ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΣΕ ΔΙΚΤΥΑ ΚΑΘΟΡΙΣΜΕΝΑ ΑΠΟ ΛΟΓΙΣΜΙΚΟ (SDN)

Εμμανουήλ Ελευθερίου
Α.Μ. 131001

Εισηγητής: Παναγιώτης Καρκαζής, Επίκουρος Καθηγητής

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΣΕ ΔΙΚΤΥΑ ΚΑΘΟΡΙΣΜΕΝΑ ΑΠΟ ΛΟΓΙΣΜΙΚΟ (SDN)

Εμμανουήλ Ελευθερίου
Α.Μ. 131001

Εισηγητής:

Παναγιώτης Καρκαζής,
Επίκουρος Καθηγητής

Εξεταστική Επιτροπή:

Αθανάσιος Βουλόδημος
Επίκουρος Καθηγητής

Athanasios Voulodimos
Digitally signed by Athanasios Voulodimos
Date: 2021.10.26 19:21:59 +03'00'

Ελένη Αικατερίνη Λελίγκου
Αναπληρώτρια Καθηγήτρια

Eleni Aikaterini Leligkou
Digitally signed by Eleni Aikaterini Leligkou
Date: 2021.10.31 21:52:03 +02'00'

Παναγιώτης Καρκαζής,
Επίκουρος Καθηγητής

Panagiotis Karkazis
Digitally signed by Panagiotis Karkazis
Date: 2021.10.25 14:00:49 +03'00'

Ημερομηνία εξέτασης 21/10/2021

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/η κάτωθι υπογεγραμμένος/η ΕΜΜΑΝΟΥΗΛ ΕΛΕΥΘΕΡΙΟΥ του ΑΝΤΩΝΙΟΥ, με αριθμό μητρώου 131001 φοιτητής/τρια του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο/Η Δηλών/ούσα
Εμμανουήλ Ελευθερίου

ΕΥΧΑΡΙΣΤΙΕΣ

Για την εκπόνηση της παρούσας πτυχιακής εργασίας, θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Καρκαζή, για τις συμβουλές του και την υποστήριξή του σε όλη την διάρκεια.

Ακόμα, θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξή τους και την υπομονή τους καθ' όλη την διάρκεια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Το Δίκτυο που έχει καθοριστεί από λογισμικό (SDN) έχει προταθεί ως αναδυόμενη αρχιτεκτονική δικτύωση, η οποία αποτελείται από τον διαχωρισμό των επιπέδων ελέγχου και των επιπέδων δεδομένων ενός δικτύου. Στην παρούσα πτυχιακή εργασία γίνεται μελέτη των δικτύων καθορισμένων από λογισμικό. Συγκεκριμένα στο 2ο κεφάλαιο αναλύεται η αρχιτεκτονική, η λειτουργία και οι εφαρμογές των SDN και γίνεται αναφορά στους ελεγκτές τους και στο πρωτόκολλο OpenFlow. Στην συνέχεια στο 3ο κεφάλαιο παρουσιάζονται τα πιο σημαντικά θέματα ασφάλειας των SDN. Δίνεται ιδιαίτερη έμφαση στις αρχές ασφάλειας, στις απειλές που αντιμετωπίζουν τα SDN και η αρχιτεκτονική τους, καθώς επίσης και στους τρόπους αντιμετώπισής τους. Στο 4ο κεφάλαιο, υλοποιείται σενάριο επίθεσης DoS σε περιβάλλον προσομοίωσης mininet και πραγματοποιείται ανίχνευση της επίθεσης με το IDS Suricata. Τέλος, στο 5ο κεφάλαιο αναγράφονται συμπεράσματα που προκύπτουν από την εκπόνηση της εργασίας.

ABSTRACT

Software-defined Network (SDN) has been proposed as an emerging network architecture, which consists of decoupling the control planes and data planes of a network. In this thesis we study the software defined networks. Specifically, the 2nd chapter analyzes the architecture, operation and applications of SDNs and refers to their controllers and the OpenFlow protocol. Then the 3rd chapter presents the most important security issues of SDNs. Particular emphasis is placed on security principles, the threats of SDNs and their architecture, as well as how to deal with them. In chapter 4, it is implemented a DoS attack scenario in a mininet simulation environment and is detected by IDS Suricata. Finally, in the 5th chapter are written conclusions that result from the elaboration of the work.

ΠΕΡΙΕΧΟΜΕΝΑ

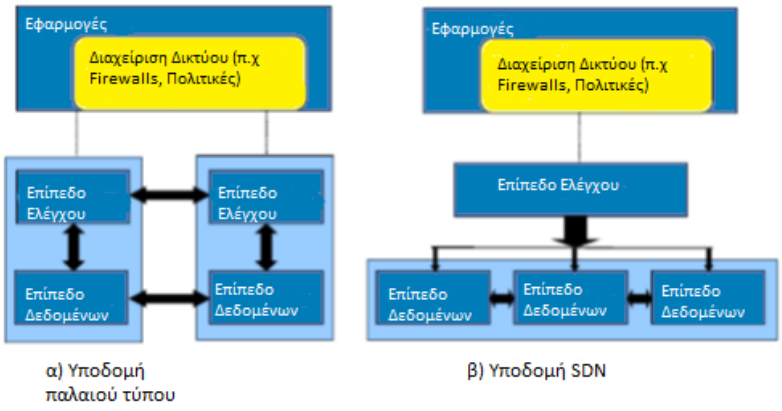
ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1

1 Εισαγωγή

Με την ανάπτυξη των δικτύων των υπολογιστών, τα τρέχοντα δικτυακά συστήματα και τα κέντρα δεδομένων, γίνονται όλο και περισσότερο πολύπλοκα και με υπερβολικά δεδομένα, έτσι ώστε οι σχεδιαστές του συστήματος συχνά χρειάζεται να τροποποιήσουν το λογισμικό δικτύου και να εναρμονίσουν τους πόρους υπολογιστή και δικτύου σύμφωνα με συγκεκριμένες απαιτήσεις. Ωστόσο, οι παραδοσιακές αρχιτεκτονικές δικτύων είναι κατάλληλες για τη συμπλήρωση των παραπάνω απαιτήσεων από τις επιχειρήσεις, τους μεταφορείς και τους τελικούς χρήστες. Για παράδειγμα, η ικανότητα λήψης αποφάσεων του δικτύου διανέμεται σε διάφορα στοιχεία του δικτύου, από νέες δικτυακές συσκευές ή υπηρεσίες. Σαν αποτέλεσμα, η διαχείριση δικτύου και η διαμόρφωση να γίνονται εξαιρετικά επίπονες και επιρρεπής σε λάθη.

Για να ξεπεράσουμε αυτούς τους περιορισμούς, στα δίκτυα που ορισμένα από λογισμικό (SDN), ο έλεγχος δικτύου αποσυνδέθηκε από τον μηχανισμό προώθησης και μπορεί να γίνει άμεσα προγραμματιζόμενος (Open Networking Foundation, 2012). Αυτό σημαίνει ότι αποσυνδέοντας την λογική ελέγχου από τις παραδοσιακές δικτυακές συσκευές (π.χ δρομολογητές και μεταγωγείς), το SDN παρέχει ενοποιημένο έλεγχο στις εφαρμογές, έτσι ώστε οι ερευνητές, οι σχεδιαστές συστημάτων και οι διαχειριστές μπορούν να σχεδιάσουν νέες λειτουργίες δικτύου και πρωτόκολλα με έναν πολύ πιο εύκολο και ευέλικτο τρόπο. Μια σύγκριση μεταξύ της παλαιού τύπου υποδομής και της SDN υποδομής απεικονίζεται στο Σχ. 1.



Εικόνα 1 Σύγκριση μεταξύ (α) της παλαιάς υποδομής και (β) της υποδομής SDN

Οι σύγχρονες υλοποιήσεις του SDN βασίζονται στο πρωτόκολλο OpenFlow, το οποίο δίνει πρόσβαση στο επίπεδο προώθησης ενός SDN switch πάνω από το δίκτυο. Αυτό το πρότυπο τυπικά ανοίγει το Διαδίκτυο στους ερευνητές, επιτρέποντας τη ροή δεδομένων τους μέσω λογισμικού, παρέχοντας στους μηχανικούς πρόσβαση σε πίνακες ροής (flow tables) και σχεδιάζοντας κανόνες για να καθοδηγούν τα switches για το πώς να κατευθύνουν την κυκλοφορία του δικτύου. Παραδοσιακά, όταν ένα πακέτο δεδομένων φτάνει σε ένα switch, αυτό το switch ελέγχει κυρίως τον προορισμό του πακέτου και το προωθεί ανάλογα τους προκαθορισμένους κανόνες. Όλα τα πακέτα που πηγαίνουν στο ίδιο μέρος δρομολογούνται στον ίδιο δρόμο και αντιμετωπίζονται με τον ίδιο τρόπο. Αντίθετα, σε ένα SDN που βασίζεται στο OpenFlow, οι διαχειριστές του δικτύου μπορούν να προσθέσουν, να αφαιρέσουν, και να παρεμβαίνουν διαφορετικά με αυτούς τους κανόνες. Εξαιτίας αυτών των πλεονεκτημάτων, οι εφαρμογές που βασίζονται στο SDN έχουν γίνει δημοφιλείς και έχουν μελετηθεί σε πολλούς τομείς εφαρμογής όπως το VLAN, τα ασύρματα δίκτυα αισθητήρων, το δίκτυο κινητής τηλεφωνίας, τον τομέα τηλεπικοινωνιών, την ανίχνευση επιθέσεων ασφάλειας και άλλα.

Συνολικά, το SDN παρέχει εξαιρετικά προγραμματιζόμενες υποδομές switch και υπολογίζει τους βέλτιστους κανόνες δρομολόγησης ροής από απομακρυσμένους χρήστες για να αναπαράγουν εικονικά υπολογιστικούς πόρους. Για παράδειγμα, ο (Takavoli A., 2009) υπολόγισε ότι ένα μεγάλο κέντρο δεδομένων που αποτελούταν από 2 εκατομμύρια εικονικές μηχανές μπορεί να παράγει έως και 20 εκατομμύρια ροές ανά δευτερόλεπτο. Στη συνέχεια, οι (Benton, 2013) εισήγαγαν ορισμένες συγκεκριμένες επιθέσεις για το OpenFlow, όπως η επίθεση man-in-the-middle και η άρνηση υπηρεσίας. Μερικά πρακτικά παραδείγματα για το πώς μπορεί να χρησιμοποιηθεί και να χρησιμοποιηθεί λάθος το SDN περιγράφονται στο (Crenshaw, 2012). Χάρη σε αυτές τις προσπάθειες, οι προκλήσεις ασφάλειας και τα θέματα του SDN έχουν αποκτήσει σημαντική προσοχή τόσο από ερευνητές όσο και από επαγγελματίες.

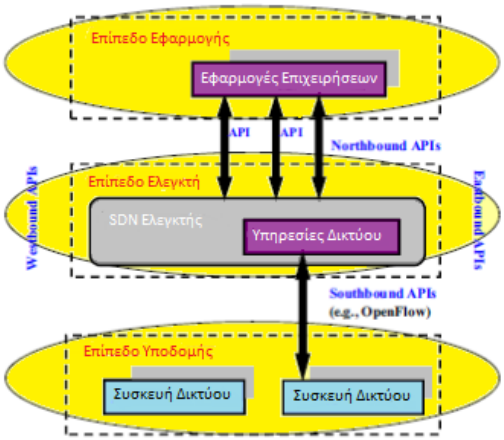
Σε αυτήν την εργασία θα μελετηθεί η αρχιτεκτονική των SDN, η λειτουργία τους και θα δοθεί ιδιαίτερη έμφαση στις απειλές ασφάλειας τους και τους τρόπους αντιμετώπισής τους. Πιο συγκεκριμένα στο κεφάλαιο 2 θα γίνει μελέτη στο ιστορικό των SDN, στην αρχιτεκτονική τους, στις εφαρμογές τους, στους ελεγκτές τους και στο OpenFlow. Στην συνέχεια στο κεφάλαιο 3, θα μελετηθούν οι αρχές ασφάλειας των SDN, οι τύποι επιθέσεων και οι τρόποι αντιμετώπισής τους, και οι έλεγχοι ασφάλειας τους. Τέλος στο κεφάλαιο 4 θα γίνει υλοποίηση ενός σεναρίου επίθεσης DoS σε ένα SDN σε περιβάλλον προσομοίωσης mininet και θα πραγματοποιηθεί ανίχνευση της επίθεσης με το IDS Suricata.

ΚΕΦΑΛΑΙΟ 2

2.1 Δίκτυο Ορισμένο από Λογισμικό (Software-Defined Networking)

Τα δίκτυα ορισμένα από λογισμικό (SDN) αποτελούνται από υποκείμενα προγραμματιζόμενα switches και ένα σύμπλεγμα οντοτήτων ελέγχου. Όπως είδαμε στην Εικ. 1, η διαφορά μεταξύ SDN και παραδοσιακών δικτύων είναι ότι ένα στοιχείο λογισμικού που τρέχει σε έναν διακομιστή ή σε έναν επεξεργαστή προστίθεται στην αρχιτεκτονική του δικτύου. Ο κεντρικός διακομιστής ελέγχου μπορεί να ενεργοποιήσει δραστικά απλοποιημένο και ευέλικτο προγραμματισμό δικτύου. Μπορεί να βελτιώσει τα οφέλη της οπτικοποίησης των κέντρων δεδομένων, αυξάνοντας την ευελιξία και την αξιοποίηση της πηγής και μειώνοντας τις δαπάνες υποδομής.

Πιο συγκεκριμένα, η αρχιτεκτονική τριών επιπέδων του SDN απεικονίζεται στο Σχ. 2, συμπεριλαμβάνοντας το επίπεδο εφαρμογής, το επίπεδο ελεγκτή και το επίπεδο υποδομής. Το επίπεδο εφαρμογής μπορεί να επιβάλλει τις πολιτικές του χωρίς να έχει άμεση αλληλεπίδραση με το επίπεδο υποδομής, μέσω του βόρειου API που υποστηρίζεται από τον ελεγκτή. Από την άλλη πλευρά, οι αλληλεπιδράσεις μεταξύ του επιπέδου ελεγκτή και του επιπέδου υποδομής υποστηρίζονται από τα νότια APIs. Βάση λογικής, η διαχείριση του δικτύου συγκεντρώνεται στους SDN ελεγκτές που βασίζονται στο λογισμικό. Επομένως, το δίκτυο είναι ικανό να λειτουργεί σαν ένα μοναδικό switch για τις εφαρμογές και τις μηχανές πολιτικής. Κάτω από αυτή την αρχιτεκτονική, το φυσικό δίκτυο και η τοπολογία δεν φαίνεται στους χρήστες. Εξ' αιτίας αυτού του σχεδιασμού, οι επιχειρήσεις μπορούν να αποκτήσουν ανεξάρτητο έλεγχο σε όλο το δίκτυο από μοναδικό σημείο, το οποίο απλοποιεί το σχεδιασμό και τις λειτουργίες του δικτύου.



Εικόνα 2 Η αρχιτεκτονική τριών επιπέδων του SDN

Συγκεντρώνοντας τις καταστάσεις του δικτύου στο επίπεδο του ελεγκτή, ο σχεδιαστής του συστήματος ή ο διαχειριστής του δικτύου στο επίπεδο εφαρμογών μπορεί να αλληλεπιδράσει με τα συμβάντα του δικτύου σε πραγματικό χρόνο και να αναπτύξει καινούριες εφαρμογές και υπηρεσίες πολύ γρήγορα. Αυτή η αρχιτεκτονική υποστηρίζει

επίσης ένα σύνολο από APIs που καθιστούν δυνατή την πραγματοποίηση κοινών υπηρεσιών δικτύου, όπως δρομολόγηση και πολλαπλή διανομή, για την επίτευξη ατομικών και επιχειρηματικών στόχων. Έτσι, με την εφαρμογή των APIs μεταξύ του ελεγκτή SDN και του επιπέδου εφαρμογών, οι επιχειρηματικές εφαρμογές μπορούν να λειτουργούν με αφαίρεση του δικτύου, αξιοποιώντας τις υπηρεσίες και τις δυνατότητες του, χωρίς να συνδέονται με τις λεπτομέρειες της συγκεκριμένης εφαρμογής τους (Open Networking Foundation, 2012). Για παράδειγμα, όταν μια νέα ροή φτάσει σε ένα SDN switch, αυτό το switch μπορεί να στείλει ένα αίτημα δρομολόγησης στον κεντρικό ελεγκτή για την επόμενη προώθηση διαδρομής. Ο ελεγκτής υπολογίζει μια διαδρομή δρομολόγησης και διανέμει τον κανόνα προώθησης σε όλα τα σχετικά switches μέσω ενός ασφαλούς καναλιού. Ως αποτέλεσμα, όλα τα σχετικά switches μπορούν να ενημερώσουν τους πίνακες ροής.

Συνολικά, το SDN είναι σε θέση να διαχειρίζεται ολόκληρο το δίκτυο διατηρώντας μια καθολική προβολή και παροχή πολλών πλεονεκτημάτων (π.χ. κατανομή πόρων κατ' απαίτηση, ασφαλείς υπηρεσίες cloud και οπτικοποιημένη δικτύωση). Πιο συγκεκριμένα, ένα χαρακτηριστικό του SDN είναι η ικανότητα παροχής ευρείας αφαίρεσης δικτύου. Η αφαίρεση επιτρέπει στο SDN να παρέχει έναν ευκολότερο τρόπο διαμόρφωσης μιας υπηρεσίας ή συσκευής κρύβοντας την πολυπλοκότητα του δικτύου. Οι συσκευές μόνες τους μπορούν να δεχτούν οδηγίες από τους ελεγκτές χωρίς την κατανόηση και την επεξεργασία χιλιάδων προτύπων των πρωτοκόλλων .Ένα άλλο χαρακτηριστικό του SDN είναι ότι επιτρέπει την καινοτομία και ευελιξία. Ο λόγος είναι προφανώς ότι οι συσκευές που βασίζονται στο υλικό είναι συνήθως δύσκολο να τροποποιηθούν, ενώ ο ελεγκτής που βασίζεται στο λογισμικό είναι πιο εύκολο να κάνει μια αλλαγή και μια αλληλεπίδραση.

2.2 Παραδοσιακά δίκτυα

Τα δίκτυα υπολογιστών (computer networks) ανήκουν στη γενικότερη κατηγορία των τηλεπικοινωνιακών δικτύων (telecommunication networks), δηλαδή σε εκείνα τα κατανεμημένα συστήματα που επιτρέπουν στους χρήστες τους να μεταβιβάζουν ή να ανταλλάσσουν πληροφορίες. Το πιο σημαντικό χαρακτηριστικό των δικτύων υπολογιστών είναι η ποικιλομορφία τους. Τα δίκτυα Η/Υ αναπτύσσονται και λειτουργούν κυρίως με προγραμματιζόμενες συσκευές γενικού σκοπού (π.χ. μία τερματική συσκευή δικτύου Η/Υ μπορεί να είναι και ο προσωπικός σας υπολογιστής). Και επειδή αυτές οι συσκευές δεν έχουν σχεδιαστεί για την εξυπηρέτηση μιας μόνο μορφής αναπαράστασης πληροφορίας (όπως, π.χ. η φωνή ή το σήμα τηλεόρασης), έχουν τη δυνατότητα να εξυπηρετούν πολλές διαφορετικές μορφές αναπαράστασης της πληροφορίας. Έτσι, τα δίκτυα υπολογιστών μπορούν να υποστηρίζουν μια μεγάλη (και ολοένα αυξανόμενη) ποικιλία εφαρμογών.

Ένα δίκτυο υπολογιστών είναι ένα σύνολο από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία (π.χ. εκκίνηση ή τερματισμό) κάποιου άλλου.

Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή πληροφοριών κάθε μορφής (προγράμματα, αρχεία, δεδομένα). Πόροι του συστήματος μπορούν να είναι είτε υλικό (hardware), π.χ. υπολογιστές, εκτυπωτές, plotters, σκληροί δίσκοι είτε λογισμικό (software), π.χ. δεδομένα, προγράμματα εφαρμογών, υπηρεσίες. Τα προγράμματα, τα δεδομένα και οι συσκευές (σκληροί δίσκοι, εκτυπωτές, κλπ) είναι διαθέσιμα σε οποιονδήποτε είναι συνδεδεμένος στο δίκτυο, ανεξάρτητα από τη φυσική του θέση. Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα. Σε ένα δίκτυο μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων (email). Επιπλέον, ανεξάρτητα της τεχνολογίας, ένα δίκτυο είναι ένα πανίσχυρο μέσο επικοινωνίας ανθρώπων που βρίσκονται σε διαφορετικά μέρη.

Σήμερα, οι περισσότεροι οργανισμοί, ιδρύματα και εταιρείες έχουν τους Η/Υ τους συνδεδεμένους σε δίκτυα. Για παράδειγμα, οι αεροπορικές εταιρείες, τα πολυκαταστήματα, οι βιομηχανίες, οι εφορείες, τα γραφεία ευρέσεως εργασίας, τα πανεπιστήμια, οι τράπεζες, τα σχολεία έχουν δίκτυα υπολογιστών, τα οποία βελτιώνουν και επεκτείνουν διαρκώς.

Τα δίκτυα φέρουν τους εξής χαρακτηρισμούς, που καθορίζουν και την κατηγορία τους:

1. Ανάλογα με το φυσικό μέσο διασύνδεσης τους χαρακτηρίζονται ως ενσύρματα ή ασύρματα.
2. Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως δημόσια ή ιδιωτικά δίκτυα.
3. Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως τοπικά (LAN και WLAN), μητροπολιτικά (MAN και WMAN), ευρείας κάλυψης (WAN και WWAN) και προσωπικά (PAN και WPAN).

2.2.1 Ασφάλεια στα Παραδοσιακά Δίκτυα

Η έννοια της ασφάλειας Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Εκτός αυτού, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Η έννοια της ασφάλειας των δικτύων υπολογιστών συνδέεται στενά με τρεις βασικές έννοιες.

- **Διαθεσιμότητα (Availability)**

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα.

- **Εμπιστευτικότητα (Confidentiality)**

Εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών

- **Ακεραιότητα (Integrity)**

Η *ακεραιότητα* μπορεί να οριστεί γενικότερα ως η πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

2.2.2 Μέθοδοι Επίθεσης στα Παραδοσιακά Δίκτυα

- **Denial-of-Service (DoS)**

Μια επίθεση Denial of Service (DoS) δημιουργεί κάποια διακοπή των υπηρεσιών δικτύου σε χρήστες, συσκευές ή εφαρμογές. Υπάρχουν δύο βασικοί τύποι επιθέσεων DoS:

Υπερβολική ποσότητα επισκεψιμότητας - Ο επιτιθέμενος στέλνει μια τεράστια ποσότητα δεδομένων με ρυθμό που δεν μπορεί να χειριστεί το δίκτυο, ο κεντρικός υπολογιστής ή η εφαρμογή. Αυτό προκαλεί επιβράδυνση των χρόνων μετάδοσης και απόκρισης. Μπορεί επίσης να καταστρέψει μια συσκευή ή μια υπηρεσία.

Πακέτα με κακόβουλη μορφή - Ο επιτιθέμενος στέλνει ένα πακέτο με κακόβουλη μορφή σε έναν κεντρικό υπολογιστή ή μια εφαρμογή και ο δέκτης δεν μπορεί να το χειριστεί. Αυτό προκαλεί στην συσκευή λήψης να λειτουργεί πολύ αργά ή καθόλου.

- **Reconnaissance Attacks (Επίθεση αναγνώρισης)**

Η αναγνώριση είναι η συλλογή πληροφοριών. Είναι ανάλογο με έναν κλέφτη που παρακολουθεί μια γειτονιά πηγαίνοντας από πόρτα σε πόρτα που προσποιείται ότι πουλάει κάτι. Αυτό που πραγματικά κάνει ο κλέφτης είναι να αναζητήσει ευάλωτα σπίτια, όπως κατοικίες, κατοικημένες πόρτες ή παράθυρα που ανοίγουν εύκολα και κατοικίες χωρίς συστήματα ασφαλείας ή κάμερες ασφαλείας.

Οι επιτιθέμενοι χρησιμοποιούν επιθέσεις αναγνώρισης για να κάνουν μη εξουσιοδοτημένη ανακάλυψη και χαρτογράφηση συστημάτων, υπηρεσιών ή τρωτών σημείων. Οι επιθέσεις Recon προηγούνται των επιθέσεων πρόσβασης ή των επιθέσεων DoS.

- **Password attacks**

Εάν οι επιτιθέμενοι ανακαλύψουν έναν έγκυρο λογαριασμό χρήστη, έχουν τα ίδια δικαιώματα με τον πραγματικό χρήστη. Οι επιτιθέμενοι θα μπορούσαν να χρησιμοποιήσουν αυτόν τον έγκυρο λογαριασμό για να λάβουν λίστες άλλων χρηστών, πληροφορίες δικτύου, αλλαγή ρυθμίσεων διακομιστή και δικτύου και να τροποποιήσουν, να αναδρομολογήσουν ή να διαγράψουν δεδομένα.

- **Trojan Horses**

Οι επιτιθέμενοι χρησιμοποιούν Trojan horses για να θέσουν σε κίνδυνο τους χρήστες. Ένα Trojan horse είναι ένα πρόγραμμα που φαίνεται χρήσιμο, αλλά έχει επίσης κακόβουλο κώδικα. Τα Trojan horses συχνά παρέχονται δωρεάν με διαδικτυακά προγράμματα, όπως παιχνίδια στον υπολογιστή. Οι ανυποψίαστοι χρήστες κάνουν λήψη και εγκατάσταση του παιχνιδιού, μαζί με το Trojan horse.

- **Επίθεση sniffer**

Το sniffer είναι μια εφαρμογή ή συσκευή που μπορεί να διαβάσει, να παρακολουθήσει και να συλλάβει ανταλλαγές δεδομένων δικτύου και να διαβάσει πακέτα δικτύου. Εάν τα πακέτα δεν είναι κρυπτογραφημένα, ένα sniffer παρέχει πλήρη εικόνα των δεδομένων μέσα στο πακέτο.

2.2.3 Τρόποι Αντιμετώπισης στα Παραδοσιακά Δίκτυα

- **Έλεγχος γνησιότητας της ταυτότητας**

(identification and authentication) των χρηστών , των προγραμμάτων ή των μηχανημάτων καθώς και των εξουσιοδοτήσεων που αυτά διαθέτουν για την προσπέλαση των προστατευμένων πόρων του συστήματος με συνδυασμένη χρήση συνθηματικών και ψηφιακών πιστοποιητικών.

- **Προστασία της εμπιστευτικότητας των δεδομένων (data confidentiality)**

Εγγυάται ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να διαβάσουν το μήνυμα. Εάν το μήνυμα υποκλαπεί, δεν μπορεί να αποκρυπτογραφηθεί εντός εύλογου χρονικού διαστήματος. Η εμπιστευτικότητα των δεδομένων υλοποιείται χρησιμοποιώντας συμμετρικούς και ασύμμετρους αλγόριθμους κρυπτογράφησης.

Υπάρχουν δύο κατηγορίες κρυπτογράφησης που χρησιμοποιούνται για την παροχή εμπιστευτικότητας δεδομένων. Αυτές οι δύο κατηγορίες διαφέρουν ως προς τον τρόπο χρήσης των κλειδιών.

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης όπως (DES), 3DES και Advanced Encryption Standard (AES) βασίζονται στην υπόθεση ότι κάθε επικοινωνιακό μέρος γνωρίζει το κοινόχρηστο κλειδί. Η εμπιστευτικότητα των δεδομένων μπορεί επίσης να διασφαλιστεί χρησιμοποιώντας ασύμμετρους αλγόριθμους, συμπεριλαμβανομένων των Rivest, Shamir και Adleman (RSA) και της υποδομής δημόσιου κλειδιού (PKI).

- **Firewall (Τείχος προστασίας)**

Το τείχος προστασίας είναι ένα σύστημα ή μια ομάδα συστημάτων που επιβάλλει μια πολιτική ελέγχου πρόσβασης μεταξύ των δικτύων.

Όλα τα τείχη προστασίας μοιράζονται μερικές κοινές ιδιότητες:

- Τα τείχη προστασίας είναι ανθεκτικά σε επιθέσεις δικτύου.
- Τα τείχη προστασίας είναι τα μόνα σημεία διέλευσης μεταξύ εσωτερικών εταιρικών δικτύων και εξωτερικών δικτύων επειδή όλη η κυκλοφορία ρέει μέσω του τείχους προστασίας.
- Τα τείχη προστασίας επιβάλλουν την πολιτική ελέγχου πρόσβασης.

Υπάρχουν πολλά οφέλη από τη χρήση τείχους προστασίας σε ένα δίκτυο:

- Αποτρέπουν την έκθεση ευαίσθητων κεντρικών υπολογιστών, πόρων και εφαρμογών σε μη αξιόπιστους χρήστες.
- Καθαρίζουν τη ροή πρωτοκόλλου, η οποία αποτρέπει την εκμετάλλευση των ελαττωμάτων πρωτοκόλλου.
- Αποκλείουν κακόβουλα δεδομένα από διακομιστές και πελάτες.

- Μειώνουν την πολυπλοκότητα της διαχείρισης της ασφάλειας φορτώνοντας το μεγαλύτερο μέρος του ελέγχου πρόσβασης δικτύου σε μερικά τείχη προστασίας στο δίκτυο.

Τα τείχη προστασίας παρουσιάζουν επίσης ορισμένους περιορισμούς:

- Ένα εσφαλμένο διαμορφωμένο τείχος προστασίας μπορεί να έχει σοβαρές συνέπειες για το δίκτυο, όπως να γίνει ένα μόνο σημείο αποτυχίας.
- Τα δεδομένα από πολλές εφαρμογές δεν μπορούν να περάσουν με ασφάλεια μέσω τείχους προστασίας.
- Οι χρήστες ενδέχεται να αναζητήσουν προληπτικά τρόπους γύρω από το τείχος προστασίας για να λάβουν αποκλεισμένο υλικό, το οποίο εκθέτει το δίκτυο σε πιθανή επίθεση.
- Η απόδοση του δικτύου μπορεί να επιβραδυνθεί.
- Η μη εξουσιοδοτημένη κυκλοφορία μπορεί να διοχετευτεί ή να κρυφτεί έτσι ώστε να εμφανίζεται ως νόμιμη κυκλοφορία μέσω του τείχους προστασίας.

- **Ενημέρωση**

Η ενημέρωση με τις τελευταίες εξελίξεις μπορεί να οδηγήσει σε μια πιο αποτελεσματική άμυνα ενάντια σε επιθέσεις δικτύου. Καθώς κυκλοφορεί νέο κακόβουλο λογισμικό, οι επιχειρήσεις πρέπει να ενημερώνουν τις τελευταίες εκδόσεις του λογισμικού προστασίας από ιούς.

Ο πιο αποτελεσματικός τρόπος για τον μετριασμό μιας επίθεσης worm είναι να κατεβάσετε ενημερώσεις ασφαλείας από τον προμηθευτή του λειτουργικού συστήματος και να διορθώσετε όλα τα ευάλωτα συστήματα. Η διαχείριση πολλών συστημάτων συνεπάγεται τη δημιουργία μιας τυπικής εικόνας λογισμικού (λειτουργικό σύστημα και διαπιστευμένες εφαρμογές που έχουν εγκριθεί για χρήση σε συστήματα πελατών) που αναπτύσσεται σε νέα ή αναβαθμισμένα συστήματα. Ωστόσο, οι απαιτήσεις ασφαλείας αλλάζουν και τα ήδη αναπτυγμένα συστήματα ενδέχεται να πρέπει να έχουν εγκαταστήσει ενημερωμένες ενημερώσεις κώδικα ασφαλείας.

- **IPS**

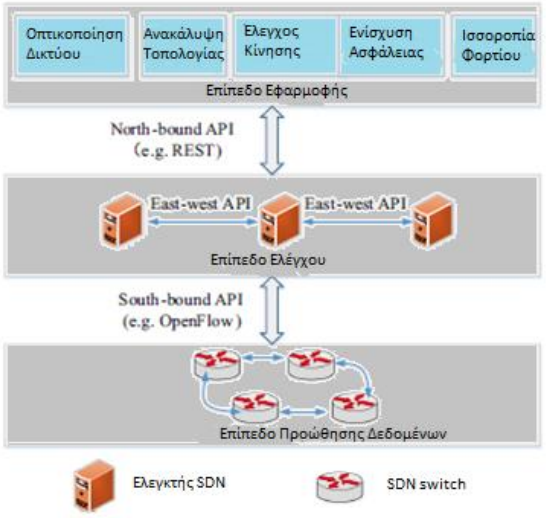
Για να υπερασπιστείτε τις γρήγορες και εξελισσόμενες επιθέσεις, ίσως χρειαστείτε οικονομικά αποδοτικά συστήματα ανίχνευσης και πρόληψης, όπως συστήματα ανίχνευσης εισβολής (IDS) ή τα πιο επεκτάσιμα συστήματα πρόληψης εισβολής (IPS). Η αρχιτεκτονική του δικτύου ενσωματώνει αυτές τις λύσεις στα σημεία εισόδου και εξόδου του δικτύου.

Οι τεχνολογίες IDS και IPS μοιράζονται πολλά χαρακτηριστικά. Οι τεχνολογίες IDS και IPS αναπτύσσονται και οι δύο ως αισθητήρες. Ένας αισθητήρας IDS ή IPS μπορεί να έχει τη μορφή πολλών διαφορετικών συσκευών:

- Ένας δρομολογητής διαμορφωμένος με λογισμικό Cisco IOS IPS
- Μια συσκευή ειδικά σχεδιασμένη για να παρέχει αποκλειστικές υπηρεσίες IDS ή IPS
- Μια μονάδα δικτύου εγκατεστημένη σε μια προσαρμοστική συσκευή ασφαλείας (ASA), διακόπτη ή δρομολογητή

2.3 Επισκόπηση της αρχιτεκτονικής SDN

Το SDN είναι ένα είδος αναδυόμενης αρχιτεκτονικής δικτύου που αποσυνδέει την προώθηση των δεδομένων από τη λογική ελέγχου. Επί του παρόντος, αυτές οι πτυχές ενσωματώνονται στενά στον παραδοσιακό εξοπλισμό του δικτύου, όπως switches και δρομολογητές. Η αποσύνδεση της προώθησης δεδομένων και η λογική ελέγχου επιτρέπουν στον έλεγχο του δικτύου και στις εφαρμογές να μπορούν να προγραμματιστούν. Γενικά, η SDN αρχιτεκτονική μπορεί να χωριστεί σε τρία επίπεδα, στο επίπεδο προώθησης δεδομένων, το επίπεδο ελέγχου και το επίπεδο εφαρμογής από κάτω προς τα πάνω, όπως φαίνεται στην Εικ 3.



Εικόνα 3 Η αρχιτεκτονική SDN

2.3.1 Επίπεδο προώθησης δεδομένων

Το επίπεδο προώθησης δεδομένων αποτελείται από πολλά SDN switches, που συνδέονται φυσικά με ενσύρματα ή ασύρματα μέσα. Κάθε switch είναι μια απλή συσκευή που είναι υπεύθυνη για την προώθηση πακέτων δικτύου και έχει έναν πίνακα προώθησης, που ονομάζεται Πίνακας Ροής, ο οποίος περιέχει χιλιάδες κανόνες που χρησιμοποιούνται για τη διατύπωση προώθησης αποφάσεων.

Κάθε στοιχείο κανόνα στον πίνακα ροής αποτελείται από τρία πεδία: την δράση, τον μετρητή και το μοτίβο. Το πεδίο μοτίβου ορίζει το μοτίβο ροής, το οποίο είναι βασικά το σύνολο των κεφαλίδων στο πεδίο τιμών του πακέτου. Όταν λαμβάνονται πακέτα δεδομένων, το switch θα αναζητήσει τον πίνακα ροής για να βρει έναν κανόνα που να ταιριάζει με τα πεδία.

Μόλις το switch εντοπίσει έναν τέτοιο κανόνα, ο μετρητής του κανόνα αυξάνεται και η ενέργεια που αντιστοιχεί στον συγκεκριμένο κανόνα θα εκτελεστεί. Διαφορετικά, το switch θα ειδοποιήσει τον ελεγκτή για να ζητήσει βοήθεια ή απλώς απορρίπτει το πακέτο. Αξίζει να σημειωθεί ότι τα στοιχεία του κανόνα προώθησης δεν δημιουργούνται από το ίδιο το switch, αλλά ωθούνται από τον ελεγκτή από το επίπεδο ελέγχου.

2.3.2 Επίπεδο ελέγχου

Ως εγκέφαλος του SDN, το επίπεδο ελέγχου διαχειρίζεται και ελέγχει ολόκληρο το δίκτυο. Αναφερόμαστε στον κόμβο δικτύου που εφαρμόζει αυτές τις λειτουργίες ως ελεγκτής SDN και γενικά αναπτύσσεται ως ξεχωριστή φυσική συσκευή με συγκεκριμένο λογισμικό. Ο ελεγκτής SDN επικοινωνεί με το switch μέσω ενός τυπικού νότιου API, π.χ. OpenFlow και έχει μια καθολική προβολή ολόκληρης της τοπολογίας του δικτύου στο επίπεδο δεδομένων προώθησης, δηλαδή switches και συνδέσμους. Διάφορα πρωτόκολλα δρομολόγησης, όπως το BGP και το OSPF, τρέχουν στον ελεγκτή SDN έτσι όλη η προώθηση δεδομένων γίνεται στο επίπεδο δεδομένων με βάση τις οδηγίες του ελεγκτή.

Ως το de facto πρότυπο του SDN, το OpenFlow ήταν αρχικά σχεδιασμένο με έναν μόνο ελεγκτή κάνοντας πιο απλή την διαδικασία, γεγονός που αποτελεί ένα πιθανό σημείο αποτυχίας. Ως εκ τούτου, σχεδόν όλες οι πρόσφατες υλοποιήσεις αρχιτεκτονικής SDN, όπως το Floodlight, το NOX και το OpenDaylight υποστηρίζουν πολλαπλούς κατανεμημένους ελεγκτές, γεγονός που βελτιώνει την επεκτασιμότητα και την διαθεσιμότητα πόρων δικτύου. Στην αρχιτεκτονική πολυ-ελεγκτή, κάθε μεμονωμένος ελεγκτής είναι υπεύθυνος για έλεγχο μόνο ενός τμήματος των switches. Για να διατηρήσει τη συνέπεια της κατάστασης και της εργασίας του δικτύου συνεργατικά, ένας μεμονωμένος ελεγκτής SDN μπορεί να επικοινωνήσει με άλλους ελεγκτές στο δίκτυο μέσω ανατολικών και δυτικών APIs.

2.3.3 Επίπεδο εφαρμογής

Το επίπεδο εφαρμογής επιτρέπει στους χειριστές δικτύου να ανταποκριθούν γρήγορα στις διάφορες επιχειρηματικές απαιτήσεις. Μία καινοτόμος εφαρμογή λογισμικού έχει κατασκευαστεί για να λειτουργεί πάνω από τους SDN ελεγκτές έτσι ώστε να πληρούνται διάφορες απαιτήσεις της εφαρμογής, όπως η οπτικοποίηση δικτύου, η ανακάλυψη τοπολογίας, η παρακολούθηση κυκλοφορίας, η βελτίωση ασφάλειας, το φορτίο εξισορρόπησης και άλλα.

Το επίπεδο εφαρμογής επικοινωνεί με το επίπεδο ελέγχου μέσω βόρειων API, όπως το REST API. Το επίπεδο ελέγχου παρέχει μια αφαίρεση των φυσικών πόρων του δικτύου για το επίπεδο εφαρμογής, που σημαίνει ότι οι διαχειριστές δικτύου μπορούν να αλλάξουν τις διαδρομές δεδομένων των πακέτων χρησιμοποιώντας μόνο προγραμματισμό λογισμικού κεντρικά στους SDN ελεγκτές και να μην διαμορφώνουν όλα τα φυσικά switches στη διαδρομή δεδομένων ένα προς ένα.

2.4 Εφαρμογές SDN

Τα SDN δίκτυα εφαρμόζονται σε αρκετά περιβάλλοντα που έχουν σχέση με τα δίκτυα υπολογιστών. Ο διαχωρισμός των επιπέδων ελέγχου και δεδομένων, τα προγραμματιζόμενα δίκτυα επιτρέπουν τον προσαρμοσμένο έλεγχο, την αποφυγή των ενδιάμεσων θυρίδων και κάνουν ευκολότερη την ανάπτυξη και διαχείριση νέων υπηρεσιών. Στην συνέχεια, παρουσιάζονται κάποια περιβάλλοντα για τα οποία έχουν προταθεί ή εφαρμοστεί SDN λύσεις.

2.4.1 Κέντρα δεδομένων

Τα κέντρα δεδομένων έχουν εξελιχτεί με εκπληκτικά βήματα τα τελευταία χρόνια, προσπαθώντας συνεχώς να επιτύχουν όλο και υψηλότερη ζήτηση. Η προσεκτική διαχείριση της κίνησης και η επιβολή της πολιτικής είναι κρίσιμες όταν λειτουργούν σε τόσο μεγάλες κλίμακες, ειδικότερα όταν οποιαδήποτε διακοπή υπηρεσίας ή πρόσθετη καθυστέρηση μπορεί να οδηγήσουν σε μαζική παραγωγικότητα ή και απώλειες κερδών. Εξ’ αιτίας των προκλήσεων της μηχανικής των δικτύων αυτής της κλίμακας και της πολυπλοκότητας για δυναμική προσαρμογή στις απαιτήσεις εφαρμογής, είναι συχνή η περίπτωση όπου τα κέντρα δεδομένων αποκτούν μεγάλη ζήτηση, με αποτέλεσμα να τρέχουν πολύ λιγότερο από όσο μπορούν τις περισσότερες φορές, αλλά είναι έτοιμα να εξυπηρετήσουν γρήγορα μεγάλους φόρτους εργασίας.

2.4.2 Δίκτυα Επιχειρήσεων

Οι επιχειρήσεις συχνά τρέχουν μεγάλα δίκτυα, ενώ επίσης έχουν αυστηρές απαιτήσεις ασφάλειας και απόδοσης. Επιπλέον, τα διαφορετικά επιχειρησιακά

περιβάλλοντα μπορεί να έχουν και διαφορετικές απαιτήσεις, χαρακτηριστικά και πλήθος χρηστών.

Η επαρκής διαχείριση είναι εξαιρετικά σημαντική στα περιβάλλοντα των επιχειρήσεων και το SDN, μπορεί να χρησιμοποιηθεί για να ενισχύσει προγραμματιστικά και να προσαρμόσει τις πολιτικές του δικτύου, καθώς επίσης και να βοηθήσει στον έλεγχο της δραστηριότητας του δικτύου και να βελτιώσει την απόδοσή του.

Ακόμη, το SDN μπορεί να χρησιμοποιηθεί για να διευκολύνει το δίκτυο αφαιρώντας τα ενδιάμεσα κουτιά (middleboxes) και να ενσωματώσει την λειτουργία τους μέσα στον ελεγκτή του δικτύου. Μερικά αξιοσημείωτα παραδείγματα της λειτουργικότητας των middleboxes που έχουν εφαρμοστεί χρησιμοποιώντας το SDN συμπεριλαμβάνουν το NAT, τα firewalls, τα φορτία εξισορρόπησης και τον έλεγχο πρόσβασης δικτύου. Στην περίπτωση όπου πιο σύνθετα middleboxes με λειτουργείες που δεν μπορούν να εφαρμοστούν άμεσα χωρίς την υποβάθμιση της απόδοσης, το SDN μπορεί να χρησιμοποιηθεί για να παρέχει ενοποιημένο έλεγχο και διαχείριση.

2.4.3 Ασύρματα δίκτυα με βάση την υποδομή

Αρκετές προσπάθειες έχουν εστιάσει στην συνεχή συνδεσιμότητα στο πλαίσιο των ασύρματων δικτύων με βάση την υποδομή , όπως το κινητό και το Wi-Fi.

Για παράδειγμα, το OpenRoads project οραματίζεται έναν κόσμο όπου οι χρήστες θα μπορούν ελεύθερα και απρόσκοπτα να κινούνται σε διαφορετικές ασύρματες υποδομές οι οποίες μπορούν να διαχειριστούν από ποικίλους παρόχους. Αυτοί προτείνουν την ανάπτυξη μιας ασύρματης αρχιτεκτονικής βασισμένης στο SDN που είναι συμβατή με τις προηγούμενες, και επίσης ανοιχτή και διαμοιραζόμενη μεταξύ των διάφορων παρόχων υπηρεσιών. Η ιδέα αυτή, τους παρείχε έμπνευση για επακόλουθη εργασία που προσπαθεί να αντιμετωπίσει συγκεκριμένες απαιτήσεις και προκλήσεις για την ανάπτυξη ενός κυψελωτού δικτύου ορισμένου από το λογισμικό.

2.4.4 Σπίτι και μικρές επιχειρήσεις

Αρκετά projects έχουν εξεταστεί για το πως το SDN θα μπορούσε να χρησιμοποιηθεί σε μικρότερα δίκτυα, όπως αυτά που βρίσκονται σε ένα σπίτι ή μια μικρή επιχείρηση. Καθώς αυτά τα περιβάλλοντα έχουν γίνει όλο και περισσότερο πολύπλοκα και διαδεδομένα με την ευρεία διαθεσιμότητα των συσκευών δικτύου χαμηλού κόστους, η ανάγκη για πιο προσεκτική διαχείριση δικτύου και αυστηρότερη ασφάλεια έχει αυξηθεί σημαντικά. Τα λιγότερο ασφαλή δίκτυα μπορεί να γίνουν ακούσιοι στόχοι ή συσκευές για κακόβουλο λογισμικό, ενώ διακοπές λειτουργίας λόγω ζητημάτων διαμόρφωσης δικτύου μπορεί να προκαλέσουν ακύρωση ή χάσιμο κάποιας δουλειάς. Δυστυχώς, αυτό δεν είναι πρακτικό να υπάρχει ένας διαχειριστής δικτύου για κάθε σπίτι ή γραφείο.

Οι (Calvert, W.K. Edwards, N. Feamster, R.E. Grinter, Y. Deng, and X. Zhou., 2011) ισχυρίζονται ότι το πρώτο βήμα στη διαχείριση ενός σπιτικού δικτύου είναι να ξέρεις τι ακριβώς συμβαίνει. Ως εκ τούτου, προτείνουν να λειτουργήσει η πύλη / ελεγκτής του

δικτύου για να ενεργήσει ως "Μηχάνημα εγγραφής δεδομένων του σπιτικού δικτύου" για να δημιουργεί αρχεία καταγραφής που μπορεί να χρησιμοποιηθούν για την αντιμετώπιση προβλημάτων ή για άλλους σκοπούς.

Ο (Feamster., 2010) προτείνει ότι τέτοια δίκτυα πρέπει να λειτουργούν με έναν τρόπο τύπου: «συνδέσου και ξέχασέ το», δηλαδή με εξωτερική ανάθεση διαχείρισης σε τρίτους ειδικούς και αυτό μπορεί να επιτευχθεί μέσω απομακρυσμένου ελέγχου προγραμματισμένων switches και εφαρμογής παρακολούθησης κατανεμημένων δικτύων και αλγόριθμων συμπερασμάτων που χρησιμοποιούνται για την ανίχνευση πιθανών προβλημάτων ασφάλειας.

Σε αντίθεση, ο (R. Mortier, 2012) πιστεύει ότι οι χρήστες επιθυμούν καλύτερη κατανόηση και έλεγχο του δικτύου τους. Είναι προτιμότερο από το να ακολουθούν παραδοσιακές πολιτικές, τα σπιτικά δίκτυα μπορούν καλύτερα να διαχειριστούν από τους χρήστες τους οι οποίοι καταλαβαίνουν καλύτερα την δυναμική και τις ανάγκες του περιβάλλοντός τους. Με αυτόν τον στόχο, δημιούργησαν ένα πρωτότυπο δίκτυο στο οποίο χρησιμοποιείται το SDN για να παρέχουν στους χρήστες μια όψη για το πώς χρησιμοποιείται το δίκτυό τους προσφέροντας ένα μόνο σημείο ελέγχου.

2.5 Ελεγκτές

Το επίπεδο ελέγχου του SDN είναι υπεύθυνο για την διαχείριση των ροών που διασχίζουν τα switches. Στο κέντρο του επιπέδου ελέγχου βρίσκεται ο ελεγκτής δικτύου, ο οποίος συνήθως τρέχει σε έναν server που είναι συνδεδεμένος στο δίκτυο. Η επιλογή ενός SDN ελεγκτή που ταιριάζει σωστά με τις ανάγκες του δικτύου είναι μία σημαντική διεργασία. Παρακάτω θα δούμε διάφορους SDN ελεγκτές, επισημαίνοντας τα κύρια χαρακτηριστικά τους.

2.5.1 NOX

Ο NOX παρέχει μία πλατφόρμα προγραμματισμού για να ελέγχει ένα ή περισσότερα OpenFlow switches. Έγινε γνωστός ως ένας από τους πρώτους που είναι ικανοί να ελέγξουν δίκτυα OpenFlow. Επιπλέον, ο NOX είναι μία ανοιχτή πλατφόρμα, η οποία επιτρέπει την ανάπτυξη της διαχείρισης των λειτουργιών στα εταιρικά και εγχώρια δίκτυα. Ο NOX σκοπεύει να παρέχει την χωρητικότητα της διαχείρισης μεγάλων δικτύων σε τιμές Gb/s χωρίς να χρειάζεται ειδικός εξοπλισμός για να τρέχει τον ελεγκτή.

Στην διεπαφή του προς βορρά είναι προσβάσιμος μέσω της C++ και της Python και προσφέρει ένα κεντρικό μοντέλο προγραμματισμού στο οποίο μια εφαρμογή μπορεί να λάβει αποφάσεις προώθησης με μία πλήρη όψη της τοπολογίας. Αυτό επιδιώκει να απλοποιήσει την ανάπτυξη της εφαρμογής. Εκτός από την Διεπαφή Προγραμματισμού εφαρμογών (API), το NOX παρέχει γραφικό περιβάλλον εργασίας χρήστη (GUI) με τρία βασικά στοιχεία: ένα πρόγραμμα προβολής καταγραφής, μια προβολή τοπολογίας και ένα πρόγραμμα κονσόλας.

Το NOX δημοσιεύεται με την άδεια Apache 2.0, η οποία επιτρέπει στον κώδικά του να τροποποιείται ελεύθερα και να αναδιανέμεται. Ενώ αυτό που θα μπορούσε να

ενισχύσει το ενδιαφέρον για τη συνέχιση του έργου, το NOX έχει σημειώσει μείωση της δημοτικότητάς του, ίσως λόγω ότι η απόδοσή του δεν ταιριάζει με εκείνη των πιο πρόσφατων ελεγκτών. Η έλλειψη υποστήριξης για multi-threading βοηθά να το εξηγήσει αυτό, καθώς και ότι το NOX δεν είναι σε θέση να εξερευνήσει αποτελεσματικά το πρόσφατους επεξεργαστές πολλαπλών πυρήνων. Επιπλέον, δεν είναι δυνατή η χρήση πολλαπλών κατανεμημένων ελεγκτών. Λόγω όλων αυτών των παραγόντων, η ανάπτυξη του NOX φαίνεται να έχει σταματήσει.

2.5.2 POX

Το POX είναι ένας ελεγκτής ανοιχτού κώδικα γραμμένος σε python και διανέμεται με την άδεια Apache 2.0. Ξεκίνησε ως OpenFlow ειδικός ελεγκτής, αλλά σήμερα παρέχει ένα γενικό πλαίσιο για τη διαχείριση των switches χρησιμοποιώντας το OpenFlow και το πρωτόκολλο διαχείρισης βάσεων δεδομένων Open vSwitch (OVSDB). Το POX είναι ιδιαίτερα δημοφιλές ως ένα εργαλείο διδασκαλίας και έρευνας, και διευκολύνει επίσης τη γρήγορη δημιουργία πρωτοτύπων νέων εφαρμογών διαχείρισης, λόγω της απλότητάς του. Είναι μία ενδιαφέρον εναλλακτική λύση για το NOX, εάν η απόδοση δεν είναι σημαντική απαίτηση.

Όπως το NOX, το POX δεν υποστηρίζει κατανεμημένους ελεγκτές και multi-threading. Επιπλέον, δεν υποστηρίζει το Ασφαλές Επίπεδο Μεταφοράς (TLS) για ασφαλή OpenFlow επικοινωνία με τα switches. Η ανάπτυξη του POX φαίνεται επίσης να έχει καθυστερήσει. Επιπλέον, η βιβλιογραφία έχει δείξει επανειλημμένα ότι το POX έχει ξεπεραστεί από άλλους πιο ισχυρούς ελεγκτές.

2.5.3 Beacon

Το Beacon είναι ένας διαμορφωμένος, ανοιχτού κώδικα OpenFlow ελεγκτής που υποστηρίζει προσανατολισμένες σε συμβάντα εκτελέσεις και multi-threading εκτελέσεις. Δημιουργήθηκε το 2010 στο Πανεπιστήμιο του Στάνφορντ, χρησιμοποιήθηκε ευρέως στον ακαδημαϊκό χώρο, τόσο για έρευνα όσο και για εκπαίδευση. Χρησιμοποιήθηκε ως βάση για τον ελεγκτή Floodlight.

Ένας από τους στόχους του Beacon ήταν να βελτιώσει την παραγωγικότητα επιτρέποντας σε έναν διαχειριστή να ξεκινήσει, να αλλάξει και να διακόψει τις εφαρμογές την ώρα εκτέλεσης. Παρέχει επίσης ένα σύνολο πρότυπων εφαρμογών που εφαρμόζουν πολλές κοινές λειτουργίες του επιπέδου ελέγχου. Η υψηλή απόδοση ήταν επίσης ένας στόχος.

Για να παρέχει υποστήριξη για το OpenFlow, το Beacon χρησιμοποιεί την βιβλιοθήκη Open-FlowJ Java, η οποία είναι μια αντικειμενοστραφής εφαρμογή του

OpenFlow 1.0. Εξαιτίας αυτού, το Beacon δεν υποστηρίζει νεότερες εκδόσεις της προδιαγραφής OpenFlow. Αυτός είναι ίσως ο κύριος περιορισμός αυτού του ελεγκτή.

2.5.4 Ryu

Ο Ryu δημιουργήθηκε από την Nippon Telegraph και την Telephone Corporation (NTT) και ακολουθεί μια σχεδίαση προσανατολισμένη στα στοιχεία για να διευκολύνει την τροποποίηση και την επέκταση των ενοτήτων ως απόκριση στις νέες απαιτήσεις των εφαρμογών. Με τη σειρά τους, οι εφαρμογές χρησιμοποιούν στοιχεία που παρέχονται από τον ελεγκτή για διασύνδεση με switches και εγκατάσταση κανόνων ροής.

Ορισμένες βασικές εφαρμογές διανέμονται με τον Ryu, συμπεριλαμβάνοντας μια υλοποίηση που βασίζεται σε SDN ενός switch αυτό-μάθησης πάνω από το OpenFlow. Μια απλή εφαρμογή παρακολούθησης, η οποία επιτρέπει σε έναν διαχειριστή να ακολουθεί την τρέχουσα κατάσταση των πορτών και των ροών, είναι επίσης διαθέσιμη. Ο Ryu είναι αρκετά ευέλικτος στην νότια API. Υποστηρίζει διάφορα πρωτόκολλα, συμπεριλαμβανομένων του OpenFlow 1.0 και 1.2 - 1.5, του OFConfig, του NETCONF και του Nicira.

Ο Ryu παρέχει ένα πολύ βασικό διαδικτυακό GUI. Εκθέτει την τοπολογία και τις πληροφορίες ροής, αλλά δεν επιτρέπει καμία τροποποίηση των πινάκων ροής των switches. Ωστόσο, για τη διευκόλυνση του εντοπισμού σφαλμάτων των νέων εφαρμογών, ο Ryu περιλαμβάνει ένα REST API που υποστηρίζει τη συλλογή στατιστικών ροής και πληροφοριών τοπολογίας, καθώς και τον χειρισμό δυναμικών πινάκων ροής.

Ο πηγαίος κώδικας είναι γραμμένος σε Python και διατίθεται ελεύθερα μέσω του GitHub υπό την άδεια Apache 2.0. Όπως ο Beacon, ο Ryu υπερέχει όσον αφορά την τεκμηρίωση, συμπεριλαμβάνοντας πολλά σεμινάρια ανάπτυξης εφαρμογών. Σε αντίθεση με τους προηγούμενους ελεγκτές, ο Ryu παραμένει ενεργός, όπως αποδεικνύεται από την υποστήριξή του σε πρόσφατες εκδόσεις του OpenFlow.

Μια άλλη θετική πτυχή του Ryu είναι η εγγενής υποστήριξη για multi-threading, αν και δεν υποστηρίζει οποιοδήποτε είδος διανεμημένου ελεγκτή. Ενώ το multi-threading επιτρέπει στον Ryu να αποδίδει καλύτερα σε βαριά φορτία, η απόδοσή του ακόμα θεωρείται κακή σε σύγκριση με τους πιο πρόσφατους ελεγκτές σύμφωνα με διάφορα σημεία αναφοράς.

2.5.5 Floodlight

Ενώ πολλοί ελεγκτές SDN έχουν ακαδημαϊκές ρίζες, ο Floodlight συντηρείται από τα Big Switch Δίκτυα και θεωρείται επαγγελματίας ελεγκτής. Το Floodlight δημιουργήθηκε το 2011, είναι γραμμένο σε Java και υποστηρίζει τις εκδόσεις 1.0 έως 1.4 του OpenFlow, καθώς και άλλα API προς νότο. Διανέμεται κάτω από το άδεια Apache 2.0.

Το Floodlight υποστηρίζει multi-threading για την βελτίωση της απόδοσης υπό βαριά φορτία. Πολλοί συγγραφείς έχουν βρει καλά αποτελέσματα με το Floodlight όσον αφορά την ικανότητα χειρισμού μεγάλου όγκου αιτημάτων, αν και παραμένει ξεπερασμένος από άλλους ελεγκτές. Όπως όλοι οι άλλοι ελεγκτές το Floodlight δεν υποστηρίζει κατανεμημένους ελεγκτές.

Το Floodlight παρέχει ένα διαδικτυακό γραφικό περιβάλλον που επιτρέπει την οπτικοποίηση της τοπολογίας του δικτύου, συμπεριλαμβανομένων των κεντρικών υπολογιστών που είναι συνδεδεμένοι σε κάθε switch. Αυτή η διεπαφή εμφανίζει επίσης λεπτομερείς πληροφορίες για το κάθε στοιχείο δικτύου, όπως η διαμόρφωση του κάρτας δικτύου και των πινάκων ροής των switches.

2.5.6 OpenDayLight

Το OpenDayLight (ODL) δημιουργήθηκε το 2013 και διατηρείται από το Ίδρυμα Linux. Πολλές εταιρείες συνεισφέρουν στο project, συμπεριλαμβανομένων των Cisco, HP, IBM και NEC. Το ODL διανέμεται σύμφωνα με το Eclipse Public License (EPL) v1.0, το οποίο είναι μια πιο περιοριστική άδεια σε σύγκριση με αυτές που χρησιμοποιούνται από το προηγούμενους ελεγκτές.

Το ODL αποτελείται από τρεις βασικές εφαρμογές. Η πρώτη, που ονομάζεται Simple Forwarding, εφαρμόζει έναν πολύ βασικό μηχανισμό προώθησης που βασίζεται στο OpenFlow. Αυτή η εφαρμογή χρησιμοποιεί κίνηση ARP για τον εντοπισμό κεντρικών υπολογιστών που είναι συνδεδεμένοι στο δίκτυο. Η δεύτερη εφαρμογή παρέχει ένα σχήμα εξισορρόπησης φορτίου μεταξύ του back-end διακομιστών. Η εξισορρόπηση επιτυγχάνεται μέσω της αντιδραστικής εγκατάστασης κανόνων ροής χαρτογραφώντας τη διεύθυνση προέλευσης των πακέτων σε διαδρομές προς έναν από τους διαθέσιμους διακομιστές. Τέλος, η τρίτη εφαρμογή επιτρέπει σε έναν διαχειριστή να παρακολουθεί τα στατιστικά του δικτύου χρησιμοποιώντας μία web διεπαφή.

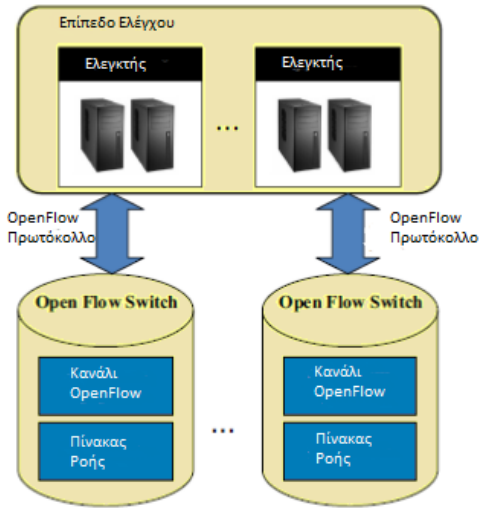
Ένα σημαντικό πλεονέκτημα του ODL σε σχέση με τους άλλους ελεγκτές είναι η υποστήριξη για κατανεμημένους ελεγκτές. Το ODL μπορεί να ρυθμιστεί ώστε να εκτελεί εξισορρόπηση φορτίου μεταξύ πολλαπλών ελεγκτών ή για χρήση δευτερεύοντος ελεγκτή ως ένα αντίγραφο ασφαλείας στο πρωτεύον. Υποστηρίζει επίσης multi-threading.

ΠΙΝΑΚΑΣ Ι
ΚΑΤΑΛΟΓΟΣ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΤΗΝ ΠΟΙΟΤΙΚΗ ΣΥΓΚΡΙΣΗ ΤΩΝ ΑΞΙΟΛΟΓΗΜΕΝΩΝ CONTROLLERS.

Controller	**NOX**	**POX**	**Beacon**	**Ryu**	**FloodLight**	**ODL**
Version	Classic	v0.5.0	v1.0.4	V4.30	v1.2	v0.9.2
Docs	2/5	3/5	1/5	5/5	4/5	3/5
GUI	3/5	3/5	5/5	3/5	3/5	4/5
Language	C++/Python	Python	Java	Python	Java	Java
Standard Applications	Yes	Yes	Yes	Yes	Yes	Yes
Distributed Controllers	No	No	No	No	No	Yes
Backup Controllers	No	No	No	No	No	Yes
Platforms	Linux	Linux, MacOS, Windows	Linux, MacOS, Windows	Linux	Linux	Linux, MacOS
Northbound APIs	REST	REST	-	REST	REST	REST
Southbound APIs	OpenFlow (1.0)	OpenFlow (1.0)	OpenFlow (1.0)	OpenFlow (1.0, 1.2-1.5) NETCONF	OpenFlow (1.0-1.4)	OpenFlow (1.0, 1.3), NETCONF
Other Protocols	-	Nicira Extensions	-	Nicira Extensions	-	SNBI, LACP, OVSDB
License	Apache 2.0	Apache 2.0	BSD v1.0	Apache 2.0	Apache 2.0	EPL v1.0
Multi-threading	No	No	Yes	Yes	Yes	Yes
Updates	None	Occasional	None	Frequent	Occasional	Frequent
TLS	No	No	No	Yes	Yes	Yes

2.6 OpenFlow

Το OpenFlow καθορίζεται από το Open Networking Foundation (ONF) ως το πρώτο πρότυπο διεπαφής μεταξύ των επικοινωνιών στο επίπεδο ελέγχου και υποδομών της SDN αρχιτεκτονικής. Αυτό παρέχει έναν τρόπο για να ελέγχει το switch χωρίς να απαιτείται από τους παρόχους να αποκαλύψουν οποιονδήποτε πηγαίο κώδικα των συσκευών τους. Με άλλα λόγια, το OpenFlow επιτρέπει την άμεση πρόσβαση της προώθησης των επιπέδων των συσκευών του δικτύου, όπως τα switches και τα routers, φυσικά και εικονικά. Για παράδειγμα, παρέχει πρόσβαση στον πίνακα ροής και κατασκευάζει switches με το πως να κατευθύνουν την κυκλοφορία του δικτύου. Σε αυτή την περίπτωση, οι διαχειριστές δικτύου μπορούν να αλλάξουν τις ροές για μια μικρή χρονική περίοδο. Σύμφωνα με τον (Jammal, 2014) υπάρχουν δύο τύποι switches βασισμένοι στο OpenFlow: το OpenFlow-only και το OpenFlow-hybrid. Το πρώτο μπορεί μόνο να υποστηρίξει λειτουργίες OpenFlow, ενώ το δεύτερο μπορεί να υποστηρίξει λειτουργίες OpenFlow και φυσιολογικά Ethernet switches.



Εικόνα 4 Βασικά στοιχεία και επικοινωνία του OpenFlow

Όπως βλέπουμε στο παραπάνω σχήμα, το OpenFlow αποτελείται κυρίως από τρία συστατικά: το OpenFlow switch,το OpenFlow channel και το OpenFlow controller.

- OpenFlow switch: Αυτά τα switch διαχειρίζονται από τους OpenFlow ελεγκτές σε ένα ασφαλές κανάλι χρησιμοποιώντας το πρωτόκολλο OpenFlow. Ένα switch αποτελείται συχνά από έναν ή περισσότερους πίνακες ροής που αποδίδουν πακέτα αναζήτησης και προώθησης. Συγκεκριμένα, ένας πίνακας ροής αποτελείται από μια λίστα καταχωρήσεων ροής ενώ κάθε καταχώριση περιέχει πεδία κεφαλίδας, μετρητές και ενέργειες. Τα πεδία κεφαλίδας συνηθίζεται να ταιριάζουν με τα πακέτα και περιέχουν πληροφορίες όπως το VLAN ID, πόρτες προέλευσης και προορισμού, διεύθυνση IP κ.ά. Οι μετρητές χρησιμοποιούνται κυρίως για τη διατήρηση στατιστικών για πακέτα όπως ο αριθμός των πακέτων, ο αριθμός των bytes και ούτω καθεξής. Οι ενέργειες δίνουν οδηγίες για τον τρόπο επεξεργασίας και αντιστοίχισης πακέτων σε ροή, καθώς επίσης και προώθηση σε μια δεδομένη θύρα, προώθηση σε έναν ελεγκτή και ρίψη του πακέτου.

- OpenFlow channel: Αυτό το κανάλι ενεργεί σαν μια διεπαφή που συνδέει OpenFlow switches και OpenFlow controllers. Μέσω αυτής της διεπαφής, ο ελεγκτής διαμορφώνει και διαχειρίζεται το switch, λαμβάνει συμβάντα από το switch και στέλνει πακέτα από το switch. Τρεις κύριοι τύποι μηνυμάτων μπορούν να σταλούν μέσω αυτού του καναλιού: ελεγκτής-προς-switch, ασύγχρονος και συμμετρικός.
  Τα μηνύματα ελεγκτή-προς-switch αποστέλλονται από τους ελεγκτές για να διαχειρίζονται και να ελέγχουν άμεσα την κατάσταση του switch. Τα ασύγχρονα μηνύματα αποστέλλονται από το switch για ενημέρωση του ελεγκτή σχετικά συμβάντα δικτύου και αλλαγές στην κατάσταση του switch. Τα συμμετρικά

μηνύματα μπορούν να ξεκινήσουν είτε από το switch είτε από τον ελεγκτή και στέλνονται χωρίς αίτημα.

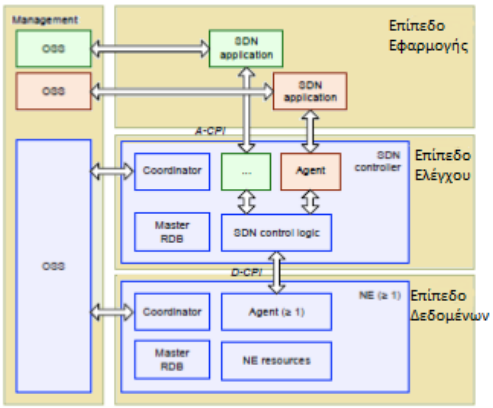
- OpenFlow controller: Αυτός ο κεντρικός ελεγκτής είναι υπεύθυνος για συντήρηση, διανομή και ενημέρωση πολιτικών και οδηγιών στις συσκευές δικτύου. Μπορεί να καθορίσει τον τρόπο χειρισμού πακέτων
χωρίς έγκυρες καταχωρήσεις ροής και μπορεί να διαχειριστεί τον πίνακα ροής του switch προσθέτοντας ή αφαιρώντας τις καταχωρήσεις ροής πάνω από το ασφαλές κανάλι. Επιπλέον, ένα OpenFlow switch μπορεί να δημιουργήσει σύνδεση και επικοινωνία με έναν ή περισσότερους ελεγκτές. Μία αρχιτεκτονική πολλαπλών ελεγκτών μπορεί να βελτιώσει την αξιοπιστία του δικτύου όταν ένα switch δεν ανταποκρίνεται. Όταν οι λειτουργίες του OpenFlow ξεκινούν, το switch πρέπει να συνδεθεί με όλους τους ρυθμισμένους ελεγκτές ταυτόχρονα, όπου σχετικά μηνύματα μπορούν να σταλούν μόνο στον αντίστοιχο διακόπτη.

Συνοψίζοντας, ένα OpenFlow switch μπορεί να περιλαμβάνει πολλαπλές ροές ενώ κάθε πίνακας ροής μπορεί να περιέχει πολλές καταχωρήσεις ροής. Σύμφωνα με έναν πίνακα ροής, το switch μπορεί να αναζητήσει τις καταχωρήσεις ροής και να κάνει αποφάσεις προώθησης για εισερχόμενα πακέτα. Για κάθε πακέτο, το switch στοχεύει να βρει μια ακριβής καταχώριση. Εάν εντοπιστεί μία που ταιριάζει, μπορούν να εκτελεστούν οι αντίστοιχες οδηγίες. Το πακέτο αντιστοιχεί στον πίνακα και πρέπει να επιλεγεί μόνο η καταχώριση ροής υψηλότερης προτεραιότητας που ταιριάζει με το πακέτο. Εάν υπάρχουν πολλές καταχωρήσεις ροής που ταιριάζουν με την ίδια υψηλότερη προτεραιότητα, η επιλεγμένη καταχώριση ροής είναι σαφώς απροσδιόριστη. Από την άλλη πλευρά, εάν ένα πακέτο δεν ταιριάζει με οποιαδήποτε καταχώριση ροής σε οποιονδήποτε πίνακα ροής, αυτό το πακέτο μπορεί να σταλεί στον ελεγκτή ή να απορριφθεί.

ΚΕΦΑΛΑΙΟ 3

3.1 Αρχές ασφάλειας

Υπάρχουν 8 αρχές ασφαλείας που ισχύουν για όλα τα πρωτόκολλα, τα στοιχεία και τις διεπαφές της αρχιτεκτονικής SDN στην Εικ 5. Σε αυτό το κεφάλαιο, αυτές οι αρχές θα συνδεθούν με τις απαιτήσεις ασφαλείας για τα πρωτόκολλα του SDN.



Εικόνα 5 Επισκόπηση του SDN

3.1.1 Αρχή 1: Ορίστε με σαφήνεια τις εξαρτήσεις ασφαλείας και τα όρια εμπιστοσύνης

Κατά τον καθορισμό ενός μηχανισμού ασφαλείας για δίκτυα SDN, οι εξαρτήσεις ασφαλείας μεταξύ διαφορετικών συστατικών πρέπει να αποσαφηνιστούν. Οι κυκλικές εξαρτήσεις πρέπει να αποφεύγονται. Ο καθαρός ορισμός των ορίων εμπιστοσύνης επιτρέπει την στοχευμένη ανάλυση κινδύνου και την αξιολόγηση ελέγχου ασφάλειας. Τα όρια εμπιστοσύνης πρέπει να καθορίζονται με βάση τους τομείς αλλαγής προνομίων, τη ροή πληροφοριών μέσα στους τομείς και την εξάρτηση από δεδομένα όπου δεν μπορούν να επαληθευτούν η εμπιστευτικότητα και η ακεραιότητα.

Τουλάχιστον, οποιαδήποτε εξωτερική εξάρτηση πρέπει να αντιπροσωπεύει ένα όριο εμπιστοσύνης, καθώς είναι λογικό να υποθέσουμε ότι μπορεί να προκύψουν επιθέσεις από εξωτερικά συστήματα. Η διεπαφή στα εξωτερικά περιβάλλοντα θα πρέπει επομένως να παρέχουν επαρκή λειτουργικότητα ασφαλείας για την πρόληψη ή τον μετριασμό εξωτερικών επιθέσεων. Τα εξωτερικά συστήματα θα πρέπει να έχουν περιορισμένη πρόσβαση μέσω μιας μεθόδου με ελάχιστο προνόμιο την μείωση του κινδύνου για το σύστημα. Επιπλέον, η διαχείριση ή ο περιορισμός εσωτερικών επιθέσεων θα πρέπει να ληφθούν υπόψη για την αποφυγή επιπτώσεων στο εξωτερικό περιβάλλον.

3.1.2 Αρχή 2: Διασφάλιση ισχυρής ταυτότητας

Η βάση για αποτελεσματική ασφάλεια είναι η δυνατότητα μοναδικής αναγνώρισης όλων των στοιχείων και των χρηστών ενός συστήματος και η επαλήθευση ταυτότητας με μια αξιόπιστη πηγή. Χωρίς ένα ισχυρό πλαίσιο ταυτότητας, η ικανότητα δημιουργίας αποτελεσματικών ελέγχων ταυτότητας, εξουσιοδότησης και λογιστικής θα είναι περιορισμένη.

Μια ισχυρή ταυτότητα πρέπει να έχει τις ακόλουθες ιδιότητες:

• Δυνατότητα διάκρισης του κατόχου του από άλλες οντότητες εντός προκαθορισμένου πεδίου.

• Δυνατότητα δημιουργίας, ενημέρωσης και ανάκλησης.

• Πρόληψη πλαστοπροσωπίας, κατά προτίμηση μέσω ισχυρών κρυπτογραφικών μηχανισμών.

Η ανάλυση της αρχιτεκτονικής SDN προσδιορίζει πολλά μέσα για στοιχεία εντός των ορίων εμπιστοσύνης του συστήματος να θέσουν σε κίνδυνο τη διαθεσιμότητα του λογικά συγκεντρωτικού ελέγχου. Ο ισχυρός έλεγχος ταυτότητας που βασίζεται στην εγγυημένη ταυτότητα είναι, επομένως, κρίσιμος για την ασφάλεια του συστήματος.

Υπάρχουν αρκετές περιπτώσεις χρήσης για τις οποίες στοιχεία εξωτερικά του συστήματος SDN (π.χ. εφαρμογές δικτύου) θα απαιτούν πρόσβαση σε ένα υποσύνολο πόρων συστήματος μέσω καθορισμένων διεπαφών. Σε τέτοιες περιπτώσεις, πρέπει να χρησιμοποιούνται μηχανισμοί ελέγχου πρόσβασης με διάφορα επίπεδα προνομίων για εξουσιοδότηση εξωτερικών μερών και έλεγχο ταυτότητας της πρόσβασής τους στο σύστημα, π.χ. έλεγχος πρόσβασης βάσει ρόλου. Κατά τη διάρκεια των επικοινωνιών, η ταυτότητα μιας συσκευής μπορεί να υποδεικνύεται ρητά από τις πληροφορίες (π.χ. αναγνωριστικά, διαπιστευτήρια, διευθύνσεις IP κ.λ.π.) που μεταφέρονται με τα πακέτα, ή σιωπηρά από το κλειδί που χρησιμοποιείται για την ασφάλεια των πακέτων.

3.1.3 Αρχή 3: Δημιουργία ασφάλειας βάσει ανοιχτών προτύπων

Η χρήση ανοικτών προτύπων μπορεί να αποφέρει οφέλη τόσο στη φορητότητα όσο και στη διαλειτουργικότητα. Όπου είναι δυνατόν, αποδεδειγμένα πρωτοκόλλα και μεθοδολογίες πρέπει να εφαρμοστούν για την ανάπτυξη ή την σχεδίασης νέων. Νέα πρωτόκολλα και αλγόριθμοι δημιουργούνται ως έσχατη λύση όταν οι υπάρχουσες απαιτήσεις δεν μπορούν να ικανοποιηθούν. Για παράδειγμα, απαιτείται προστασία επιπέδου μεταφοράς για την ασφάλεια επικοινωνίας του καναλιού OpenFlow και για την κυκλοφορία κεφαλίδας του Πρωτοκόλλου Ελέγχου Μεταφοράς (TCP) και για το ωφέλιμο φορτίο. Διάφορες τεχνικές βελτίωσης του TCP προηγουμένως έχουν προταθεί για το σκοπό αυτό και χρησιμοποιούνται ευρέως. Συνιστάται λοιπόν να υιοθετήσουν μια τέτοια υπάρχουσα τεχνική παρά να αναπτυχθεί μια νέα λύση επιπέδου μεταφοράς.

Η έννοια της επαναχρησιμοποίησης πρωτοκόλλου / αλγορίθμου είναι ιδιαίτερα σημαντική στην περίπτωση της ασφάλειας της λειτουργικότητας όπως η κρυπτογράφηση,

ο έλεγχος ταυτότητας και η ακεραιότητα, οι λύσεις για τις οποίες απαιτείται σημαντικός έλεγχος για να αποδείξουν τη δύναμή τους. Να σημειωθεί ότι η χρήση παλαιών πρωτοκόλλων ή αλγορίθμων (π.χ. MD5, Transport Layer Security (TLS) 1.0) έχουν αποδειχθεί ανασφαλείς και δεν συνιστάται πλέον από οργανισμούς τυποποίησης.

3.1.4 Αρχή 4: Προστασία της Τριάδας Ασφάλειας Πληροφοριών

Αν και οι έλεγχοι ασφαλείας από τη φύση τους πρέπει να αυξάνουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα (CIA) ενός συστήματος, η στάση ασφαλείας του ελέγχου πρέπει να αξιολογείται για την επιρροή του στη συνολική αρχιτεκτονική. Μια αποτελεσματική μέθοδος για την αξιολόγηση νέων ελέγχων είναι να προσδιοριστεί εάν η συνολική διαθεσιμότητα του συστήματος ενδέχεται να μειωθεί ως αποτέλεσμα. Ο έλεγχος δεν πρέπει να εισαγάγει νέες ευπάθειες ή εκμεταλλεύσεις.

Οποιαδήποτε μείωση της αποτελεσματικότητας του πυρήνα (CIA) πρέπει να εντοπιστεί και να μετριαστεί. Για παράδειγμα, η εισαγωγή ενός κεντρικού διακομιστή ασφαλείας στην αρχιτεκτονική SDN πρέπει να αξιολογηθεί προσεκτικά σε περίπτωση πιθανής ευπάθειας του διακομιστή σε επιθέσεις άρνησης υπηρεσίας (DoS) ενδέχεται να επηρεαστεί η διαθεσιμότητα του συστήματος. Εάν μπορεί, τότε πρέπει να βρεθεί μία λύση σε αυτό το πρόβλημα. Επιπλέον, οι έλεγχοι ασφαλείας πρέπει να κατασκευάζονται με τρόπο που να μην το κάνουν να υποβαθμίζει άσκοπα την απόδοση του συστήματος ή να επιβάλλει πρόσθετη πολυπλοκότητα του συστήματος που θα το κάνει πιθανώς να εισαγάγει νέες ευπάθειες ασφαλείας. Στην πράξη, η τελική λύση ενός ελέγχου ασφαλείας είναι να επηρεάζεται συνθετικά από τις απαιτήσεις ασφάλειας, το κόστος και τη δυνατότητα διαχείρισης.

3.1.5 Αρχή 5: Προστασία δεδομένων επιχειρησιακής αναφοράς

Η αποτελεσματικότητα ενός ελέγχου ασφαλείας επηρεάζεται άμεσα από την ακεραιότητα των δεδομένων αναφοράς (π.χ., διαπιστευτήρια και αριθμοί ακολουθίας), που αποτελεί βασική προϋπόθεση για τις λειτουργικές αποφάσεις. Οι λανθασμένες πληροφορίες μπορεί να οδηγήσουν σε απροσδόκητη συμπεριφορά του συστήματος που μπορεί να οδηγήσει σε απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Επιπλέον, η διαρροή ορισμένων ευαίσθητων δεδομένων αναφοράς όπως κρυπτογραφικά κλειδιά θα προκαλέσουν πιθανές παραβιάσεις του ελέγχου ασφαλείας. Τα επιχειρησιακά δεδομένα αναφοράς για όλους τους ελέγχους ασφαλείας πρέπει να ορίζονται με σαφήνεια και να προστατεύονται σε επίπεδο συνέχειας σύμφωνα με την πολιτική ασφάλειας και τις υποθέσεις ασφάλειας της αρχιτεκτονικής.

Τα δεδομένα αναφοράς πρέπει να δημιουργούνται, να υποβάλλονται σε επεξεργασία, να συντηρούνται και να μεταφέρονται με ασφάλεια στις αναμενόμενες λειτουργικές καταστάσεις, μεταβάσεις κατάστασης και κατά τη διάρκεια του κύκλου ζωής του συστήματος — δηλ. αρχικοποίηση συστήματος, την κανονική λειτουργία συστήματος, την κατάσταση αναμονής συστήματος, την κατάσταση ανακατεύθυνσης συστήματος και

την ανάκτηση του συστήματος και κατά τη διάρκεια των μεταβάσεων μεταξύ αυτών των καταστάσεων.

Για παράδειγμα, αρκετά πρωτόκολλα ασφαλείας χρησιμοποιούν μονοτονικά αυξανόμενους αριθμούς ακολουθίας για να εντοπίσουν επιθέσεις επανάληψης. Τυχόν ανεξέλεγκτη επαναφορά αυτών των αριθμών - ιδιαίτερα μετά από βλάβη του συστήματος - πρέπει να αποφεύγεται. Αυτό έχει ιδιαίτερη σημασία όταν η διαχείριση αυτοματοποιημένου κλειδιού δεν υποστηρίζεται.

3.1.6 Αρχή 6: Εξασφάλιση από προεπιλογή συστημάτων

Οι έλεγχοι ασφαλείας πρέπει να παρέχουν πολλαπλά επίπεδα ασφάλειας για να ικανοποιούν τις απαιτήσεις όλων των πιθανών περιπτώσεων χρήσης συστήματος. Αυτά τα επίπεδα ενδέχεται να διαφέρουν από μια κατάσταση στην οποία ένα στοιχείο ελέγχου είναι απενεργοποιημένο σε κατάσταση που μπορεί να ικανοποιήσει τις πιο αυστηρές απαιτήσεις ασφαλείας (π.χ., απόρριψη από προεπιλογή). Ανεξάρτητα από την προβλεπόμενη περίπτωση χρήσης, το σύστημα πρέπει να καθορίζει ένα ελάχιστο επίπεδο στο οποίο η πλειονότητα των πρωτογενών ελέγχων ασφαλείας είναι ενεργοποιημένοι από προεπιλογή. Εκτός από την ενεργοποίηση, αυτά τα στοιχεία ελέγχου πρέπει να είναι διαμορφωμένα με τρόπο που πληροί τα ελάχιστα κριτήρια για να διασφαλίσει ότι ο έλεγχος είναι αποτελεσματικός. Οι έλεγχοι ασφαλείας πρέπει να έχουν τη δυνατότητα να ρυθμιστούν εκ νέου ή ακόμη και να απενεργοποιηθούν, αλλά αυτό πρέπει να είναι συνειδητή απόφαση του ιδιοκτήτη / χειριστή του συστήματος.

Για παράδειγμα, κατά την εφαρμογή ελέγχου ταυτότητας, είναι σημαντικό να διασφαλιστεί ότι υπάρχει κάποια μορφή ελέγχου ταυτότητας από προεπιλογή. Για να γίνει ο έλεγχος αποτελεσματικός, ο έλεγχος ταυτότητας πρέπει να μην οριστεί στο μηδέν ή να απενεργοποιηθεί εντελώς. Ομοίως, οι βασικές ιδιότητες ασφαλείας (που θα μπορούσαν να είναι διάφορες σε διαφορετικές περιπτώσεις) ενός συστήματος θα πρέπει να διασφαλίζουν όλες τις ενημερώσεις, την ανάκτηση από αστοχίες, τις επανεκκινήσεις κ.λ.π.

3.1.7 Αρχή 7: Παροχή λογοδοσίας και ιχνηλασιμότητας

Όλοι οι έλεγχοι ασφαλείας πρέπει να είναι ελεγχόμενοι για την κατάσταση και τις ενέργειες που είναι κρίσιμες για την ασφάλεια του συστήματος. Τα καταγεγραμμένα δεδομένα πρέπει να περιέχουν επαρκείς πληροφορίες για ελεγκτικούς σκοπούς. Με βάση τα καταγεγραμμένα δεδομένα, ένας ελεγκτής θα πρέπει να είναι σε θέση όχι μόνο να προσδιορίζει μοναδικά την οντότητα για λογαριασμό της οποίας μια ενέργεια έχει πραγματοποιηθεί αλλά επίσης να ανακαλύπτει τη σχετική ακολουθία της δράσης. Η 2^{η} Αρχή βοηθάει στην ανίχνευση των ενεργειών σε συγκεκριμένες οντότητες.

Ωστόσο, είναι επίσης σημαντικό να διασφαλιστεί ότι τα ελεγχθέντα δεδομένα δεν πρέπει να περιέχουν περιττές πληροφορίες και οι ενέργειες του ελέγχου δεν θα οδηγήσουν σε παραβίαση της πολιτικής ασφάλειας.

Οι ιδιότητες ασφαλείας των καταγεγραμμένων δεδομένων πρέπει να προστατεύονται σε ένα επίπεδο συνέχειας σύμφωνα με την πολιτική ασφάλειας και τις παραδοχές κατά τη διάρκεια του κύκλου ζωής της. Βασικά, τα δεδομένα πρέπει να προστατεύονται κατά τη μη εξουσιοδοτημένη πρόσβαση και τις τροποποιήσεις.

3.1.8 Αρχή 8: Ιδιότητες ελεγχόμενων ελέγχων ασφαλείας

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

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

• Οι έλεγχοι ασφαλείας πρέπει να είναι κλιμακούμενοι και σχεδιασμένοι για να υποστηρίζουν εγκαταστάσεις από το μικρότερο σύστημα αναφοράς στη μεγαλύτερη ανάπτυξη χωρίς εισαγωγή αδικαιολόγητης περιπλοκότητας.

• Κατά την εισαγωγή νέων ελέγχων, η επιρροή της εφαρμογής της λύσης και του κύκλου ζωής διαχείρισης πρέπει να εξεταστεί. Οι νέες λειτουργίες ασφαλείας πρέπει να εισαχθούν μόνο με ελάχιστη πολυπλοκότητα στην εφαρμογή. Μια καλή εφαρμογή πρέπει να είναι επεκτάσιμη έτσι ώστε να μπορούν να εισαχθούν στο μέλλον πρόσθετες λειτουργίες ελέγχου ασφάλειας.

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

• Βεβαιωθείτε ότι τα στοιχεία ελέγχου είναι συμβατά προς τα πίσω ή παρέχετε μια διαδρομή αναβάθμισης που επιτρέπει τρέχοντες και παλαιούς ελέγχους για συνύπαρξη.

• Βεβαιωθείτε ότι τα στοιχεία ελέγχου είναι καλά τεκμηριωμένα και βασίζονται σε καλά καθορισμένα πρότυπα.

• Θα πρέπει πάντα να είναι δυνατή η ανάκληση και η τροποποίηση διαπιστευτηρίων ασφαλείας ως μέρος του κύκλος ζωής του συστήματος

• Όπου είναι δυνατόν, όλοι οι έλεγχοι ασφαλείας θα πρέπει να υποστηρίζουν αυτοματοποίηση για να διασφαλίζεται ότι τα στοιχεία ελέγχου εφαρμόζονται σωστά. Σε πολλές περιπτώσεις, οι χειροκίνητες διαδικασίες μπορεί να οδηγήσουν σε ακατάλληλη διαμόρφωση, η οποία μπορεί να μειώσει την αποτελεσματικότητα ενός ελέγχου.

• Η δυνατότητα παρακολούθησης, αντιμετώπισης προβλημάτων και εντοπισμού σφαλμάτων οποιουδήποτε συστήματος είναι θεμελιώδους σημασίας στην επιτυχημένη υιοθέτηση.

3.2 Απειλές στο SDN και αντίμετρα

Σε αυτήν την ενότητα, θα χρησιμοποιήσουμε το παραδοσιακό μοντέλο απειλών STRIDE για την ανάλυση του είδους των απειλών που μπορεί να εκτεθεί το δίκτυο SDN. Ενώ αυτό το μοντέλο προτείνεται με βάση τα παραδοσιακά δίκτυα, οι απειλές που περιγράφονται παρακάτω ισχύουν για τα δίκτυα γενικά. Εναλλακτικά, οι απειλές στο SDN μπορούν να ταξινομηθούν με βάση τα κύρια λειτουργικά συστατικά του, που περιγράφηκαν νωρίτερα και τον τύπο και την φύση των επιθέσεων που μπορεί κάθε συστατικό να υποβληθεί. Οι επιθέσεις στο SDN μπορούν επίσης να ταξινομηθούν βάσει του τύπου περιουσιακών στοιχείων ή πόρων που μπορεί να έχει ένα τυπικό SDN. Για παράδειγμα, οι επιθέσεις μπορούν να εστιαστούν στους πίνακες ροής των switches όπου αυτοί περιλαμβάνουν πληροφορίες που σχετίζονται με την διαχείριση δικτύου, την δρομολόγηση και τον έλεγχο πρόσβασης. Οι επιθέσεις μπορούν επίσης να εστιαστούν στον ελεγκτή ως κεντρική τοποθεσία για διαχείριση και έλεγχο. Το κανάλι μεταξύ του ελεγκτή και των switches είναι μια άλλη σημαντική στοχευμένη επίθεση όπου ένα τέτοιο κανάλι περιλαμβάνει σημαντικά μηνύματα που μπορεί να υποκλαπούν. Στο ανώτερο επίπεδο, ο ελεγκτής επικοινωνεί με εφαρμογές υψηλού επιπέδου χρησιμοποιώντας μια τυπική διεπαφή (π.χ. REST). Μια τέτοια διεπαφή μπορεί επίσης να επιτεθεί για να ξεγελάσει τον ελεγκτή, επιτρέποντας έτσι την σύνδεση κακόβουλων εφαρμογών στο δίκτυο και την αλληλεπίδραση με αυτόν, το δίκτυο και την κυκλοφορία του.

3.2.1 Πλαστογράφηση (Spoofing)

Η πλαστογράφηση αναφέρεται σε μια διαδικασία όπου οι πληροφορίες δικτύου (π.χ. IP, MAC, ARP, κ.λπ.) πλαστογραφούνται σκόπιμα για να κρύψουν την πραγματική ταυτότητα του δημιουργού της κυκλοφορίας ή του εισβολέα. Για παράδειγμα, οι χρήστες μπορούν να χρησιμοποιούν πλαστογραφημένες διευθύνσεις IP για πρόσβαση σε πόρους δικτύου. Η πλαστογράφηση είναι συχνά μέρος μιας μεγαλύτερης επίθεσης, όπως η πλημμύρα SYN, Smurf και η ενίσχυση DNS. Πλαστογραφημένες διευθύνσεις μπορεί επίσης να είναι μέρος ενός botnet ή ενός δικτύου ζόμπι για την εκκίνηση Distributed DoS (DDoS) επιθέσεων. Πρόσφατες πλαστογραφημένες απειλές στο SDN περιλαμβάνουν κυρίως πλαστογράφηση στο Πρωτόκολλο Μετατροπής Διευθύνσεων (ARP) και πλαστογράφηση IP.

3.2.1.1 Πλαστογράφηση ARP

Το ARP spoofing περιλαμβάνει τη σύνδεση μιας διεύθυνσης MAC επιτιθέμενου με μία νόμιμη διεύθυνση IP. Ο αρχικός σκοπός του ARP είναι η μετατροπή διευθύνσεων IP σε MAC. Η επίθεση ARP spoofing μπορεί να προκαλέσει παραβίαση της κυκλοφορίας από τον αρχικό προβλεπόμενο δέκτη και ως αποτέλεσμα, ένας νόμιμος χρήστης ή κεντρικός υπολογιστής να αποκλείεται από το δίκτυο. Οι πίνακες αντιστοίχισης IP σε MAC μπορούν να χρησιμοποιηθούν για την ανίχνευση της ARP πλαστογράφησης.

Ο (Matias, 2012) πρότεινε μία μονάδα αντιστοίχισης ανάλυσης διευθύνσεων (ARM) στον ελεγκτή που παρακολουθεί τις διευθύνσεις MAC από εξουσιοδοτημένους

χρήστες ή κεντρικούς υπολογιστές. Ο ελεγκτής τότε συμβουλεύεται αυτήν την μονάδα ARP και απορρίπτει τις απαντήσεις ARP που δεν επαληθεύονται από τη μονάδα ARP. Στο OpenFlow, ο ιός ARP μπορεί να εμφανιστεί μεταξύ του ελεγκτή και των switches, εάν η προαιρετική SSL κρυπτογράφηση δεν χρησιμοποιείται. Ο ιός από την προσωρινή μνήμη ARP εμφανίζεται όταν ένας εισβολέας βρίσκεται στο ίδιο υποδίκτυο του δικτύου θυμάτων (π.χ. εσωτερικές επιθέσεις). Ο επιτιθέμενος μπορεί να χρησιμοποιήσει σαρωτές για να ακούσουν την κυκλοφορία του δικτύου μεταξύ των στοιχείων του δικτύου. Ο Al-Shabibi, 2014 έχει αναπτύξει μία εφαρμογή κατά του ιού ARP των switches στον ελεγκτή POX OpenFlow. Οι επιθέσεις ARP spoofing μπορούν να αντιμετωπιστούν με πληροφορίες επιπέδου πακέτου. Ο (Zaalouk Adel, 2014) διαίρεσε τις μεθόδους ανίχνευσης επιθέσεων σε μεθόδους υψηλής και χαμηλής ανάλυσης με βάση το ποσό των πληροφοριών που του δόθηκαν ως εισαγωγή. Οι επιθέσεις χαμηλής ανάλυσης απαιτούν πληροφορίες κατά τη ροή, όχι σε επίπεδο πακέτου. Οι λεπτομέρειες επιπέδου πακέτου απαιτούνται μόνο σε επιθέσεις επιπέδου υψηλής ανάλυσης. Για παράδειγμα, επιθέσεις όπως DoS και ενίσχυση του διακομιστή DNS μπορούν να αντιμετωπιστούν με πληροφορίες στο επίπεδο ροής λεπτομερειών. Από την άλλη πλευρά, το ARP spoofing και οι επιθέσεις ιού cache απαιτούν πληροφορίες στο επίπεδο πακέτου.

3.2.1.2 Πλαστογράφηση IP

Το IP spoofing χρησιμοποιείται συνήθως ως άνοιγμα σε άλλους τύπους επιθέσεων ασφαλείας, όπως η παραβίαση ή η ενίσχυση DNS. Ένας DNS είναι ένας κατάλογος που συσχετίζει τις διευθύνσεις IP με τον τομέα ονομάτων. Για να ανακατευθύνει την κυκλοφορία σε παράνομους ιστότοπους, ένας εισβολέας μπορεί να παραποιήσει DNS κατάλογους. Αυτό μπορεί επίσης να είναι μέρος μίας μεγάλης πλημμύρας ή επιθέσεων worm. Αυτό που όλες οι μέθοδοι πλαστογράφησης έχουν κοινό είναι ότι προσπαθούν να ανακατευθύνουν την επισκεψιμότητα παράνομων χρηστών. Μπορούν επίσης να θεωρηθούν ότι επιτυγχάνουν επιθέσεις Man in the Middle (MiM). Η πλαστογράφηση μπορεί να μετριαστεί από ένα κατάλληλο σχήμα ελέγχου ταυτότητας. Ο ισχυρός κωδικός πρόσβασης και οι μέθοδοι κρυπτογράφησης πρέπει να επιβάλλονται για να αποφεύγεται η μη εξουσιοδότηση εισχώρηση.

Έχει συζητηθεί σε υπάρχουσα έρευνα η απόκρυψη των ταυτοτήτων των κεντρικών υπολογιστών για να προστατευτούν από διάφορους τύπους επιθέσεων, συμπεριλαμβανομένων την πλαστογράφηση. Αυτή είναι μια μορφή δυναμικής διαμόρφωσης δικτύου όπου οι πληροφορίες δικτύου αλλάζουν συχνά ή είναι κρυμμένες από εξωτερικά. Οι πληροφορίες δικτύου δεν περιλαμβάνουν μόνο Διευθύνσεις IP ή MAC, αλλά και πίνακες τοπολογίας και δρομολόγησης. Σε μια προσπάθεια απόκρυψης των ταυτοτήτων των τελικών χρηστών και προστασίας τους από σαρωτές και πλαστογραφίες, οι (Jafarian Jafar Haadi, 2012) πρότειναν μια κινούμενη αμυντική προσέγγιση. Οι τελικοί κεντρικοί υπολογιστές και οι ταυτότητές τους πρέπει να αλλάζουν συνεχώς και τυχαία για να αποφύγουν να στοχεύονται από αντιπάλους. Το OpenFlow εκχωρεί εικονικές Διευθύνσεις IP σε τερματικούς κεντρικούς υπολογιστές που μπορούν να αντιστοιχιστούν σε πραγματικούς ή σε φυσικές διευθύνσεις IP.

Στο SDN, ο ελεγκτής πρέπει να έχει μια μέθοδο για να απομονώνει τις πληροφορίες του τοπικού του δικτύου από τα εξωτερικά δίκτυα. Όμοια με το NAT, ο ελεγκτής μπορεί να έχει πίνακες για να μετατρέψει την εξωτερική σε εσωτερική διεύθυνση. Στην πραγματικότητα, το OpenFlow μπορεί να το κάνει αυτό εγγενώς όπως μπορούν οι συσκευές OpenFlow να ξαναγράψουν τα πεδία κεφαλίδας των πακέτων που θα τα δημιουργήσουν να εμφανίζονται ως προερχόμενα από εξωτερικές διευθύνσεις. Αυτή η μετάφραση NAT πρέπει να επικοινωνείται με πολλά middleboxes ενώ ταυτόχρονα να είναι κρυμμένο από εξωτερικά. Τα δίκτυα OpenFlow και άλλες μέθοδοι οπτικοποίησης δικτύου επιτρέπουν στους χρήστες να διαιρούν το δίκτυο σε κομμάτια και κάνουν ροές για να συμπεριφέρονται διαφορετικά στα διαφορετικά κομμάτια ανεξάρτητα αν θα έχουν τις ίδιες πραγματικές IP διευθύνσεις ή όχι. Για παράδειγμα, μπορεί να απαιτείται για επιχειρηματικούς σκοπούς να κατευθύνουν ορισμένες συγκεκριμένες ροές σε έλεγχο ασφαλείας (π.χ. τείχος προστασίας). Εναλλακτικά μπορεί να απαιτείται η κατανομή περισσότερου εύρους ζώνης και πόρων σε κάποια συγκεκριμένη κίνηση.

Ενδέχεται να προκύψουν πλαστογραφημένες διευθύνσεις IP μέσα στο δίκτυο. Με βάση τη φύση της πλαστογράφησης της διεύθυνσης IP, η επικύρωση της πηγής διεύθυνσης από το δίκτυο μπορεί να είναι δύσκολη να ανιχνευθεί. Ο (Xiao Peiyao, 2013) επέκτεινε μια προηγούμενη έρευνα σχετικά με το OpenRouter. Σε γενικές γραμμές, μια προσέγγιση SDN μπορεί να μην χρειάζεται σε έναν αποκλειστικό δρομολογητή όπου περιλαμβάνονται οι λειτουργίες δρομολόγησης του OpenFlow Ελεγκτή και των switches.

3.2.2 Παραβίαση (Tampering)

Η παραβίαση είναι η σκόπιμη και μη εξουσιοδοτημένη τροποποίηση ή καταστροφή πληροφοριών δικτύου, όπως η τοπολογία, οι ροές στους πίνακες ροής, οι πολιτικές και οι λίστες πρόσβασης. Για παράδειγμα, ένας εισβολέας μπορεί να προσπαθήσει να εισάγει κανόνες ροής που θα προκαλέσουν κακή συμπεριφορά του δικτύου. Μπορεί να εισάγουν κανόνες ροής ή κανόνες τείχους προστασίας που θα το κάνουν να αρνείται νόμιμους κεντρικούς υπολογιστές ή να επιτρέπει παράνομους κεντρικούς υπολογιστές. Οι εισβολείς μπορεί επίσης να προσπαθήσουν να παραβιάσουν τις πληροφορίες τοπολογίας και κατά συνέπεια να προκαλέσουν εισβολή σε κάποια κίνηση. Στην κατανομή του ελεγκτή SDN, διαφορετικοί ελεγκτές επικοινωνούν με σημαντικές πληροφορίες. Είναι πολύ σημαντικό να διασφαλίσει αυτό το κανάλι επικοινωνίας από το να υποκλαπεί ή να παραβιαστεί

Οι απειλές ασφαλείας ενδέχεται να στοχεύουν τείχη προστασίας ή κανόνες πινάκων ροής. Οι (Porras Phillip, 2012) περιέγραψαν το πρόβλημα ασφάλειας της δυναμικής του τούνελ ροής που σχετίζεται με συγκρούσεις στην ερμηνεία των κανόνων ροής. Αυτό το πρόβλημα παρουσιάζεται αφού οι κανόνες αξιολογούνται ένας προς ένας. Ένας εισβολέας μπορεί να προσπαθήσει να ενορχηστρώσει περισσότερους από έναν κανόνες όπου όλες αυτές οι ροές παραβιάζουν το τείχος προστασίας, ενώ από την άλλη πλευρά, μία ροή από μόνη της δεν παραβιάζει το τείχος προστασίας. Στην προτεινόμενη λύση τους, προσπάθησαν να ελέγξουν τη σύγκρουση μεταξύ κανόνων ροής και τείχους

προστασίας βάσει όλων των πιθανών συνδυασμών των εισερχόμενων ροών. Ωστόσο, αυτό μπορεί να μην είναι επεκτάσιμο ή εφαρμόσιμο σε σύνθετα σενάρια.

Ως διαχείριση της κυκλοφορίας βάσει ροής, το SDN μπορεί να συμβάλει στην πρόληψη ακούσιας παραβίαση της κυκλοφορίας. Τα πακέτα μπορούν να ελεγχθούν πριν προχωρήσουν στον προορισμό τους με ακέραια τα χαρακτηριστικά τους. Τα αποτελέσματα επικύρωσης μπορούν να πραγματοποιηθούν με την κίνηση που πρέπει να ελεγχθεί στο σημείο προορισμού. Η παραβίαση μπορεί να μετριαστεί με τη διανομή του ελέγχου και της παρακολούθησης σε πολλά σημεία του δικτύου. Εάν ένα σημείο δέχεται επίθεση, τα υπόλοιπα σημεία μπορούν να χρησιμοποιηθούν για να εντοπίσουν και να διορθώσουν τέτοιες παραβιάσεις.

Για προστασία από την παραβίαση, ο ελεγκτής πρέπει να διαχειρίζεται και να ελέγχει τακτικά τις μεθόδους κρυπτογράφησης και τις νόμιμες συνδέσεις. Οι κύριοι περιορισμοί κρυπτογράφησης του επιπέδου ασφάλειας μεταφοράς (TLS) που χρησιμοποιούνται στο OpenFlow είναι ότι πρώτα είναι προαιρετικοί για χρήση ή επιβολή από τους χρήστες και το δεύτερο είναι ότι πολλοί πραγματικοί ελεγκτές δεν το εφαρμόζουν ούτε το υιοθετούν. Άλλο ένα σχετικό ζήτημα είναι οι τρόποι αστοχίας του ελεγκτή. Είναι δυνατόν να τεθεί σε κίνδυνο η ακεραιότητα ή η εμπιστευτικότητα όταν ωθούνται ο ελεγκτής ή τα switches σε έναν από αυτούς τους τρόπους αποτυχίας.

Σε εικονικά περιβάλλοντα, μοιράζονται διαφορετικά λογικά δίκτυα τους ίδιους φυσικούς πόρους ή τους πόρους δικτύου. Ως αποτέλεσμα, υπάρχει μία σοβαρή ανησυχία για το επίπεδο ορθότητας και ακεραιότητας όχι μόνο από εξωτερική επεξεργασία ή παραβίαση αλλά και από εσωτερικές τροποποιήσεις. Τα υπάρχοντα πειράματα έδειξαν ότι κομμάτια ή εικονικές μηχανές (VMs) στον ίδιο μισθωτή ή στο κέντρο δεδομένων cloud έχουν μία πιθανότητα το ένα VM να έχει πρόσβαση σε πόρους από το άλλο VM που μοιράζονται τους ίδιους φυσικούς πόρους. Ίδια ανησυχία μπορεί επίσης να είναι ότι οι εικονικοί διαχωρισμένοι πόροι μοιράζονται τους ίδιους φυσικούς πόρους (π.χ. διαφορετικούς πίνακες δοκιμών πειραμάτων, διαφορετικούς χρήστες ασύρματου ή οικιακού δικτύου κ.λπ.).

3.2.3 Απόρριψη (Repudiation)

«Η απόρριψη είναι η άρνηση μιας από τις οντότητες που εμπλέκονται σε μία επικοινωνία που συμμετέχει σε ολόκληρη ή ένα μέρος της επικοινωνίας» (ISO,1989). Η μη απόρριψη, που θεωρείται ως νομική παρά τεχνική έννοια, προσπαθεί να βεβαιώσει ότι δεν υπάρχει τέτοια άρνηση. Ο δέκτης χρειάζεται να επιβεβαιώσει ότι τα πακέτα αποστέλλονται από τον πραγματικό αποστολέα που περιλαμβάνεται στην κεφαλίδα του πακέτου και ο αποστολέας πρέπει να επιβεβαιώσει ότι τα πακέτα που αποστέλλονται στον πραγματικό δέκτη περιλαμβάνουν την κεφαλίδα του πακέτου. Η μη απόρριψη

σχετίζεται συχνά με τη λογοδοσία, που αφορά την υποχρέωση λογοδοσίας ατόμων ή οντοτήτων ή ευθύνη για τις πράξεις τους.

3.2.3.1 Επαλήθευση μη απόρριψης

Στον τρέχοντα ιστό, το ηλεκτρονικό εμπόριο, κ.λπ. με έμμεσους ή απομακρυσμένους τύπους επικοινωνίας, αυτή η απόρριψη ή η άρνηση από ένα μέρος που ήταν μέρος αυτής της επικοινωνίας μπορεί να προκληθεί συνήθως ως αποτέλεσμα επιθέσεων Man in the Middle (MiM), στις οποίες ένας εισβολέας βρίσκεται μεταξύ των δύο πλευρών και ενώ είναι με την μία παριστάνει ότι είναι στην άλλη. Έτσι, η κρυπτογράφηση μπορεί να είναι αποτελεσματικό μέτρο MiM και κατά συνέπεια να απορριφθεί. Με βάση αυτήν την υπόθεση, περιγράφουμε μεθόδους που βασίζονται σε κρυπτογράφηση σε αυτήν την ενότητα για επαλήθευση μη απόρριψης.

Οι μέθοδοι κρυπτογράφησης χρησιμοποιούνται για την επαλήθευση της επικοινωνίας, ότι τα μηνύματα πιστοποιήθηκαν από τις πηγές προέλευσης και δεν έχουν παραβιαστεί σε όλο το δίκτυο. Η έρευνα έχει δείξει ότι προβλήματα ασφαλείας με την κρυπτογράφηση στα πρωτόκολλα Secure Socket Layer / Transport Layer Security (SSL / TLS) χρησιμοποιούνται στον αλγόριθμο OpenFlow για την επικοινωνία μεταξύ ελεγκτή και switches. Ο (Namal Suneth, 2013) πρότεινε για εναλλακτική λύση σχήματα κρυπτογράφησης, το HIP-BEXv1 και το HIP-EEX που προσφέρουν καλύτερες δυνατότητες ασφαλείας για μη απόρριψη, για DoS και για MiM απειλές.

Επαληθεύσεις τρίτων (π.χ. Κρυπτογράφηση δημόσιου κλειδιού PKE και ψηφιακά πιστοποιητικά) μπορούν να χρησιμοποιηθούν για την εξάλειψη της απόρριψης. Επί του παρόντος, ένας τέτοιος μηχανισμός και αρχιτεκτονική ασφάλειας (δηλ. PKE) χρησιμοποιείται ευρέως σε συστήματα ηλεκτρονικού εμπορίου και επιχειρηματικές συναλλαγές. Οι συγχωνεύσεις μεταφοράς μηνυμάτων χρησιμοποιούνται επίσης για την παροχή ψηφιακών αποδείξεων σχετικά με ένα μήνυμα. Η αλυσίδα σημάτων μπορεί να χρησιμοποιείται επίσης για την παροχή μη απόρριψης. Για παράδειγμα, ένας έλεγχος στο σύστημα θα πρέπει να περιλαμβάνει τις διαδρομές ή την ακολουθία των βημάτων που ένα μήνυμα ή ένα πακέτο πέρασε μεταξύ του αρχικού αποστολέα και του τελικού δέκτη.

Σωστές μέθοδοι ελέγχου και καταγραφής για όλους τους τύπους δραστηριοτήτων που εμφανίζονται στους πίνακες ροής μπορούν να βοηθήσουν στη μη απόρριψη. Αυτά μπορούν να παρασχεθούν ως αποδείξεις σχετικά με τις δραστηριότητες της κυκλοφορίας. Ωστόσο, η αντιστάθμιση μεταξύ της απόδοσης και της καταγραφής θα πρέπει να τοποθετηθεί για να επιλέξει σωστά τι ακριβώς θα ελεγχθεί. Ακόμη και οι ίδιες οι μέθοδοι καταγραφής και ελέγχου μπορούν να παραβιαστούν από κάποιες επιθέσεις ασφαλείας. Ο (Porras Phillip, 2012) προτείνει το Fort-Nox, ένα σύστημα ελέγχου ταυτότητας βάσει ροής, για την παροχή μιας ασφαλούς διαδρομής ελέγχου για εντολές κανόνων ροής, διενέξεις κανόνων και επίλυση αποτελεσμάτων. Δεν είναι ξεκάθαρο ωστόσο, τι πληροφορίες περιλαμβάνονται στον έλεγχο ή πώς μπορεί να χειριστούν οι συγκρούσεις. Εκτός από τα χαρακτηριστικά ροής που περιγράφονται στις προδιαγραφές του OpenFlow, για τον έλεγχο ενδέχεται να χρειαστεί να γνωρίζουμε άλλες πληροφορίες

όπως αναγνωριστικό εφαρμογής, επίπεδο προνομίων, χρόνος ροής και ημερομηνία. Εάν προκύψει παραβίαση ασφαλείας, αυτές οι πληροφορίες είναι χρήσιμες για διερεύνηση συμβάντων.

Ο (Andersen David G, 2008) πρότεινε Πρωτόκολλο Υπεύθυνου Διαδικτύου (AIP) ως αντικατάσταση του Internet Πρωτοκόλλου IP. Ο στόχος ήταν να προστεθούν περισσότερες πληροφορίες εκτός από αυτές που συνήθως υπάρχουν σε κεφαλίδες πακέτων που μπορούν να αναγνωρίσουν μοναδικά η εφαρμογή του αποστολέα, ο χρήστης, το μηχάνημα κ.λπ. Ο (Bifulco Roberto, 2014) πρότεινε την αναγνώριση κεντρικών υπολογιστών βάσει τοποθεσίας εκτός από τη διεύθυνση IP που σχετίζεται με το κοινό κλειδί κρυπτογράφησης του χρήστη ή του κεντρικού υπολογιστή.

Επαλήθευση μη απόρριψης σε πολύ ευέλικτα και δυναμικά δίκτυα μπορεί να είναι δύσκολο να επιτευχθούν. Υπάρχουν πολλές περιπτώσεις SDN χρήσης (π.χ. Φέρτε τη δική σας συσκευή (BYOD), δίκτυα πανεπιστημιουπόλεων, δίκτυα peer to peer) που απαιτούν ποιότητες μη απόρριψης όπου τα τρέχοντα δίκτυα δύσκολα μπορούν να παρέχουν (Feamster Nick, 2004). Σε αυτά τα δίκτυα, οι χρήστες και οι προτιμήσεις δικτύου τους ποικίλλουν συνεχώς. Ο χειρισμός της μη απόρριψης είναι ασήμαντος δεδομένου του μεγάλου αριθμού χρηστών και την ευελιξία του δικτύου. Ο προγραμματισμός του SDN και η ικανότητά του να ορίζει χρήστες ή κεντρικούς υπολογιστές βάσει ροών μπορεί να είναι σημαντικά εργαλεία για την επίτευξη αυτών των ποιοτικών χαρακτηριστικών και περισσότερο γερά.

3.2.3.2 Ευθύνη (Accountability)

Η τρέχουσα αρχιτεκτονική SDN καθιστά υπεύθυνο κάθε ελεγκτή για τα δικά του switches. Ανταλλαγή επικοινωνίας στους τομείς μεταξύ των διαφορετικών ελεγκτών δεν υποστηρίζεται. Πακέτα που σχετίζονται με switches σε άλλα δίκτυα ελεγκτών πρόκειται να εγκαταλειφθούν από τον τοπικό ελεγκτή. Ωστόσο, υπάρχουν πολλές περιπτώσεις χρήσης που δικαιολογούν την ανάγκη ανταλλαγής πληροφοριών από διαφορετικούς ελεγκτές ειδικά όταν ένα δίκτυο ελεγκτή δεν είναι μία πρακτική σχεδίαση δικτύου για τα περισσότερα δίκτυα παραγωγής. Διαφορετικοί ελεγκτές πρέπει να ανταλλάσσουν πληροφορίες μέσω καλά καθορισμένων διεπαφών έτσι ώστε να μην παρεμβαίνουν ο ένας τον άλλον ή προκαλούν προβλήματα ασφαλείας.

Ο (Karame, 2013)συζήτησε θέματα λογοδοσίας που σχετίζονται με ποιότητα υπηρεσιών (QoS). Οι συνεργάτες επικοινωνίας πρέπει να ανταλλάσσουν πληροφορίες σχετίζεται με: τον χρόνο απόκρισης, το ποσοστό σφάλματος κ.λπ. Αυτό είναι ένα από τις τρέχουσες σοβαρές προκλήσεις στο υπολογιστικό νέφος που σχετίζονται με επίπεδο συμφωνίας υπηρεσίας (SLA). Οι επιθέσεις στο δίκτυο μπορεί να έχουν άμεσο αντίκτυπο στις μετρήσεις δικτύου όπου ενδέχεται να καθυστερήσουν τον χρόνο απόκρισης ή να προκαλέσουν την αποστολή ορισμένης κίνησης εγκαίρως ή σωστά. Ο (Karame, 2013) πρότεινε μια προσέγγιση ασφάλειας βασισμένη στο Open-Flow που μπορεί να χειριστεί ορισμένες από τις ανησυχίες σε αυτή την συγκεκριμένη άποψη.

Η ευθύνη μπορεί να αμφισβητηθεί από πολλά στοιχεία του δικτύου, συμπεριλαμβανομένων των ελέγχων ασφαλείας. Οι έλεγχοι ασφαλείας στις περισσότερες περιπτώσεις λειτουργούν ως εμπόδια που περιορίζουν την ικανότητα ελέγχου της κυκλοφορίας των πόρων. Για παράδειγμα, τα συστήματα NAT ή μεσολάβησης κρύβουν την ταυτότητα εσωτερικών κεντρικών υπολογιστών όπου ένα τείχος προστασίας ενδέχεται να μην είναι σε θέση να γνωρίζει την πηγή κίνησης ή την πραγματική διεύθυνση IP του κεντρικού υπολογιστή. Αυτό συμβαίνει επειδή υπάρχει εσωτερική αντιστοίχιση στο NAT / διακομιστής μεσολάβησης μεταξύ εσωτερικών σε εξωτερικές διευθύνσεις IP. Σε αυτό το πεδίο, ο (Fayaz Seyed, 2013) πρότεινε τα FlowTags ως ένα σύστημα που επιτρέπει την ασφάλεια middleboxes για την αναγνώριση εφαρμογών. Οι πληροφορίες προσθήκης ετικετών πρέπει να ενσωματωθούν με τις πληροφορίες ροής. Διαφορετικές εφαρμογές που δημιουργούν ροές αναμένεται να προσθέσουν αυτήν την ετικέτα ροής πληροφοριών που βασίζεται σε ένα ομοιόμορφο πρότυπο (δηλαδή μέσω Μονάδας ελεγκτή FlowTag). Η μονάδα FlowTag πρέπει να χειρίζεται την επανεγγραφή των κεφαλίδων των πακέτων για να συμπεριλάβει πληροφορίες FlowTag από το αρχικό middlebox.

3.2.4 Γνωστοποίηση πληροφοριών (Information disclosure)

Οι επιθέσεις γνωστοποίησης πληροφοριών δεν έχουν καμία άμεση πρόθεση να καταστρέψουν ή να διαταράξουν το δίκτυο αλλά να κατασκοπεύσουν τις πληροφορίες του. Επιπρόσθετα με τις ευαίσθητες πληροφορίες που οι επιτιθέμενοι προσπαθούν να πάρουν, αρχικά θα προσπαθήσουν να κατασκοπεύσουν πληροφορίες δικτύου, όπως η τοπολογία, τα χαρακτηριστικά των κόμβων ή τα στοιχεία επικοινωνίας μεταξύ των κόμβων. Οι επιπτώσεις της SDN αρχιτεκτονικής στη σάρωση των επιθέσεων μπορούν να αναμειχθούν. Ο ελεγκτής είναι μια κεντρική τοποθεσία για τον έλεγχο όλων των switches του δικτύου. Όντας ικανός να εισβάλει στον ελεγκτή, ο εισβολέας μπορεί να έχει μια τεράστια πρόσβαση στο δίκτυο. Από την άλλη πλευρά, τα δεδομένα απομονώνονται από τον ελεγκτή, σε αντίθεση με τα παραδοσιακά switches όπου ο έλεγχος είναι συνδεδεμένος με τα δεδομένα μέσα στο switch. Στο SDN, υπάρχουν κανόνες ροής στους πίνακες ροής των switches. Εάν οι εισβολείς επιτύχουν να αποκτήσουν άμεση πρόσβαση στα switches, μπορούν να παραβλέψουν τους κανόνες ροής και προκαλούν την κυκλοφορία να μεταβεί σε λάθος προορισμούς. Εάν καταφέρουν να αποσυνδέσουν ένα switch από την επικοινωνία με τον ελεγκτή, μπορούν να αναλάβουν τον έλεγχο και να προκαλέσουν σημαντική ανακατεύθυνση της κυκλοφορίας. Αν μπορούσαν να υποκλέψουν την κυκλοφορία από έναν νόμιμο υπολογιστή, μπορούν να εμποδίσουν τον υπολογιστή και να ενταχθούν στο δίκτυο ως κατάσκοποι. Η MiM επίθεση είναι μια επίθεση γνωστοποίησης πληροφοριών που στοχεύει τις πληροφορίες κατά τη μεταφορά και όχι στο χώρο τους. Οι επιθέσεις MiM θεωρούνται σήμερα σημαντικά πιθανές στην τρέχουσα αρχιτεκτονική OpenFlow (Benton, 2013). Το τρέχον κρυπτογραφημένο σχήμα στην OpenFlow επικοινωνία, TLS, είναι προαιρετικό. Επιπλέον, η επικοινωνία στη βόρεια διεπαφή με τον ελεγκτή δεν έχει ακόμη τυποποιηθεί. Πρόσθετες εφαρμογές με πιθανές ευπάθειες μπορούν να χρησιμοποιηθούν για την εκκίνηση των επιθέσεων MiM και για πρόσβαση στους πόρους του ελεγκτή.

3.2.4.1 Σάρωση αντιμέτρων

Οι μέθοδοι σάρωσης και τα εργαλεία χρησιμοποιούνται συχνά στα αρχικά βήματα των επιθέσεων αποκάλυψης πληροφοριών. Οι σαρωτές δικτύου αναζητούν μέσω του δικτύου πιθανή διαρροή πληροφοριών και ευπάθειες.

Οι μέθοδοι κρυπτογράφησης μπορούν να χρησιμοποιηθούν για την αντιμετώπιση της σάρωσης με βάση τις επιθέσεις. Το γεγονός ότι τα switches στο SDN ελέγχονται απομακρυσμένα μπορεί να είναι από μόνο του απειλή για την ασφάλεια. Όπως αναφέρθηκε πριν, η κρυπτογράφηση TSL / SSL μεταξύ του ελεγκτή και των switches παραμένει προαιρετική από την τελευταία έκδοση του OpenFlow (δηλ. 1.4). Δεν είναι σαφές εάν τα OpenFlow switches εξασφαλίζουν μόνο μια σχέση ελέγχου ένα προς ένα (δηλαδή μεταξύ του switch και του ελεγκτή του) και πώς εφαρμόζεται.

Μπορούν να χρησιμοποιηθούν ενεργές μέθοδοι ασφαλείας για τον εντοπισμό σαρωτών (δηλ. εάν χρησιμοποιούνται εξωτερικά εργαλεία για τη σάρωση του δικτύου προορισμού). Ο (Mehdi Sayed Akbar, 2011) περιέγραψε χρησιμοποιώντας πληροφορίες ροής OpenFlow για την ανίχνευση ανωμαλίας της κυκλοφορίας συμπεριλαμβανομένης της ανίχνευσης σάρωσης των worms. Οι (Schehlmann Lisa, Harald Baier., 2013) επέκτειναν την προσέγγιση και το έκαναν πιο επεκτάσιμο σε δίκτυα επιπέδου ISP. Χρησιμοποίησαν το NetFlow για να φιλτράρουν την αρχική ύποπτη επισκεψιμότητα και στη συνέχεια να την ανακατευθύνουν για περαιτέρω ανάλυση στο σύστημα ανίχνευσης με βάση το OpenFlow.

Έχουν προταθεί διάφορες μέθοδοι για την πρόληψη της OpenFlow σάρωσης δικτύου. Μερικοί από αυτούς χρησιμοποίησαν μια ενεργή προσέγγιση για τους επιτιθέμενους ανιχνευτές / σαρωτές. Μερικοί βασίζονται στην απάντηση του σαρωτή με λανθασμένη ή ψεύτικη κυκλοφορία ή αντεπίθεση πλημμυρίζοντας τον εισβολέα με μεγάλη κυκλοφορία. Άλλες μέθοδοι αλλάζουν συνεχώς την ταυτότητα των υπολογιστών.

Ορισμένες μέθοδοι απόκρυψης τοπικών ταυτοτήτων από εξωτερικούς χρήστες μπορούν επίσης να χρησιμοποιηθούν για την αντιμετώπιση των sniffers ή των σαρωτών. Αυτοί περιλαμβάνουν εικονικά ιδιωτικά δίκτυα (VPN), Μετάφραση διεύθυνσης δικτύου (NAT) και διακομιστές μεσολάβησης (proxy), αν και οι αρχικοί τους σκοποί δεν σχετίζονται με την απόκρυψη ταυτότητας κεντρικών υπολογιστών. Για παράδειγμα, ο (Mendonca Marc, 2012) εισήγαγε το AnonyFlow, μία βασισμένη στο OpenFlow υπηρεσία ανωνυμοποίησης. Σε αντίθεση με το παραδοσιακό NAT όπου η μετάφραση πραγματοποιείται μεταξύ εικονικών και πραγματικών διευθύνσεων IP, το AnonyFlow χρησιμοποιεί ειδικά αναγνωριστικά ανωνυμίας που μπορούν και άλλα μέρη να δουν μόνο αντί για τις διευθύνσεις IP.

3.2.4.2 Αντίμετρα αποκάλυψης πληροφοριών

Για την προστασία των ιδιωτικών πληροφοριών, υπάρχουν και άλλες ενέργειες. Η λευκή και η μαύρη λίστα μπορούν να χρησιμοποιηθούν για φιλτράρισμα της κυκλοφορίας.

Οι λευκές και οι μαύρες λίστες στα παραδοσιακά δίκτυα ορίζονται με βάση τις διευθύνσεις IP και MAC. Μπορούν επίσης να χρησιμοποιηθούν σε δίκτυα OpenFlow. Καθώς τα OpenFlow switches μπορούν να αλληλεπιδράσουν με πληροφορίες επιπέδου ροής, μπορούμε να ορίσουμε μετρήσεις βάσει των ροών και στη συνέχεια ορίζονται άσπρες και μαύρες λίστες με βάση τη ροή των πληροφοριών επιπέδου. Αυτό μπορεί να αποτρέψει ορισμένες επιθέσεις που χρησιμοποιούν παραδείγματος χάριν μεγάλη κυκλοφορία όπου δεν μπορούν να αναγνωριστούν ορισμένα χαρακτηριστικά με βάση τις διευθύνσεις IP ή MAC.

Οι (Kloeti Rowan, 2013) πρότειναν αρκετές συστάσεις μείωσης της αποκάλυψης πληροφοριών σε δίκτυα OpenFlow. Για παράδειγμα, οι έξυπνοι κανόνες για την τυχαιοποίηση χρονικού ορίου μπορούν να δυσκολεύουν τους σαρωτές ή τους sniffers να κατανοήσουν τα μοτίβα δικτύου. Ομοίως αυτό μπορεί να εφαρμοστεί στο χρόνο απόκρισης μεταξύ ελεγκτή και switches. Ένα εργαλείο παρακολούθησης μπορεί να ανιχνεύσει τη διαφορά στο χρόνο απόκρισης μεταξύ αποστολής νέου και υφιστάμενου κανόνα ροής. Η ύπαρξη τέτοιων διαφορών στο χρόνο απόκρισης είναι ένας δείκτης ενός OpenFlow δικτύου. Μπορεί να χρειαστούν για την αντιμετώπιση αυτού του τύπου πληροφοριών πολλά σενάρια. Σε μία επιλογή, αυτό μπορεί να αντιμετωπιστεί χρησιμοποιώντας μία πλήρως προληπτική προσέγγιση όπου εγκαθίστανται όλοι οι κανόνες ροής από τους διαχειριστές δικτύου. Οι κατευθυνόμενοι και έξυπνοι μέθοδοι μέτρησης μετρητών μπορούν επίσης να είναι αποτελεσματικές στην κατασκευή ψεύτικων χρόνων απόκρισης με βάση τη φύση της επίθεσης στο δίκτυο. Πρότυπα δέντρων επίθεσης που προτείνονται από τους (Kloeti Rowan, 2013) και πολλούς άλλους ερευνητές μπορούν να χρησιμοποιηθούν για την αυτόματη ανίχνευση του τύπου της επίθεσης στο δίκτυο. Ωστόσο, τέτοια μοντέλα εξακολουθούν να φαίνονται πολύ σημαντικά και δεν περιλαμβάνουν μετρήσεις που μπορεί να ερμηνεύονται άμεσα ή να σχετίζονται με δεδομένα ροής ή πακέτων. Ορισμένες χρήσιμες μετρήσεις ροής ή πακέτων είναι APf (Μέσος αριθμός πακέτων ανά ροή (ANPPF), Μέσος όρος byte ανά ροή (ABf), Μέσος όρος διάρκειας ανά ροή (ADf), Ποσοστό ροής ζευγαριού (PPf) και Ανάπτυξη μονής ροής (GSf).

3.2.5 Άρνηση Υπηρεσίας (DoS - Denial of Service)

Οι επιθέσεις DoS είναι από τις πιο σοβαρές απειλές επειδή αυτές επηρεάζουν την απόδοση του δικτύου, αυξάνουν τον χρόνο καθυστέρησης και μειώνουν τα νόμιμα πακέτα. Μπορούν ακόμη και να απενεργοποιήσουν ολόκληρο το δίκτυο ή να το σταματήσουν να λειτουργεί. Για τα δίκτυα OpenFlow, το DoS μπορεί να είναι πιο καταστροφικό καθώς υπάρχει συνεχής ροή μεταξύ του ελεγκτή και των switches. Η συνεχής επικοινωνία μεταξύ του ελεγκτή και των switches μπορεί να δελεάσει τους εισβολείς να σπρώξουν την ροή μεταξύ του ελεγκτή και των switches και να διακόψουν τις κανονικές δραστηριότητες του δικτύου. Οι πλημμύρες και η ενίσχυση του DNS

θεωρούνται επιθέσεις ανάλυσης επιπέδου ροής επειδή οι πληροφορίες σε επίπεδο ροής είναι αρκετές για τον εντοπισμό τέτοιων επιθέσεων (Zaalouk Adel, 2014). Οι πληροφορίες για το επίπεδο ροής είναι συνήθως αρκετές για τον εντοπισμό των περισσότερων τύπων επιθέσεων DoS. Συνήθως οι πληροφορίες της κυκλοφορίας που συλλέγονται από την κεφαλίδα ροής είναι στο επίπεδο ροής. Τα συστήματα ανίχνευσης επιθέσεων βασισμένα σε ροή που βασίζονται μόνο στις πληροφορίες της κεφαλίδας μπορούν να αντιμετωπίσουν τις ακόλουθες απειλές δικτύου: DoS, σαρώσεις, worms και botnets. Αυτοί οι τέσσερις τύποι επιθέσεων έχουν μερικά κοινά στοιχεία. Για παράδειγμα, έχουν μία μεγάλη μη ισορροπημένη κίνηση μεταξύ του εσωτερικού και εξωτερικού ανεμιστήρα όπου η περισσότερη κίνηση πηγαίνει προς μία κατεύθυνση. Στις περισσότερες περιπτώσεις η μεγάλη κίνηση έρχεται προς τα μέσα. Ωστόσο, εάν το τοπικό μηχάνημα είναι botnet ή ένα θύμα, μπορεί να στέλνει μεγάλο όγκο κυκλοφορίας. Ο αριθμός πόρτας μπορεί επίσης να είναι μια πολύτιμη πληροφορία σε αυτούς τους τύπους επιθέσεων όπου υπάρχουν γνωστές πόρτες που χρησιμοποιούνται ευρέως. Άλλοι τύποι επιθέσεων δικτύου ενδέχεται να απαιτούν πληροφορίες σε επίπεδο πακέτου για ανίχνευση. Στα δίκτυα βασισμένα σε ροή, το SDN παρέχει εγχώριες μεθόδους για την ανίχνευση DoS. Οι πληροφορίες που εξάγονται από κεφαλίδες ροής είναι πολύτιμες για την ανίχνευση DoS επιθέσεων. Ορισμένες επιθέσεις DoS προκαλούν μεταβολή στον όγκο της κυκλοφορίας που είναι ορατή από την όψη της ροής. Ωστόσο, οι επιθέσεις DoS που βασίζονται σε σημασιολογικό επίπεδο, ενδέχεται να μην εντοπιστούν από την αλλαγή του όγκου της κυκλοφορίας.

Το κύριο χαρακτηριστικό των επιθέσεων DoS είναι το μεγάλο μέγεθος της κυκλοφορίας. Οι μέθοδοι για τον εντοπισμό του μεγάλου μεγέθους της κυκλοφορίας είναι οι πιο δημοφιλείς τεχνικές που χρησιμοποιούνται για την ανίχνευση πλημμυρών ή DoS επιθέσεων. Ωστόσο, μπορεί να προκύψουν ψευδείς θετικοί συναγερμοί όταν είναι τόσο μεγάλη η κίνηση που προέρχεται ή πηγαίνει σε νόμιμους κεντρικούς υπολογιστές. Υπάρχουν άλλες μέθοδοι για την ανίχνευση πιθανών πλημμυρών. Μια μέθοδος σχετίζεται με τη μελέτη της διαφοράς μεταξύ όγκου εισερχόμενης και εξερχόμενης κίνησης. Συνήθως στην επικοινωνία μεταξύ πηγής και προορισμού, θα υπάρχει κίνηση και από τις δύο πλευρές. Εάν η κίνηση είναι μεγάλη και πηγαίνει από τη μία πλευρά χωρίς καμία απάντηση από την άλλη πλευρά, αυτό μπορεί να είναι ένδειξη περίπτωσης πλημμύρας. Για παράδειγμα, στη μετάδοση TCP, ακόμα και αν τα δεδομένα είναι από τη μία πλευρά στην άλλη, ο δέκτης θα στείλει ACK μηνύματα περιοδικά. Ακόμη και η μετάδοση UDP θα έχει ένα αίτημα / απάντηση από το επίπεδο εφαρμογής.

Στην ενίσχυση DNS, μπορούν να χρησιμοποιηθούν δημόσιοι διακομιστές DNS για να αυξήσουν την επίδραση του DDoS. Αυτό μπορεί να προκαλέσει πολύ μεγάλη κλίμακα του δικτύου ή διακοπή του Διαδικτύου. Πρόσφατες εκθέσεις έδειξαν μία από τις μεγαλύτερες επιθέσεις DoS στην ιστορία, στον ιστότοπο (www.Spamhaus.Org) που ξεκινά με βάση την ενίσχυση DNS. Η παρακολούθηση και η συνεχής ανάκτηση των κορυφαίων ερωτημάτων DNS μπορεί να μας βοηθήσει να εντοπίσουμε την ενίσχυση DNS. Για παράδειγμα ένα ερώτημα που ζητά από το διακομιστή ονομάτων όλες τις εγγραφές σε αυτόν τον τομέα έχει ως αποτέλεσμα μια μεγάλη απόκριση που προκαλεί

ενίσχυση της κυκλοφορίας. Η επιλογή απόφασης του ελεγκτή (οριακή κυκλοφορία) μπορεί να σχεδιαστεί με ένα τρόπο που περιορίζει τέτοιες περιπτώσεις.

Οι βρόχοι μπορεί να προκαλέσουν DoS ή μπορούν να χρησιμοποιηθούν για επιθέσεις δικτύου. Σε τέτοιους βρόχους, τα πακέτα ταξιδεύουν από το ένα switch στο άλλο χωρίς να φτάνουν στον τελικό προορισμό τους. Οι (Kazemian Peyman, 2013) έχουν συζητήσει για το πως να χειρίζονται οι βρόχοι σε δίκτυα OpenFlow.

Για να πραγματοποιήσει επιθέσεις DoS σε SDN, ο εισβολέας μπορεί να ωθήσει έναν μεγάλο όγκο κυκλοφορίας που συνεχίζει να αλλάζει τυχαία τα χαρακτηριστικά ροής. Αυτό γίνεται για να διασφαλιστεί ότι κάθε ροή είναι νέα, από την προοπτική του switch, και ως εκ τούτου θα σταλεί στον ελεγκτή για να λάβει απόφαση σχετικά με αυτό. Ένας εισβολέας μπορεί να χρησιμοποιήσει μια γεννήτρια κίνησης που διασφαλίζει να αλλάξει τις τιμές των χαρακτηριστικών ανά ροή. Καθώς κάθε χαρακτηριστικό έχει ένα ευρύ φάσμα έγκυρων και μη έγκυρων εισόδων (π.χ. διεύθυνση IP: 0.0.0.0 έως 255.255.255.255), ο αριθμός των πιθανών ροών μπορεί να είναι τεράστιος. Μια τέτοια επίθεση μπορεί να έχει δύο στόχους: Πρώτον, θα πλημμυρίσει τον πίνακα ροής του switch και θα τον κατακλύσει με παράνομους κανόνες. Αυτό ενδέχεται να απενεργοποιήσει την ικανότητα του πίνακα ροής να αποδεχτεί νόμιμους κανόνες. Ο δεύτερος στόχος για τους επιτιθέμενους που στέλνουν αυτόν τον μεγάλο όγκο ροών είναι ότι αυτή η πλημμύρα θα κρατήσει τον ελεγκτή απασχολημένο από την απάντηση σε νόμιμες ροές από άλλα switches και μπορεί να το φέρει σε αποτυχία. Ισχυρές και αξιόπιστές μέθοδοι κρυπτογράφησης μπορούν να βοηθήσουν στη διασφάλιση της ιδιωτικής επικοινωνίας μεταξύ των switches και του ελεγκτή. Ωστόσο, δεν μπορούν να αποτρέψουν τις πλημμύρες ή το DoS, καθώς αυτά εκκινούνται από κεντρικούς υπολογιστές στέλνοντας κίνηση σε δίκτυα OpenFlow. Το σύστημα Avant-Guard που προτείνεται από τον (Shin Seungwon, 2013) ως ενίσχυση για το OpenFlow, έδειξε ότι είναι δυνατό να αντιμετωπιστούν οι επιθέσεις DoS και να εξαλείψουν τις αρνητικές επιπτώσεις τους στο δίκτυο.

3.2.5.1 Ανίχνευση DoS

Οι (Braga Rodrigo, 2010) συζήτησαν μια ελαφριά μέθοδο ανίχνευσης επιθέσεων DDoS στο SDN. Η κύρια πρόκληση ήταν να γίνει διάκριση κανονικών πακέτων από πακέτα πλημμύρας DDoS. Ταξινόμησαν την κυκλοφορία του δικτύου σε μια επίθεση ή την κανονική κίνηση βάσει του Self Organizing Map (SOM). Τα επιλεγμένα χαρακτηριστικά ροής βασίστηκαν σε προηγούμενες προσεγγίσεις, συμπεριλαμβανομένου του APf (Μέσος αριθμός πακέτων ανά ροή (ANPPF), του μέσου όρου Byte ανά ροή (ABf), του μέσου όρου διάρκειας ανά ροή (ADf), του ποσοστού των ροών ζεύγους (PPf) και της αύξησης των μονών ροών (GSf). Αυτές οι μετρήσεις ή τα χαρακτηριστικά συλλέγονται συνεχώς και παρακολουθούνται για ανίχνευση πιθανών DDoS. Μια σημαντική ανησυχία είναι ότι η παρακολούθηση και η διατήρηση του τόσο τεράστιου όγκου δεδομένων θα υποβαθμίσει σημαντικά την απόδοση του ελεγκτή που είναι ήδη κατακλισμένος με άλλες εργασίες. Έχοντας μία αφοσιωμένη ξεχωριστή μονάδα ή έναν ελεγκτή για την εκτέλεση αυτής της εργασίας μπορεί να είναι πιο ρεαλιστική λύση.

Οι (Shirali-Shahreza and Ganjali Sajad Yashar., 2013) πρότειναν την δειγματοληψία της κίνησης για να μειωθεί η γενική κίνηση του ελεγκτή από τη διαδικασία παρακολούθησης.

Μια απλή μέθοδος για τον εντοπισμό πιθανών επιθέσεων DoS μπορεί να διατηρήσει την παρακολούθηση του όγκου των ροών κίνησης. Το όριο μπορεί να καθορίζεται από το τι μπορεί να θεωρηθεί μεγάλη ή ανώμαλη κίνηση. Μόλις ξεπεραστεί αυτό το όριο, μπορεί να συμβεί μία ενεργοποίηση DoS και ο ελεγκτής να εισάγει έναν κανόνα ροής για την πτώση των πακέτων. Ομοίως, ο χάρτης κυκλοφορίας ή τα σχέδια μπορούν να αναλύονται συχνά για να προβλέπουν εάν κάποια κίνηση είναι ανώμαλη ή μεγάλη. Ο (Suh Junho, 2010) πρότεινε ένα περιεχόμενο βασισμένο στην αρχιτεκτονική δικτύωσης. Ο ελεγκτής ενεργοποιεί την ειδοποίηση DoS εάν η κυκλοφορία υπερβαίνει ένα συγκεκριμένο όριο. Στη συνέχεια εισάγονται κανόνες από τον ελεγκτή στα switches για να εξαλείψουν την πηγή του DoS.

Οι (Schehlmann Lisa, Harald Baier., 2013) πρότειναν μία προσέγγιση βασισμένη στο OpenFlow για τον εντοπισμό και τον μετριασμό των botnets. Τα botnets είναι δίκτυα ή ομάδες παραβιασμένων κεντρικών υπολογιστών που χρησιμοποιούνται για να ξεκινήσουν επιθέσεις όπως το DDoS, για να διαδώσουν worms ή για αποστολή ανεπιθύμητων mail. Η προτεινόμενη λύση τους, το COFFEE, χρησιμοποιεί την ικανότητα του SDN να έχει πρόσβαση σε όλη την κίνηση για να μειώσει το ποσοστό ψευδών ανιχνεύσεων.

Στις συνδέσεις TCP, το μήνυμα επιβεβαίωσης (TCP ACK) απαιτείται για την επαλήθευση της επικοινωνίας μεταξύ αποστολέων και δεκτών. Ωστόσο, μπορεί επίσης να ενεργοποιηθούν από πλημμύρες ή DoS επιθέσεις. Ο (Shin Seungwon, 2013) πρότεινε έναν απλό αλγόριθμο για τον χειρισμό πακέτων TCP ACK. Ο (Liyanage Madhusanka, 2014) πρότεινε ένα επίπεδο ασφαλείας ή μία διεπαφή για το συντονισμό της επικοινωνίας μεταξύ των OpenFlow switches και του ελεγκτή. Μια υπόθεση της επίθεσης TCP SYN DoS χρησιμοποιείται για την αξιολόγηση του μοντέλου. Η επίθεση περιλαμβάνει κατοχή όλων των πακέτων και των διευθύνσεων IP που είναι πιθανοί συνδυασμοί. Η απόδοση του δικτύου μετριέται μέσω της επίθεσης που αξιολογεί τον χρόνο που χρειάζεται το δίκτυο να υπολογίσει και να εξαλείψει την επίθεση.

Οι (Benton, 2013) αξιολόγησαν τις ευπάθειες του OpenFlow για επιθέσεις DoS και επιθέσεις ακεραιότητας. Έδειξαν ότι το πρωτόκολλο OpenFlow και ο μηχανισμός επικοινωνίας μεταξύ ελεγκτή και των switches πρέπει να διερευνηθούν διεξοδικά. Ο Dover, 2013 διεξήγαγε ένα πείραμα για την προσομοίωση επιθέσεων DoS στον Floodlight ελεγκτή χρησιμοποιώντας μεθόδους όπως TCP SYN ή τον ιό ARP cache. Μια ευπάθεια που εντοπίστηκε στον Floodlight αποσυνδέει ένα παλιό switch εάν έχει καταχωρηθεί νέος switch στο ίδιο αναγνωριστικό διαδρομής δεδομένων (DPID) με το παλιό. Μια τέτοια ευπάθεια μπορεί να χρησιμοποιηθεί από κακόβουλα switches για να ισχυριστούν ότι είναι νόμιμα. Η μόνη πληροφορία που χρειάζεται ο εισβολέας είναι το DPID που μπορεί να αποκτηθεί από τον ελεγκτή REST API.

Ο (YuHunag Chu, 2010) πρότεινε ένα αυτόνομο DDoS σύστημα ανίχνευσης που βασίζεται στο OpenFlow. Το σύστημα χρησιμοποιεί την απλή μέτρηση όγκου (δηλ. ροές

/ πακέτα ανά ώρα) για να κρίνει την εμφάνιση του DoS ή του DDoS. Το πρόβλημα με την τόσο απλή μέτρηση είναι ότι μπορεί να εμφανιστούν πολλοί ψευδείς θετικοί συναγερμοί όπου η κυκλοφορία μεγάλου όγκου μπορεί να είναι νόμιμη.

3.2.5.2 Αντιμετώπιση του DoS

Το DoS μπορεί να αντιμετωπιστεί με αποτελεσματική και δυναμική απόκριση μεθόδων για τον χειρισμό περιστατικών DoS. Ο περιορισμός της κυκλοφορίας από τον ελεγκτή και η παρακολούθηση των μη φυσιολογικών συμπεριφορών κυκλοφορίας είναι επίσης σημαντικά αντίμετρα. Συζητήσαμε νωρίτερα μερικά αντίμετρα για πλαστογράφηση. Ομοίως, υπάρχουν μερικές προτάσεις για ενεργά αντίμετρα του DoS ή για επιθέσεις πλημμυρών σε δίκτυα SDN συγκεκριμένα.

Ένας εισβολέας μπορεί να εστιάσει το DoS στα μηνύματα από το επίπεδο δεδομένων ή στα switches του ελεγκτή και να προσπαθήσει να κατακλύσει και τον πίνακα ροής του switch και τους πόρους του ελεγκτή. Οι μηχανισμοί προστασίας πρέπει να διασφαλίζουν ότι ο ελεγκτής και τα switches έχουν την ικανότητα να ανακάμψουν γρήγορα από τέτοιες πλημμύρες. Ο μηχανισμός πρέπει επίσης να είναι σε θέση να διακρίνει την νόμιμη από την ψεύτικη κυκλοφορία. Προτείνεται οι παθητικοί ή οι αδρανείς παράγοντες παρακολούθησης να ενεργοποιούνται μόνο όταν βλέπουν την εμφάνιση ψεύτικων πλημμυρών.

Ο (Koponen Teemu, 2011) πρότεινε το FII (Πλαίσιο για Καινοτομία του Διαδικτύου) για την αντιμετώπιση DoS μεταξύ τομέων, με βάση το σχήμα διεθύνσεων IP AIP (Andersen David G, 2008). Το AIP περιλαμβάνει πληροφορίες σχετικά με κεντρικούς υπολογιστές στην κεφαλίδα του πακέτου που σχετίζονται με τον κεντρικό υπολογιστή με ένα καθολικό αναγνωριστικό, αντί για διεύθυνση IP. Αυτό μπορεί να βοηθήσει εξαλείφοντας επιθέσεις που εισβάλλουν σε κεντρικούς υπολογιστές με βάση τις διευθύνσεις IP τους. Ισχυρίστηκαν ότι επικεντρώνεται η προσέγγισή τους στην διαθεσιμότητα για να διασφαλιστεί ότι κάθε συμμετέχων σε μια επικοινωνία μπορεί να φτάσει στον προορισμό. Η προσέγγιση διαιρεί τον χειρισμό του DoS σε δύο μέρη: Inter και intra-domain επιθέσεις. Για τους τοπικούς, ή τις επιθέσεις εντός τομέα, σε κάθε τομέα πρέπει να δοθεί η επιλογή να επιλέξουν τον δικό τους τρόπο επικύρωσης τοπικών κεντρικών υπολογιστών. Από την άλλη πλευρά, το FII παρέχει μια ενιαία μέθοδο για το χειρισμό των διατομών DoS επιθέσεων. Ως αντίμετρο, ένα μήνυμα κλεισίματος (SUM) μπορεί να εκδοθεί σε εισβολείς που επιτίθενται στο δίκτυο με DoS επιθέσεις.

Οι πλημμύρες ή το DoS μπορούν επίσης να επιλυθούν με τη βελτιστοποίηση κανόνων ροής ή συγχωνευμένων κανόνων σε πίνακες ροής. Οι πίνακες ροής μπορούν να είναι δυναμικά πλημμυρισμένοι με κανόνες που προκαλούν υπερχείλιση μνήμης ή κορεσμό μνήμης του switch και να προκαλέσουν το κλείσιμο ή την άρνηση υπηρεσίας για νόμιμους κεντρικούς υπολογιστές ή για την κυκλοφορία. Ως εκ τούτου, είναι απαραίτητο για τα switches να έχουν δυναμική ικανότητα για να επανεκτιμούν συνεχώς τους κανόνες του πίνακα ροής και να συγχωνεύουν τις ροές που μπορεί να είναι συγχωνευμένες. Ωστόσο, μια τέτοια αξιολόγηση και διαδικασία λήψης αποφάσεων είναι έξυπνη και

περίπλοκη. Με βάση την τρέχον OpenFlow αρχιτεκτονική, τέτοια νοημοσύνη δεν υπάρχει σε switches. Επιπλέον, εάν ο ελεγκτής το κάνει, μπορεί να ενισχύσει τους πόρους του ελεγκτή.

3.2.6 Ανύψωση προνομίων

Μόλις εισέλθει στο σύστημα, ο εισβολέας προσπαθεί να αυξήσει τα προνόμια πρόσβασής του για να έχει πρόσβαση σε πόρους συστήματος και εφαρμογές που απαιτούν ειδικά δικαιώματα. Η ικανότητα εντοπισμού επιθέσεων ανύψωσης προνομίων απαιτεί μία διαδικασία ισχυρού και έξυπνου ελέγχου. Για παράδειγμα, ο (Ramachandran Anirudh, 2009) πρότεινε το Pedigree, ένα σύστημα εντοπισμού εκτελέσιμων εφαρμογών που τις επισημαίνει με ειδική αναγνώριση. Ένα μεγάλο πρόβλημα με τις μεθόδους καταγραφής ή ελέγχου είναι η επεκτασιμότητα, επειδή αυτές αποθηκεύουν μεγάλο όγκο δεδομένων που μπορεί να επηρεάσουν την αποθήκευση, την μνήμη και το εύρος ζώνης. Δεδομένου ότι τα δικαιώματα εκχωρούνται σε εξουσιοδοτημένες μονάδες ελέγχου πρόσβασης, οι επιθέσεις κλιμάκωσης στοχεύουν συχνά αυτές τις μονάδες και προσπαθούν να παραβιάσουν τις πληροφορίες τους. Έχουν προταθεί διάφορες προσεγγίσεις για να δοθεί στους χρήστες το σωστό επίπεδο άδειας.

Οι (Porras Phillip, 2012) πρότειναν ένα σύστημα RBAC βασισμένο στο OpenFlow. Η ιδέα είναι να δοθεί προνόμιο σε μια βάση ροής αντί για μία βάση χρήστη ή κεντρικού υπολογιστή. Ένα πλεονέκτημα του ελέγχου ταυτότητας βάσει ροής είναι ότι πρέπει ο χρήστης να επαληθεύεται συχνά με βάση τη ροή. Αυτό μπορεί να μειώσει το πρόβλημα ανύψωσης των προνομίων καθώς οι χρήστες συχνά εξετάζονται για αυτό. Ένα άλλο πλεονέκτημα είναι ότι ο ελεγκτής μπορεί να απομονωθεί από όλες τις άλλες ροές. Επιπλέον, οι εσωτερικές ροές μπορούν να διακριθούν από εξωτερικές ροές. Τα δικαιώματα μπορούν στη συνέχεια να έχουν έναν κύκλο ζωής που ξεκινά και τελειώνει με τον κύκλο ζωής της ροής. Μια μονάδα ελέγχου ταυτότητας της πηγής, περιλαμβάνει την εισαγωγή κάθε κανόνα ροής στα switches και την επαλήθευση μέσω μίας ψηφιακής υπογραφής. Εάν δεν παρέχεται υπογραφή, δίνεται η χαμηλότερη προτεραιότητα. Ωστόσο, αυτό μπορεί να δώσει την ευκαιρία για ανύψωση προνομίων αργότερα (δηλαδή εντός του πίνακας ροής του switch). Η χρήση της προεπιλεγμένης ή λιγότερο προνομιακής προσέγγισης έχει ένα πλεονέκτημα της μη πτώσης ροών εάν ο έλεγχος ταυτότητας αποτύχει. Ωστόσο, δεν επιλύει τις επιθέσεις ασφαλείας που προέρχονται από ανύψωση προνομίων. Επιπλέον, ξεκινούν πολλές τρέχουσες επιθέσεις την εισβολή, κάνοντας επίθεση σε μια νόμιμη εφαρμογή και τη θέτουν σε κίνδυνο. Τα προνόμια της εφαρμογής του θύματος είναι ότι χρησιμοποιούνται για περαιτέρω επιθέσεις. Ίσως είναι απαραίτητη μια υβριδική προσέγγιση να συνδυαστεί μεταξύ αυτού του συστήματος προνομίων ή δικαιωμάτων, εκτός από μια άλλη μονάδα που μπορεί να παρακολουθεί την χρήση του προφίλ της εφαρμογής. Μια νόμιμη εφαρμογή που ξαφνικά αλλάζει τον τρόπο με τον οποίο επικοινωνεί με άλλες εφαρμογές ή προορισμούς, πρέπει να ενεργοποιεί μια προειδοποίηση ασφαλείας.

Οι (Wen Xitao, 2013) πρότειναν το PermOF, ένα σύστημα πρόσβασης διαχείρισης ελέγχου που περιλαμβάνει ολοκληρωμένα επίπεδα πρόσβασης για τους πόρους του ελεγκτή και του δικτύου. Απλά επίπεδα περιορισμένης εξουσιοδότησης με μόνο δύο ή

τρία επίπεδα (συμπεριλαμβανομένου του διαχειριστή) μπορεί να είναι ένας εύκολος στόχος για να παραβιάσει ή να προκαλέσει ανύψωση προνομίων. Συμπεριλαμβανομένου ενός σχετικά μεγάλου αριθμού επιπέδων πρόσβασης, θα πρέπει να έχει ως αποτέλεσμα τον περιορισμό της χρήσης δυνατοτήτων διαχείρισης υψηλού επιπέδου, που μπορεί να έχει πολύ ισχυρά δικαιώματα πρόσβασης και τροποποίησης. Η προτεινόμενη προσέγγιση παρέχει ένα σύνολο 18 πιθανών επιπέδων αδειών. Ένα προεπιλεγμένο ελάχιστο προνόμιο δίνεται στις εφαρμογές. Οι κλήσεις ενός API ελεγκτή ενεργοποιούν την επικοινωνία με τις εφαρμογές. Μια πρόκληση για μια τέτοια προσέγγιση, είναι εάν διαφορετικά λειτουργικά συστήματα μπορούν να δημιουργήσουν την ίδια διαδικασία αναγνωριστικών (τα οποία δεν έχουν), ή αλλιώς εμείς πρέπει να επισημάνουμε το αναγνωριστικό διαδικασίας ανά λειτουργικό σύστημα ή σε ένα ξεχωριστό ειδικό σύστημα ετικετών.

3.3 Θέματα ασφαλείας στην αρχιτεκτονική SDN

Όλες οι επιθέσεις στην ασφάλεια του δικτύου μπορούν να κατηγοριοποιηθούν ανάλογα τον κύριο στόχο της επίθεσης, για παράδειγμα η παρακολούθηση μίας διεπαφής ελέγχου μπορεί να χαρακτηριστεί ως επίθεση της οποίας ο κύριος στόχος είναι η παραβίαση ιδιωτικών και ευαίσθητων δεδομένων που ανταλλάσσονται μεταξύ συσκευών δικτύου, όπου αυτό αποτελεί μη εξουσιοδοτημένη αποκάλυψη πληροφοριών με μία ευρύτερη έννοια. Η ακόλουθη λίστα περιγράφει γενικευμένα ζητήματα και απειλές στην ασφάλεια του δικτύου εξηγώντας τις επιφάνειες επίθεσης, τις αποκλίνουσες συμπεριφορές και τις ατέλειες ασφάλειας που έχουν εντοπιστεί στο πλαίσιο SDN.

3.3.1 Μη εξουσιοδοτημένη πρόσβαση (Sloan, R.H., Warner, R.,., 2013): Οι εισβολείς παραχωρούν στους εαυτούς τους πρόσβαση χωρίς επιτήρηση στα στοιχεία του SDN που εκμεταλλεύονται είτε αδύναμους είτε ανύπαρκτους μηχανισμούς ελέγχου πρόσβασης, ξεκινώντας βίαιες επιθέσεις εναντίον διοικητικών τερματικών και REST API που εκθέτουν συνεδρίες καταγραφής ή εκμεταλλεύονται ευπάθειες σε στοιχεία δικτύου και στη συνέχεια, εγκαθιστούν συσκευές απατεώνες ή δεσμεύουν απομακρυσμένες συνδέσεις στο δίκτυο.

3.3.2 Μη εξουσιοδοτημένη αποκάλυψη πληροφοριών (Lindqvist, U., Jonsson, E.,, 1997): Μπορούν να χρησιμοποιηθούν αρκετές επιφάνειες επίθεσης για αφαίρεση ευαίσθητων πληροφοριών του δικτύου, για παράδειγμα, ένας εισβολέας μπορεί να συμπεράνει την συμπεριφορά προώθησης δικτύου με τη μετάδοση πακέτων ανιχνευτή προς εντοπισμό των στοιχείων του δικτύου. Ένας εισβολέας που θέτει σε κίνδυνο μία ευάλωτη εφαρμογή δικτύου μπορεί να αποκτήσει πρόσβαση σε βάσεις δεδομένων πολιτικής δικτύου και άλλες εσωτερικές αποθήκες δεδομένων δικτύου. Τα μη ασφαλή κανάλια μπορούν να κατασχεθούν για παρακολούθηση των πακέτων και υποκλοπές.

Τέλος, οι επιθέσεις πλαστοπροσωπίας της συσκευής επιτρέπουν σε έναν εισβολέα να λαμβάνει πληροφορίες που προορίζονται αρχικά για ένα συμβιβασμένο στοιχείο δικτύου.

3.3.3 Μη εξουσιοδοτημένη τροποποίηση πληροφοριών δικτύου (Lindqvist, U., Jonsson, E.,, 1997): Οι εισβολείς μπορούν να αξιοποιήσουν ευάλωτα πρωτόκολλα και APIs και την έλλειψη μηχανισμών επαλήθευσης και ελέγχου ταυτότητας για να παρακάμψουν τους υπάρχοντες κανόνες ροής μέσω κανόνων ροής που αντιμετωπίζουν θέματα κακόβουλων εφαρμογών. Εκτός αυτού, μια μη εξουσιοδοτημένη πρόσβαση στον εσωτερικό αποθηκευτικό χώρο προσφέρει στον εισβολέα τη δυνατότητα εισαγωγής αντιφατικών πολιτικών δικτύου ή τροποποίησης των υπαρχουσών. Αφ 'ετέρου, αλλαγές στην τοπολογία του δικτύου μπορούν να προκληθούν αξιοποιώντας εσφαλμένες διαμορφώσεις πρωτοκόλλου μαζί με πλαστοπροσωπία συσκευών και επιθέσεις πλαστών πακέτων.

3.3.4 Καταστροφή πληροφοριών δικτύου (Lindqvist, U., Jonsson, E.,, 1997): Τα πιο εμφανή σενάρια σε αυτήν την περίπτωση αναφέρονται για να προκαλέσουν έξαψη κανόνων ροής σε switches, απόρριψη κακόβουλων εφαρμογών πακέτων ελέγχου που προορίζονται είτε για άλλη εφαρμογή είτε για μία αλυσίδα υπηρεσιών και κατάργηση πολιτικής δικτύου ως συνέπεια μη εξουσιοδοτημένης πρόσβασης σε διοικητικούς σταθμούς ή σε βάσεις δεδομένων εσωτερικού δικτύου.

3.3.5 Διακοπή υπηρεσίας (Lindqvist, U., Jonsson, E.,, 1997): Έχουν εντοπιστεί τρεις κύριες πηγές διακοπής της υπηρεσίας, πρώτον οι επιθέσεις πλημμύρας: έλεγχος πλημμύρας πακέτων και πλημμύρες πινάκων κανόνων ροής. Δεύτερον, η εσφαλμένη εισαγωγή πακέτου προκαλεί συχνά κλείσιμο σύνδεσης ή τερματισμό της συσκευής προορισμού. Τέλος, επιθέσεις δηλητηρίαση ς της τοπολογίας όπου παραβιάζεται η προβολή δικτύου του ελεγκτή, με αποτέλεσμα την αποσύνδεση δικτύου από στοχευμένες συσκευές.

3.3.6 Λανθασμένες διαμορφώσεις (Kendall, 1999): Εσφαλμένες διαμορφώσεις σε πρωτόκολλα, διεπαφές, APIs και συστήματα μεταφράζονται σε νέες ευπάθειες και παραβιάσεις ασφάλειας, σε πολιτικές δικτύου σε διένεξη και κανόνες ροής, σε ακατάλληλους μηχανισμούς επαλήθευσης και ελέγχου ταυτότητας και σε καταστρατήγηση σε ήδη εφαρμοσμένα μέτρα ασφαλείας.

3.3.7 Μηχανισμοί ελέγχου ταυτότητας, εμπιστοσύνης και επαλήθευσης με κακή ρύθμιση (Simmons, 2014)**:** Απλά κανάλια κειμένου και ακατάλληλοι ή αδύναμοι μηχανισμοί ελέγχου ταυτότητας ανοίγουν το δρόμο για τη συντριπτική πλειονότητα των επιθέσεων και την αποκλίνουσα συμπεριφορά: η υποκλοπή, η έγχυση πακέτων, η κατασκευή πακέτων, η υποκλοπή κίνησης, η δηλητηρίαση πληροφοριών δικτύου και η υποκλοπή ταυτότητας**.**

3.4 Έλεγχοι ασφαλείας SDN

Οι έλεγχοι ασφαλείας στοχεύουν στην παροχή πρόσβασης σε νόμιμους χρήστες, την προστασία των συστημάτων από επιθέσεις και την παροχή μετριασμού και αντιμέτρων όταν συμβαίνουν επιθέσεις. Η πολυπλοκότητα και τα ακριβή καθήκοντα κάθε ελέγχου μπορούν να διαφέρουν από έναν τομέα σε έναν άλλο. Οι κύριες εργασίες ελέγχου μπορούν γενικά να περιλαμβάνουν ανίχνευση, προστασία και αντίμετρα.

3.4.1 Τείχη προστασίας SDN

Το τείχος προστασίας είναι ένας από τους πιο δημοφιλείς μηχανισμούς ασφαλείας. Τα τείχη προστασίας είναι υπεύθυνα για την παρακολούθηση της κυκλοφορίας του δικτύου που επιτρέπει ή αποτρέπει το πέρασμα ή την εισβολή τους βάσει ορισμένων κριτηρίων που καθορίζονται από χρήστες ή διαχειριστές δικτύου. Τυπικά, λειτουργούν στα επίπεδα 2 και 3 (δηλ. επίπεδα διασύνδεσης δεδομένων και δικτύου) του μοντέλου OSI των 7 επιπέδων. Μπορούν να καθοριστούν κανόνες τείχους προστασίας για να αποτρέψουν ή να επιτρέψουν την κυκλοφορία βάσει διευθύνσεων IP, πορτών, πρωτοκόλλων και διευθύνσεων MAC. Ενώ τα παραδοσιακά τείχη προστασίας έχουν μελετηθεί επαρκώς, η έρευνα σχετικά με τα τείχη προστασίας SDN ακόμη εξελίσσεται. Ο ίδιος ο ελεγκτής SDN εκτελεί ορισμένες από τις εργασίες που συνήθως επιτυγχάνονται με παραδοσιακά τείχη προστασίας. Για παράδειγμα, οι ελεγκτές στο SDN λαμβάνουν αποφάσεις σχετικά με την τύχη των ροών και γράφουν σχετικούς κανόνες ροής στους πίνακες ροής των switches.

3.4.1.1 Τείχη προστασίας SDN έναντι παραδοσιακών τειχών προστασίας

Όσον αφορά τα χαρακτηριστικά που χρησιμοποιούνται στους κανόνες τείχους προστασίας, οι τρέχουσες υλοποιήσεις των τείχων προστασίας των SDN είναι παρόμοιες με αυτές στα παραδοσιακά τείχη προστασίας. Από την άλλη πλευρά, οι πρόσφατες εκδόσεις του OpenFlow έχουν επεκτείνει τη λίστα χαρακτηριστικών που μπορούν να συμπεριληφθούν στους κανόνες ροής. Αυτό τελικά θα επηρεάσει τις μελλοντικές υλοποιήσεις τειχών προστασίας των SDN.

Ο κύριος αντίκτυπος που έχει το SDN στα τείχη προστασίας είναι ότι ο SDN ελεγκτής λαμβάνει αποφάσεις για τη μοίρα των ροών. Στα παραδοσιακά δίκτυα, αυτός

ήταν ο κύριος ρόλος του τείχους προστασίας. Στο SDN, ο ελεγκτής ενεργεί ως τείχος προστασίας. Οι ελεγκτές συνεχώς αξιολογούν ή γνωρίζουν την τρέχουσα τοπολογία χρησιμοποιώντας μια μονάδα ανακάλυψης. Ο ελεγκτής δημιουργεί LLDP και πακέτα εκπομπών τακτικά σε γειτονικά switches. Με βάση την απάντηση από αυτά τα switches, ο ελεγκτής μπορεί συχνά να προβλέψει την τρέχουσα τοπολογία δικτύου. Ο ελεγκτής περιλαμβάνει επίσης μία μονάδα switch εκμάθησης που μαθαίνει για νέες συσκευές με βάση τις MAC διευθύνσεις τους. Οι κανόνες μπορούν να προστεθούν δυναμικά από τον ελεγκτή στους πίνακες ροής των switches. Εάν μια νέα ροή προστίθεται στο δίκτυο, το switch εκμάθησης ελέγχει την είσοδο και την έξοδο των switches ροής και επίσης την καλύτερη διαδρομή για τη ροή. Αυτό στη συνέχεια προστέθηκε ως νέος κανόνας στο κατάλληλο switch.

Στο SDN, οι ελεγκτές αποθηκεύουν κανόνες ή λίστες ελέγχου πρόσβασης (ACL) για όλα τα switches του δικτύου. Τέτοια σύνδεση (δηλαδή μεταξύ τείχους προστασίας και switches) δεν υπάρχει στα παραδοσιακά δίκτυα. Σαν αποτέλεσμα, οι κανόνες τείχους προστασίας στα παραδοσιακά δίκτυα είναι στατικοί και δεν είναι συνδεδεμένοι με την κυκλοφορία δικτύου. Αυτοί οι κανόνες προστίθενται και αξιολογούνται χειροκίνητα από διαχειριστές δικτύου. Είναι λοιπόν πιθανό ότι ορισμένοι κανόνες στα παραδοσιακά τείχη προστασίας είναι ξεπερασμένοι ή ανεφάρμοστοι. Από την άλλη πλευρά, οι κανόνες του πίνακα ροής στο SDN είναι πολύ δυναμικοί. Οι ξεπερασμένοι κανόνες τελικά καταργούνται από τους πίνακες ροής.

Καθώς οι πρόσφατες εκδόσεις του OpenFlow έχουν εκτεταμένη ροή χαρακτηριστικών, τα τείχη προστασίας που βασίζονται σε SDN μπορεί να είναι πιο συγκεκριμένα και να αντιμετωπίζουν με χαρακτηριστικά ροής ή επιπέδου πακέτου. Το OpenFlow 1.0 περιλαμβάνει 12 πεδία κεφαλίδας. Εκτός από αυτά, υπάρχουν νέα πεδία που σχετίζονται με το πρωτόκολλο IP, το VLAN, κ.λπ. Το OpenFlow 1.2 και παραπάνω περιλαμβάνει 40 πεδία κεφαλίδας, δίνοντας στους χρήστες περισσότερη δυνατότητα ελέγχου ή αλληλεπίδρασης με ροές δικτύου. Έχοντας έλεγχο στο επίπεδο ροής επιτρέπει στους διαχειριστές δικτύου να εκτελούν εργασίες που δεν ήταν δυνατή η χρήση τους στα παραδοσιακά δίκτυα. Σε ορισμένες περιπτώσεις, αυτοί θέλουν να πραγματοποιήσουν ανακατεύθυνση κυκλοφορίας μέσω των middle-boxes. Αυτό το πρόβλημα είναι αρκετά κοινό στο περιβάλλον cloud όπου η αυτόματη διαμόρφωση μιας νέας παρουσίας ενός VM δεν θα ολοκληρωθεί καθώς οι διαχειριστές δικτύου δεν έχουν κανένα έλεγχο στα middle-boxes (π.χ. ένα τείχος προστασίας) για να οδηγήσουν αυτά τα middle-boxes να κατανείμουν πόρους στο νέο VM.

3.4.1.2 Τείχη προστασίας που βασίζονται σε SDN

Στο SDN, μια μονάδα τείχους προστασίας μπορεί να προστεθεί συνήθως ως βόρεια διεπαφή (REST) API στον ελεγκτή. Το REST API είναι ένα τυπικό πρόσθετο περιβάλλον για αλληλεπίδραση με τους περισσότερους ελεγκτές SDN. Αυτό επιτρέπει στις εφαρμογές που έχουν αναπτυχθεί από τον χρήστη να επικοινωνούν με τον ελεγκτή. Οι κανόνες του τείχους προστασίας διαφέρουν από τους κανόνες του πίνακα ροής αν και μπορεί να μοιάζουν.

Αρκετά άρθρα έχουν συζητήσει τον τρόπο υλοποίησης των τειχών προστασίας με βάση το SDN. Ο (Casado Martin T. G., 2006) πρότεινε το SANE, ως αρχιτεκτονική προστασίας για δίκτυα επιχειρήσεων μέσω ενός μόνο επιπέδου προστασίας. Αυτή είναι μία από τις πρώτες συνεισφορές στον κεντρικό έλεγχο στη λειτουργία του δικτύου συστημάτων ή του ελεγκτή SDN. Τα switches και άλλα στοιχεία του δικτύου έχουν απλά και ελάχιστα αξιόπιστα στοιχεία προώθησης. Σε αυτήν την αρχική αρχιτεκτονική SDN, ο ελεγκτής περιλαμβάνει κανόνες ελέγχου πρόσβασης αντί να τους έχει σε τείχη προστασίας όπως στα παραδοσιακά δίκτυα. Ένας από τους ρητούς δηλωμένους στόχους είναι να ενώσουμε όλες τις προσπάθειες και τις πληροφορίες ασφαλείας σε ένα μέρος. Αυτό, ωστόσο, μπορεί να έχει διαφορετικές ερμηνείες. Δεν πρέπει η συγκέντρωση των αποφάσεων των κανόνων στον ελεγκτή να αναμειγνύεται με συνδυασμό λειτουργιών, καθώς διαφορετικοί έλεγχοι ασφαλείας δεν εκτελούν συνεκτικά τις ίδιες εργασίες. Η ιδέα ενός κεντρικού ελεγκτή προσφέρει ένα άλλο πλεονέκτημα, επειδή το τείχος προστασίας που αλληλεπιδρά με τον ελεγκτή, μπορεί να έχει καθολική όψη ολόκληρου του δικτύου.

Ο (Hu Hongxin, 2014) πρότεινε το FlowGuard, βασισμένο σε πλαίσιο παρακολούθησης SDN για τον εντοπισμό πιθανών συγκρούσεων μεταξύ κανόνων και ροών τείχους προστασίας. Όποτε η κατάσταση δικτύου αλλάζει, το FlowGuard ελέγχει τους χώρους διαδρομών για να δει αν μία πολιτική τείχους προστασίας παραβιάζεται. Σε αυτή τη μελέτη, πολλές προκλήσεις και ευκαιρίες τείχους προστασίας που βασίζονται σε SDN συζητούνται, όπως η ικανότητα να αξιολογεί δυναμικά τις αλλαγές πολιτικής, τις συγκρούσεις ζητημάτων στους κανόνες του πίνακα ροής, την κεντρική θέση του ελεγκτή και την ικανότητα του τείχους προστασίας να πραγματοποιεί επιθετική επιθεώρηση κυκλοφορίας.

Οι Jia and Wang, 2013 πρότειναν τείχη προστασίας με βάση το SDN για τα P2P δίκτυα. Η μονάδα τείχους προστασίας παρέχεται ως API ενσωματωμένη σε SDN. Η περίπτωση χρήσης των δικτύων P2P μπορεί να ωφελήσει το SDN επειδή τα δίκτυα P2P έχουν πολύ δυναμικούς χρήστες. Η ζήτηση εύρους ζώνης ή δικτύου ποικίλλει επίσης συχνά. Η ευελιξία που έχει το SDN σε αντίθεση με τα παραδοσιακά δίκτυα και η ικανότητά του να προσαρμόζεται δυναμικά στις απαιτήσεις των χρηστών ταιριάζουν στις περισσότερες περιπτώσεις χρήσης P2P. Καθώς η ασφάλεια είναι πάντα μια σημαντική ανησυχία των P2P δικτύων, οι SDN λύσεις χρειάζεται να παρέχουν μηχανισμούς ασφαλείας για την αποφυγή πιθανών εισβολέων.

Οι (Suh Michelle, 2014) παρουσίασαν ένα τείχος προστασίας βασισμένο σε SDN μέσω POX ελεγκτή. Χρησιμοποίησαν χαρακτηριστικά από το OpenFlow 1.1 για να επιτρέψουν στους χρήστες να προσθέσουν κανόνες τείχους προστασίας. Έδειξαν προκαταρκτικά πειραματικά αποτελέσματα με βάση τις παραγόμενες ροές. Οι (Sethi Divjyot, 2013) τυπικά μοντελοποίησαν την συμπεριφορά του ελεγκτή SDN. Αξιολόγησαν την εγκυρότητα του μοντέλου τους χρησιμοποιώντας μία απλή μονάδα τείχους προστασίας με κατάσταση. Ένα παράδειγμα ενός απλού σεναρίου για την αποφυγή άμεσης σύνδεσης από το Διαδίκτυο στο εταιρικό δίκτυο χρησιμοποιείται στην αξιολόγηση. Οι δραστηριότητες ή οι διαδικασίες μεταξύ του τείχους προστασίας, του ελεγκτή και των

switches ορίζονται επίσημα. Γενικά εφαρμόζονται τυπικές προσεγγίσεις μοντελοποίησης σε χαμηλές κλίμακες και έχουν περιορισμούς επεκτασιμότητας.

3.4.1.3 Τείχη προστασίας σε κατάσταση ελέγχου που βασίζονται σε SDN

Με τη δυνατότητα του SDN να έχει μια καθολικό έλεγχο του δικτύου, ελπίζεται ότι η ανάλυση ελέγχου του δικτύου ή συγκεκριμένων ροών θα είναι πιθανή. Οι αναλύσεις δικτύου χωρίς κατάσταση ελέγχου μελετούν πακέτα ή ροές μεμονωμένες χωρίς την εξέταση άλλων πακέτων, ροών ή κανόνων ροής και χωρίς να επικεντρώνονται κάποια άλλα δίκτυα, συστήματα ή μεταβλητές περιβάλλοντος. Από την άλλη πλευρά, η ανάλυση σε κατάσταση ελέγχου λαμβάνει συνδυασμένες απόψεις από τους κανόνες ή την κυκλοφορία στο δίκτυο. Ένα τείχος προστασίας σε κατάσταση ελέγχου πρέπει να μπορεί να καταγράφει και να παρακολουθεί το ιστορικό κίνησης. Επίσης χρειάζεται να χειρίζεται διαφορετικά πρωτόκολλα μαζί (π.χ. TCP, UDP, ARP, ICMP, κ.λπ.). Ο ελεγκτής μπορεί να προκαλέσει έλεγχο πακέτου δίνοντας εντολή στα switches να στείλουν όλα τα πακέτα σε αυτό. Ωστόσο, υπάρχουν πολλές προκλήσεις στην εφαρμογή αυτού του χαρακτηριστικού. Για παράδειγμα, πραγματικά χρονικά σενάρια καθιστούν δύσκολη την παρατήρηση πολλών πακέτων πάνω από ένα χρονικό διάστημα. Η ανακατασκευή μιας πλήρους ροής ενδέχεται να μην είναι δυνατή δεδομένου ότι κάποιο περιεχόμενο μπορεί να αλλάξει σε όλο το δίκτυο μεταξύ εμπρός και αντίστροφης κυκλοφορίας ή λόγω της προώθησης. Η δυναμική αλλαγή της τοπολογίας κάνει την επαλήθευση των τρεχουσών / ιστορικών μεταβλητών πολύ περίπλοκη. Τα switches ενδέχεται να αλλάξουν δυναμικά ή να επαναπροσδιορίσουν κάποιες καταχωρήσεις κεφαλίδας όταν προωθούν πακέτα σε προορισμούς. Αυτά είναι μερικά παραδείγματα των προκλήσεων και των ανοιχτών ερευνητικών τομέων σχετικά με τον τρόπο διεξαγωγής εργασιών τείχους προστασίας με κατάσταση με βάση το SDN.

Μια ολοκληρωμένη επιθεώρηση πακέτων στο σύνολο του δικτύου μπορεί να συμβεί μόνο μέσω του ελεγκτή και όχι των switches. Παρέχονται πληροφορίες επιπέδου πακέτου στον ελεγκτή με περιορισμένη πρόσβαση. Τα επίπεδα προώθησης είναι χωρίς κατάσταση και χωρίς τον ελεγκτή να παρακολουθεί ενεργά τις ροές επιθεώρησης με κατάσταση είναι αδύνατο.

Τα τείχη προστασίας με κατάσταση μπορούν να χρησιμοποιηθούν για τον εντοπισμό επιθέσεων ασφαλείας. Οι (Katta Naga Praven, 2012) παρουσίασαν το Flog, στο οποίο μία εφαρμογή τείχους προστασίας σε κατάσταση ελέγχου μπορεί να δημιουργηθεί χρησιμοποιώντας γλώσσες προγραμματισμού, σε λίγες γραμμές. Χρησιμοποίησαν τείχη προστασίας σε κατάσταση ελέγχου για τον εντοπισμό πιθανών κακόβουλων κωδικών από εσωτερικούς χρήστες. Ωστόσο, η προσέγγισή τους αντιπροσωπεύει μόνο ένα μικρό παράδειγμα για το τι πρέπει ένα τείχος προστασίας να κάνει. Το Flog αποθηκεύει διευθύνσεις αποστολέων και παραληπτών και βεβαιώνει ότι οι εξωτερικοί χρήστες είναι αξιόπιστοι εάν είχαν λάβει προηγουμένως πακέτα από εσωτερικούς χρήστες του δικτύου.

Ο (Zhu Shuyong, 2014) εισήγαγε το SFA, αφαίρεση προώθησης σε κατάσταση ελέγχου στο επίπεδο δεδομένων SDN. Ο στόχος είναι η παροχή πακέτων σε κατάσταση ελέγχου για επεξεργασία δικτύου που μπορεί να απαιτεί πληροφορίες ανώτερων επιπέδων (L4-L7). Προτείνεται ένας επεξεργαστής προώθησης (FP) για την επέκταση της λειτουργικότητας του ελεγκτή SDN. Τα πακέτα προωθούνται σε αυτόν τον επεξεργαστή που θα εκτελέσει περαιτέρω επεξεργασία σε αυτά τα πακέτα, συμπεριλαμβανομένης της κατάστασης αποθήκευσης και επιθεώρησης. Η μονάδα FP μπορεί επίσης να αλληλεπιδράσει με συμβάντα ή ενεργοποιήσεις από τον ίδιο τον ελεγκτή, όπως αλλαγές που σχετίζονται με το δίκτυο ή την τοπολογία.

Ο (Stoenescu Radu, 2013) πρότεινε τη χρήση συμβολικής εκτέλεσης για τον έλεγχο των δικτύων σε κατάσταση ελέγχου. Ανέπτυξαν ένα εργαλείο που ονομάζεται Sym-Net για μοντελοποίηση βασικών middle-boxes. Ο έλεγχος του δικτύου σε κατάσταση ελέγχου μπορεί να βοηθήσει στη λήψη αποφάσεων τείχους προστασίας. Οι αποφάσεις αυτές δεν εξαρτώνται μόνο από τις πληροφορίες επιπέδων L2-L3 αλλά μπορεί να έχουν πληροφορίες από πιθανώς όλα τα επίπεδα του δικτύου. Ενώ οι πρόοδοι σε αυτόν τον τομέα είναι πολύ πρόωρες, ωστόσο, τα χαρακτηριστικά του SDN υπόσχονται την επέκταση και την πρόοδο σε αυτήν την περιοχή. Παρόμοια με τις περισσότερες προκλήσεις ασφαλείας που αντιμετωπίζουν οι λύσεις του SDN, η ευρωστία και η επεκτασιμότητα είναι σημαντικά ζητήματα. Στην περίπτωση των επιθεωρήσεων σε κατάσταση ελέγχου μεγάλοι πόροι μνήμης, χώρος αποθήκευσης και όλοι οι πόροι του δικτύου είναι απαραίτητοι και αναγκαίοι για την διεξαγωγή επιθεώρησης σε κατάσταση ελέγχου σε ώριμα επίπεδα ή περιπτώσεις. Η έκρηξη της κατάστασης είναι επίσης μια άλλη πρόκληση. Εάν εξετάσουμε την κατάσταση δικτύου καθώς η κυκλοφορία ρέει και τους κανόνες στο δίκτυο, αυτό σημαίνει ότι οποιαδήποτε μεμονωμένη αλλαγή σε μία από αυτές τις ροές ή στα στοιχεία του δικτύου θα προκαλέσουν αλλαγή της κατάστασης. Αυτό μπορεί να παράγει μία τεράστια ποσότητα πιθανών καταστάσεων.

3.4.1.4 Υβριδικά τείχη προστασίας

Τα υβριδικά τείχη προστασίας αναφέρονται σε τείχη προστασίας που λειτουργούν σε ένα περιβάλλον με ανάμειξη SDN και παραδοσιακών δικτύων. Ο (Pan Heng, 2013) πρότεινε το FlowAdapter για τον χειρισμό ροών σε ετερογενή OpenFlow switches. Οι πίνακες ροής στα OpenFlow switches πρέπει να είναι σε θέση να ασχοληθούν με παλαιό hardware. Επιπλέον, κάποιοι τύποι πεδίου που υπάρχουν στους πίνακες ροής δεν έχουν ίσες δυνατότητες με τα παλαιά switches. Στην πραγματικότητα, το ίδιο το πρωτόκολλο OpenFlow εξελίσσεται καθώς οι προηγούμενες εκδόσεις έχουν 12 χαρακτηριστικά και οι νέες εκδόσεις έχουν 40. Πάντα υπάρχει ανάγκη για υποστήριξη συμβατότητας προς τα πίσω και ταυτόχρονα διασφάλιση ότι πολύτιμες πληροφορίες δεν χάθηκαν ή αγνοήθηκαν λόγω τέτοιου μετασχηματισμού. Οι προσαρμογείς είναι απαραίτητοι για την παροχή τέτοιου μετασχηματισμού δυναμικά.

Η διαδικασία μετατροπής ACL τείχους προστασίας από ένα σύστημα σε έναν άλλο ή από έναν τομέα στον άλλο μπορεί να είναι χρόνος κατανάλωσης. Συνήθως οι διαχειριστές ασφαλείας χρησιμοποιούν την έκφραση «Η λεπτομέρεια κάνει την διαφορά» για να δείξουν ότι το πραγματικά σύνθετο και χρονοβόρο μέρος της διαδικασίας δεν είναι το τεχνικό μέρος. Πρόσφατη έρευνα απέδειξε την μετεγκατάσταση του ACL τείχους προστασίας από τα παραδοσιακά δίκτυα στο SDN. Αυτές οι αναφορές αποδεικνύουν ότι η διαδικασία μπορεί να διαρκέσει λιγότερο χρόνο και προσπάθεια δεδομένης της δυνατότητας του SDN ή του δικτύου OpenFlow για αυτόματη αξιολόγηση των κανόνων πολιτικής.

Ο (Shin Seungwon, 2013) πρότεινε ένα πλαίσιο ασφαλείας για να επιτρέψει στα παλαιά συστήματα να αλληλεπιδρούν με το OpenFlow δίκτυο. Οι (Hand Ryan, 2013) εισήγαγαν την "ενεργή ασφάλεια" ως περιβάλλον προγραμματισμού για την διαμόρφωση και την αξιολόγηση των ρυθμίσεων του τείχους προστασίας. Επέκτειναν το Floodlight συνδέοντας το στον ανοιχτό κώδικα IDS Snort μαζί με κάποιες άλλες εφαρμογές. Η Ενεργή ανίχνευση σημαίνει συνδυασμός παρακολούθησης και πρόληψη ή ανίχνευση με προστασία. Ωστόσο, αυτή η αλληλεπίδραση μεταξύ Snort και SDN είναι πρωτόγονη και δεν συντονίζεται (δηλαδή καμία αλληλεπίδραση με τον πραγματικό χρόνο). Η έξοδος καταγραφής Snort εξάγεται όταν εμφανίζονται ειδοποιήσεις και στη συνέχεια προστίθεται ως είσοδος στον ελεγκτή. Σε τυπικά σύνθετα σενάρια, μεγάλες ανησυχίες θα σχετίζονται με την ακρίβεια ανίχνευσης και επίσης την απόδοση ή επιβάρυνση του δικτύου. Υπάρχουν μερικές άλλες δοκιμές για ενσωμάτωση του Snort με το OpenFlow. Η πρόκληση είναι ότι το SDN συλλέγει και εισάγει ροές σε μια δομή που δεν είναι συμβατή με την παραδοσιακή δικτύωση που υιοθετούν οι τρέχουσες εκδόσεις Snort.

3.4.2 Έλεγχος πρόσβασης

Το SDN είναι υποψήφιο για να προσφέρει λύση ευέλικτου και δυναμικού ελέγχου πρόσβασης. Ο (Casado Martin M. F., 2009) πρότεινε την αρχιτεκτονική Ethane SDN που επιτρέπει στους διαχειριστές να ενισχύσουν τα στοιχεία ελέγχου των κεντρικών υπολογιστών μέσω λεπτομερών πολιτικών ελέγχου πρόσβασης. Το Ethane αντιπροσωπεύει μία πρώιμη προσπάθεια στο SDN που ενέπνευσε το πρωτόκολλο OpenFlow και κεντρική διαχείριση του δικτύου ή παγκόσμιων πολιτικών. Το Ethane χρησιμοποίησε δίκτυα με βάση τη ροή και έναν κεντρικό ελεγκτή. Τα switches κατευθύνουν τις ροές στον ελεγκτή για τη λήψη αποφάσεων. Οι πολιτικές κρατούνται σε έναν κεντρικό ελεγκτή.

Εμπνευσμένοι από το Ethane, οι (Nayak Ankur, 2009) συζήτησαν τον δυναμικό έλεγχο πρόσβασης και την παρακολούθηση σε δίκτυα SDN. Ένα σύστημα ελέγχου πρόσβασης που ονομάζεται Resonance συνδέεται απευθείας με την παρακολούθηση σε πραγματικό χρόνο που μπορεί να επιταχύνει τον κύκλο από την λήψη ειδοποιήσεων στη λήψη ενεργειών. Το σύστημα ελέγχου πρόσβασης μπορεί να είναι πιο κοντά στα σημεία δράσης και μπορεί να ανταποκριθεί και να αναλάβει ενέργειες σε πραγματικό χρόνο με

βάση την τρέχουσα κυκλοφορία. Τα παραδοσιακά middle-boxes, όπως τα τείχη προστασίας, κ.λπ. συχνά τοποθετούνται στο άκρο του δικτύου. Η μελέτη έδειξε ότι το να ασχολείσαι με αλληλεπιδράσεις δυναμικού ελέγχου πρόσβασης στο SDN μπορεί να είναι ευκολότερο από ότι στα παραδοσιακά δίκτυα. Οι πολιτικές ελέγχου πρόσβασης επιβάλλονται βάσει των πληροφοριών επιπέδου ροής και ειδοποιήσεων σε πραγματικό χρόνο. Τα υποσυστήματα παρακολούθησης είναι ενσωματωμένα στον ελεγκτή για να βοηθήσουν στη διαδικασία ελέγχου πρόσβασης. Παρόμοια με το Ethane, ο ελεγκτής επιβάλλει ελέγχους πρόσβασης μέσω πολιτικών που είναι εγκατεστημένοι σε switches.

Ο (Wen Xitao, 2013) πρότεινε το PermOF, ένα λεπτομερές σύστημα ελέγχου πρόσβασης σε SDN. Ο κύριος στόχος είναι να εξασφαλιστεί ο ελεγκτής και η ασφαλής επικοινωνία με τον ελεγκτή. Το PermOF περιλαμβάνει μια λίστα με 18 πιθανά επίπεδα άδειας ελαχιστοποιώντας την πιθανή εισβολή ή την κλιμάκωση προνομίων. Το σύστημα αδειών συνδυάζεται με απομόνωση χρόνου εκτέλεσης (μεταξύ ελεγκτή και εφαρμογών). Προσφέρει τουλάχιστον μια προεπιλογή δικαιώματος προνομίων για εφαρμογές OpenFlow. Η δυνατότητα να απομονώσει επιτυχημένα τις εφαρμογές από τον ελεγκτή είναι κλειδί για την εφαρμογή τέτοιων προσεγγίσεων.

Οι (Yamasaki Yashuiro, 2011) πρότειναν μια λύση SDN βασισμένη στο VLAN για δίκτυα πανεπιστημίων. Εκτός από το πρόβλημα των αναγνωριστικών VLAN, οι συγγραφείς ανέφεραν ένα γενικό πρόβλημα που σχετίζεται με τον εκτεταμένο χρόνο που απαιτείται για την εφαρμογή και τη συντήρηση της βάσης δεδομένων του VLAN. Η λειτουργική μονάδα Access Management Function (AMF) προστέθηκε για την παρακολούθηση και τον έλεγχο ταυτότητας χρηστών ή κεντρικών υπολογιστών. Το σύστημα αξιολογήθηκε με 10.000 αναγνωριστικά. Οι αξιολογήσεις έδειξαν ότι η λύση βασισμένη στο SDN μπορεί να ξεπεράσει την παραδοσιακή λύση. Η λύση SDN είναι επίσης δυναμική και αναμένεται να μειώσει ένα σημαντικό ποσό των γενικών εξόδων συντήρησης.

Ο (Kinoshita Shunichi, 2012) πρότεινε μια προσέγγιση για τον έλεγχο πρόσβασης βασισμένο στο OpenFlow και το σύστημα ελέγχου ταυτότητας για ασύρματο δίκτυο πανεπιστημιουπόλεων. Επισήμαναν δύο περιορισμούς στην (Yamasaki Yashuiro, 2011) προσέγγιση και πρότειναν βελτιώσεις σχετικά με αυτούς τους περιορισμούς. Ο πρώτος περιορισμός σχετίζεται με την αδυναμία του προηγούμενου συστήματος να λειτουργεί σε λειτουργία ελέγχου ταυτότητας ανώνυμου χρήστη. Ο δεύτερος περιορισμός σχετίζεται με το κόστος συντήρησης των βάσεων δεδομένων των χρηστών. Αντί να αντιμετωπίζουν κάθε άτομο ξεχωριστά, μπορούν να συγκεντρωθούν σε ομάδες και ο έλεγχος ταυτότητας μπορεί να δημιουργηθεί με βάση τις ομάδες χρηστών. Αυτό μπορεί να μειώσει το μέγεθος της βάσης δεδομένων που χρειάζεται το σύστημα ελέγχου ταυτότητας να αναζητήσει. Το σύστημα ελέγχου ταυτότητας δεν χρειάζεται να αναζητά ονόματα, αλλά για ομάδες που μπορούν επίσης να βοηθήσουν στην αντιμετώπιση ανώνυμων χρηστών.

Οι (Wu Yong-juan, 2013) συζήτησαν προγραμματιζόμενα εικονικά δίκτυα (PVN) στο cloud με βάση την απομόνωση της MAC. Ένας διακομιστής PVN προτείνεται στο OpenStack να λειτουργεί ως ελεγκτής OpenFlow. Οι τοπικοί agents παραδίδονται στο

δίκτυο για την υποστήριξη του ελεγκτή PVN για να φιλτράρουν την κίνηση με βάση τις διευθύνσεις MAC.

3.4.3 IDS / IPS

Τα συστήματα ανίχνευσης / προστασίας εισβολής (IDS / IPS) σταματούν ή επιτρέπουν πακέτα βασισμένα σε διεξοδική διερεύνηση πακέτων που χρησιμοποιούν εξόρυξη δεδομένων, αναγνώριση προτύπων, αντιστοίχιση υπογραφών με υπάρχουσα απογραφή απειλών, κ.λπ. Σε αντίθεση με τα παραδοσιακά IDS, το SDN IDS μπορεί να αξιοποιήσει την τεράστια ποσότητα πληροφοριών ροής σε πραγματικό χρόνο. Το SDN μπορεί να αλλάξει τον τρόπο που οι μηχανισμοί ασφαλείας διανέμονται. Για παράδειγμα, υπάρχει ένα IDS σε μία τοποθεσία στα παραδοσιακά δίκτυα (συνήθως στις εγκαταστάσεις του δικτύου). Στο SDN, οι εργασίες IDS μπορούν να διανεμηθούν μέσω των switches ή agents στο δίκτυο. Ο ελεγκτής ή μία από τις μονάδες του μπορεί να ενορχηστρώσει τη διαδικασία.

3.4.3.1 Ενσωμάτωση με παραδοσιακά εργαλεία

Πρόσφατη έρευνα προσπάθησε να ενσωματώσει ορισμένα δημοφιλή IDS όπως το Snort με SDN. Η ενσωμάτωση του Snort στο SDN αντιμετωπίζει πολλές προκλήσεις. Ο ελεγκτής SDN λαμβάνει συνήθως δείγματα και όχι πλήρεις ροές που έρχονται σε αντίθεση με τον τρόπο λειτουργίας του Snort. Ένας κοινός τρόπος ρύθμισης των πραγμάτων για τον ελεγκτή είναι να λάβει το πρώτο πακέτο ή τα πρώτα λίγα πακέτα μιας δεδομένης ροής. Μόλις τα παραλάβει, ο ελεγκτής εγκαθιστά κανόνες στα switches που θα χειριστούν τα υπόλοιπα πακέτα σε αυτή τη ροή. Αυτό γίνεται επειδή συνήθως η αποστολή κάθε πακέτου στον ελεγκτή δεν είναι πρακτική. Δεδομένου ότι το Snort αναμένει να δει κάθε πακέτο σε ροή, δεν θα μπορούμε να βάλουμε το Snort στον ελεγκτή αποτελεσματικά χωρίς να επηρεαστεί σε μεγάλο βαθμό η απόδοση και η δομή του δικτύου OpenFlow. Ένας εναλλακτικός σχεδιασμός θα ήταν να δημιουργηθεί μία υπηρεσία στον ελεγκτή για τη διαχείριση ενός συνόλου μηχανών που λειτουργούν το Snort και να εγκαταστήσουν κανόνες που ανακατευθύνουν την κυκλοφορία στα μηχανήματα που τρέχουν το Snort.

Το Snort έχει τους δικούς του περιορισμούς όσον αφορά τον τύπο επιθέσης που μπορεί να ανιχνεύσει. Ενώ είναι ένας καλός ανοιχτός κώδικας το IPS / IDS (με μια γλώσσα βασισμένη σε κανόνες που συνδυάζει υπογραφή, πρωτόκολλο και επιθεώρηση με βάση την ανωμαλία), το Snort εξακολουθεί να βασίζεται στην τακτική ενημέρωσης υπογραφών. Δεν έχει κανέναν τρόπο να εντοπίσει εκμεταλλεύσεις υψηλότερου επιπέδου όπως εκμεταλλεύσεις ιστού (π.χ. κακόβουλα σενάρια Java). Το Snort ίσως δεν βοηθάει επίσης σε επιθέσεις όπως: Προχωρημένες Επίμονες Απειλές (APT). Το SDN και το Snort διαφέρουν επίσης στον τρόπο που συλλέγουν, ανακατευθύνουν και παρακολουθούν την

κυκλοφορία. Στην παραδοσιακή δικτύωση οι πόρτες span χρησιμοποιούνται για την αναδρομολόγηση της κυκλοφορίας για παρακολούθηση ή ασφάλεια των εφαρμογών. Στο SDN, τα δεδομένα μπορούν να εξαχθούν από τον ελεγκτή μέσω API προς βορρά. Τα φίλτρα μπορούν να εφαρμοστούν στο SDN για εξαγωγή κυκλοφορίας βάσει συγκεκριμένων κριτηρίων και εντολών του ελεγκτή για να ξαναγράψουν την κυκλοφορία με βάση αυτά τα κριτήρια.

Οι (Xing Tianyi, 2013) διερεύνησαν την ενσωμάτωση του Snort με δίκτυα OpenFlow. Το SnortFlow είναι ικανό να αναδιαμορφώσει το σύστημα cloud εν κινήσει για τον εντοπισμό και την αντιμετώπιση των εισβολών. Αυτή η εργασία ήρθε ως επέκταση ή βελτίωση για το σύστημα NICE. Χρησιμοποιεί το Snort για συντονισμένες επιθέσεις ανίχνευσης. Το SnortFlow περιλαμβάνει τρία στοιχεία: Ένα daemon για τη συλλογή δεδομένων ειδοποιήσεων από τον πράκτορα Snort, έναν διερμηνέα ειδοποιήσεων για να αναλύει τις ειδοποιήσεις και να αποφασίζει ποια κυκλοφορία θα στοχεύσει και τέλος μία γεννήτρια κανόνων που θα εισάγει κανόνες σε OpenFlow switches. Οι αλλαγές που προκαλούνται από τους νέους κανόνες αποθηκεύονται για να είναι δυνατή η επαναφορά ή η αποκατάσταση. Τα αντίμετρα που πρέπει να ληφθούν ταξινομούνται με βάση το κόστος και την εισβολή. Πρέπει να γίνει προσεκτική εξέταση με το κατάλληλο αντίμετρο για να ληφθεί ότι δεν θα υπάρχουν διακοπές στις κανονικές λειτουργίες.

Η FRESCO και το διάδοχο έργο της SE-Floodlight (Shin Seungwon, 2013) παρήγαγε διάφορες εφαρμογές ασφαλείας που σχετίζονται με το SDN. Μία από αυτές τις πρόσφατες επεκτάσεις είναι το FlowBoss. Το FlowBoss φιλοξενείται στο SE-Floodlight και μιμείται το OpenFlow με ότι κάνει το Snort σε παραδοσιακά δίκτυα. Οι πολιτικές δικτύου μπορούν να ορίζονται για την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Οι πολιτικές μπορούν επίσης να ορίζονται για να οριοθετούν την κυκλοφορία σε συγκεκριμένες ώρες ή να φιλτράρουν την κυκλοφορία με βάση ορισμένα χαρακτηριστικά.

3.4.3.2 Εφαρμογή του SDN IDS

Οι (Goodney Andrew, 2010) παρουσίασαν μια υλοποίηση βάσει στο SDN NIDS στην πλατφόρμα δικτύωσης NetFPGA. Μπορεί να χρησιμοποιείται για τη δοκιμή αλγορίθμων FPGA για Βαθιά επιθεώρηση πακέτων (DPI) ή για υψηλής ταχύτητας προγραμματιζόμενη επεξεργασία πακέτων. Η μονάδα μπορεί να πραγματοποιήσει ανίχνευση εισβολής δικτύου μέσω DPI.

Οι (Skowyra Rick, 2013) συζήτησαν το NIDS με βάση το OpenFlow στις ενσωματωμένες κινητές συσκευές και στα Κυβερνο-Φυσικά Συστήματα (CPS). Οι εφαρμογές ή οι περιπτωσιολογικές μελέτες περιλαμβάνουν ρομποτική μεταφορά και βιοϊατρικές συσκευές καθώς έχουν παρόμοια μοντέλα απειλής. Γενικά, οι κινητές συσκευές υπόκεινται σε επιθέσεις εντός του εύρους κάλυψης της συσκευής (π.χ. μόντεμ, Wi-Fi ή Bluetooth). Η κρυπτογράφηση συνήθως προτείνεται ως ο κύριος μηχανισμός ασφαλείας για την εξάλειψη τέτοιων επιθέσεων. Ωστόσο, για μερικές μικρές εμπορικές εφαρμογές, ισχυρές μέθοδοι κρυπτογράφησης μπορεί να είναι ανέφικτες ή ακριβές. Μηχανισμοί ασφαλείας βάσει τοποθεσίας ενδέχεται να μην προστατεύονται από τοπικούς

ή εσωτερικούς χρήστες. Προτεινόμενα IDS ή το Learning IDS (L-IDS) μπορεί να χρησιμοποιηθούν για την υποστήριξη κρυπτογράφησης ή μηχανισμών ασφαλείας βάσει τοποθεσίας. Οι ανωμαλίες ορίζονται με βάση διάφορα χαρακτηριστικά: Αποστολή πακέτων, θέση, ώρα, μέγεθος κ.λπ. Για κάθε ένα από αυτά τα χαρακτηριστικά, το κανονικό εύρος καθορίζεται. Η απόκλιση από αυτό το κανονικό εύρος μπορεί να ταξινομηθεί ως ανωμαλία.

Ο (Michael., 2012) αντιπροσωπεύει την εμπειρία του Πανεπιστημίου της Ιντιάνα με τη δημιουργία ενός (Συστήματος προστασίας από εισβολές) IPS με βάση το SDN. Τα κύρια πλεονεκτήματα του νέου συστήματος σχετίζονταν με το φορτίο εξισορρόπησης και την ικανότητα του δικτύου να χειρίζεται και να διανέμει την κυκλοφορία βάσει ελέγχων ασφαλείας. Η καθολική πολιτική βασισμένη στην διαχείριση ασφάλειας δικτύου είναι ένας άλλος σημαντικός στόχος που αναμένεται να επιτύχει το IPS με βάση το SDN.

Οι (Giotis K, 2014) πρότειναν να συνδυάσει το OpenFlow με το sFlow για βελτίωση της ανίχνευσης ανωμαλιών με βάση τη ροή. Τα στατιστικά στοιχεία ροής μπορεί να είναι μια καλή πηγή για τον έλεγχο πιθανής ανωμαλίας των συμπεριφορών στο δίκτυο. Η συλλογή στατιστικών δεδομένων μέσω του ελεγκτή αντιμετωπίζει ένα σοβαρό ζήτημα κλιμάκωσης. Συνεπώς υπάρχουν πολλές ερευνητικές προτάσεις για την ανάθεση αυτού του έργου σε μία ξεχωριστή υποστηρικτική ενότητα. Οι (Giotis K, 2014) διεξήγαγαν μία μελέτη με υψηλά ποσοστά πακέτων (έως 130.000 πακέτα ανά δευτερόλεπτο). Οι πληροφορίες ροής που συλλέγονται βασίζονται σε ένα υποσύνολο χαρακτηριστικών από την παλιά έκδοση του OpenFlow που περιλαμβάνει μόνο 12 χαρακτηριστικά. Αξιολόγησαν τη συλλογή δεδομένων με βάση τα εγγενή OpenFlow και επίσης χρησιμοποιώντας το sFlow. Οι εγγενείς μέθοδοι μπορούν να εφαρμόζονται σε κυκλοφορία χαμηλού έως μεσαίου μεγέθους. Αυτό συμβαίνει επειδή υπάρχουν μερικοί περιορισμοί στο μέγεθος των καταχωρήσεων ροής στους πίνακες ροής των switches. Η προσέγγιση sFlow αποσυνδέει τη διαδικασία συλλογή ροής από τη λογική προώθηση όπου τα δείγματα πακέτων παρέχουν όλες τις απαραίτητες πληροφορίες. Αυτό μπορεί να δείξει μία σημαντική μείωση του μεγέθους.

Η παραπάνω εργασία επικεντρώθηκε σε πληροφορίες που σχετίζονται με L2-L3 επίπεδα χωρίς να κοιτάξουμε το περιεχόμενο των πραγματικών πακέτων. Οι (Shirali-Shahreza and Ganjali Sajad Yashar., 2013) πρότειναν επέκταση στο τρέχον πρωτόκολλο OpenFlow για να επιτρέπεται στον ελεγκτή να έχει πρόσβαση στα περιεχόμενα των πακέτων. Οι τρέχουσες πληροφορίες που ανταλλάσσονται μεταξύ του ελεγκτή και των switches σχετίζονται σε μεγάλο βαθμό με τις πληροφορίες δρομολόγησης. Στόχος είναι η χρήση τέτοιων πληροφοριών για ασφάλεια εφαρμογών συμπεριλαμβανομένων των NIDS / NIPS ή εργαλείων ανίχνευσης ανωμαλιών. Σε ορισμένες περιπτώσεις, τα δείγματα και όχι η πλήρης κυκλοφορία αποστέλλονται στον ελεγκτή. Διαφορετικές μέθοδοι δειγματοληψίας (π.χ. ντετερμινιστική ή στοχαστική δειγματοληψία) μπορεί να ζητηθεί από τον ελεγκτή με βάση τη φύση της εφαρμογής ασφαλείας ή του middle-box. Τα πλήρη πακέτα ζητούνται μόνο κάτω από ορισμένες συνθήκες.

3.4.4 Πολιτικές SDN

Το SDN αναμένεται να διευκολύνει την αυτόματη διαμόρφωση, την αξιολόγηση και την επιβολή πολιτικών δικτύου. Ενώ οι πολιτικές στα παραδοσιακά δίκτυα ενσωματώνονται σε τείχη προστασίας και τις ACLs τους, το SDN επιτρέπει πολιτικές σε διαφορετικά επίπεδα. Έτσι, διαχωρίζουμε τη συζήτησή μας σχετικά με τις πολιτικές SDN από αυτές στα τείχη προστασίας.

Οι πολιτικές που ρυθμίζουν τις λειτουργικές δραστηριότητες θεωρούνται οδηγίες υψηλού επιπέδου που μπορούν να μεταφραστούν και να εφαρμοστούν από μηχανισμούς ασφαλείας χαμηλού επιπέδου, όπως τείχη προστασίας, διακομιστές μεσολάβησης κ.λπ. Παραδοσιακά, η μετάφραση από πολιτικές υψηλού επιπέδου σε συγκεκριμένους μηχανισμούς ασφαλείας διεξάγεται συνήθως χειροκίνητα από τους διαχειριστές δικτύου. Το SDN προσφέρει μια νέα ευκαιρία για πολιτικές ασφαλείας προς ερμηνεία, ενημέρωση, αξιολόγηση και επιβάλλεται από αυτόματα εργαλεία με ελάχιστη ανθρώπινη παρέμβαση.

3.4.4.1 Γλώσσες πολιτικής SDN

Οι γλώσσες πολιτικής έχουν προταθεί για τη σύνταξη επίσημων ή ημι-επίσημων πολιτικών. Ο κύριος στόχος είναι να γεφυρωθεί το χάσμα μεταξύ δύο διαφορετικών επιπέδων αφαίρεσης: ανθρώπινες φυσικές γλώσσες στις οποίες οι διαχειριστές αρχίζουν να γράφουν υψηλού επιπέδου πολιτικές και κανόνες χαμηλού επιπέδου που οι μηχανές μπορούν να κατανοήσουν ή να ερμηνεύσουν.

Ο (Hinrichs Timothy, 2008) πρότεινε την Γλώσσα Διαχείρισης βάσει ροής (FML) για να εκφράσει λίστες πρόσβασης και πολιτικές για ελεγκτή NOX. Το ίδιο το FML βασίζεται στο DATALOG, μία δηλωτική λογική γλώσσα που χρησιμοποιείται σε σύνδεση με βάσεις δεδομένων. Στον πυρήνα των πολιτικών υπάρχουν κανόνες και λίστες ελέγχου πρόσβασης (ACL). Η επιβολή της πολιτικής εφαρμόζεται με απόφαση δέντρου για να επιτευχθεί ο σωστός κανόνας αντιστοίχισης για την τρέχουσα ροή ή το πακέτο με βάση τους κανόνες στον πίνακα ροής και / ή το τείχος προστασίας. Το FML διατηρεί καταστάσεις που σχετίζονται με λίστες χρηστών και τις συσκευές ή τους κεντρικούς υπολογιστές τους. Λαμβάνεται τότε απόφαση ελέγχου πρόσβασης με βάση τις τιμές αυτών των πεδίων ροής ή των χαρακτηριστικών. Εκτός από την «αποδοχή» και την «άρνηση», υπάρχουν και άλλες αποφάσεις στο FML: Τα σημεία, η αποφυγή και το όριο τιμών. Σημεία ή σημεία αναφοράς ορίζονται για να επισημάνουν ορισμένα γνωστά σημεία (π.χ. υπολογιστές, έναν διακομιστή, μια πύλη). Τα «σημεία» και η «αποφυγή» είναι αντίθετα το ένα στο άλλο (δηλαδή για την αναδρομολόγηση της κυκλοφορίας ή για παράλειψη αυτών των σημείων του δικτύου). Το όριο τιμής υποδεικνύει έναν περιορισμό τιμής στην κυκλοφορία.

Για τη βελτίωση της εκφραστικότητας στις πολιτικές δικτύου και ασφάλειας, οι (Voellmy Andreas, 2012) εισήγαγαν το Procera, μια αρχιτεκτονική ελέγχου που περιλαμβάνει μια δηλωτική πολιτική γλώσσας που βασίζεται στον λειτουργικό αντιδραστικό προγραμματισμό. Το Procera προσπαθεί να βοηθήσει σχεδιαστές δικτύου

για την εφαρμογή εκφραστικών πολιτικών χωρίς την ανάγκη χρήσης γλωσσών προγραμματισμού. Το Procera περιλαμβάνει σήματα και λειτουργίες σήματος ως αντιδραστικές έννοιες. Τα σήματα είναι όπως οι παροδικές συναρτήσεις όπου οι συναρτήσεις συνδέονται με ένα χρονικό διάστημα. Οι συναρτήσεις ή οι κατασκευές σήματος προκαλούν μετασχηματισμούς στα σήματα. Υπάρχουν και άλλα ερευνητικά έγγραφα που σχετίζονται με τον προγραμματισμό και το προγραμματισμός δικτύου. Οι Voellmy και Hudak, 2011 συζήτησαν παραδείγματα εφαρμογών που χρησιμοποιούν προγραμματισμό δικτύου συμπεριλαμβανομένου ενός switch εκμάθησης και παρακολούθησης της κυκλοφορίας των εφαρμογών. Οι (Kim Hyojoon, Feamster Nick., 2013) επέκτειναν το έργο του Procera και περιέγραψαν πώς μπορεί να βοηθήσει στη διαχείριση του δικτύου. Κύριος στόχος ήταν να προτείνουν μια λύση που μπορεί να συμβιβαστεί μεταξύ της ανάγκης για πλούσιο και εκφραστικό υψηλό επίπεδο χαρακτηριστικών πολιτικής και ταυτόχρονα την ανάγκη αλληλεπίδρασης λεπτομερειών χαμηλού επιπέδου στα switch ή του επιπέδου στοιχείων δικτύωσης. Ο (Anderson Carolyn Jane, 2014) πρότεινε την γλώσσα προγραμματισμού δικτύου NetKAT βασισμένη σε μια μαθηματική δομή που ονομάζεται άλγεβρα Kleene με δοκιμές (KAT). Το NetKAT μπορεί να χρησιμοποιηθεί για να εκφράσει απαιτήσεις του OpenFlow μέσω προσθήκης και αλληλεπίδρασης με ροές. Παρέχει άλγεβρα υψηλού επιπέδου για περίπλοκους συλλογισμούς και αναζήτηση των ροών.

3.4.4.2 Ασφάλεια στο SDN και δικτυακές πολιτικές

Οι (Casado, Freedman, Pettit, & Luo, 2007) περιέγραψαν τις αλληλεπιδράσεις μεταξύ του ελεγκτή και πολιτικών ασφαλείας ως κανόνες που εισάγονται από τον ελεγκτή στα switches. Αυτοί ωστόσο χρησιμοποιούσαν παραδοσιακές ACL. Ο (Nayak Ankur, 2009) πρότεινε τον μηχανισμό ασφάλειας Resonance για αξιολόγηση ελέγχου δυναμικής πρόσβασης βάσει πληροφοριών για το επίπεδο ροής. Ο συντονισμός αλληλεπιδρά με πολιτικές υψηλού επιπέδου για τη λήψη αποφάσεων σχετικά με τις ροές. Χρησιμοποιεί μια πολιτική πλαισίου προδιαγραφών που βασίζεται στην παραδοσιακή ή τα υπάρχοντα πλαίσια πρόσβασης ελέγχου.

Οι (Feamster., 2010) χρησιμοποίησαν το OpenFlow για την επίλυση της πολιτικής προβλημάτων στα δίκτυα πανεπιστημίων και επιχειρήσεων. Αντιμετώπισαν δύο προκλήσεις: τους ελέγχους πρόσβασης και ροής πληροφοριών. Το χάσμα μεταξύ των εκφραστικών πολιτικών υψηλού επιπέδου και ελέχγου πρόσβασης χαμηλού επιπέδου που υπάρχει στα switches ή τα τείχη προστασίας εξακολουθούν να είναι σοβαρή πρόκληση για τους διαχειριστές στην αντιμετώπιση μεγάλων δικτύων. Για τον έλεγχο ροής πληροφοριών, οι παραδοσιακές προσεγγίσεις βασίζονται στους υπολογιστές. Εάν ο κεντρικός υπολογιστής είναι σε κίνδυνο, η ροή πληροφοριών μπορεί να βγει εκτός ελέγχου.

Οι (Wang Xiang, 2012) παρουσίασαν μια αρχιτεκτονική διαχείρισης ασφάλειας με διαδραστική επιβολή πολιτικής. Η εκδοχή του ελεγκτή υποστηρίζεται με έναν πίνακα πολιτικής που αλληλεπιδρά με πακέτα ενώ διασχίζουν το δίκτυο. Η απόδοση μπορεί να είναι ένα ζήτημα εδώ ειδικά καθώς εφαρμόζεται το μοντέλο σε δίκτυο μικρού μεγέθους με μόνο 50 χρήστες. Χρησιμοποίησαν διαφορετικά στοιχεία υπηρεσίας ασφαλείας, όπως: IDS, πρωτόκολλο αναγνώρισης, σάρωση ιών, εξισορρόπηση φορτίου, παρακολούθηση κυκλοφορίας και επιθεώρηση περιεχομένου. Οι (Son Sooel, 2013) εισήγαγαν το σύστημα ελέγχου μοντέλου Flover για την επαλήθευση της ροής που βασίζεται στις OpenFlow πολιτικές. Επικεντρώθηκαν στη δοκιμή για δυνατότητα παράκαμψης ή να ελέγξουν ότι οι τρέχουσες ροές συμμορφώνονται με τους κανόνες του τείχους προστασίας. Επέκτειναν παλαιότερες προσεγγίσεις συμπεριλαμβάνοντας νέες δυνατότητες όπως το «set» και το «goto».

Η μετεγκατάσταση πολιτικής από τα παραδοσιακά δίκτυα στο SDN ήταν επίσης το αντικείμενο πολλών ερευνητικών εργασιών. Η μετεγκατάσταση πολιτικής θεωρείται ένα άλλο πλεονέκτημα για τη χρήση του SDN όπου αναμένεται ότι η διαδικασία μετεγκατάστασης πολιτικών καταναλώνεται σε λιγότερο χρόνο στο SDN σε σύγκριση με τα παραδοσιακά δίκτυα. Παραδοσιακά, η διαδικασία μετεγκατάστασης που εφαρμόζεται χειροκίνητα μπορεί να πάρει πολύ ώρα και η ανθρώπινη δύναμη είναι ειδική για την αντιμετώπιση παρωχημένων ή αντικρουόμενων κανόνων.

3.4.4.3 Επιβολή πολιτικής

Η αυτόματη επιβολή των πολιτικών ασφαλείας είναι ένα σημαντικό έργο που μπορεί να επιτύχει το SDN. Οι (Bellessa John, 2011) παρουσίασαν μία προσέγγιση για τη δυναμική επιβολή πολιτικών επιπέδου ροής στα cloud δίκτυα. Οι πολιτικές γράφονται από διαχειριστές σε υψηλού επιπέδου γλώσσες. Αυτές οι πολιτικές ερμηνεύονται στη συνέχεια από το σύστημα αξιολόγησης της πολιτικής και παρακολούθησης της συμμόρφωσης (ODESSA) με βάση τα στοιχεία του δικτύου και τις πραγματικές ροές. Με άλλα λόγια, το ODESSA είναι υπεύθυνο για τη μεταφορά αφηρημένων πολιτικών στην συγκεκριμένη εφαρμογή με βάση τις προδιαγραφές δικτύου.

Οι (Fayaz Seyed, 2013) επικεντρώθηκαν στο θέμα της συνεπούς επιβολής πολιτικής και παρακολούθηση ροής. Στη δική τους προτεινόμενη βελτίωση στην αρχιτεκτονική SDN, πρότειναν να προσθέσουν πληροφορίες με βάση τα συμφραζόμενα στις ροές. Στην παρούσα πρόταση το μεσαίο πλαίσιο του νότιου ελεγκτή θα προσθέτει ετικέτες στα εξερχόμενα πακέτα όπου αυτές οι ετικέτες μπορούν να χρησιμοποιηθούν για συστηματική επιβολή πολιτικής. Προς το παρόν το OpenFlow είναι το μόνο τυπικό πρωτόκολλο στην επικοινωνία του νότιου ελεγκτή. Οι εφαρμογές ενδέχεται να αλλάξουν δυναμικά τις κεφαλίδες των πακέτων. Οι τροποποιήσεις των κεφαλίδων ενδέχεται να έχουν αρνητικό αντίκτυπο στην επιβολή πολιτικής και ενδέχεται να παραπλανήσουν τη διαδικασία που επιβάλλει πολιτικές. Σε ορισμένες περιπτώσεις, η ίδια εφαρμογή που υποτίθεται ότι εκτελεί την επιβολή πολιτικής ενδέχεται να αλλάξει αυτές τις κεφαλίδες και κατά συνέπεια να κάνει τη διαδικασία δύσκολη από μόνη της.

Ο (Qazi Zafar, 2013) πρότεινε ένα στρώμα μεσαίου πλαισίου για να αντιμετωπίσει την καθοδήγηση της κίνησης για αυτά τα middle-boxes. Ένας μηχανισμός συσχέτισης ροής προτείνεται για την αντιμετώπιση του προβλήματος της μετεγκατάστασης των πακέτων που αναφέρεται στην προηγούμενη έρευνα (Fayaz Seyed, 2013). Υπάρχει μία προτεινόμενη λύση που ονομάζεται SIMPLE, η οποία προσπάθησε να αντιμετωπίσει την υπάρχουσα αρχιτεκτονική OpenFlow και τους περιορισμούς. Αυτή η λύση αντιπροσωπεύει ένα επίπεδο επιβολής πολιτικής για τη διαχείριση της επικοινωνίας μεταξύ των middle-boxes και του επιπέδου δεδομένων. Αυτός ο σχεδιασμός, ωστόσο, επιβάλλει έναν ελεγκτή ειδικού σκοπού για αλληλεπίδραση με switches και middle-boxes. Ωστόσο, δεν είναι σαφές πώς αυτός ο ελεγκτής ειδικού σκοπού πρόκειται να επικοινωνήσει, με το πρωτόκολλο OpenFlow και με τον κύριο ελεγκτή.

3.4.5 Παρακολούθηση και έλεγχος

Η παρακολούθηση και ο έλεγχος είναι πολύ σημαντικά εργαλεία για πολλούς ελέγχους ασφαλείας. Μια σημαντική ευκαιρία στα δίκτυα SDN σχετίζεται με τον αριθμό των λεπτομερειών που μπορούν να συγκεντρωθούν στη ροή και ακόμη και στο επίπεδο πακέτου. Ήταν δύσκολο η κατανάλωση πόρων να επιτευχθεί σε παραδοσιακά δίκτυα IP.

3.4.5.1 Εργαλεία παρακολούθησης της κυκλοφορίας

Ο (Nayak Ankur, 2009) πρότεινε το συντονισμό (Resonance), μία λύση με βάση το OpenFlow που παρέχει συνεχή παρακολούθηση που διανέμεται σε όλο το δίκτυο. Στοιχεία δικτύου ή switches προωθούν την κυκλοφορία στον ελεγκτή. Ως πρώιμη συνεισφορά στο OpenFlow, η φύση της αρχιτεκτονικής OpenFlow ή η ροή της διαδικασίας μπορεί να βοηθήσει, φυσικά, τη διαδικασία παρακολούθησης.

Ο (Ballard Jeffrey, 2010) πρότεινε το OpenSAFE (Ανοικτός έλεγχος ασφάλειας και εξέταση ροής). Αυτό είναι ένα εργαλείο που αξιοποιεί το SDN για βελτίωση της παρακολούθησης δικτύου. Τα εργαλεία παρακολούθησης χρησιμοποιούν τις πόρτες Span για τη δημιουργία αντιγράφων της κίνησης δικτύου για σκοπούς παρακολούθησης. Συνήθως τα εργαλεία δικτύου επιτρέπουν ένα περιορισμένο αριθμός πορτών Span. Οι μονάδες τείχους προστασίας και τα IDS στα παραδοσιακά δίκτυα χρησιμοποιούν συνήθως μία ή περισσότερες από αυτές τις πόρτες Span. Αυτό συμβαίνει γιατί αυτά τα εργαλεία παρακολούθησης προκαλούν σημαντική επιβάρυνση του δικτύου εάν εφαρμόζονται πλήρως. Τα φίλτρα που χρησιμοποιούνται για αναδρομολόγηση της κυκλοφορίας μπορεί να μοιάζουν με αυτούς τους κανόνες τείχους προστασίας ή τους πίνακες ροής. Μπορούν να κατασκευαστούν χρησιμοποιώντας τα ίδια πεδία αντιστοίχισης ή τα ίδια χαρακτηριστικά. Ωστόσο, θα πρέπει να υπάρχουν πιο εκφραστικά εργαλεία / μηχανισμοί για την ανακατασκευή πακέτων από αυτά που είναι διαθέσιμα στο τείχος προστασίας ή στον πίνακα των κανόνων ροής. Περιλαμβάνουν μαθηματικές

πράξεις όπως μικρότερο από, μεγαλύτερο από και επιλογές ταξινόμησης που σχετίζονται με τη συλλογή, το ερώτημα και στατιστικά στοιχεία κίνησης. Με τη χρήση του δικτύου OpenFlow, το OpenSAFE μπορεί να κατευθύνει την εκτεταμένη κίνηση με αυθαίρετους τρόπους ενώ τέτοια κυκλοφορία μπορεί να χρησιμοποιηθεί από πολλές ταυτόχρονες υπηρεσίες ή ελέγχους ασφαλείας όπως το IDS και τα τείχη προστασίας.

Ο (Karame, 2013) επικεντρώθηκε σε θέματα ασφάλειας σε εργαλεία μέτρησης του δικτύου και την επίδραση των OpenFlow switches. Οι έρευνες των συγγραφέων έδειξαν ότι τα περισσότερα εργαλεία μέτρησης δεν αναπτύσσονται έχοντας κατά νου την ασφάλεια. Οι από άκρο σε άκρο μετρήσεις εμπιστεύονται τους υπολογιστές και αγνοούν τις πιθανές απειλές στους εσωτερικούς χρήστες ή απειλές που θέτουν σε κίνδυνο τους κεντρικούς υπολογιστές. Ο συγγραφέας ανέλυσε πολλά παραδείγματα απειλών για την ασφάλεια του δικτύου. Επίσης έδειξε παραδείγματα για το πώς μπορεί να βελτιωθεί καλύτερα το OpenFlow με όρους ασφαλείας ως απάντηση σε επιλεγμένες απειλές ασφαλείας. Επέλεξε δύο ζητήματα: την εκτίμηση της συμφόρησης του εύρους ζώνης και τις μετρήσεις συντεταγμένων δικτύου. Ο συντάκτης πρότεινε ένα σύστημα βασισμένο στο OpenFlow για την ασφαλή επικοινωνία ή την ροή της κυκλοφορίας από επίθεση ή παραβίαση.

Οι (Zaalouk Adel, 2014) αξιολόγησαν τις δυνατότητες του SDN όπως την ορατότητα του δικτύου και την επικέντρωση του ελέγχου ως πιθανές λύσεις για ορισμένες ευπάθειες ασφαλείας. Πρότειναν το OrchSec, έναν ενορχηστρωτή που χρησιμοποιεί την παρακολούθηση δικτύου και τον έλεγχο του SDN για ανάπτυξη εφαρμογών ασφαλείας. Αυτή η αρχιτεκτονική μπορεί να μετριάσει κάποιες επιθέσεις που δεν χρειάζονται μια βαθιά ματιά στα περιεχόμενα των πακέτων (π.χ. Worms, DoS, κ.λπ.).

3.4.5.2 Διαχείριση κυκλοφορίας

Ο (Curtis Andrew, 2011) πρότεινε το Mahout, ένα σύστημα διαχείρισης για την αντιμετώπιση μεγάλης κυκλοφορίας. Υπάρχουν πολλές απειλές για την ασφάλεια ή επιθέσεις που ωθούν μεγάλες κυκλοφορίες. Κάποια παραδείγματα περιλαμβάνουν: Worms, DoS ή πλημμύρες. Το Mahout είναι ένας ελεγκτής με βάση την αρχιτεκτονική OpenFlow όπου οι υπολογιστές, σε αντίθεση από τα switches, αναμένεται να παρακολουθούν πιθανές μεγάλες κυκλοφορίες. Οι κεντρικοί υπολογιστές παρακολουθούν τόσο μεγάλη κίνηση σε συντονισμό με τον ελεγκτή που διαχειρίζεται τη διαδικασία χειρισμού αυτής της μεγάλης κυκλοφορίας. Κάθε κεντρικός υπολογιστής παρακολουθεί πιθανές μεγάλες κινήσεις και επικοινωνεί μαζί με τον ελεγκτή μόλις εντοπιστεί μια μεγάλη κίνηση. Οι εγγενής ενιαίοι ελεγκτές OpenFlow αντιμετωπίζουν προβλήματα επεκτασιμότητας ειδικά στην αντιμετώπιση της μεγάλης κυκλοφορίας. Χρησιμοποιώντας τον κεντρικό υπολογιστή για χειρισμό των μεγάλων κυκλοφοριών μπορούν να απαλλάξουν το δίκτυο από το χειρισμό και την αναμονή για κυκλοφορία σε εξέλιξη, η οποία μπορεί να καθυστερήσει για αρκετά πιθανά προβλήματα. Για την ανίχνευση πιθανών μεγάλων κυκλοφοριών από τους τελικούς υπολογιστές, μπορούν να

χρησιμοποιηθούν buffer υποδοχής. Ένα όριο ορίζεται ως μεταβλητή που μπορεί να καθορίσει την άκρη ενός μεγάλου όγκου κυκλοφορίας.

Οι (Choi Taesang, 2014) συζήτησαν για την διαχείριση του OpenFlow και τις προκλήσεις του ελέγχου λόγω των θεμάτων κεντρικότητας και κλιμάκωσης. Πρότειναν έναν παράγοντα παρακολούθησης SDN ή ένα middle-box (SUMA). Το SUMA προτείνεται για να ενσωματώσει λογικά τη διαχείριση, τις υπηρεσίες ελέγχου και παρακολούθησης. Δέχεται την επιβάρυνση της διαδικασίας παρακολούθησης από τον ελεγκτή. Αυτό προειδοποιεί τον ελεγκτή σε περίπτωση ανωμαλιών. Αυτοί έδειξαν κάποια σενάρια επίθεσης και πώς μπορούν να εντοπιστούν χρησιμοποιώντας το SUMA. Αυτό το middle-box δρα στη νότια πλευρά μεταξύ του ελεγκτή και των switches. Ένα πρόβλημα με μια τέτοια προσέγγιση είναι ότι αλλάζει σημαντικά την αρχιτεκτονική SDN που επί του παρόντος έχει μόνο το OpenFlow ως το μόνο υιοθετημένο πρωτόκολλο σε αυτήν την πλευρά.

Οι (Rasley Jeff, 2014) παρουσίασαν το Planck, ένα πλαίσιο διαχείρισης της κυκλοφορίας για την παροχή κλιμακούμενων δεδομένων κίνησης με σύντομες ή μικρές χρονικές κλίμακες χρησιμοποιώντας μηχανισμούς κατοπτρισμού πόρτας. Η κυκλοφορία των switches αντικατοπτρίζεται σε μια καθορισμένη πόρτα. Τα δεδομένα κίνησης είναι ένα σημαντικό πλεονέκτημα για όλες τις εφαρμογές ασφαλείας. Η συλλογή και η ανάλυση αυτών των δεδομένων με υψηλή ακρίβεια, σε πραγματικό χρόνο και λιγότερη συμβολή του δικτύου συμβάλλουν στη βελτίωση των ελέγχων ασφαλείας και την ανίχνευση επιθέσεων. Ο κατοπτρισμός στο OpenFlow έχει ένα πλεονέκτημα έναντι του παραδοσιακού κατοπτρισμού χρησιμοποιώντας πόρτες Span. Αυτό συμβαίνει δεδομένου ότι ο κατοπτρισμός στο OpenFlow μπορεί να προσαρμοστεί. Μπορούμε να καθορίσουμε ή να εξάγουμε συγκεκριμένη κίνηση βάσει προσαρμοσμένων κριτηρίων ή ερωτημάτων. Διαφορετικά εργαλεία ασφαλείας μπορούν να εξαγάγουν διαφορετικές πληροφορίες με βάση τις ανάγκες τους. Αυτό κάνει τη διαδικασία κατοπτρισμού πολύ εστιασμένη και βελτιστοποιημένη.

ΚΕΦΑΛΑΙΟ 4

Σε αυτό το κεφάλαιο, θα δούμε την υλοποίηση ενός σεναρίου επίθεσης DoS στο περιβάλλον προσομοίωσης Mininet και στην συνέχεια θα πραγματοποιηθεί ανίχνευση της επίθεσης από το IDS Suricata. Αρχικά, θα γίνει περιγραφή της αρχιτεκτονικής του Mininet και του IDS Suricata. Στην συνέχεια του κεφαλαίου περιγράφεται αναλυτικά το σενάριο της επίθεσης και ακολούθως πραγματοποιείται η υλοποίησή του.

4.1 Αρχιτεκτονική του Mininet

Το Mininet είναι ένας εξομοιωτής δικτύου που δημιουργεί ένα δίκτυο εικονικών κεντρικών υπολογιστών, switches, και ελεγκτών. Οι κεντρικοί υπολογιστές του Mininet εκτελούν τυπικό λογισμικό δικτύου Linux και τα switches του υποστηρίζουν το OpenFlow για εξαιρετικά ευέλικτη προσαρμοσμένη δρομολόγηση και δικτύωση που καθορίζεται από λογισμικό.

Το Mininet υποστηρίζει την έρευνα, την ανάπτυξη, τη μάθηση, τη δημιουργία πρωτοτύπων, τις δοκιμές, τον εντοπισμό σφαλμάτων και οποιεσδήποτε άλλες εργασίες που θα μπορούσαν να ωφεληθούν από την ύπαρξη ενός πλήρους πειραματικού δικτύου σε φορητό υπολογιστή ή άλλο υπολογιστή.

Το Mininet:

- Παρέχει ένα απλό και φθηνό δοκιμαστικό δίκτυο για την ανάπτυξη εφαρμογών OpenFlow
- Επιτρέπει σε πολλούς ταυτόχρονους προγραμματιστές να εργάζονται ανεξάρτητα στην ίδια τοπολογία
- Υποστηρίζει δοκιμές παλινδρόμησης σε επίπεδο συστήματος, οι οποίες είναι επαναλαμβανόμενες και συσκευάζονται εύκολα
- Επιτρέπει πολύπλοκες δοκιμές τοπολογίας, χωρίς να χρειάζεται να συνδεθεί ένα φυσικό δίκτυο
- Περιλαμβάνει ένα CLI που γνωρίζει την τοπολογία και γνωρίζει το OpenFlow, για εντοπισμό σφαλμάτων ή εκτέλεση δοκιμών σε όλο το δίκτυο
- Υποστηρίζει αυθαίρετες προσαρμοσμένες τοπολογίες και περιλαμβάνει ένα βασικό σύνολο παραμετρικών τοπολογιών

Το Mininet παρέχει έναν εύκολο τρόπο για να έχετε σωστή συμπεριφορά συστήματος (και, στο βαθμό που υποστηρίζεται από το υλικό σας, την απόδοση) και να πειραματιστείτε με τοπολογίες.

Τα δίκτυα Mininet εκτελούν πραγματικό κώδικα συμπεριλαμβανομένων των τυπικών εφαρμογών δικτύου Unix/Linux καθώς και τον πραγματικό πυρήνα Linux και την στοίβα δικτύου.

Εξαιτίας αυτού, ο κώδικας που αναπτύσσετε και δοκιμάζετε στο Mininet, για τον ελεγκτή OpenFlow, το τροποποιημένο switch ή τον κεντρικό υπολογιστή, μπορεί να μετακινηθεί σε ένα πραγματικό σύστημα με ελάχιστες αλλαγές, για δοκιμές σε πραγματικό κόσμο, αξιολόγηση απόδοσης και ανάπτυξη. Είναι σημαντικό ότι αυτό σημαίνει ότι ένας σχεδιασμός που λειτουργεί στο Mininet μπορεί συνήθως να μετακινηθεί απευθείας σε switches υλικού για προώθηση πακέτων γραμμής.

4.2 IDS Suricata

Το Suricata είναι η κορυφαία ανεξάρτητη μηχανή εντοπισμού απειλών ανοιχτού κώδικα. Συνδυάζοντας την ανίχνευση εισβολής (IDS), την πρόληψη εισβολής (IPS), την παρακολούθηση ασφάλειας δικτύου (NSM) και την επεξεργασία PCAP, το Suricata μπορεί γρήγορα να εντοπίσει, να σταματήσει και να αξιολογήσει τις πιο εξελιγμένες επιθέσεις.

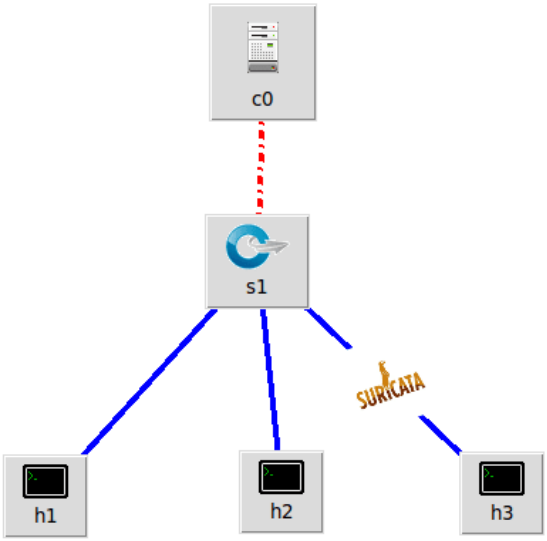
Ενώ πολλά από τα χαρακτηριστικά και τις λειτουργίες του είναι παρόμοια με το Snort, το Suricata διαφέρει με διάφορους σημαντικούς τρόπους:

- Είναι πολλαπλών σπειρωμάτων, έτσι ώστε ένα μοναδικό στιγμιότυπο να μπορεί να αποδώσει σε πολύ μεγαλύτερο όγκο επισκεψιμότητας.
- Υπάρχει περισσότερη διαθέσιμη υποστήριξη για πρωτόκολλα επιπέδου εφαρμογής.
- Υποστηρίζει κατακερματισμό και εξαγωγή αρχείων.
- Διαθέτει άγκιστρα για τη γλώσσα δέσμης ενεργειών Lua, τα οποία μπορούν να χρησιμοποιηθούν για την τροποποίηση των εξόδων και ακόμη και για τη δημιουργία σύνθετης και λεπτομερούς λογικής ανίχνευσης υπογραφών.

Συνοψίζοντας, το Suricata είναι η καλύτερη πλατφόρμα ανίχνευσης εισβολών που βασίζεται σε υπογραφές και είναι μία από τις τρεις σημαντικές μηχανές ανίχνευσης στην πλατφόρμα Bricata.

4.3 Περιγραφή σεναρίου

Δημιουργούμε ένα SDN δίκτυο το οποίο αποτελείται από έναν controller, ένα switch με 3 πόρτες και 3 hosts. Η πόρτα 3 του switch που συνδέεται ο host 3 είναι mirror πόρτα η οποία μπορεί να ελέγχει την κίνηση στις πόρτες 1 και 2. Ο host 3 που συνδέεται στην πόρτα 3 έχει ένα σύστημα ανίχνευσης εισβολών (Suricata) που τρέχει σε αυτήν. Όταν αυτό ανιχνεύσει πιθανή DoS επίθεση, θα ενεργοποιηθεί και θα το δούμε στο αρχείο καταγραφής του.



Εικόνα 6 Τοπολογία του δικτύου SDN

4.4 Υλοποίηση σεναρίου

Αρχικά το σενάριο υλοποιήθηκε σε λειτουργικό ubuntu-20.04.2.0 το οποίο είναι εγκατεστημένο σε VirtualBox. Στην συνέχεια έγινε εγκατάσταση του Mininet στο λειτουργικό Ubuntu με τις παρακάτω εντολές:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install git
git clone
git://github.com/mininet/mininet
cd mininet
git tag
git checkout -b mininet-2.3.0 2.3.0
cd ..
```

```
mininet/util/install.sh
sudo mn --switch ovsbr --test pingall
```

Βήμα 1ο

Εγκατάσταση του IDS Suricata στο Ubuntu με τις παρακάτω εντολές

```
sudo add-apt-repository ppa:oisf/suricata
stable
sudo apt update && sudo apt upgrade -y
sudo apt install suricata suricata-dbg
```

Βήμα 2ο

Πρόσθεση κανόνα ανίχνευσης DoS

Δημιουργούμε το αρχείο detect-dos.rules με τους παρακάτω κανόνες:

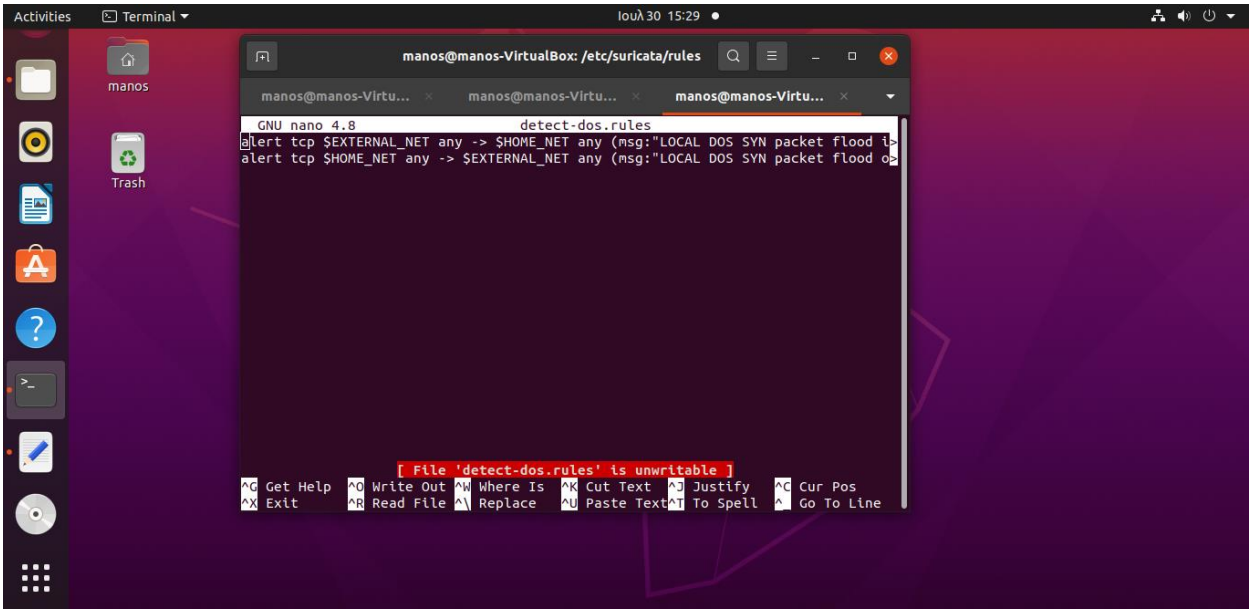
- alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"LOCAL DOS SYN packet flood inbound, Potential DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:5;)
- alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"LOCAL DOS SYN packet flood outbound, Potential DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:6;)

Το αρχείο τοποθετείται στον φάκελο /etc/suricata/rules. Το αρχείο περιλαμβάνει 2 κανόνες οι οποίοι χρησιμοποιούνται για την προειδοποίηση επιθέσεων πλημμύρας SYN. Οι κοινές παράμετροι στους κανόνες είναι οι ενέργειες:

- alert που ειδοποιεί όταν πληρούνται οι προϋποθέσεις στον κανόνα
- tcp το πρωτόκολλο που εστιάζει ο κανόνας

- $EXTERNAL_NET & $HOME_NET οι διευθύνσεις που αναγράφονται στο αρχείο /etc/suricata/suricata.yaml
- msg η παράμετρος που έχει το περιεχόμενο που εμφανίζεται κατά τη διάρκεια της ειδοποίησης
- flags περιέχει το S για το πακέτο SYN
- threshold η παράμετρος που ορίζεται σε 2 μέρη, τα οποία περιλαμβάνουν:
    - threshold για να ορίσετε ένα ελάχιστο όριο για έναν κανόνα προτού δημιουργήσει ειδοποιήσεις.
    - όριο για να βεβαιωθείτε ότι το σύστημα δεν πλημμυρίζει από ειδοποιήσεις.

Εδώ η ειδοποίηση θα δημιουργηθεί εάν υπάρχουν περισσότερα από 5000 πακέτα TCP SYN εντός των επόμενων 5 δευτερολέπτων.



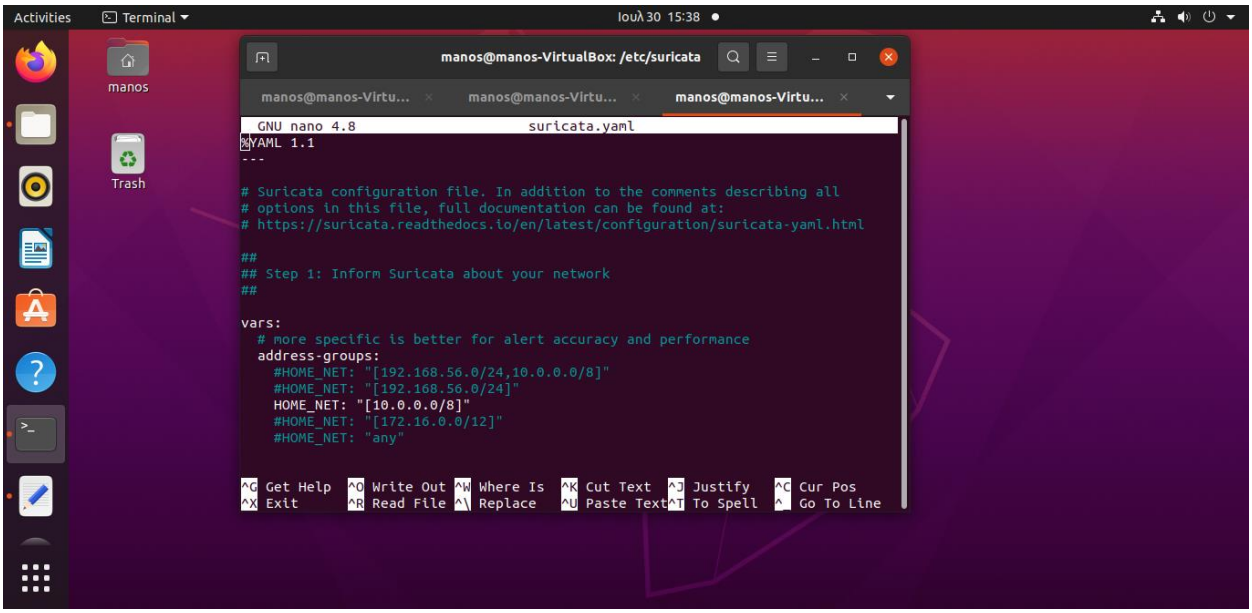
Εικόνα 7 detect-dos.rules

Βήμα 3ο

Ρύθμιση του Suricata

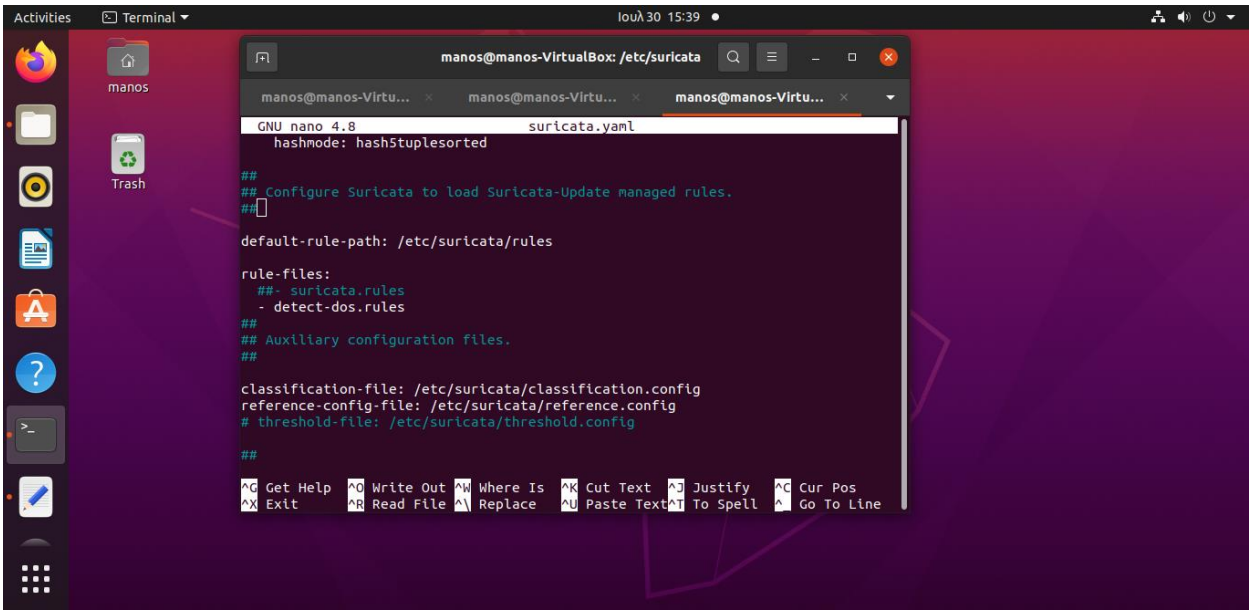
Τα περιεχόμενα του suricata.yaml ενημερώνονται ως εξής:

Η τιμή HOME_NET ενημερώνεται με την διεύθυνση IP της τοπολογίας που θα δημιουργηθεί.



Εικόνα 8 suricata.yaml

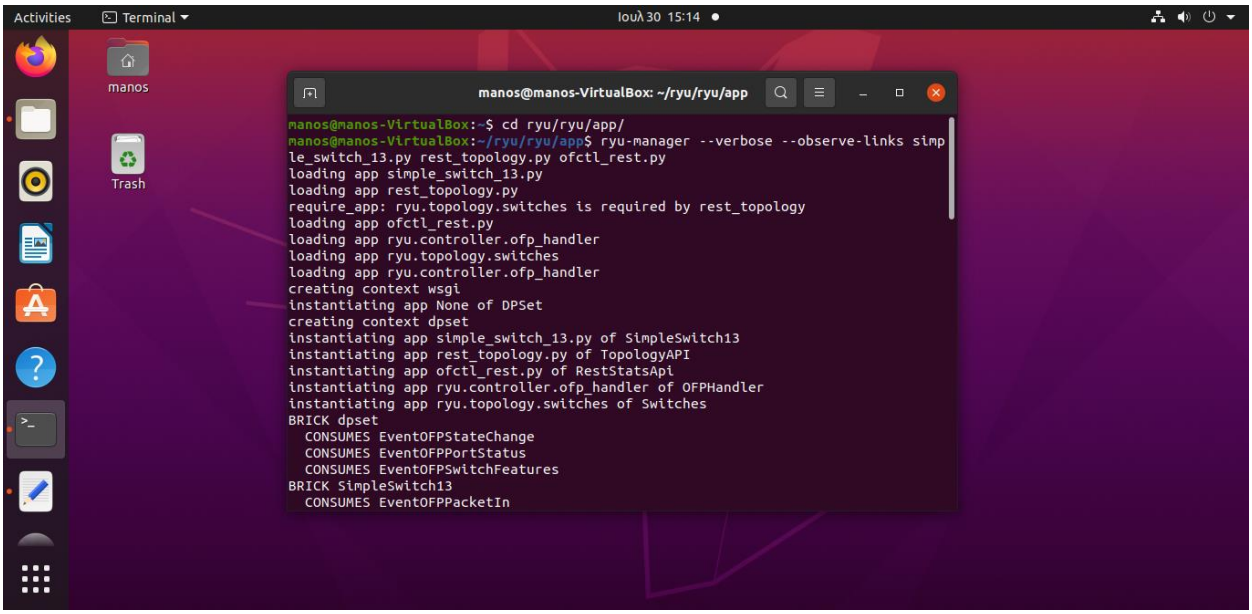
Το αρχείο κανόνων που δημιουργήσαμε τοποθετείται στην λίστα με τα αρχεία-κανόνες

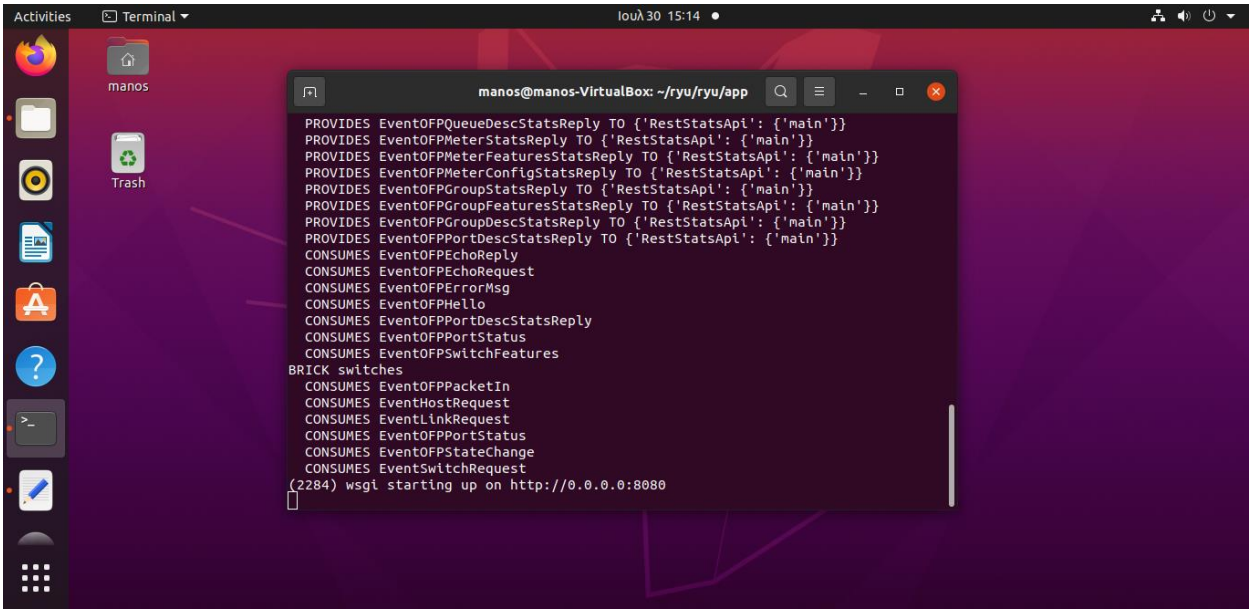


Εικόνα 9 suricata.yaml

Βήμα 4ο

Εκτέλεση του ελεγκτή Ryu

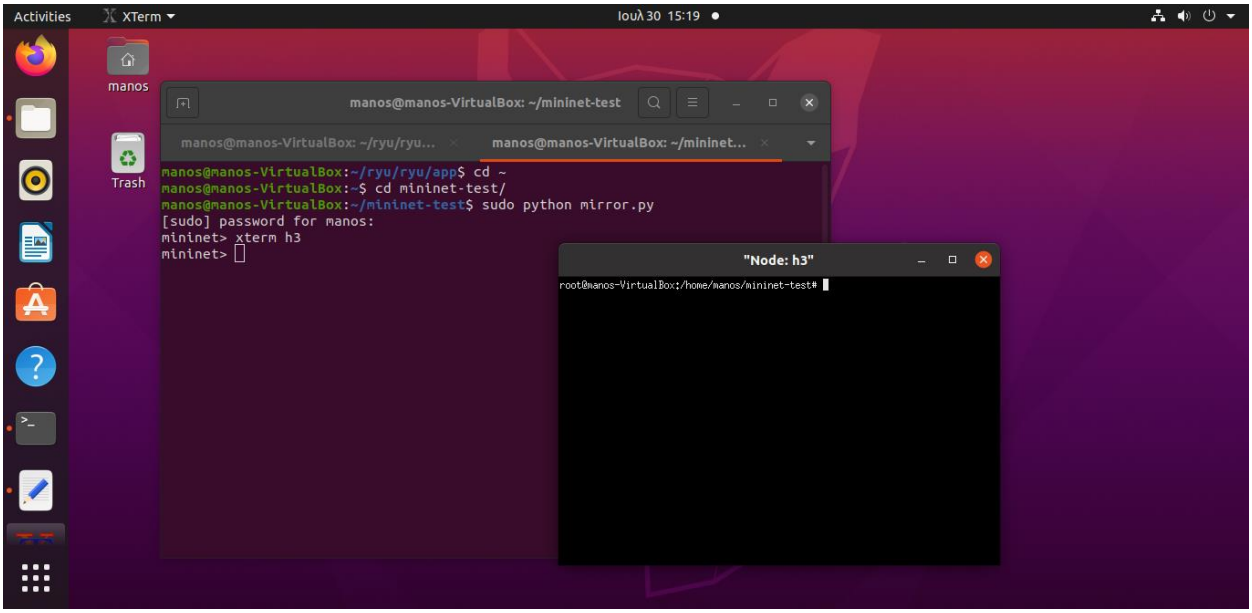




Εικόνα 10 Εκκίνηση Ryu controller

Βήμα 5ο

Εκκίνηση της τοπολογίας μας στο mininet από το αρχείο mirror.py. Η τοπολογία αποτελείται από έναν controller, ένα switch και 3 hosts.



Εικόνα 11 Εκκίνηση τοπολογίας στο Mininet

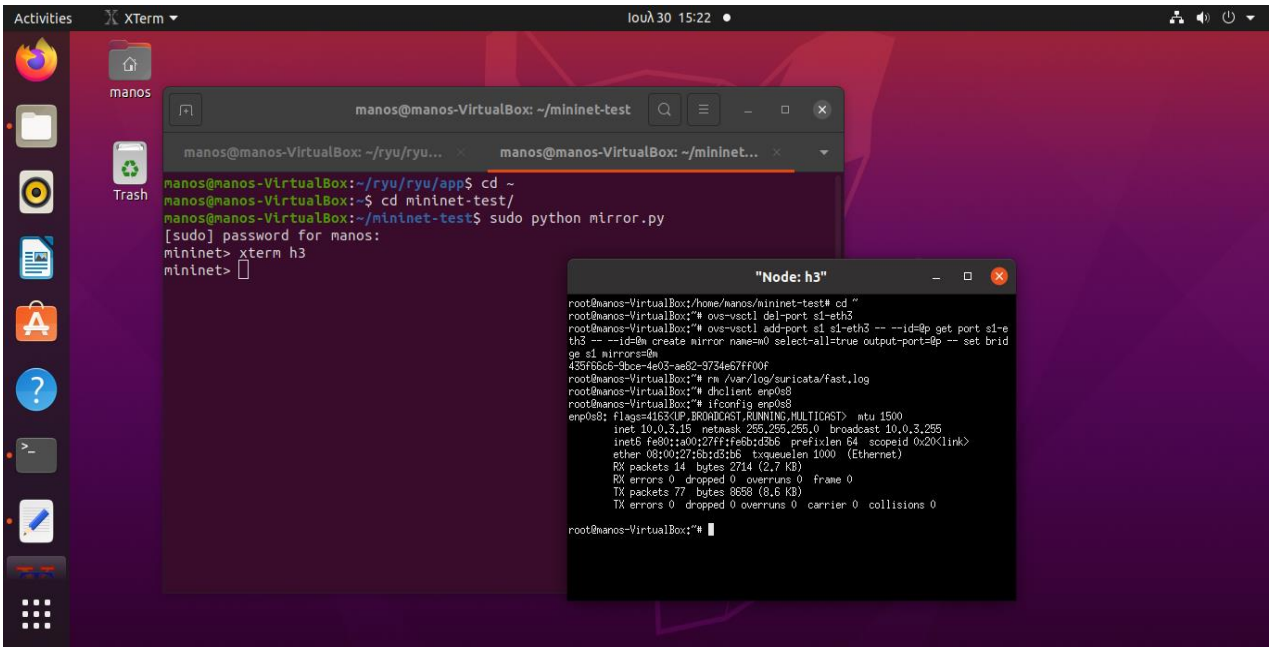
Βήμα 6ο

Ορισμός της πόρτας 3 ως mirror πόρτα και διαγραφή του αρχείου καταγραφής του Suricata με τις παρακάτω εντολές:

```
ovs-vsctl del-port s1-eth3

ovs-vsctl add-port s1 s1-eth3 -- --id=@p get port s1-eth3 --
--id=@m create mirror name=@m0 select-all=true output-port=@p
-- set bridge s1 mirrors=@m

rm /var/log/suricata/fast.log
```

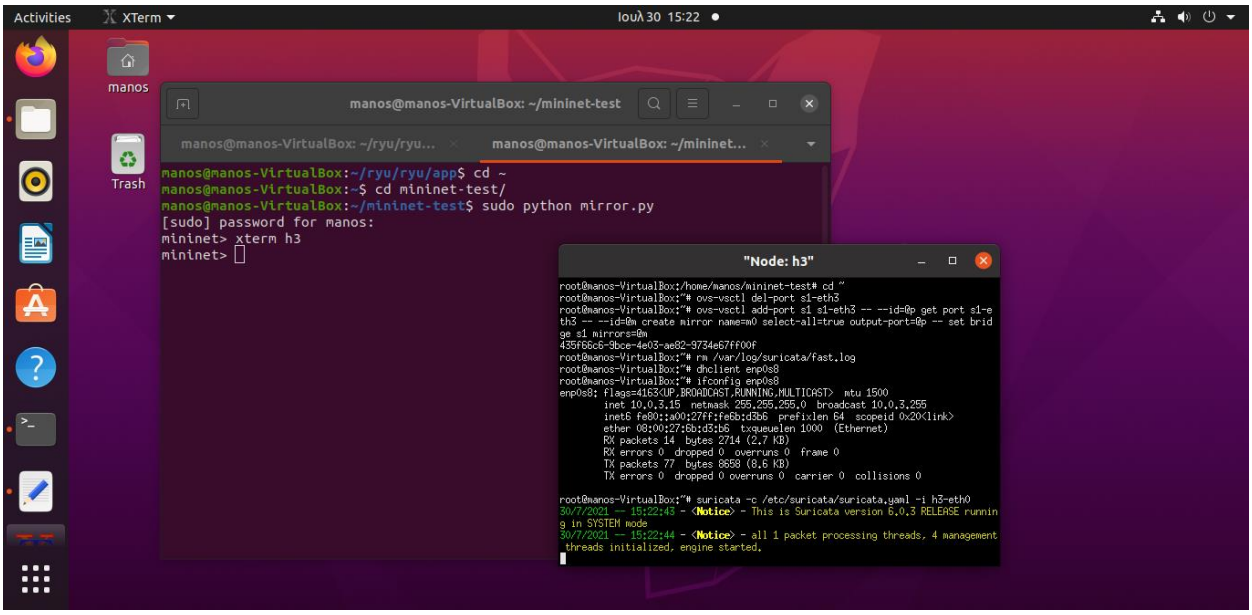


Εικόνα 12 Ορισμός της πόρτας 3 ως mirror πόρτα και διαγραφή του αρχείου καταγραφής του Suricata

Βήμα 7ο

Εκκίνηση του Suricata στον host 3 με την παρακάτω εντολή:

```
suricata -c
/etc/suricata/suricata.yaml -i h3
eth0
```

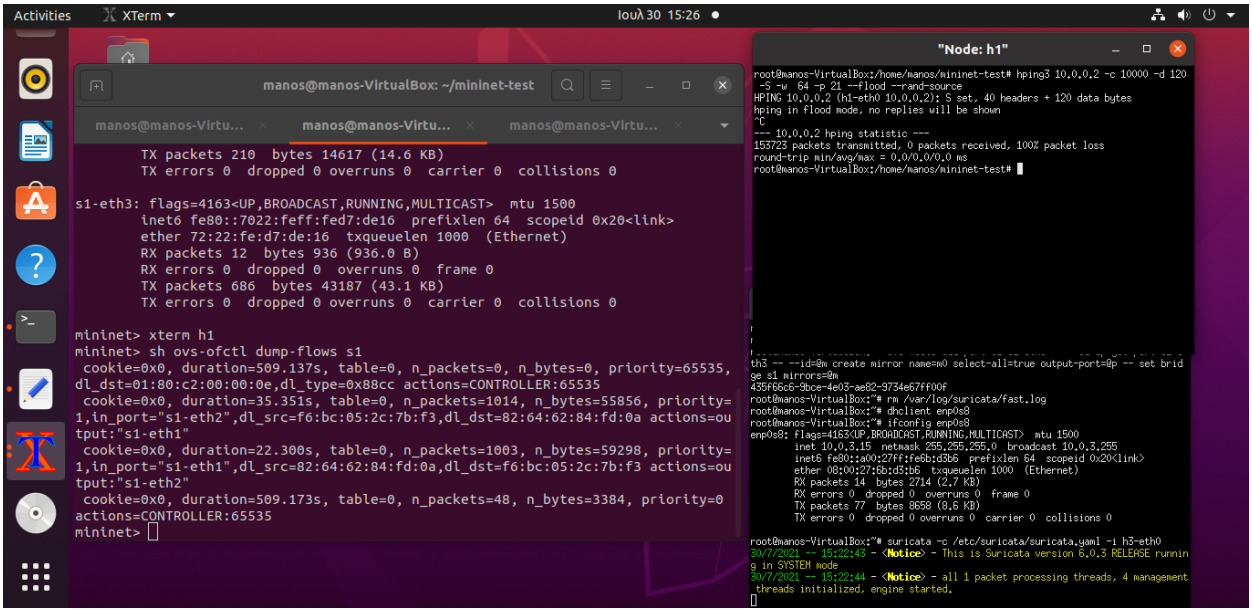


Εικόνα 13 Εκκίνηση του Suricata στον host 3

Βήμα 8ο

Πραγματοποίηση επίθεσης DoS από τον host 1 στον host 2 χρησιμοποιώντας το βοηθητικό πρόγραμμα δικτύου hping3 για να δημιουργήσει και να κατακλύσει με TCP SYN πακέτα την διεύθυνση IP προορισμού.

```
hping3 10.0.0.2 -c 10000 -d 120 -s -w 64 -p 21 --
flood --rand-source
```

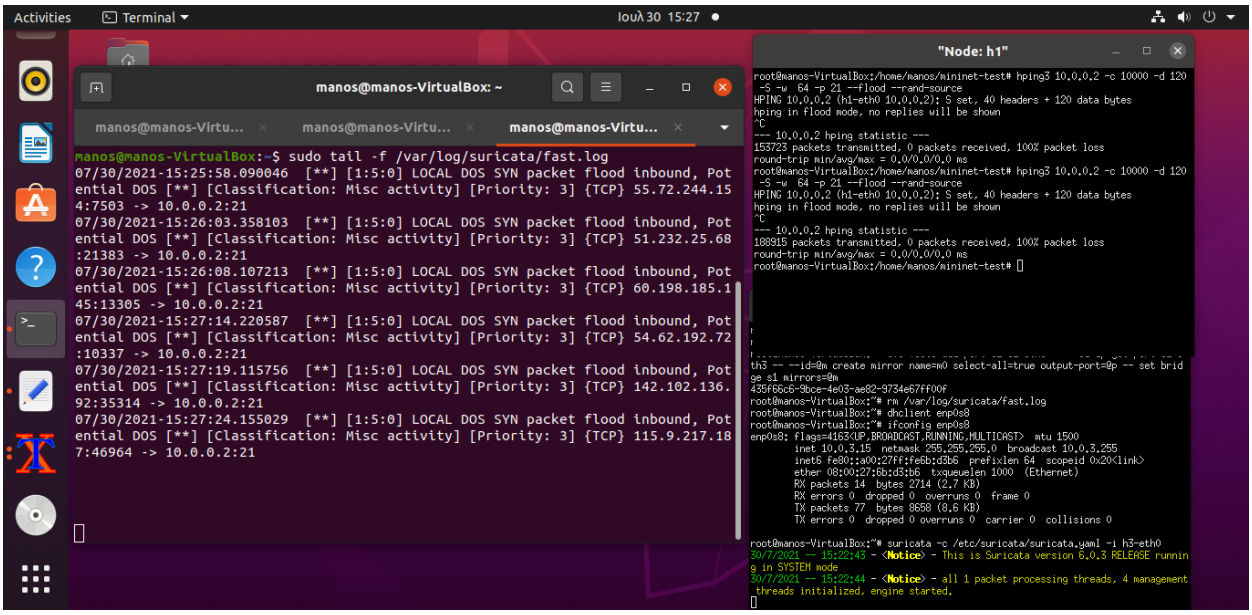


Εικόνα 14 Επίθεση DoS από τον h1 στον h2 με την εντολή hping3

Βήμα 9ο

Τώρα οι κανόνες IDS ενεργοποιούνται και το Suricata ειδοποιεί ότι υπάρχει πιθανή επίθεση DOS. Αυτό μπορεί να φανεί στα αρχεία καταγραφής με την εντολή:

```
sudo tail -f
/var/log/suricata/fast.log
```



Εικόνα 15 Ενεργοποίηση των κανόνων IDS και ειδοποίηση του suricata ότι υπάρχει πιθανή επίθεση DOS

Επομένως, το Suricata ενέργησε ως IDS και εντόπισε την επίθεση DoS.

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η αρχιτεκτονική SDN είναι μια επανάσταση στη διαχείριση και τον έλεγχο του δικτύου, προσθέτοντας ειδικές λειτουργίες που ενισχύουν διαφορετικές λειτουργίες του δικτύου και ταυτόχρονα παρέχουν λύσεις σε δύσκολα ζητήματα που υπάρχουν στα συμβατικά δίκτυα. Ο κεντρικός έλεγχος και ο προγραμματισμός του δικτύου στο SDN συνεργάζονται για την επιτάχυνση της πρωτοτυπίας και την ανάπτυξη των λειτουργιών του δικτύου και γενικά, οι περισσότερες από τις λειτουργίες του που βρίσκονται στις συμβατικές αρχιτεκτονικές μπορούν να αποδίδονται σε SDN με τη μορφή απλών εφαρμογών λογισμικού. Η ασφάλεια βρίσκεται επίσης στο πεδίο καινοτομίας του δικτύου μέσω της επιβολής χαρακτηριστικών SDN, όπως εργασίες και προτάσεις στην υπερσύγχρονη λεπτομέρεια, η αύξηση της επιβολής των χαρακτηριστικών SDN στην ανάπτυξη και την απόδοση διαφορετικών λειτουργιών ασφαλείας δικτύου.

Παρά την εισαγωγή νέων συστημάτων ασφαλείας και την ενίσχυση των υφιστάμενων που με τη σειρά τους παρέχουν νέα εργαλεία και μηχανισμούς για ισχυρότερη ασφάλεια δικτύου και προστασία, αξιόπιστη ασφάλεια στο SDN δεν μπορεί να διασφαλιστεί πλήρως. Επιπλέον, τα πρόσθετα επίπεδα και οι διεπαφές στο SDN προωθούν απρόσκοπτα την εμφάνιση νέων τρωτών σημείων και απειλών στην ασφάλεια. Αυτή η τελευταία δήλωση ορίζει δύο χάρτες πορείας έρευνας και ανάπτυξης στις αρχές ασφάλειας του SDN, αφενός, ο ένας κλάδος της έρευνας που αποσκοπεί στη μόχλευση των συστατικών χαρακτηριστικών του SDN για την ενίσχυση της ασφάλειας του δικτύου, αφετέρου ο άλλος κλάδος επικεντρώνεται στην προώθηση μια ασφαλούς και αξιόπιστης αρχιτεκτονικής SDN με τα σχετικά επίπεδα και τις διεπαφές.

Τα ευάλωτα σημεία και οι επιθέσεις δικτύου στο SDN γίνονται όλο και πιο περίπλοκα. Επομένως, η εμφάνιση νέων προκλήσεων αναγκάζει την έρευνα ασφάλειας να διαμορφώσει την αρχιτεκτονική SDN για: να βρίσκεται σε συνεχή αλληλεπίδραση με διαφορετικές τεχνολογίες και να προσπαθεί να ενσωματώνει στοιχεία και χαρακτηριστικά που μπορούν να εφαρμοστούν στην κατασκευή καινοτόμων και πολύ-επιστημονικών πλαισίων ασφαλείας. Οι αλγόριθμοι μηχανικής μάθησης, οι υπηρεσίες Cloud, οι εικονικοποιημένες λειτουργίες δικτύου, είναι καλά παραδείγματα τεχνολογιών που μπορούν να συνδυαστούν για την κατασκευή του περιβάλλοντος ασφαλείας SDN επόμενης γενιάς.

Η ανάπτυξη των SDN στα δίκτυα παραγωγής είναι ακόμα ένα όραμα και πρέπει ακόμα να γίνει πολλή δουλειά με την ασφάλεια SDN για να γίνει αυτό το όραμα πραγματικότητα. Υπάρχουν ουσιαστικά προβλήματα ασφάλειας που απαιτούν προσοχή και αδρανή ζητήματα που δεν έχουν ακόμη αποκαλυφθεί, επομένως το πεδίο της έρευνας είναι ακόμη ανοιχτό και κάθε νέα συμβολή βοηθά στο να κλείσει το χάσμα μεταξύ αυτού του οράματος και της πραγματικότητας. Ο στόχος ασφαλείας του SDN θα πρέπει να στοχεύει στην επίτευξη ενός αυτοματοποιημένου, αυτό-

εποικοδομητικού, αυτοελεγχόμενου και αυτοδιαγνωστικού πλαισίου ασφαλείας, αρκετά ευρύ για να παρακολουθεί διαφορετικές καταστάσεις και επίπεδα κρισιμότητας, επαρκώς προσαρμόσιμα για να αναδιαμορφώσουν αποτελεσματικά την δομή ανάλογα με τη σοβαρότητα και τον αντίκτυπο της αντίστοιχης κατάστασης, και ικανό να διακρίνει και να επιλύει τις ασυνέπειες που υπάρχουν στη δική του συστατική δομή του συστήματος που θα μπορούσε να προκαλέσει απρόβλεπτη ανώμαλη απόδοση.

Αν και έχει περάσει σχεδόν μια δεκαετία από τότε που δημοσιεύτηκαν οι πρώτες προτάσεις για την ασφάλεια των SDN, υπάρχουν αρκετές ανοιχτές προκλήσεις και θέματα και απαιτούνται εκτεταμένες προσπάθειες σε αυτά τα πεδία, π.χ. διαμεσολαβητές πολιτικής, εντοπισμός σφαλμάτων SDN και ανακάλυψη ευπάθειας. Κάπως έτσι η δημοσιότητα στην έρευνα ασφαλείας SDN οδήγησε την επιστημονική κοινότητα να επικεντρωθεί σε ορισμένα μοντέρνα θέματα, π.χ. μηχανές ανίχνευσης που βασίζονται σε μηχανική μάθηση, προγραμματιζόμενα επίπεδα δεδομένων και οπτικοποιημένες λειτουργίες ασφαλείας, αφήνοντας σημαντικές πτυχές ασφάλειας σε μια αργή καμπύλη εξέλιξης με πολύ λίγα δημοσιευμένα έργα και ανοίγοντας ένα νέο κεφάλαιο στην ανάπτυξη στρατηγικών ασφαλείας που όχι μόνο παρακολουθούν τέτοια υπερτιμημένα θέματα, αλλά είναι απαραίτητα για την κατασκευή ισχυρών και πλήρων ενοποιημένων πλαισίων ασφαλείας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Andersen David G, H. B. (2008). Accountable internet protocol (AIP). SIGCOMM'08;, 17-22.

Anderson Carolyn Jane, N. F. (2014). NetkAT: semantic foundations for networks. POPL, 113-26.

Ballard Jeffrey, I. R. (2010). Extensible and scalable network monitoring using OpenSAFE. Proceedings of the 2010 Internet Net- work Management Conference on Research on Enterprise Networking,.

Bellessa John, E. K. (2011). NetODESSA: dynamic policy enforcement in cloud networks. Proceedings of the 2011 IEEE 30th Symposium on Reliable Distributed Systems Workshops.

Benton, K. (2013). OpenFlow vulnerability assessment. Proceedings of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN), 151-152.

Bifulco Roberto, K. G. (2014). Towards a richer set of services in software-defined networks. SENT'14;.

Braga Rodrigo, E. M. (2010). Lightweight DDoS flooding attack detection using NOX/OpenFlow. Proceedings of the IEEE Conference on Local Computer Networks (LCN),, 408-15.

Calvert, W.K. Edwards, N. Feamster, R.E. Grinter, Y. Deng, and X. Zhou. (2011). Instrumenting home networks. ACM SIGCOMM Computer Commun. Review, 84-89.

Casado Martin, M. F. (2009). Rethinking enterprise network control. IEEE/ACM transactions on Networking (TON), 1270-83.

Casado Martin, T. G. (2006). SANE: a protection architecture for enterprise networks. Proceedings of the 15th conference on USENIX Security Symposium.

Casado, M., Freedman, M., Pettit, J., & Luo, J. (2007). Ethane: taking control of the enterprise. ACM SIGCOMM Comput Commun Rev.

Choi Taesang, S. S. (2014). SUMA: software-defined unified monitoring agent for SDN. NOMS;, 1-5.

Crenshaw, A. (2012). Security and Software Defined Networking: Practical Possibilities and Potential Pitfalls. Ανάκτηση από http://www.irongeek.com/i.php?page=security/security-and-software-defined-networking-sdn-openflow

Curtis Andrew, M. J. (2011). DevoFlow: scaling flow management for high-performance networks. SIGCOMM Comput Commun Rev, 254-65.

Fayaz Seyed, S. V. (2013). FlowTags: enforcing network-wide policies in the presence of dynamic middlebox actions. Proceedings of the Second Workshop on Hot Topics in Software Defined Networks. ACM;.

Feamster Nick, H. B. (2004). The case for separating routing from routers. Proceedings of the ACM SIGCOMM Workshop on Future Directions in Network Architecture,, 5-12.

Feamster., N. (2010). Outsourcing home network security. In Proc. 2010 ACM SIGCOMM workshop on Home networks, 37-42.

Giotis K, A. C. (2014). Combining OpenFlow and sFlow for an effectiveand scalable Anomaly detection and mitigation mechanism on SDN Environments. Comput Netw, 122-36.

Goodney Andrew, N. S. (2010). Pattern based packet filtering using NetFPGA in DETER infrastructure. 1st Asia NetFPGA developers workshop;.

Hand Ryan, M. T. (2013). Active security. Twelfth ACM Workshop on Hot Topics in Networks.

Hinrichs Timothy, N. G. (2008). Expressing and enforcing flow-based network security policies. Technical report. University of Chicago;.

Hu Hongxin, H. W.-J. (2014). FlowGuard: building robust firewalls for software-defined networks. HotSDN'14,.

Jafarian Jafar Haadi, E. A.-S. (2012). Openflow random host mutation: transparent moving target defense using software defined networking. Proceedings of the ACM Workshop on Hot Topics in Software Defined Networks, 127-132.

Jammal, M. (2014). Softwaredefined networking:state oftheartandresearchchallenges. Comput.Netw., 74-98.

Karame, G. (2013). Towards trustworthy network measurements. TRUST, 83-91.

Katta Naga Praven, J. R. (2012). Logic programming for software-defined networks. ACM SIGPLAN Workshop on Cross- Model Language Design and implementation,.

Kazemian Peyman, C. M. (2013). Real time network policy checking using header space analysis. NSDI.

Kendall. (1999). A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems. Ph.D. thesis. Massachusetts Institute of Technology.

Kim Hyojoon, Feamster Nick. (2013). Improving network management with software defined networking. Commun Mag IEEE, 104-9.

Kinoshita Shunichi, T. W. (2012). Implementation and evaluation of an OpenFlow-based access control system for wireless LAN roaming. Computer Software and Applications Conference Workshops , 82-87.

Kloeti Rowan, V. K. (2013). OpenFlow: a security analysis. Proceedings of the 8th Workshop on Secure Network Protocols (NPSec), Part of IEEE ICNP,.

Koponen Teemu, S. S. (2011). Architecting for innovation. Comput Commun, 24-36.

Lindqvist, U., Jonsson, E.,. (1997). How to systematically classify computer security intrusions. Proceedings. 1997 IEEE Symposium on Security and Privacy. IEEE,.

Liyanage Madhusanka, Y. M. (2014). Securing the control channel of software-defined mobile networks. Proc. of 1st IEEE WoWMoM Workshop on Software Defined Networking Architecture and Applications.

Matias, J. T. (2012). Implementing Layer 2 Network Virtualization Using OpenFlow: Challenges and Solutions. Ανάκτηση από https://ieeexplore.ieee.org/abstract/document/6385044?casa_token=i3hVtmZt8e8AAAAA:y0MbaMIU7-DiL-MoZpiToyQDFUQPJ2vD9fMVX9yg5ox-n42OzGxL7uLHNe2uK6iu-7tIrWnbi2Bm

Mehdi Sayed Akbar, K. J. (2011). Revisiting traffic anomaly detection using software defined networking. Recent advances in intrusion detection. Springer;, 161-180.

Mendonca Marc, S. S. (2012). A flexible innetwork IP anonymization service. The IEEE ICC Workshop on Software Defined Networks;.

Michael., K. S. (2012). OpenFlow can provide security, too. Ανάκτηση από http://www.enterprisenetworkingplanet.com/datacenter/openflow-can-provide-security-too.html

Namal Suneth, A. I. (2013). Enabling secure mobility with OpenFlow. IEEE software defined networks for future networks and services, 11-13.

Nayak Ankur, R. A. (2009). Resonance: inference-based dynamic access control for enterprise networks. Proceedings of the Workshop on Research on Enterprise Networking (WREN),, 11-18.

Pan Heng, G. H. (2013). FlowAdapter: enable flexible multi-table processing on legacy hardware. HotSDN;.

Porras Phillip, S. S. (2012). A framework for enabling security controls in OpenFlow networks. ACM.

Qazi Zafar, C.-C. T. (2013). SIMPLE-fying middlebox policy enforcement using SDN. ACM SIGCOMM;.

R. Mortier, T. R. (2012). Control and understanding: Owning your home network. In 2012 4th Int. Conf. on Commun. Syst. and Netw., 1-10.

Ramachandran Anirudh, M. Y. (2009). Securing enterprise networks using traffic tainting. Technical Report GTCS-09e15. .

Rasley Jeff, S. B. (2014). Low-latency network monitoring via oversubscribed port mirroring. ONS.

Schehlmann Lisa, Harald Baier. (2013). COFFEE: a concept based on OpenFlow to filter and erase events of botnet activity at highspeed nodes. INFORMATIK;.

Sethi Divjyot, N. S. (2013). Abstractions for model checking sdn controllers. FMCAD;.

Shin Seungwon, Y. V. (2013). Avant-guard: scalable and vigilant switch flow management in software-defined networks. Proceedings of the ACM Conference on Computer and Communications Security,.

Shirali-Shahreza and Ganjali Sajad Yashar. (2013). Efficient implementation of security applications in OpenFlow controller with FleXam,. HotSDN'13,.

Simmons, C. E. (2014). Avoidit: a cyber attack taxonomy. In: 9th Annual Symposium on Information Assurance. ASIA14,, 2-12.

Skowyra Rick, B. S. (2013). Software-defined IDS for securing embedded Mobile devices. Proceedings of HPEC'13: The IEEE high Performance Extreme Computing Conference,.

Sloan, R.H., Warner, R.,. (2013). Unauthorized Access: the Crisis in Online Privacy and Security. CRC press.

Son Sooel, S. S. (2013). Model checking invariant security properties in OpenFlow. IEEE International Conference on Communications (ICC),.

Stoenescu Radu, P. M. (2013). SymNet: static checking for stateful networks. HotMiddlebox'13;.

Suh Junho, C. H.-g. (2010). Implementation of contentoriented networking architecture (CONA): a focus on DDoS countermeasure. Proc of 1st European NetFPGA Developers Workshop,.

Suh Michelle, P. S. (2014). Building firewall over the software-defined network controller. ICACT2014;.

Takavoli A., Casado,M.,Koponen,T.,Shenker,S.,. (2009). Applying NOX to the datacenter. . Proceedings of HotNet. ACMPress, 1–6.

Tamihiro., Y. (2013). OpenFlow 1.0 actual use-case: RTBH of DDoS. Ανάκτηση από http://packetpushers.net/openflow-1-0-actual-use-case-rtbh-of-ddos-traffic-while-keeping-the-target-online.

Voellmy Andreas, K. H. (2012). Procera: a language for high-level reactive network control. Proceedings of the 1st Workshop on hot topics in software defined networks;, 43-8.

Wang Xiang, L. Z. (2012). LiveCloud: A Lucid Orchestrator for Cloud Datacenters. 2012 IEEE 4th International Conference on Cloud Computing Technology and Science;.

Wen Xitao, C. Y. (2013). HotSDN, towards a secure controller platform for openflow applications. HotSDN.

Wu Yong-juan, L. J.-x.-w. (2013). Programmable virtual network instantiation in IaaS cloud based on SDN. Universities Posts Telecommun, 21-25.

Xiao Peiyao, J. B. (2013). O-CPF: an OpenFlow based intra-AS source address validation application. CFI'13.

Xing Tianyi, H. D.-J. (2013). SnortFlow: a openflow-based intrusion prevention system in cloud environment. Second GENI Research and Educational Experiment Workshop;.

Yamasaki Yashuiro, M. Y. (2011). Flexible access management system for campus VLAN based on OpenFlow. Applications and the Internet (SAINT),, 347-51.

YuHunag Chu, T. M.-C. (2010). A novel design for future on-demand service and security. Proceedings of the International Conference on Communication Technology (ICCT),, 385-8.

Zaalouk Adel, R. K. (2014). OrchSec: an orchestrator-based architecture for enhancing network-security using Network Monitoring and SDN control functions. NOMS, 1-9.

Zhu Shuyong, B. J. (2014). SFA: stateful forwarding abstraction in SDN data plane. USENIX/Open Networking Summit Research Track.

Wenjuan Li, Weizhi Meng, Lam For Kwok, “A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures”, Journal of Network and Computer Applications, Vol 68, Pages 126-139, June 2016

Zhaogang Shu & Jiafu Wan & Di Li & Jiaxiang Lin & Athanasios V. Vasilakos &

Muhammad Imran, “Security in Software-Defined Networking:

Threats and Countermeasures”, Springer Science + Business Media, New York 2016

Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, “A Survey of Software-Defined Networking: Past,

Present, and Future of Programmable Networks”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 3, THIRD QUARTER 2014

Silvio E. Quincozes, Arthur A. Zopellaro Soares, Wilker Oliveira, Eduardo B. Cordeiro,

Robson A. Lima, D´ebora Muchaluat-Saade, Vinicius C. Ferreira, Yona Lopes,

Juan Lucas Vieira, Luana M. Uchˆoa, Helio N. C. Neto, Leonardo F. Soares,

Natalia C. Fernandes, Diego Passos, and C´elio Albuquerque, “Survey and Comparison of SDN Controllers for Teleprotection and Control Power Systems”, Laborat´orio M´ıdiaCom Universidade Federal Fluminense Niter´oi/RJ, Brazil

OPEN NETWORKING FOUNDATION, “Principles and Practices for

Securing Software-Defined Networks”, 2015

Juan Camilo Correa Chica, Jenny Cuatindioy Imbachi, Juan Felipe Botero Vega, “Security in SDN: A comprehensive survey”, Journal of Network and Computer Applications, Vol 159, June 2020

Izzat Alsmadi, Dianxiang Xu, “Security of Software Defined Networks:

A survey”, Computers & Security, Vol 53, Pages 79-108, September 2015

Kiho Nam, Keecheon Kim, “A Study on SDN security enhancement using open

source IDS/IPS Suricata”, Dept. of Computer Science & Engineering, Konkuk University

Seoul, Korea

Mininet. http://mininet.org/overview/

Tanenbaum Wetherall 2011, "Δίκτυα Υπολογιστών", 5η Αμερικάνικη Έκδοση, Εκδόσεις Κλειδάριθμος

Παραδοσιακά Δίκτυα https://sites.google.com/site/eisagogestadiktyaypologiston1/home

Ασφάλεια δικτύων υπολογιστών https://sites.google.com/site/eisagogestadiktyaypologiston1/diadiktyo-internet/asphaleia-diktyon-ypologiston

Καθηγητής Χρήστος Ι. Μπούρας, “Ασφάλεια δικτύων”, Τμήμα Μηχανικών Η/Υ & Πληροφορικής, Πανεπιστήμιο Πατρών, https://eclass.upatras.gr/modules/document/file.php/CEID1064/%CE%94%CE%B9%CE%B1%CE%BB%CE%AD%CE%BE%CE%B5%CE%B9%CF%82/11_Security.pdf

Shanshan Bian, Peng Zhang, Zheng Yan, “A Survey on Software-Defined Networking Security”, State Key Lab on Integrated Services Networks Xidian University Xi’an, China

Sandra Scott-Hayward, Gemma O’Callaghan and Sakir Sezer “SDN Security: A Survey”, Centre for Secure Information Technolocy (CSIT) Queen’s University Belfast

Lobna Dridi, Mohamed Faten Zhani, “SDN-Guard: DoS Attacks Mitigation

in SDN Networks”, 5th IEEE International Conference on Cloud Networking, 2016

M. Janat Vinnarasi, Dr. N. Sudha, “Security Solution for SDN Using Host-Based IDSs Over DDoS Attack”, International Journal of Emerging Technology and Innovative Engineering Volume 5, Issue 9, September 2019

Maham Iqbal, Farwa Iqbal, Fatima Mohsin, Dr. Muhammad Rizwan, Dr. Fahad Ahmad, “Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions”, International Journal of Advanced Computer Science and Applications, Vol. 10, No. 10, 2019

Danda B. Rawat, Senior Member, IEEE, and Swetha R. Reddy, Member, IEEE, “Software Defined Networking Architecture,Security and Energy Efficiency: A Survey”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 1, FIRST QUARTER 2017

Yifan Liu, Bo Zhao, Pengyuan Zhao, Peiru Fan, Hui Liu, “A Survey: Typical Security Issues of Software-Defined Networking”, 2019