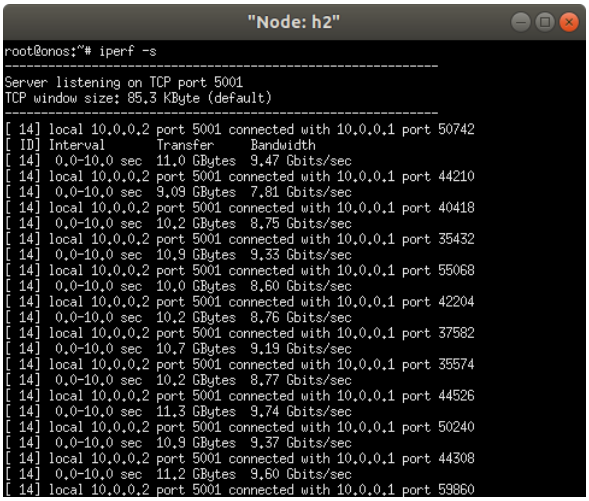


Εικόνα 59: Μέτρηση της υπερφόρτωσης του ελεγκτή

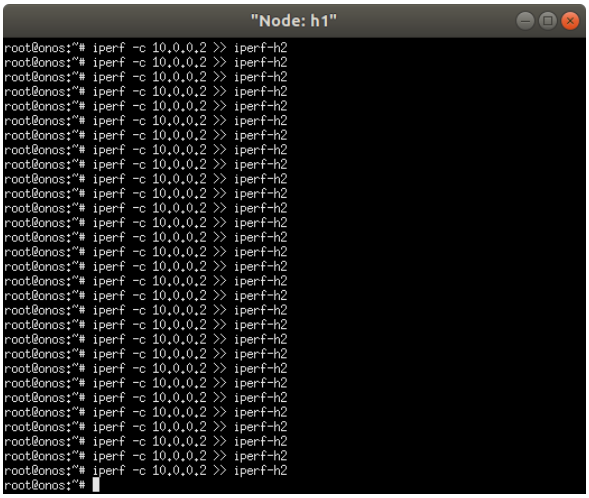
4.4.3 Μέτρηση εύρους ζώνης δικτύου

Για την μέτρηση του εύρους ζώνης και της απόδοσης του δικτύου με τη δημιουργία κίνησης TCP μεταξύ των δύο κεντρικών υπολογιστών χρησιμοποιήσαμε το πρόγραμμα iPerf. Με την εντολή «*iperf -s*» (εικόνα 60) δηλώσαμε τον h2 ως διακομιστή και μέσω του πελάτη h1 εκτελέσαμε την εντολή «*iperf -c 10.0.0.2*» (εικόνα 61) καταγράφοντας το μέγιστο εύρος ζώνης μεταξύ των hosts στο αρχείο iperf-h2. Η λειτουργία του διακομιστή μας μέτρησε τον όγκο των δεδομένων που μεταφερθήκανε μεταξύ των δύο κεντρικών υπολογιστών μέσω του δικτύου και το μέγιστο εύρος ζώνης που επιτεύχθηκε ενώ η λειτουργία πελάτη μας μέτρησε το εύρος ζώνης και την απόδοση της σύνδεσης δικτύου στέλνοντας πακέτα δεδομένων και μετρώντας το χρόνο που απαιτείται για

τη μετάδοση και τη λήψη των πακέτων. Επαναλάβαμε τις μετρήσεις για να λάβουμε έναν ακριβέστερο μέσο όρο εύρους ζώνης.



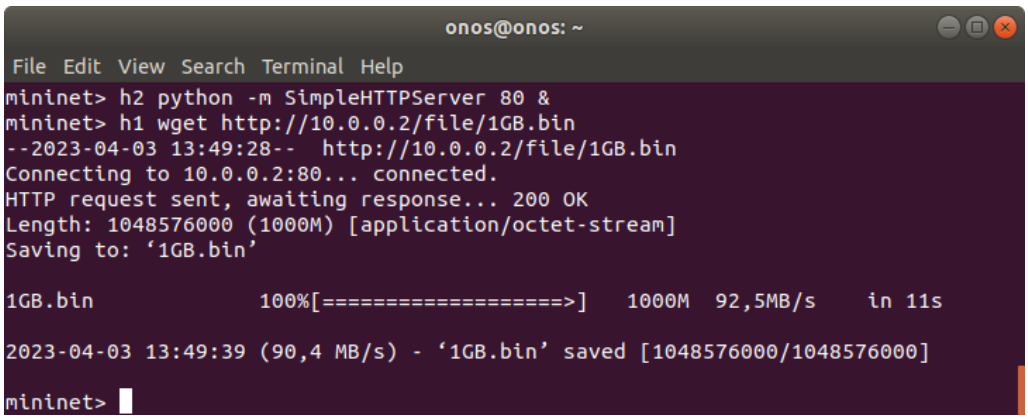
Εικόνα 60: Μέτρηση bandwidth μέσω iPerf



Εικόνα 61: Μέτρηση bandwidth μέσω iPerf

4.4.4 Μέτρηση εύρους ζώνης διακομιστή ιστού

Για τη μέτρηση του εύρους ζώνης διακομιστή ιστού εκκινήσαμε ένα διακομιστή ιστού στον host h2 εισάγοντας την εντολή «*h2 python -m SimpleHTTPServer 80 &*» (εικόνα 62). Η εντολή θα εκκινήσει στο παρασκήνιο ένα HTTP Server στη θύρα 80 (η οποία είναι η προεπιλεγμένη θύρα για το πρωτόκολλο HTTP). Το εύρος ζώνης αναφέρεται στη μέγιστη ποσότητα δεδομένων που μπορεί να μεταφερθεί μέσω ενός δικτύου σε δεδομένο χρονικό διάστημα, ενώ η καθυστέρηση στο χρόνο που χρειάζεται ένα πακέτο δεδομένων για να ταξιδέψει μεταξύ των hosts h1 και h2. Η απόδοση αναφέρεται στην ποσότητα των δεδομένων που μπορεί να μεταφερθεί μέσω του δικτύου σε δεδομένο χρονικό διάστημα, λαμβάνοντας υπόψη τον αντίκτυπο των συνθηκών του δικτύου, όπως η συμφόρηση και η απώλεια πακέτων. Στη συνέχεια, εκτελέσαμε διαδοχικά την εντολή «*h1 wget http://10.0.0.2/1GB.bin*» στον host h1 (εικόνα 62) για να κάνουμε λήψη του αρχείου 1GB.bin μεγέθους 1GB από το διακομιστή ιστού h2. Επαναλάβαμε τις μετρήσεις και καταγράψαμε το συνολικό χρόνο που χρειάστηκε για τη λήψη ολόκληρου του αρχείου αλλά και την ταχύτητα με την οποία έγινε η λήψη του αρχείου.



Εικόνα 62: Λήψη αρχείου από το web server

4.5 Αξιολόγηση SDN κατά την προσομοίωση επίθεσης DDoS

Ο ελεγκτής ONOS απαιτεί αρκετές θύρες για διαφορετικές λειτουργίες, όπως η επικοινωνία με το OpenFlow, η πρόσβαση στο REST API, η ομαδοποίηση και η ανταλλαγή μηνυμάτων και η πρόσβαση μέσω SSH. Από προεπιλογή, το πρωτόκολλο OpenFlow χρησιμοποιεί τις θύρες 6653 και 6640, ενώ το REST API είναι προσβάσιμο στη θύρα 8181. Οι θύρες ομαδοποίησης και ανταλλαγής μηνυμάτων περιλαμβάνουν τις 8101, 5701 και 61616. Ο διακομιστής SSH είναι προσβάσιμος στη θύρα 8101 στην οποία και θα εκτελέσουμε την επίθεση πλημμύρας TCP SYN μέσω της εφαρμογής hping3.

4.5.1 Μέτρηση του χρόνου απόκρισης

Εισαγάγαμε την εντολή «*sudo hping3 --flood -S -i u1000 --rand-source -p 8101 10.0.10.11*» (εικόνα 63) για να εκκινήσουμε την επίθεση πλημμύρας TCP SYN εναντίον του απομακρυσμένου ελεγκτή με διεύθυνση IP 10.0.10.11 και θύρα 8101. Έχοντας ενεργοποιημένο το SYN flag υπερφορτώσαμε τον ελεγκτή ONOS με εισερχόμενα TCP αιτήματα σύνδεσης, επηρεάζοντας την απόδοση του.

Με την εντολή hping3 χρησιμοποιήσαμε τις ακόλουθες ρυθμίσεις:

- --flood: Αποστολή πακέτων χωρίς καθυστέρηση.

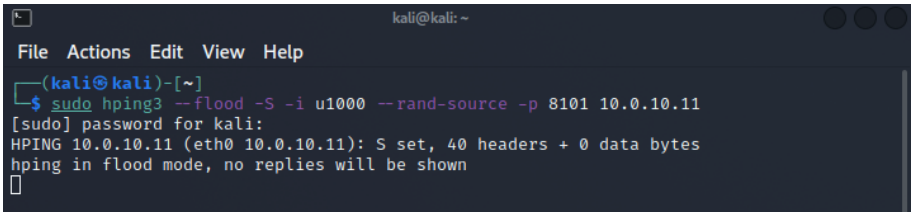
- -S: Θέσαμε τη σημαία (flag) SYN στα πακέτα TCP, υποδεικνύοντας αίτημα για έναρξη σύνδεσης.

- -i u1000: Διάστημα μεταξύ των πακέτων που αποστέλλονται σε 1 millisecond.

- --rand-source: Επιλογή τυχαίων διευθύνσεων IP για κάθε πακέτο που αποστέλλεται. Αυτό βοηθά στην αποφυγή ανίχνευσης ή φιλτραρίσματος με βάση τη διεύθυνση IP.

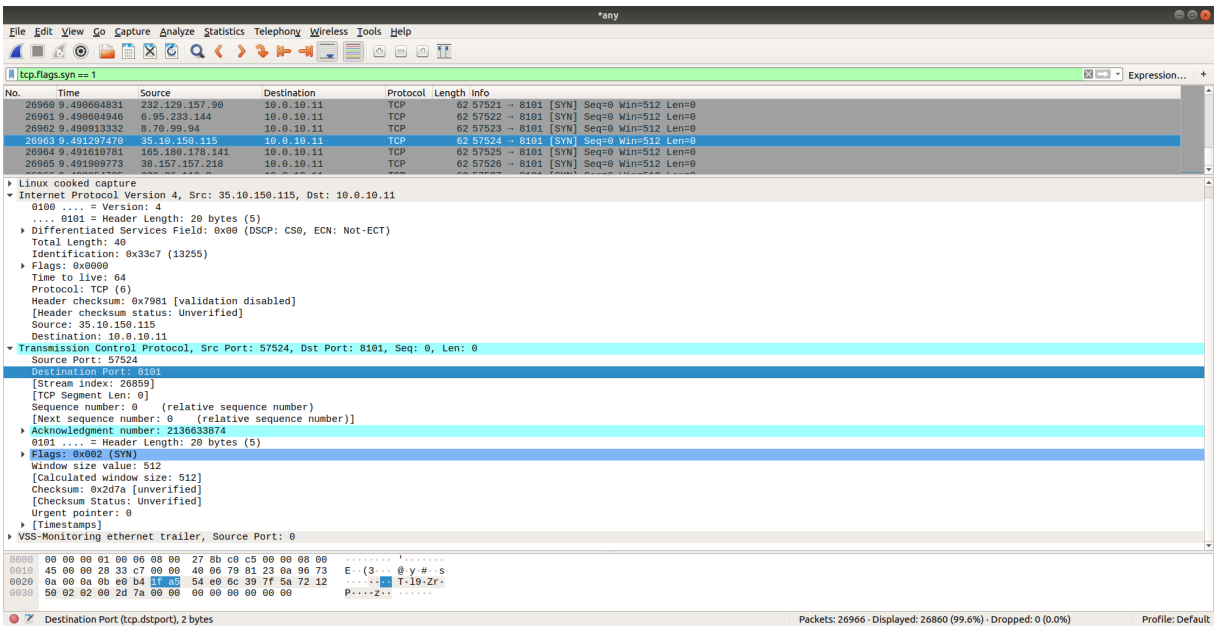
- -p 8101: Επιλογή θύρας προορισμού σε 8101.

- 10.0.10.11: Καθορισμός της IP διεύθυνσης στόχου της επίθεσης.



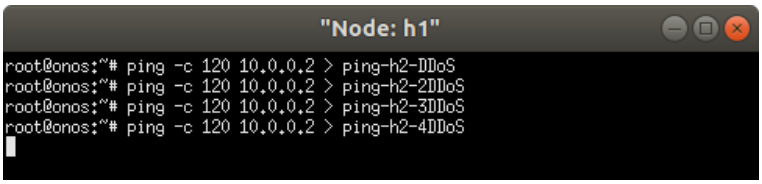
Εικόνα 63: Kali Linux εκτέλεση επίθεσης πλημμύρας TCP SYN

Χρησιμοποιώντας το Wireshark (εικόνα 64) καταγράψαμε την επίθεση στον ελεγκτή έχοντας ενεργοποιημένο το φίλτρο TCP SYN (*tcp.flags.syn == 1*) όπου παρουσιάζεται η εκθετική αύξηση της κίνησης TCP SYN κατά τη διάρκεια της πλημμύρας TCP SYN. Το φίλτρο επιλέγει όλα τα πακέτα που έχουν ενεργοποιημένο το TCP SYN flag ίσο με 1, υποδεικνύοντας το αίτημα για έναρξη σύνδεσης.



Εικόνα 64: Wireshark ενεργοποίηση φίλτρου TCP SYN

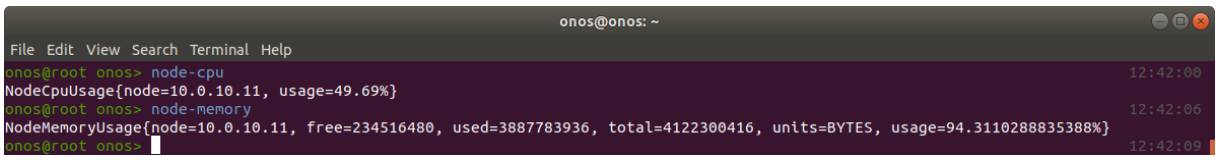
Επαναλάβαμε τα βήματα εκτελώντας κλιμακωτά (εικόνα 65) ταυτόχρονες επιθέσεις πλημμύρας TCP SYN στον ελεγκτή και αποθηκεύσαμε τα αποτελέσματα στα αρχεία ping-h2-DDoS, ping-h2-DDoS, ping-h2-3DDoS, ping-h2-4DDoS και ping-h2-6DDoS.



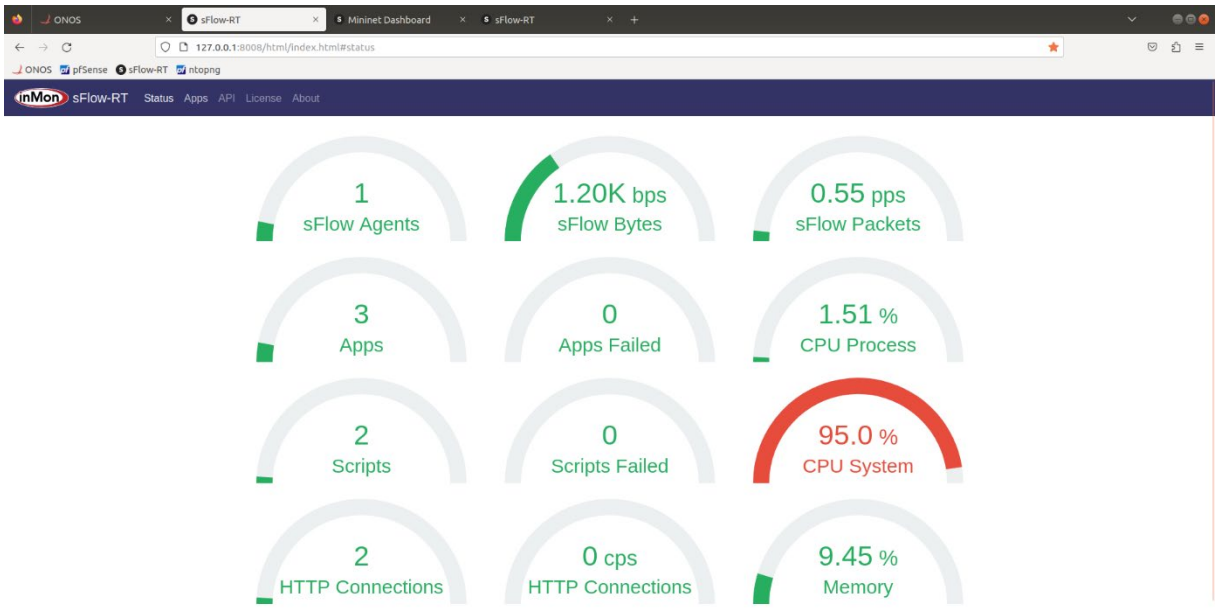
Εικόνα 65: Μέτρηση χρόνου απόκρισης κατά τη εκτέλεση επίθεσης DDoS

4.5.2 Μέτρηση υπερφόρτωσης του ελεγκτή

Κατά την διάρκεια εκτέλεσης της επίθεσης DDoS και της ανταλλαγής των πακέτων μεταξύ των hosts καταγράψαμε τις μετρήσεις του φορτίου του επεξεργαστή (CPU) και της μνήμης (memory) με τη χρήση των εντολών «*node-cpu*» και «*node-memory*» (εικόνα 66). Μέσω του προγράμματος sFlow-RT, εμφανίσαμε το φορτίο του ελεγκτή σε πραγματικό χρόνο (εικόνα 67).



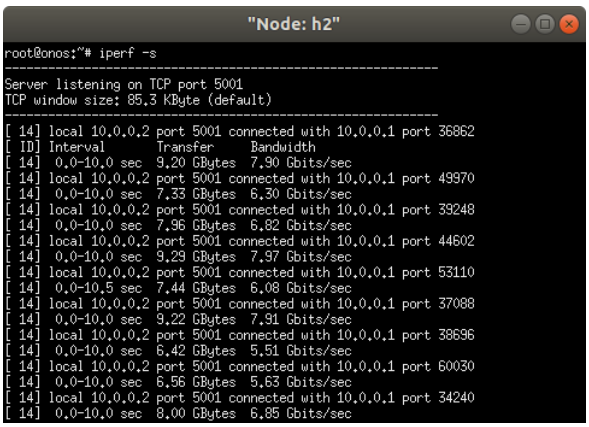
Εικόνα 66: Φορτίο επεξεργαστή και μνήμης ONOS



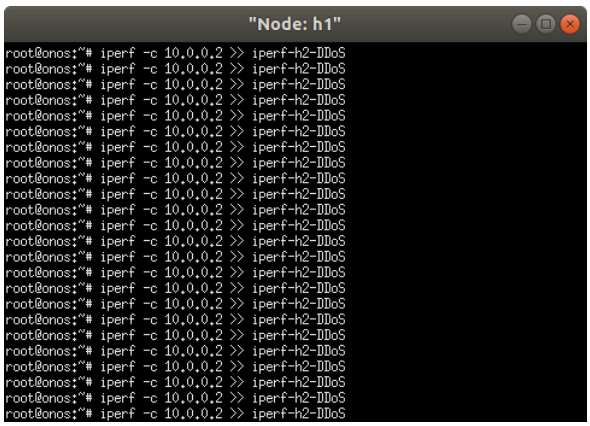
Εικόνα 67: Υπερφόρτωση του επεξεργαστή του ελεγκτή

4.5.3 Μέτρηση εύρους ζώνης δικτύου

Για την μέτρηση του εύρους ζώνης χρησιμοποιήσαμε το εργαλείο iPerf. Με την εντολή «*iperf -s*» (εικόνα 68) δηλώσαμε τον h2 ως διακομιστή και μέσω του h1 εκτελέσαμε την εντολή «*iperf -c 10.0.0.2*» (εικόνα 69) διαδοχικά καταγράφοντας το εύρος ζώνης μεταξύ των hosts.



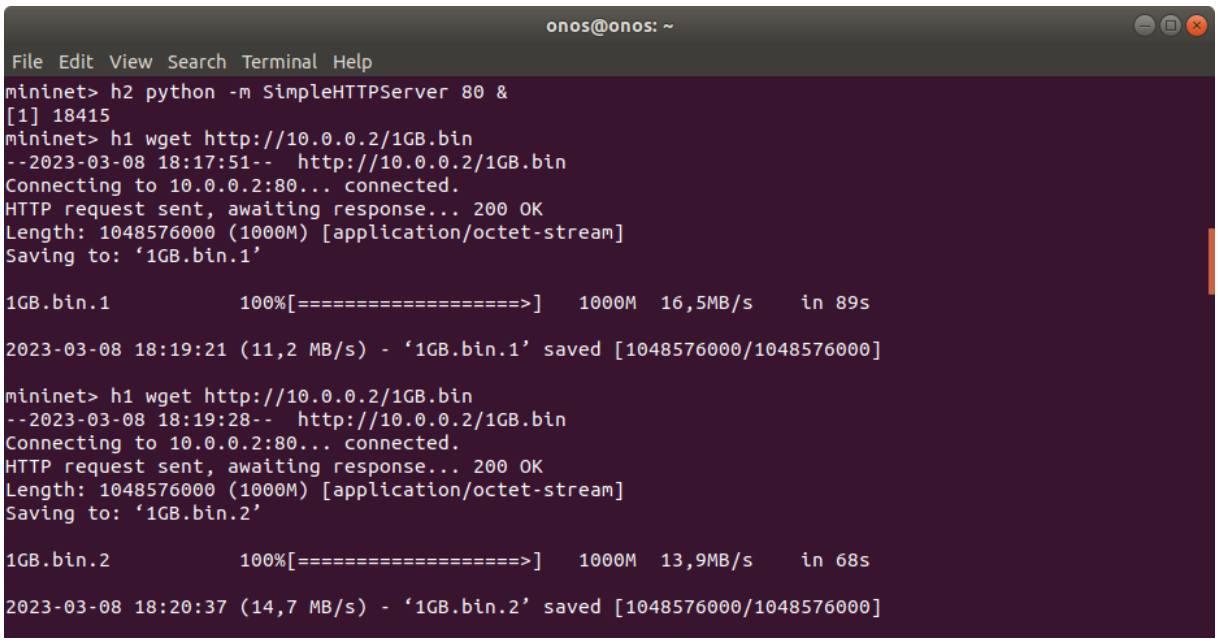
Εικόνα 68: Μέτρηση bandwidth μέσω iPerf



Εικόνα 69: Μέτρηση bandwidth μέσω iPerf

4.5.4 Μέτρηση εύρους ζώνης διακομιστή ιστού

Κατά τη διάρκεια της επίθεσης πλημμύρας TCP SYN εισαγάγαμε διαδοχικά την εντολή «*h1 wget http://10.0.0.2/1GB.bin*» στον host h1 για να κάνουμε λήψη του αρχείου 1GB.bin μεγέθους 1GB από το διακομιστή ιστού h2 (εικόνα 70). Επαναλάβαμε τις μετρήσεις και καταγράψαμε το συνολικό χρόνο που χρειάστηκε για τη λήψη ολόκληρου του αρχείου αλλά και της ταχύτητας με την οποία έγινε η λήψη του αρχείου.

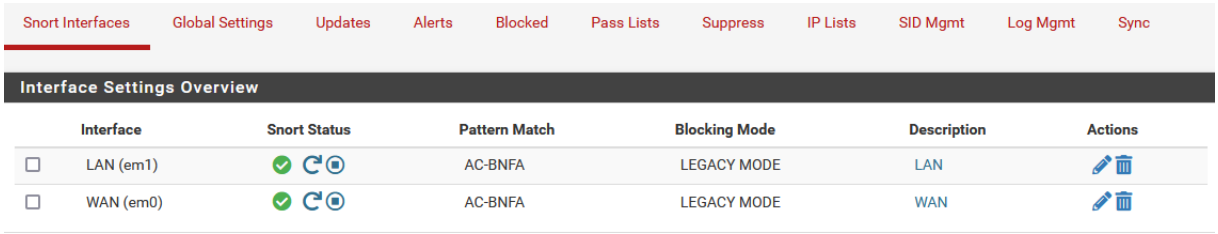


Εικόνα 70: Λήψη αρχείου από Web server κατά τη διάρκεια επίθεσης DDoS

4.6 Αξιολόγηση SDN με τη χρήση συστήματος IDS/IPS κατά την προσομοίωση επίθεσης DDoS

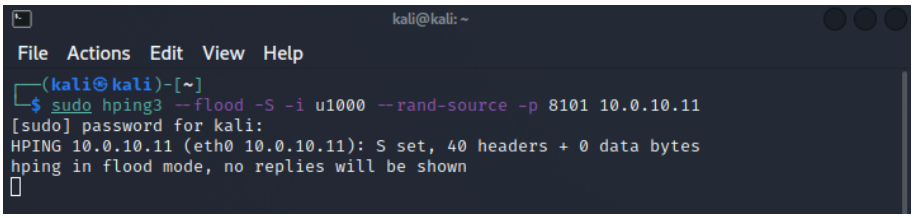
4.6.1 Ρύθμιση συστήματος IDS/IPS

Ενεργοποιήσαμε το Snort στα interfaces του pfSense (εικόνα 71) για να θέσουμε σε λειτουργία το σύστημα IDS/IPS. Ακολούθως, διαμορφώσαμε το blocking mode σε legacy mode για να ρυθμίσουμε το Snort να εκτελείται ως ανιχνευτής πακέτων και να αναλύει την κυκλοφορία του δικτύου αποκλείοντας ταυτόχρονα την IP διεύθυνση πηγής.



Εικόνα 71: snort interfaces

Από το Kali Linux εκτελέσαμε την εντολή «*sudo hping3 –flood -S -I u1000 –rand-source -p 8101 10.0.10.11*» (εικόνα 72) για να ξεκινήσουμε την επίθεση πλημμύρας TCP SYN εναντίον του απομακρυσμένου ελεγκτή 10.0.10.11 στη θύρα 8101 έχοντας ενεργοποιημένο το σύστημα IDS/IPS.



Εικόνα 72: Επίθεση πλημμύρας στον ελεγκτή

Όπως φαίνεται από το στιγμιότυπο της εικόνας 73 του αρχείου καταγραφής, που δημιουργείται από το σύστημα του τείχους προστασίας του pfSense, η κακόβουλη κυκλοφορία έχει αποκλειστεί.

Εικόνα 73: pfSense filter logs

Με βάση την τελευταία καταχώριση της εικόνας 73 που προέρχεται από την IP διεύθυνση πηγής 249.136.233.166 έχουμε τις πιο κάτω πληροφορίες:

- Mar 9 08:28:24: Ημερομηνία και ώρα που συνέβη το συμβάν.

- pfSense filterlog[21949]: Η διεργασία (αρχείο καταγραφής φίλτρου pfSense) που δημιούργησε την καταχώρηση.

- 4,,,1000000103,em1,match,block,in: Πληροφορίες για τον αριθμό του κανόνα (4), τη διασύνδεση στην οποία ανιχνεύθηκε η κυκλοφορία (em1) και την ενέργεια που έγινε (block) από το τείχος προστασίας. Το "in" υποδεικνύει ότι η κυκλοφορία ήταν εισερχόμενη.

- 4,0x0,,64,0,0,DF,6,tcp,44: Πληροφορίες σχετικά με την κυκλοφορία, συμπεριλαμβανομένου του rule ID (4), τα packet flags (0x0), το packet length (64), το fragmentation offset (0), το πρωτοκόλλου IP (IPv4, που υποδεικνύεται από το "DF,6") και μέγεθος πακέτου TCP 44 bytes.

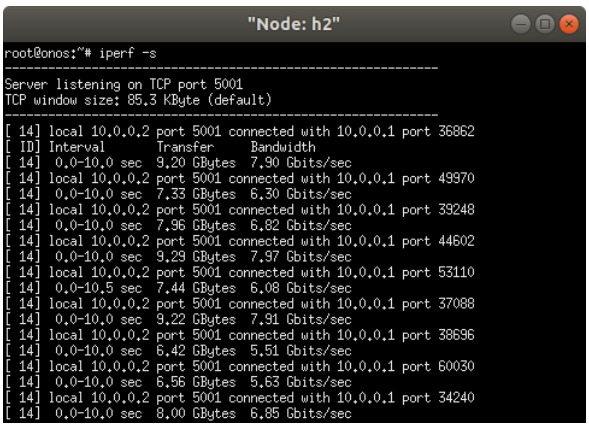
- 10.0.10.11, 249.136.233.166,8101,8523: IP διευθύνσεις προέλευσης και προορισμού, καθώς και τις θύρες προέλευσης και προορισμού της κίνησης αντίστοιχα.

- 0,SA,2994630287,1001793200,64240: Σημαίες TCP που τέθηκαν στο πακέτο. Σε αυτή την περίπτωση, η σημαία SYN-ACK (SA), αριθμός ακολουθίας (sequence number) (2994630287), αριθμός επιβεβαίωσης (acknowledge number) (1001793200) και το μέγεθος παραθύρου (windows size) (64240).

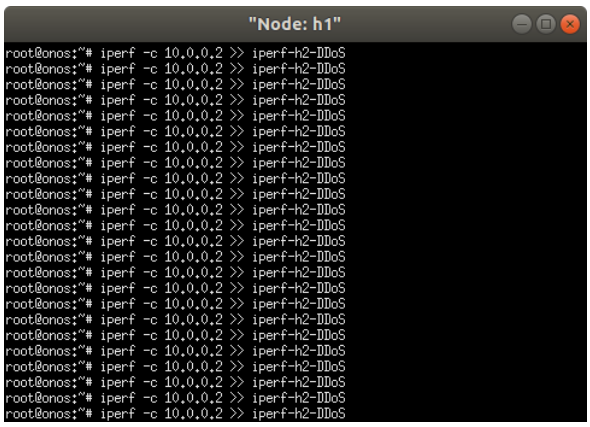
- mss: Τιμή MSS (Maximum Segment Size) του TCP, η οποία χρησιμοποιείται για τον καθορισμό της μέγιστης ποσότητας δεδομένων που μπορεί να μεταδοθεί σε ένα μόνο τμήμα TCP.

4.6.1 Μέτρηση του χρόνου απόκρισης

Κατά τη διάρκεια της επίθεσης DDoS και έχοντας ενεργοποιημένο το σύστημα IDS/IPS καταγράψαμε το χρόνο απόκρισης μεταξύ των hosts στο αρχείο καταγραφής iperf-h2-DDoS (εικόνες 74-75). Επαναλάβαμε τις μετρήσεις μας για να λάβουμε έναν ακριβέστερο μέσο όρο απόκρισης και να εντοπίσουμε τυχόν διακυμάνσεις.



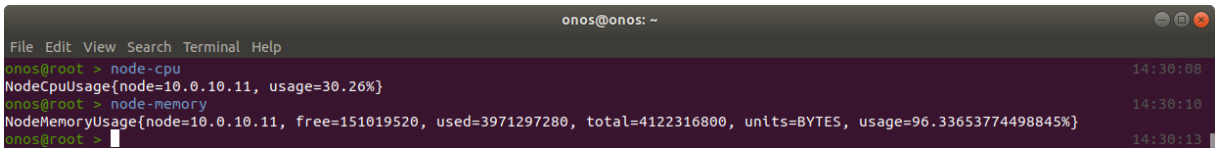
Εικόνα 74: Μέτρηση bandwidth μέσω iPerf



Εικόνα 75: Μέτρηση bandwidth μέσω iPerf

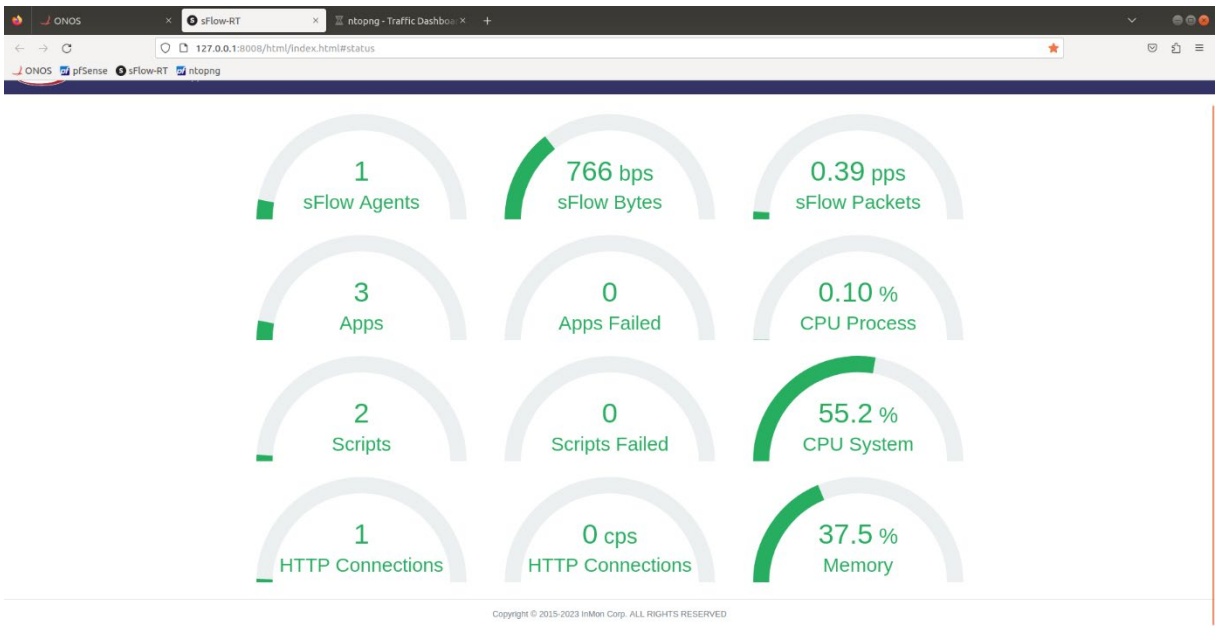
4.6.2 Μέτρηση φορτίου ελεγκτή

Κατά την διάρκεια εκτέλεσης της επίθεσης DDoS και της ανταλλαγής των πακέτων μεταξύ των hosts καταγράψαμε τις μετρήσεις του φορτίου του επεξεργαστή (CPU) και της μνήμης (memory) έχοντας ενεργοποιημένο το σύστημα IDS/IPS.



Εικόνα 76: Φορτίο επεξεργαστή και μνήμης ONOS

Η καταγραφή των μετρήσεων έγινε με τη χρήση των εντολών «*node-cpu*» και «*node-memory*» (εικόνα 76). Μέσω του προγράμματος sFlow-RT, εμφανίσαμε το φορτίο του ελεγκτή σε πραγματικό χρόνο (εικόνα 77). Επαναλάβαμε τις μετρήσεις μας για να λάβουμε έναν ακριβέστερο μέσο όρο του φορτίου και να εντοπίσουμε τυχόν διακυμάνσεις.



Εικόνα 77: Φορτίο επεξεργαστή και μνήμης ONOS

Το pfSense έχει αποκλείσει τα αιτήματα TCP:SA (εικόνα 78). Το TCP:SA είναι πακέτο έναρξης σύνδεσης TCP, όπου η σημαία TCP SYN (S) είναι ενεργοποιημένη ενώ η σημαία TCP Acknowledgment (A) είναι απενεργοποιημένη. Η κυκλοφορία του πρωτοκόλλου TCP:SA έχει ελεγχθεί μέσω των κανόνων του τείχους προστασίας και των πολιτικών διαμόρφωσης της κυκλοφορίας και έχει αποκλειστεί από το σύστημα IDS/IPS.

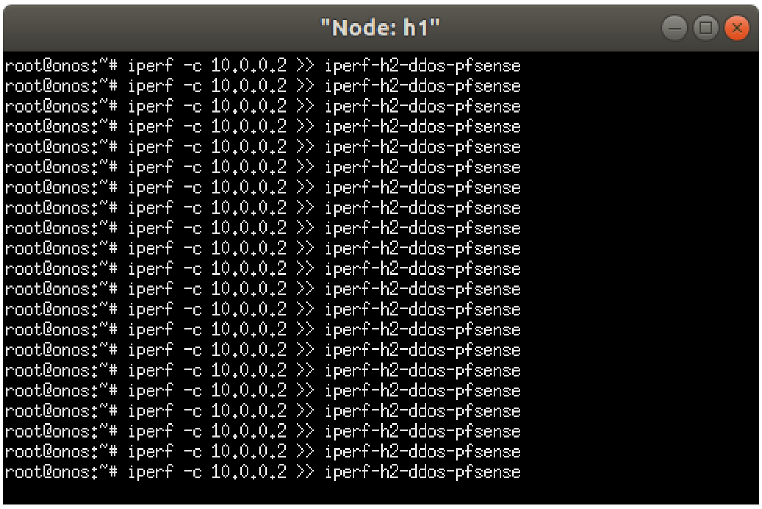
Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Mar 11 14:40:14	LAN	Default deny rule IPv4 (1000000103)	10.0.10.11:8101	63.228.151.79:19845	TCP:SA
✕	Mar 11 14:40:14	LAN	Default deny rule IPv4 (1000000103)	10.0.10.11:8101	255.225.58.207:19846	TCP:SA
✕	Mar 11 14:40:14	LAN	Default deny rule IPv4 (1000000103)	10.0.10.11:8101	62.161.70.21:19847	TCP:SA

Εικόνα 78: Πρωτόκολλο TCP:SA

4.6.3 Μέτρηση εύρους ζώνης δικτύου

Για την μέτρηση του εύρους ζώνης εκτελέσαμε την εντολή «*iperf -s*» στον διακομιστή h2 και μέσω του client h1 καταγράψαμε το εύρος ζώνης με τη χρήση της εντολής «*iperf -c 10.0.0.2*» (εικόνα 79) μεταξύ των δυο hosts. Η μέτρηση του εύρους ζώνης έγινε κατά τη διάρκεια της επίθεσης DDoS αλλά με την ταυτόχρονη χρήση της λειτουργίας IDS/IPS. Εκτελέσαμε διαδοχικά την εντολή καταγράφοντας το εύρος ζώνης στο αρχείο iperf-h2-ddos-pfsense.

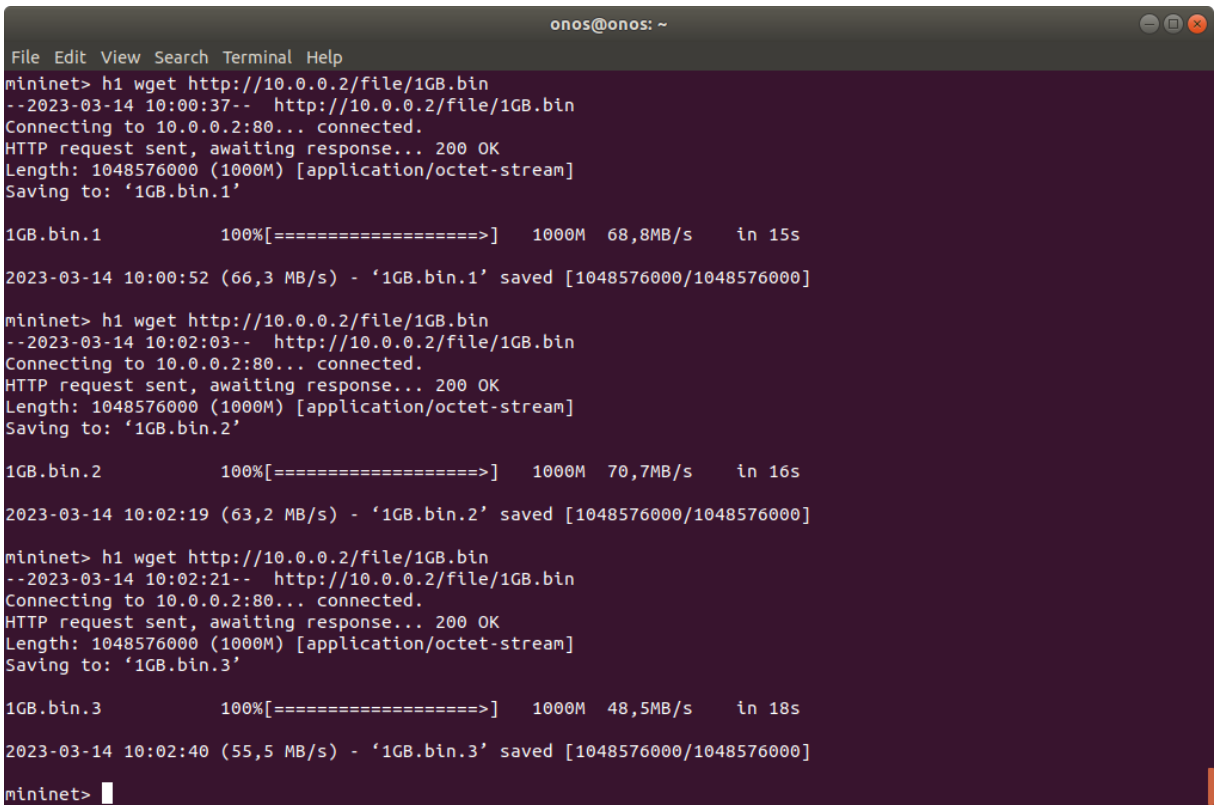


Εικόνα 79: Μέτρηση του εύρους ζώνης κατά τη διάρκεια επίθεσης DDoS με ενεργοποιημένη τη λειτουργία IDS/IPS

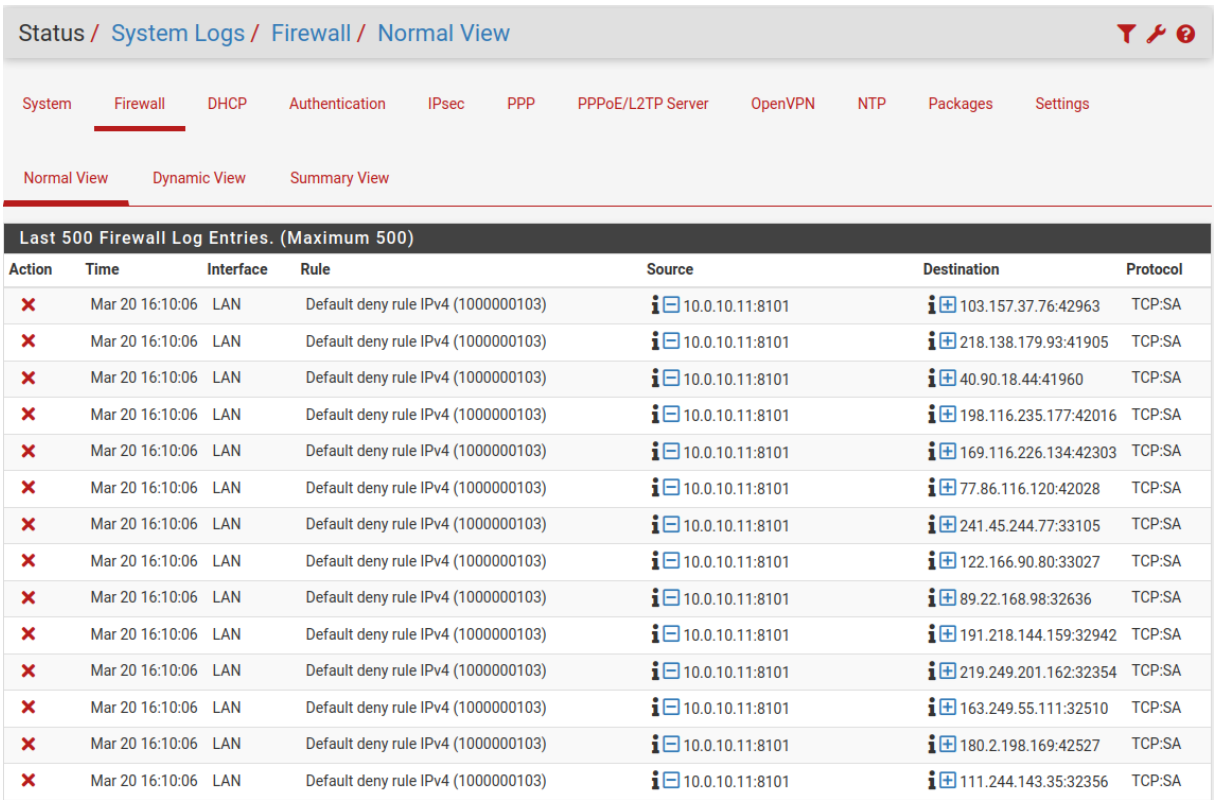
4.6.4 Μέτρηση εύρους ζώνης διακομιστή ιστού

Κατά τη διάρκεια της προσομοίωσης της επίθεσης πλημμύρας TCP SYN εισαγάγαμε διαδοχικά την εντολή «*h1 wget http://10.0.0.2/file/1GB.bin*» στον host h1 και κάναμε λήψη του αρχείου 1GB.bin μεγέθους 1GB από το διακομιστή ιστού h2 (εικόνα 80). Επαναλάβαμε τη λήψη και καταγράψαμε το συνολικό χρόνο που χρειάστηκε για τη λήψη ολόκληρου του αρχείου αλλά και της ταχύτητας με την οποία έγινε η λήψη.

Ωστόσο, το σύστημα IDS/IPS μπόρεσε να μετριάσει αποτελεσματικά την επίθεση αποκλείοντας όλα τα αιτήματα που αφορούσαν το πρωτόκολλο TCP:SA, το οποίο χρησιμοποιείται συνήθως σε επιθέσεις TCP SYNC. Αυτό απέτρεψε την κακόβουλη κίνηση να κατακλίσει τον ελεγκτή ONOS (εικόνας 81).



Εικόνα 80: Λήψη αρχείου από το διακομιστή ιστού κατά τη διάρκεια επίθεσης DDoS με ενεργοποιημένη τη λειτουργία IDS/IPS



Εικόνα 81: pfSense logs

Κεφάλαιο 5
Αποτελέσματα

Η στατιστική ανάλυση των αποτελεσμάτων αποτελεί σημαντικό βήμα για την κατανόηση και την ερμηνεία των μετρήσεων που έχουμε λάβει. Στην παρούσα μεταπτυχιακή διατριβή, πραγματοποιήθηκαν μετρήσεις σε δίκτυο Mininet για τέσσερα διαφορετικά σενάρια: το πρώτο χωρίς επίθεση DDoS (μεταβλητή NoDDoS) στον ελεγκτή, το δεύτερο με προσομοίωση επίθεσης DDoS (μεταβλητή DDoS) στον ελεγκτή, το τρίτο με DDoS αλλά έχοντας σε λειτουργία σύστημα IDS/IPS (μεταβλητή IDSIPS1) και το τέταρτο με DDoS διαφορετικής ισχύος αλλά έχοντας σε λειτουργία σύστημα IDS/IPS (μεταβλητή IDSIPS2). Η διαφορά του τρίτου και του τέταρτου σεναρίου έγκειται στην ισχύ της επίθεσης DDoS. Συγκεκριμένα στο τρίτο σενάριο ο ρυθμός μετάδοσης των πακέτων ήτανε στο 1 χιλιοστό του δευτερολέπτου (παράμετρος hping3 - u1000) ενώ στο τέταρτο σενάριο ο ρυθμός μετάδοσης των πακέτων ήτανε στο 0,1 χιλιοστό του δευτερολέπτου (παράμετρος hping3 - u100). Η εκτέλεση της εντολής με παράμετρο u100 οδήγησε σε χαμηλότερο συνολικό ρυθμό μετάδοσης πακέτων. Η στατιστική ανάλυση των δεδομένων μας παρείχε πολύτιμες πληροφορίες σχετικά με τον αντίκτυπο των επιθέσεων DDoS και την αποτελεσματικότητα του συστήματος IDS/IPS στον μετριασμό τέτοιων επιθέσεων.

Σημειώνεται ότι κατά την εκτέλεση ενός πέμπτου σεναρίου με ισχύ επίθεσης στα u10000, προκάλεσε υψηλό φορτίο επεξεργασίας στον host που φιλοξενούσε την εικονική μηχανή για το σύστημα IDS/IPS με αποτέλεσμα να υπάρχει μεγάλη καθυστέρηση που δεν οφειλόταν αποκλειστικά και μόνο στην επίθεση DDoS και στον υψηλό ρυθμό αποστολής των αιτημάτων TCP SYN. Με βάση το εύρημα αυτό, οι μετρήσεις που έγιναν για το πέμπτο σενάριο δεν κρίνονται αντιπροσωπευτικές, για αυτό το λόγο δεν έχουν παρατεθεί πιο κάτω.

5.1 Στατιστική ανάλυση αποτελεσμάτων

5.1.1 Στατιστική ανάλυση χρόνου απόκρισης του δικτύου

Η εικόνα 82 παρουσιάζει τα γενικά στατιστικά των τεσσάρων μεταβλητών (NoDDoS, DDoS, IDSIPS1, IDSIPS2) στο πλαίσιο της μέτρησης του χρόνου απόκρισης. Το σύνολο των μετρήσεων για όλες τις πιο πάνω μεταβλητές ήταν 118. Όπως φαίνεται και στην εικόνα 82 ο ελάχιστος χρόνος απόκρισης καταγράφηκε με το σενάριο NoDDoS ενώ ο μέγιστος χρόνος απόκρισης καταγράφηκε με το σενάριο DDoS. Οι μέσες τιμές με τη λειτουργία IPSIDS1 και IDSIPS2 (0.082805 και 0.081076 ms αντίστοιχα) κυμαίνονται μεταξύ των αντίστοιχων μέσων τιμών όπως αυτές έχουν καταγραφεί για τις μεταβλητές NoDDoS και DDoS (0.066797 ms και 0.126610 ms αντίστοιχα). Η ενεργοποίηση του συστήματος IDS/IPS στο δίκτυο προκάλεσε επιπλέον καθυστέρηση λόγω της πρόσθετης επεξεργασίας που απαιτήθηκε για την επιθεώρηση της κυκλοφορίας του δικτύου. Η ανάλυση των πακέτων σε πραγματικό χρόνο, αναζητώντας κακόβουλη δραστηριότητα προκάλεσε -όπως ήταν αναμενόμενο- επιπρόσθετη καθυστέρηση. Ωστόσο, τα οφέλη της ύπαρξης ενός συστήματος IDS/IPS για τον εντοπισμό και την πρόληψη πιθανών παραβιάσεων της ασφάλειας μπορεί να αντισταθμίσουν τη μικρή αύξηση της καθυστέρησης του δικτύου.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
NoDDoS	118	.0460	.4610	.066797	.0435632
DDoS	118	.0430	3.1500	.126610	.3102759
IDSIPS1	118	.0400	.6010	.082805	.0856569
IDSIPS2	118	.0440	.5900	.081076	.0801764
Valid N (listwise)	118				

Εικόνα 82: Στατιστική ανάλυση του χρόνου απόκρισης μεταξύ των hosts

5.1.2 Στατιστική ανάλυση φορτίου επεξεργαστή του ελεγκτή

Συνεχίζοντας την έρευνα μας, στην εικόνα 83 παρουσιάζονται τα γενικά στατιστικά των τεσσάρων μεταβλητών (NoDDoS, DDoS, IDSIPS1, IDSIPS2) στο πλαίσιο της μέτρησης του φορτίου του επεξεργαστή στον ελεγκτή. Το σύνολο των μετρήσεων για όλες τις πιο πάνω μεταβλητές ήταν 30. Όπως παρουσιάζεται στην εικόνα 83 η ελάχιστη χρήση CPU από τον ελεγκτή είναι με το σενάριο IPSIDS2 ενώ η μέγιστη χρήση της CPU είναι με το σενάριο DDoS (6% και 27% αντίστοιχα – η χρήση του επεξεργαστή εκφράζεται ως ποσοστό επί της συνολικής χωρητικότητας του επεξεργαστή του ελεγκτή). Αυτό οφείλεται στο γεγονός ότι το σύστημα IDS/IPS ήταν σε θέση να εντοπίσει και να αποκλείσει την κακόβουλη κυκλοφορία πιο αποτελεσματικά από ό,τι θα μπορούσε να χειριστεί ο ελεγκτής χωρίς IDS/IPS μειώνοντας ταυτόχρονα τη συνολική επεξεργαστική ισχύ που απαιτείται για τη διαχείριση της κυκλοφορίας δικτύου, με αποτέλεσμα τη χαμηλότερη χρήση της CPU. Αυτό οδήγησε σε χαμηλότερη συνολική χρήση της CPU από τον ελεγκτή παρά το πρόσθετο φορτίο επεξεργασίας του συστήματος IDS/IPS.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
NoDDoS	30	.0600	.1400	.083667	.0232651
DDoS	30	.2600	.3000	.277333	.0201603
IDSIPS1	30	.0300	.1800	.135000	.0699137
IDSIPS2	30	.0600	.0600	.060000	.0000000
Valid N (listwise)	30				

Εικόνα 83: Στατιστική ανάλυση του φορτίου επεξεργαστή του ελεγκτή

5.1.3 Στατιστική ανάλυση φορτίου μνήμης του ελεγκτή

Η εικόνα 84 παρουσιάζει τα γενικά στατιστικά των τεσσάρων μεταβλητών (NoDDoS, DDoS, IDSIPS1, IDSIPS2) στο πλαίσιο της μέτρησης του φορτίου της μνήμης στον ελεγκτή. Το σύνολο των μετρήσεων για κάθε ένα από τα σενάρια αυτά ήταν 30. Διαπιστώνουμε ότι το σενάριο χωρίς επίθεση DDoS στον ελεγκτή έχει τη χαμηλότερη μέση χρήση RAM (0.157562 GB), ενώ το σενάριο με επίθεση DDoS έχει την υψηλότερη μέση χρήση RAM (3.707104 GB). Με την ταυτόχρονη λειτουργία του συστήματος IDS/IPS προστέθηκε επιπρόσθετη επιβάρυνση στην επεξεργασία του ελεγκτή, η οποία προκάλεσε αύξηση στη χρήση μνήμης.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
NoDDoS	30	.1565	.1605	.157262	.0016466
DDoS	30	3.7063	3.7081	3.707104	.0006898
IPSIDS1	30	3.5917	3.6033	3.601123	.0044753
IDSIPS2	30	3.5766	3.5792	3.577350	.0012322
Valid N (listwise)	30				

Εικόνα 84: Στατιστική ανάλυση φορτίο μνήμης του ελεγκτή

5.1.4 Στατιστική ανάλυση εύρους ζώνης δικτύου

Η εικόνα 85 παρουσιάζει τα γενικά στατιστικά των τεσσάρων μεταβλητών (NoDDoS, DDoS, IDSIPS1, IDSIPS2) στο πλαίσιο της μέτρησης του εύρους ζώνης του δικτύου. Το σύνολο των μετρήσεων για κάθε σενάριο ήταν 31. Από τα αποτελέσματα, μπορούμε να διαπιστώσουμε ότι το σενάριο χωρίς επίθεση DDoS στον ελεγκτή έχει το καλύτερο μέτρο εύρος ζώνης δικτύου, με μια μέση τιμή της τάξης των 9.097097 Gbps, ενώ το σενάριο με επίθεση DDoS έχει το χαμηλότερο μέτρο εύρος ζώνης δικτύου (6.788387 Gbps). Αυτή η σύγκριση μας βοηθά να κατανοήσουμε τον αντίκτυπο των επιθέσεων DDoS στο εύρος ζώνης του δικτύου και τη σημασία της εφαρμογής αντιμέτρων, όπως IDS/IPS, για τον μετριασμό του αντίκτυπου τέτοιων επιθέσεων.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
NoDDoS	31	5.5000	10.2000	9.097097	.8557928
DDoS	31	5.4200	8.0600	6.788387	.7803636
IDSIPS1	31	7.5900	9.2500	8.664516	.4066681
IDSIPS2	31	6.7400	9.5600	8.695484	.5414846
Valid N (listwise)	31				

Εικόνα 85: Στατιστική ανάλυση του εύρους ζώνης δικτύου

5.1.5 Στατιστική ανάλυση εύρους ζώνης διακομιστή ιστού

Η εικόνα 86 παρουσιάζει τα γενικά στατιστικά των τεσσάρων μεταβλητών (NoDDoS, DDoS, IDSIPS1, IDSIPS2) στο πλαίσιο της μέτρησης του εύρους ζώνης του διακομιστή ιστού. Το σύνολο των μετρήσεων για κάθε σενάριο ήταν 29. Από τα αποτελέσματα, μπορούμε να διαπιστώσουμε ότι το σενάριο χωρίς επίθεση DDoS στον ελεγκτή έχει το καλύτερο μέτρο απόδοσης του

διακομιστή ιστού, ενώ το σενάριο με επίθεση DDoS έχει το χειρότερο μέτρο (66.492069 Mbps και 13.920 Mbps αντίστοιχα).

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
NoDDoS	29	9.4700	85.2000	66.492069	19.6347351
DDoS	29	7.2800	20.0000	13.920000	2.6111902
IDSIPS1	29	30.9000	70.5000	46.610345	6.3026834
IDSIPS2	29	21.3000	79.2000	60.168966	11.3512146
Valid N (listwise)	29				

Εικόνα 86: Στατιστική ανάλυση εύρους ζώνης διακομιστή ιστού

5.1.5 Στατιστική ανάλυση χρόνου λήψης αρχείου από το διακομιστή ιστού

Η εικόνα 87 παρουσιάζει τα γενικά στατιστικά των τεσσάρων μεταβλητών (NoDDoS, DDoS, IDSIPS1, IDSIPS2) στο πλαίσιο της μέτρησης του χρόνου λήψης αρχείου από το διακομιστή ιστού. Το σύνολο των μετρήσεων για κάθε σενάριο ήταν 29. Από τα αποτελέσματα, διαπιστώνουμε ότι το σενάριο IDSIPS2 έχει τον ταχύτερο χρόνο λήψης του αρχείου με μέσο όρο στα 16.4828 s, ενώ το σενάριο με επίθεση DDoS έχει τον υψηλότερο χρόνο λήψης (75.4483 s) του αρχείου από το διακομιστή ιστού. Ακολουθεί με ελάχιστη διαφορά από το IDSIPS2 το σενάριο χωρίς επίθεση DDoS στον ελεγκτή.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
NoDDoS	29	12.00	50.00	16.9310	10.36454
DDoS	29	65.00	122.00	75.4483	11.92712
IDSIPS1	29	22.00	27.00	23.7241	1.13063
IDSIPS2	29	14.00	37.00	16.4828	4.14574
Valid N (listwise)	29				

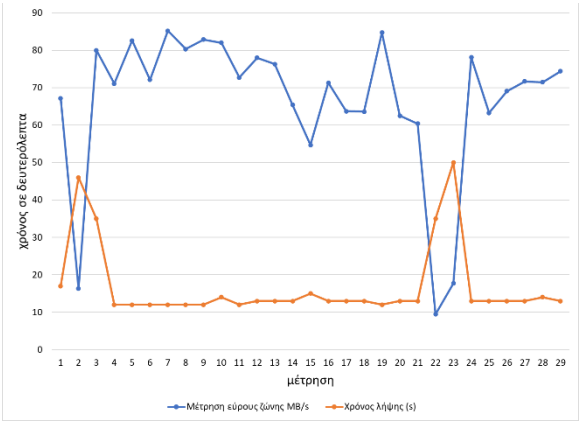
Εικόνα 87: Στατιστική ανάλυση του χρόνος λήψης αρχείου από το διακομιστή ιστού

5.1.5 Διαγράμματα διασποράς

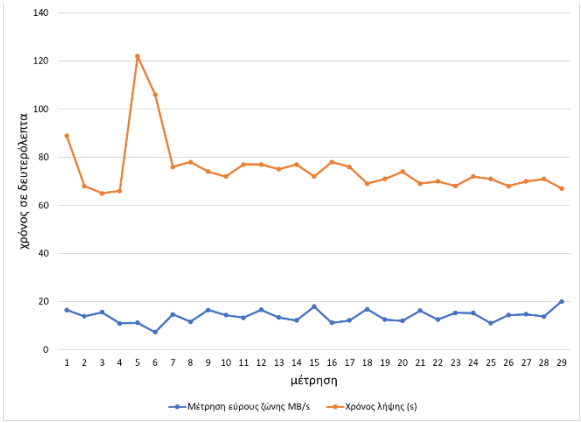
Έγινε προσπάθεια να διερευνήσουμε τυχών συσχέτιση μεταξύ των πιο πάνω μεταβλητών (NoDDoS, DDoS, IDSIPS1, IDSIPS2). Η συσχέτιση τους ανά ζεύγος μεταβλητών είναι πολύ μικρή.

Όπως υπολογίστηκε μέσα από το λογισμικό SPSS η συσχέτιση των πιο κάτω μεταβλητών είναι πολύ μικρή ($r^2 < 0.20$) με γραμμικές ή με γραμμικές συσχέτισης (π.χ. εκθετική, λογαριθμική).

Κατά τη διάρκεια της επίθεσης DDoS TCP SYN, το φορτίο στον ελεγκτή ONOS είχε αυξηθεί λόγω της πλημμύρας των πακέτων TCP SYN. Το σύστημα IDS/IPS που εφαρμόσαμε ήταν σε θέση να ανιχνεύσει και να αποκλείσει τις επιθέσεις πλημμύρας TCP SYN από το να κατακλύσουν τον ελεγκτή. Κατά τη διάρκεια της επίθεσης DDoS TCP SYN, η ταχύτητα λήψης του αρχείου έχει μειωθεί λόγω της αυξημένης συμφόρησης του δικτύου που προκαλείται από την πλημμύρα των πακέτων TCP SYN. Ωστόσο, η χρήση του συστήματος IDS/IPS είχε συμβάλει στην αποτροπή της επίθεσης από το να προκαλέσει πλήρη διακοπή της λειτουργίας του δικτύου με τον εντοπισμό και τον αποκλεισμό της κακόβουλης κίνησης πριν κατακλίσει τον ελεγκτή. Όσο αφορά το χρόνο λήψης του αρχείου (εικόνα 89), κατά τη διάρκεια της επίθεσης DDoS TCP SYN, που απαιτήθηκε για τη λήψη του έχει αυξηθεί λόγω της αυξημένης συμφόρησης του δικτύου και της πιθανής απώλειας πακέτων σε σύγκριση με το χρόνο λήψης του αρχείου χωρίς επίθεση DDoS (εικόνα 88).

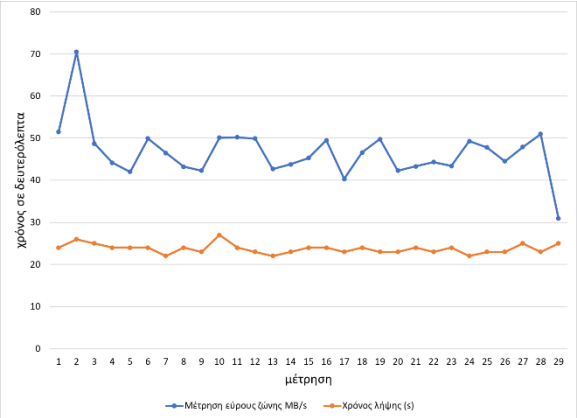


Εικόνα 88: NoDDoS - Εύρος ζώνης λήψης αρχείου / χρόνο λήψης αρχείου

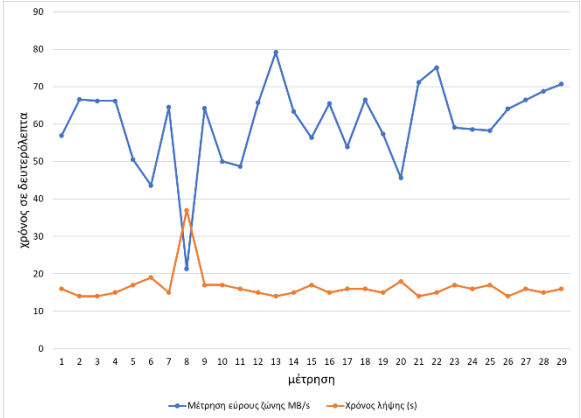


Εικόνα 89: DDoS - Εύρος ζώνης λήψης αρχείου / χρόνο λήψης αρχείου

Ωστόσο, η χρήση του συστήματος IDS/IPS συνέβαλε στη μείωση του αντίκτυπου της επίθεσης, εμποδίζοντας την κυκλοφορία της επίθεσης να φτάσει στο στόχο της (εικόνες 90-91). Η καθυστέρηση στο δίκτυο κατά τη διάρκεια της επίθεσης έχει αυξηθεί λόγω της αυξημένης συμφόρησης του δικτύου και της πιθανής απώλειας πακέτων. Η χρήση του συστήματος IDS/IPS συνέβαλε στο μετριασμό των επιπτώσεων της επίθεσης με τον εντοπισμό και τον αποκλεισμό της κακόβουλης κυκλοφορίας πριν φτάσει στο στόχο της.



Εικόνα 90: IDSIPS1 - Εύρος ζώνης λήψης αρχείου / χρόνο λήψης αρχείου



Εικόνα 91: IDSIPS2 - Εύρος ζώνης λήψης αρχείου / χρόνο λήψης αρχείου

Κεφάλαιο 6
Επίλογος

Η δικτύωση που καθορίζεται από το λογισμικό έχει φέρει την επανάσταση στον κλάδο των δικτύων με την άνευ προηγουμένου δυνατότητα προγραμματισμού και προσαρμογής της. Με την έλευση του SDN, οι ερευνητές έχουν τη δυνατότητα να εξερευνήσουν νέες δυνατότητες στον τομέα της διαχείρισης των δικτυών και της βελτιστοποίησης της κυκλοφορίας της κίνησης. Ακόμη και μετά από χρόνια εμφάνισης του, το SDN εξακολουθεί να παραμένει ένας από τους πιο δημοφιλής ερευνητικούς τομείς στον κλάδο. Αυτό οφείλεται στο γεγονός ότι αποτελεί μια συνεχώς εξελισσόμενη τεχνολογία στην οποία οι ερευνητές ανακαλύπτουν συνεχώς νέες περιπτώσεις χρήσης και εφαρμογής.

Ωστόσο, ο ελεγκτής αποτελεί το κρίσιμο στοιχείο της αρχιτεκτονικής SDN, το οποίο παρέχει τον κεντρικό έλεγχο για τη διαχείριση της υποδομής ολόκληρου του δικτύου. Είναι υπεύθυνο για τη διαχείριση των κανόνων προώθησης, της τοπολογίας και των ροών κυκλοφορίας του δικτύου. Χρησιμεύει επίσης ως διεπαφή μεταξύ της υποδομής δικτύου και των εφαρμογών υψηλότερου επιπέδου που χρησιμοποιούν τους πόρους του δικτύου. Ως εκ τούτου, η οποιαδήποτε δυσλειτουργία ή διακοπή ή παραβίαση του ελεγκτή μπορεί να έχει σοβαρές συνέπειες για ολόκληρο το δίκτυο. Η επίθεση DDoS είναι ιδιαίτερα επιζήμια και μπορεί να προκαλέσει ακόμη και

αστοχία στη λειτουργία του. Συγκεκριμένα, η επίθεση πλημμύρας TCP SYN που εκτελέσαμε, κατέκλυσε το δίκτυο με πακέτα TCP SYN, γεγονός που οδήγησε στην εξάντληση των πόρων και σε ορισμένες περιπτώσεις στην αδυναμία δημιουργίας νέων συνδέσεων. Ως αποτέλεσμα, ο ελεγκτής ONOS δεν ήταν σε θέση να επεξεργαστεί την κυκλοφορία οδηγώντας στην υποβαθμισμένη απόδοση του δικτύου. Η προστασία του ελεγκτή ήταν απαραίτητη για να διασφαλιστεί η συνεχής λειτουργία και αξιοπιστία του δικτύου. Μια προσέγγιση για την προστασία του ελεγκτή από επιθέσεις DDoS είναι η εφαρμογή ενός συστήματος ανίχνευσης και πρόληψης εισβολών. Το σύστημα IDS/IPS που εφαρμόσαμε μπόρεσε να αναλύσει την κυκλοφορία του δικτύου και να εντοπίσει την οποιαδήποτε κυκλοφορία συνδέονταν με τις επιθέσεις DDoS. Μόλις εντοπίστηκε, το σύστημα IDS/IPS ανέλαβε δράση και απέκλεισε την κακόβουλη κίνηση πριν αυτή κατακλίσει τον ελεγκτή, αποτρέποντας ή μετριάζοντας τον αντίκτυπο της επίθεσης.

Αν και τα αποτελέσματα της παρούσας έρευνας δεν είναι εξαντλητικά και μερικές αδυναμίες έχουν ήδη καταγραφεί, όπως για παράδειγμα ο περιορισμός στο συγκεκριμένο υλισμικό (hardware) του ερευνητή, και η πολυπλοκότητα της έρευνας με δυνατότητα διεξαγωγής πειραμάτων με άλλα πρωτόκολλα, άλλες τοπολογίες δικτύων και άλλους τύπους επιθέσεων, η παρούσα έρευνα καταγράφει σημαντικά ευρήματα τα οποία μπορεί να αξιοποιηθούν στο μέλλον. Για παράδειγμα μέσα από τα διάφορα πειράματα διαφάνηκε ότι ο εκλεκτής είναι ευάλωτος σε επιθέσεις τύπου DDoS και η προστασία του μέσω ενός συστήματος IDS/IPS κρίνεται αναγκαία για το φιλτράρισμα αρχικά και τον αποκλεισμό εν τέλει της κακόβουλης κίνησης. Ο ποσοτικός έλεγχος της ανθεκτικότητας των δικτύων SDN που αναδεικνύουμε στην παρούσα έρευνα πρόκειται για ένα σημαντικό εύρημα που μπορεί να χρησιμοποιηθεί για την αξιολόγηση και τη βελτίωση της ανθεκτικότητας των δικτύων SDN και της απόκρισης τους σε επιθέσεις τύπου DDoS. Η σημασία της σωστής διαμόρφωσης του δικτύου εισάγοντας ένα επιπρόσθετο επίπεδο, το επίπεδο ασφαλείας (security plane), έπαιξε καθοριστικό ρόλο στην αντιμετώπιση των επιθέσεων πλημμύρας TCP SYN και στη βελτίωση της ανθεκτικότητας παρέχοντας μια σαφή επιβεβαίωση ότι η χρήση τέτοιων συστημάτων είναι απαραίτητη για την προστασία ολόκληρου του δικτύου SDN. Το επίπεδο ασφαλείας λειτουργεί ως ρυθμιστικό στοιχείο μεταξύ του ελεγκτή και του υπόλοιπου δικτύου, φιλτράροντας την κυκλοφορία και εντοπίζοντας πιθανές απειλές πριν αυτές κατακλίσουν τον ελεγκτή.

Βελτιώσεις στην παρούσα εργασία μπορεί να γίνουν σε διάφορα επίπεδα και να επεκταθεί και σε άλλους τομείς. Για παράδειγμα, το επίπεδο ασφαλείας Θα μπορούσε να περιλαμβάνει εξειδικευμένο υλικό ή λογισμικό σχεδιασμένο να διαχειρίζεται και να δρομολογεί υψηλό όγκο

κίνησης που σχετίζεται με τις επιθέσεις DDoS Η αναδρομολόγηση της κυκλοφορίας θα μείωνε σημαντικά τον κίνδυνο επιτυχημένων επιθέσεων DDoS και θα εξασφάλιζε τη συνολική σταθερότητα και αξιοπιστία των δικτύων SDN. Σε συνδυασμό με τη χρήση πολλαπλών ελεγκτών που θα μπορούν να αναλάβουν ακόμη και αν ένα στοιχείο αποτύχει, θα διασφαλιζότανε η συνεχής λειτουργία του δικτύου χωρίς διακοπές προσφέροντας υψηλής διαθεσιμότητας δίκτυα.

Το επίπεδο ασφαλείας δύναται επίσης να προσφέρει πολλαπλά οφέλη που σχετίζονται με την ασφάλεια του ελεγκτή όπως, στον εντοπισμό και την αποτροπή μη εξουσιοδοτημένης πρόσβασης, παρακολουθώντας μοτίβα κίνησης και αποτρέποντας κακόβουλους χρήστες από το να αποκτήσουν τον πλήρη έλεγχο του. Επιπλέον, με την επιβολή πολιτικών δικτύου και ελέγχων πρόσβασης μπορεί να διασφαλιστεί ότι η κυκλοφορία ρέει μόνο μέσω εξουσιοδοτημένων διαδρομών και συσκευών. Μια άλλη προσέγγιση για την προστασία του ελεγκτή από επιθέσεις DDoS είναι η εφαρμογή ελέγχων σε επίπεδο δικτύου, όπως ο περιορισμός του ρυθμού και η διαμόρφωση της κυκλοφορίας. Ο έλεγχος του ρυθμού περιλαμβάνει τον περιορισμό της κυκλοφορίας που μπορεί να σταλεί στον ελεγκτή ONOS μέσα σε μια δεδομένη χρονική περίοδο, ενώ η διαμόρφωση της κυκλοφορίας περιλαμβάνει την ιεράρχηση της κυκλοφορίας με βάση τη σημασία της. Οι έλεγχοι αυτοί μπορούν να βοηθήσουν στην αποτροπή της υπερφόρτωσης του ελεγκτή ONOS από επιθέσεις πλημμύρας, διασφαλίζοντας την κυκλοφορία του δικτύου με βάση την προτεραιότητα της.

Περαιτέρω, μπορούν να εφαρμοστούν επιπρόσθετα μέτρα όπως, η χρήση αλγορίθμων κρυπτογράφησης, για την προστασία των ευαίσθητων δεδομένων που ανταλλάσσονται μεταξύ του ελεγκτή και των δικτυακών συσκευών. Ωστόσο, μια από τις κυριότερες προκλήσεις της κρυπτογράφησης των δεδομένων στον ελεγκτή είναι η επίτευξη μιας ισορροπίας μεταξύ ασφάλειας και απόδοσης του συστήματος. Αυτό σημαίνει ότι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται πρέπει να είναι αρκετά ισχυροί ώστε να προστατεύουν αποτελεσματικά τα δεδομένα, αλλά παράλληλα να μην επιβαρύνουν υπερβολικά την απόδοση του συστήματος που μπορεί να οδηγήσει σε καθυστέρηση στην επικοινωνία μεταξύ του ελεγκτή και των δικτυακών συσκευών. Επιπλέον, μια άλλη δυνατότητα που παρουσιάζει το SDN και αξίζει η μελλοντική της διερεύνηση, είναι η ενσωμάτωση αλγορίθμων μηχανικής μάθησης με εργαλεία διαχείρισης δικτύων. Αυτό θα επιτρέψει στον ελεγκτή SDN να λαμβάνει αποφάσεις σχετικά με τα μοτίβα κίνησης φιλτράροντας ανάλογα την κακόβουλη κίνηση.

Ωστόσο, καθώς οι τρέχουσες και αναδυόμενες εφαρμογές και υπηρεσίες του διαδικτύου γίνονται ολοένα και πιο περίπλοκες και απαιτητικές, είναι επιτακτική η ανάγκη το διαδίκτυο να μπορεί να

εξελιχθεί για να αντιμετωπίσει τις νέες αυτές προκλήσεις. Παρόλες τις ανησυχίες των ερευνητών σχετικά με την ανθεκτικότητα των δικτύων SDN, αυτές μπορούν να αντιμετωπιστούν μέσω του κατάλληλου σχεδιασμού και εφαρμογών καθιστώντας το μια ελκυστική επιλογή για τους οργανισμούς που επιθυμούν να βελτιώσουν την απόδοση και την επεκτασιμότητα του δικτύου τους. Καθώς η ζήτηση για υπηρεσίες και εφαρμογές που βασίζονται στο υπολογιστικό νέφος αυξάνεται, τα δίκτυα SDN αποκτούν ολοένα και μεγαλύτερη σημασία για την παροχή αξιόπιστης και κλιμακούμενης υποδομής δικτύων που απαιτείται για την υποστήριξη των εφαρμογών αυτών. Σημαντικές εταιρείες του κλάδου της πληροφορικής επενδύουν στην έρευνα, την ανάπτυξη και την τυποποίηση των πρωτοκόλλων της τεχνολογίας SDN. Οι τεχνολογίες SDN σε συνδυασμό με τις NFV πρωτοστατούν ήδη ως τα νέα πρότυπα για τη δικτύωση και είναι σχεδόν βέβαιο ότι η υιοθέτηση τους θα αποτελέσει την τάση για τα επόμενα χρόνια, αποτελώντας στην ουσία, μια απάντηση στις ραγδαίες τεχνολογικές αλλαγές ως ένα υποσχόμενο παράδειγμα για τη διαχείριση και τον έλεγχο των δικτύων.

Γενικά η παρούσα έρευνα κατέδειξε τη σημασία των συστημάτων IDS/IPS για την προστασία του ελεγκτή ONOS μέσα από διάφορα σενάρια και υποθέσεις.

Βιβλιογραφία

van Asten, B.J., van Adrichem, N.L.M. and Kuipers, F.A. (2014) *Scalability and Resilience of Software-Defined Networking: An Overview*. Available from http://arxiv.org/abs/1408.6760.

Benzekki, K., El Fergougui, A. and Elbelrhiti Elalaoui, A. (2016) Software-defined networking (SDN): a survey. *Security and Communication Networks*, 9(18) 5803–5833.

Blenk, A., Basta, A., Reisslein, M. and Kellerer, W. (2016) Survey on network virtualization hypervisors for software defined networking. IEEE Communications Surveys and Tutorials 18 (1) p.655–685.

Deng, S., Gao, Xing, Lu, Z., Li, Z. and Gao, Xieping (2019) DoS vulnerabilities and mitigation strategies in software-defined networks. *Journal of Network and Computer Applications*, 125 209–219.

Haji, S.H., Zeebaree, S.R.M., Saeed, R.H., Ameen, S.Y., Shukur, H.M., Omar, N., Sadeeq, M.A.M., Ageed, Z.S., Ibrahim, I.M. and Yasin, H.M. (2021) Comparison of Software Defined Networking with Traditional Networking. *Asian Journal of Research in Computer Science*, 1–18.

Heller, B., Seetharaman, S., Mahadevan, P., Yiakoumis, Y., Sharma, P., Banerjee, S. and McKeown, N. (n.d.) *ElasticTree: Saving Energy in Data Center Networks*.

Huang, T., Yu, F.R., Zhang, C., Liu, J., Zhang, J. and Liu, Y. (2017) A Survey on Large-Scale Software Defined Networking (SDN) Testbeds: Approaches and Challenges. IEEE Communications Surveys and Tutorials 19 (2) p.891–917.

Kindervag, J. (2010) Build security into your network's DNA: The zero trust network architecture.

Kotani, D. and Okabe, Y. (2014) A packet-in message filtering mechanism for protection of control plane in OpenFlow networks. In: *ANCS 2014 - 10th 2014 ACM/IEEE Symposium on Architectures for Networking and Communications Systems*. 20 October 2014 Association for Computing Machinery, Inc, 29–40.

Kreutz, D., Ramos, F.M.V., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S. and Uhlig, S. (2015) Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1) 14–76.

Lara, A., Kolasani, A. and Ramamurthy, B. (2014) Network innovation using open flow: A survey. *IEEE Communications Surveys and Tutorials*, 16(1) 493–512.

Li, W., Meng, W. and Kwok, L.F. (2016) A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. Journal of Network and Computer Applications 68 p.126–139.

Mckeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S. and Turner, J. (n.d.) *OpenFlow: Enabling Innovation in Campus Networks*.

Mehdi, S.A., Khalid, J. and Khayam, S.A. (n.d.) *LNCS 6961 - Revisiting Traffic Anomaly Detection Using Software Defined Networking*.

Mousa, M., Bahaa-ElDin, A.M. and Sobh, M. (2017) Software Defined Networking concepts and challenges. In: *Proceedings of 2016 11th International Conference on Computer Engineering and Systems, ICCES 2016*. 17 January 2017 Institute of Electrical and Electronics Engineers Inc., 79–90.

Murugaiyan, D. (2012) *International Journal of Information Technology and Business Management WATEERFALLVs V-MODEL Vs AGILE: A COMPARATIVE STUDY ON SDLC*. 2(1). Available from www.jitbm.com.

Nunes Astuto, B., Mendonça, M., Nam Nguyen, X., Obraczka, K., Turletti, T., Turletti, T.A., Astuto Nunes, B.A., Mendonca, M. and Nguyen, X.-N. (2014) *A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks*. 16(3) 1617–1634. Available from https://hal.inria.fr/hal-00825087v5.

Obaidat, M.S. (Mohammad S., Institute of Electrical and Electronics Engineers, IEEE Communications Society, Society for Modeling and Simulation International and Dalian li gong da xue (n.d.) *IEEE CITS 2017 : 2017 International Conference on Computer, Information and Telecommunication Systems : July 21-23, 2017, Dalian, China*.

Oktian, Y.E., Lee, S., Lee, H. and Lam, J. (2015) Secure your Northbound SDN API. In: *International Conference on Ubiquitous and Future Networks, ICUFN*. 7 August 2015 IEEE Computer Society, 919–920.

OpenFlow Switch Specification (2015).

Rifai, M., Huin, N., Caillouet, C., Giroire, F., Moulierac, J., Lopez Pacheco, D. and Urvoy-Keller, G. (2017) MINNIE: An SDN world with few compressed forwarding rules. *Computer Networks*, 121 185–207.

Rohrer, J.P., Jabbar, A. and Sterbenz, J.P.G. (2009) Path diversification: A multipath resilience mechanism. In: *Proceedings of the 2009 7th International Workshop on the Design of Reliable Communication Networks, DRCN 2009*. 2009 343–351.

Salman, O., Elhajj, I.H., Kayssi, A. and Chehab, A. (2016) SDN controllers: A comparative study. In: *Proceedings of the 18th Mediterranean Electrotechnical Conference: Intelligent and Efficient Technologies and Services for the Citizen, MELECON 2016*. 20 June 2016 Institute of Electrical and Electronics Engineers Inc.,.

Sezer Sakir, Scott-Hayward Sandra and Chouhan Pushpinder Kaur (2013) *Are We Ready for SDN? Implementation Challenges for Software-Defined Networks*.

Software-Defined Networking (SDN) Definition - Open Networking Foundation (n.d.) Available from https://opennetworking.org/sdn-definition/ [accessed 13 February 2023].

Software-Defined Networking: The New Norm for Networks - Open Networking Foundation (n.d.) Available from https://opennetworking.org/sdn-resources/whitepapers/software-defined-networking-the-new-norm-for-networks/ [accessed 13 February 2023].

Xia, W., Wen, Y., Foh, C.H., Niyato, D. and Xie, H. (2015) A Survey on Software-Defined Networking. IEEE Communications Surveys and Tutorials 17 (1) p.27–51.

Yao, G., Bi, J. and Xiao, P. (2011) Source address validation solution with OpenFlow/NOX architecture. In: *Proceedings - International Conference on Network Protocols, ICNP*. 2011 7–12.

Zhou, W., Li, L., Luo, M. and Chou, W. (2014) REST API design patterns for SDN northbound API. In: *Proceedings - 2014 IEEE 28th International Conference on Advanced Information Networking and Applications Workshops, IEEE WAINA 2014*. 2014 IEEE Computer Society, 358–365.

Παράρτημα Α
Τίτλος Παραρτήματος

Α.1 Αποτελέσματα Μετρήσεων

Στο Παράρτημα Α παραθέτουμε τις μετρήσεις που έχουμε καταγράψει για όλα τα σενάρια που έχουμε εκτελέσει στο κεφάλαιο 4 «Υλοποίηση».

Μέτρηση χρόνου απόκρισης (σε ms)			
no DDoS	**DDoS**	**DDoS & IDS/IPS (1)**	**DDoS & IDS/IPS (2)**
0.052	0.266	0.553	0.590
0.054	0.047	0.059	0.055
0.052	1.120	0.057	0.069
0.055	0.234	0.061	0.050
0.057	0.212	0.061	0.051
0.063	0.046	0.063	0.054
0.055	0.256	0.060	0.050
0.082	0.049	0.062	0.212
0.055	0.046	0.052	0.055
0.072	0.046	0.063	0.078
0.053	0.059	0.062	0.050
0.052	0.144	0.042	0.053
0.054	0.047	0.042	0.056
0.070	0.047	0.041	0.057

0.075	0.229	0.058	0.055
0.070	0.044	0.060	0.063
0.052	0.058	0.044	0.309
0.056	0.256	0.159	0.078
0.242	3.150	0.053	0.054
0.087	0.045	0.601	0.060
0.055	0.047	0.040	0.055
0.072	0.046	0.044	0.052
0.049	0.066	0.056	0.076
0.054	0.045	0.062	0.087
0.060	0.043	0.073	0.224
0.056	0.054	0.064	0.086
0.058	0.075	0.062	0.057
0.050	0.161	0.062	0.054
0.050	0.202	0.055	0.558
0.049	0.046	0.043	0.056
0.064	0.061	0.063	0.059
0.065	0.046	0.058	0.055
0.062	0.215	0.044	0.243
0.071	0.047	0.041	0.052
0.064	0.374	0.066	0.049
0.079	0.065	0.113	0.062
0.066	0.056	0.065	0.238
0.057	0.058	0.056	0.058
0.073	0.046	0.070	0.055
0.063	0.060	0.062	0.076
0.054	0.044	0.051	0.056
0.059	0.059	0.062	0.053
0.055	0.061	0.194	0.078
0.056	0.057	0.069	0.051
0.056	0.049	0.060	0.052
0.058	0.048	0.062	0.053
0.062	0.078	0.043	0.057
0.057	0.047	0.222	0.076
0.071	0.069	0.048	0.071
0.071	0.167	0.065	0.075
0.051	0.180	0.063	0.083
0.071	0.208	0.044	0.068
0.054	0.046	0.043	0.071
0.054	0.057	0.066	0.053
0.056	0.046	0.061	0.068
0.052	0.043	0.205	0.045
0.053	0.184	0.185	0.044
0.052	0.084	0.196	0.046
0.049	0.048	0.061	0.083
0.080	0.055	0.045	0.083

0.054	0.066	0.051	0.070
0.050	0.047	0.072	0.065
0.049	0.049	0.062	0.056
0.085	0.047	0.063	0.074
0.053	0.056	0.066	0.058
0.070	0.063	0.061	0.054
0.072	0.063	0.065	0.073
0.051	0.045	0.078	0.076
0.056	0.047	0.070	0.055
0.071	0.175	0.048	0.056
0.054	0.046	0.066	0.083
0.050	0.048	0.073	0.055
0.053	0.169	0.069	0.159
0.053	0.073	0.066	0.073
0.055	0.047	0.047	0.054
0.073	0.299	0.049	0.048
0.162	0.047	0.052	0.056
0.063	0.064	0.056	0.059
0.073	0.172	0.057	0.057
0.050	0.055	0.062	0.058
0.085	0.463	0.058	0.078
0.051	0.061	0.051	0.055
0.056	0.045	0.069	0.073
0.056	0.045	0.077	0.077
0.461	0.044	0.062	0.053
0.054	0.067	0.050	0.052
0.055	0.046	0.066	0.079
0.046	0.046	0.068	0.054
0.051	0.045	0.490	0.050
0.054	0.055	0.067	0.054
0.052	0.139	0.065	0.063
0.053	0.054	0.076	0.070
0.077	0.075	0.070	0.052
0.077	0.047	0.064	0.057
0.059	0.077	0.065	0.090
0.096	0.190	0.304	0.052
0.079	0.045	0.047	0.069
0.076	0.177	0.065	0.055
0.073	0.047	0.049	0.056
0.053	0.066	0.066	0.051
0.055	0.046	0.066	0.055
0.053	0.047	0.071	0.051
0.055	0.062	0.066	0.052
0.056	0.044	0.064	0.053
0.056	0.047	0.070	0.056
0.055	0.680	0.068	0.287

0.070	0.046	0.083	0.055
0.055	0.046	0.047	0.051
0.059	0.046	0.193	0.056
0.054	0.064	0.049	0.059
0.049	0.065	0.048	0.055
0.073	0.065	0.071	0.051
0.053	0.048	0.072	0.049
0.053	0.046	0.065	0.054
0.049	0.043	0.063	0.049
0.056	0.055	0.075	0.216
0.166	0.065	0.072	0.056
0.058	0.069	0.069	0.066

Μέτρηση φορτίου ελεγκτή (used CPU %)			
no DDoS	**DDoS**	**DDoS & IDS/IPS (1)**	**DDoS & IDS/IPS (2)**
0.06	0.26	0.03	0.06
0.06	0.26	0.03	0.06
0.06	0.26	0.03	0.06
0.06	0.26	0.03	0.06
0.06	0.30	0.03	0.06
0.06	0.30	0.03	0.06
0.06	0.30	0.03	0.06
0.06	0.30	0.03	0.06
0.07	0.30	0.03	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.07	0.30	0.18	0.06
0.11	0.26	0.18	0.06
0.11	0.26	0.18	0.06
0.11	0.26	0.18	0.06
0.11	0.26	0.18	0.06

0.11	0.26	0.18	0.06
0.11	0.26	0.18	0.06
0.11	0.26	0.18	0.06
0.11	0.26	0.18	0.06
0.11	0.26	0.18	0.06
0.14	0.26	0.18	0.06
0.09	0.26	0.18	0.06
0.09	0.26	0.18	0.06
0.09	0.26	0.18	0.06

Μέτρηση φορτίου ελεγκτή (memory used/bytes) (Total RAM=4122300416)			
no DDoS	**DDoS**	**DDoS & IDS/IPS (1)**	**DDoS & IDS/IPS (2)**
172335104	3979587584	3856560128	3840299008
172335104	3979587584	3856560128	3840299008
172335104	3979587584	3869036544	3840299008
172335104	3979587584	3869036544	3840299008
172335104	3979587584	3869036544	3840299008
172335104	3979587584	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008
167989248	3980193792	3869036544	3840299008

167989248	3980193792	3869036544	3840299008
167989248	3981529088	3869036544	3843137536
167989248	3981529088	3869036544	3843137536
167989248	3981529088	3869036544	3843137536
167989248	3981529088	3869036544	3843137536
167989248	3981529088	3869036544	3843137536
167989248	3981529088	3857575936	3843137536
167989248	3981529088	3857575936	3843137536
167989248	3981529088	3857575936	3843137536
167989248	3981529088	3857575936	3843137536

Μέτρηση εύρους ζώνης δικτύου (σε Gbits/s)			
no DDoS	**DDoS**	**DDoS & IDS/IPS (1)**	**DDoS & IDS/IPS (2)**
9.91	7.90	9.17	8.54
9.47	6.29	8.82	8.24
7.81	6.83	8.87	6.74
8.75	7.97	8.50	8.75
9.34	6.39	8.68	8.53
8.61	7.91	8.05	8.98
8.78	5.51	8.11	8.72
9.19	5.63	9.25	9.06
8.78	6.87	8.70	8.89
9.74	7.28	8.84	8.34
9.37	6.11	7.59	9.44
9.60	7.14	8.75	9.37
8.67	7.07	8.75	9.17
9.59	5.97	8.92	8.24
9.61	7.20	8.63	8.63
10.20	7.42	9.02	7.94
9.84	7.31	8.77	8.35
9.59	6.25	7.90	8.54
9.27	6.97	8.94	8.18

8.90	7.43	8.53	8.82
9.51	6.84	8.18	9.15
9.35	5.69	9.11	8.85
8.97	6.62	9.22	8.59
8.44	7.57	9.08	9.56
5.50	8.06	8.35	8.53
8.14	6.16	8.13	8.82
9.14	5.42	8.68	8.26
9.68	5.55	9.10	8.90
9.39	7.19	8.65	9.27
9.74	6.52	8.73	9.06
9.13	7.37	8.58	9.10

Μέτρηση εύρους ζώνης διακομιστή ιστού (σε MB/s)			
no DDoS	**DDoS**	**DDoS & IDS/IPS (1)**	**DDoS & IDS/IPS (2)**
67.20	16.50	51.50	57.00
16.30	13.90	70.50	66.60
80.00	15.60	48.70	66.20
71.10	10.90	44.20	66.20
82.60	11.20	42.00	50.50
72.10	7.28	49.90	43.60
85.20	14.60	46.50	64.50
80.30	11.60	43.20	21.30
82.90	16.50	42.30	64.20
82.00	14.40	50.10	50.00
72.70	13.30	50.20	48.70
78.00	16.60	49.90	65.70
76.30	13.40	42.70	79.20
65.40	12.20	43.80	63.40
54.70	17.90	45.30	56.40
71.30	11.20	49.50	65.50
63.70	12.20	40.30	53.90

63.60	16.80	46.60	66.50
84.70	12.50	49.80	57.40
62.50	12.00	42.30	45.70
60.40	16.20	43.30	71.20
9.47	12.50	44.30	75.10
17.70	15.30	43.40	59.10
78.10	15.20	49.30	58.60
63.30	11.00	47.80	58.30
69.10	14.40	44.50	64.10
71.70	14.70	47.90	66.50
71.50	13.80	51.00	68.80
74.40	20.00	30.90	70.70

Χρόνος λήψης αρχείου από διακομιστή ιστού (σε s)			
no DDoS	**DDoS**	**DDoS & IDS/IPS (1)**	**DDoS & IDS/IPS (2)**
17	89	24	16
46	68	26	14
35	65	25	14
12	66	24	15
12	122	24	17
12	106	24	19
12	76	22	15
12	78	24	37
12	74	23	17
14	72	27	17
12	77	24	16
13	77	23	15
13	75	22	14
13	77	23	15
15	72	24	17
13	78	24	15
13	76	23	16

13	69	24	16
12	71	23	15
13	74	23	18
13	69	24	14
35	70	23	15
50	68	24	17
13	72	22	16
13	71	23	17
13	68	23	14
13	70	25	16
14	71	23	15
13	67	25	16