Ατομική Διπλωματική Εργασία

‘DHCP SNOOPING’ IN SOFTWARE DEFINED NETWORKS

Άδωνης Παναγίδης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2015

‘DHCP SNOOPING’ IN SOFTWARE DEFINED NETWORKS

Άδωνης Παναγίδης

Επιβλέπων Καθηγητής

Καθ. Ανδρέας Πιτσιλλίδης

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2014

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω την εκτίμησή μου προς τον επιβλέποντα καθηγητή μου Δρ Ανδρέας Πιτσιλλίδης για τη βοήθεια και τη συμβολή του στην ολοκλήρωση της παρούσας μελέτης μέσα από την πολύτιμη καθοδήγησή του.

ΠΕΡΙΛΗΨΗ

Software Defined Networks(SDN) και Network FunctionsVirtualization (NFV) θεωρείται επανάσταση στα δίκτυα υπολογιστών. Στην παρούσα μελέτη παρουσιάζουμε αυτές τις αναδυόμενες τεχνολογίες, πλεονεκτήματα, τις επιπτώσεις, τους χρήστες τους. Εξετάζεται επίσης , εν συντομία τη χρήση της τεχνολογίας SDN σε σπίτια. Επιπλέον εξετάζεται επιθέσεις σε SDN και κάποιες ενδιαφέρουσες λύσεις ασφαλείας που υλοποιούνται πιο εύκολα και έχουν αυξημένες δυνατότητεςχρησιμοποιώντας SDN. Τέλος, παρουσιάζετε η Layer 2 DHCP masquerade επίθεση, και πώς αντιμετωπίζεται με χρήση του ελεγκτή NOX.

Περιεχόμενα

Εισαγωγή

1.1 Επισκόπηση

Τα τελευταία χρόνια η ανερχόμενη τεχνολογία SDN και NFV έχει προσελκύσει πολλή προσοχή από την ακαδημαϊκή κοινότητα και από τη βιομηχανία.

Το SDN επιχειρεί την αποσύνδεση του επιπέδου ελέγχου και του επιπέδου δεδομένων του δικτύου που επιτρέπει την ανάπτυξη και τη μείωση του κόστους λειτουργίας, καθώς και αυξημένη λειτουργικότητα. Στο SDN το υλικό χειρίζεται την προώθηση της κυκλοφορίας σύμφωνα με τους κανόνες που καθορίζονται από τον ελεγκτή. Ο ελεγκτής επικοινωνεί με όλες τις συσκευές του δικτύου χρησιμοποιώντας ένα πρωτόκολλο. Το OpenFlow [3], είναι το πρωτόκολλο που χρησιμοποιείται ευρύτετερα σήμερα.

NFV είναι η ιδέα ότι οποιαδήποτε εφαρμογή του δικτύου που τρέχει σε ειδικές μηχανές μπορεί να τρέξει τώρα σε εικονικές μηχανές. Οι υπηρεσίες περιλαμβάνουν δρομολογητές, firewalls, load balancers, το DNS, caching, NAT. Οι λειτουργίες του δικτύου σε εικονικές μηχανές μπορούν τώρα να χρησιμοποιηθούν ως δομικά στοιχεία, και μπορεί να αλυσοδεθούν για τη δημιουργία υπηρεσιών επικοινωνιών και ιδιωτικών δικτύων. Τα οφέλη είναι τεράστια, όπως το χαμηλό κόστος επένδυσης, η διαλειτουργικότητα, καθώς και ο χρόνος επιτάχυνσης στην αγορά.

Η ασφάλεια δικτύων κερδίζει προσοχή, κυρίως επειδή οι ζωές μας γίνονται όλο και πιο δίκτυο κεντρικές και επειδή αρχίσαμε να ενδιαφερόμαστε περισσότερο για την ψηφιακή προστασία της ιδιωτικής ζωής μας, ειδικά μετά τις αποκαλύψεις του Σνόουντεν. Επίσης με το Ίντερνετ των πραγμάτων (IoT) που κερδίζει έδαφος, οι ζωές μας γεμίζουν με αισθητήρες που

παράγουν πολλά δεδομένα (Big Data) Ως εκ τούτου, ζητήματα προστασίας της ιδιωτικής ζωής και της ασφάλειας εγείρονται.

1.2 Στόχοι

Η παρούσα μελέτη επιχειρεί να αναδημιουργήσει ένα Layer2 μηχανισμό ασφαλείας, DHCP snooping, χρησιμοποιώντας SDN.

Το DHCP snooping μετριάζει τις επιθέσεις, όπως: DHCP rogue attack, ARP spoofing.

Η επίδειξη της επίθεσης γίνεται σε προσομοιωμένο περιβάλλον δικτύου χρησιμοποιώντας Mininet προσομοιωτή δικτύου, OpenVSwitch, και τον ελεγκτή POX, όλα εκ των οποίων είναι ανοιχτού κώδικα.

Έχουμε αντιμετωπίση την επίθεση με την προσθήκη "λογικής" .στο πρότυπο Switch που διατίθεται μαζί με τον ελεγκτή POX.

1.3 Γιατί η Ασφάλεια είναι Σημαντική

Η ασφάλεια των δεδομένων είναι εξαιρετικά σημαντική. Στην εποχή της πληροφορίας, «everything is about data". Η ασφάλεια συχνά παραβλέπεται, μέχρι να συμβεί κάτι κακό. Υποκλοπή δεδομένων μπορεί να καταστρέψει τη φήμη από εταιρείες που χρειάστηκαν χρόνια για να κτίσουν. Η εμπιστοσύνη και η ικανοποίηση των πελατών είναι στενά συνδεδεμένη με το πώς οι εταιρείες χειρίζονται ευαίσθητα δεδομένα των πελατών. Οι ρυθμιστικοί φορείς δημιουργούν απαιτήσεις και πολιτικές για τις επιχειρήσεις, που χειρίζονται ευαίσθητες πληροφορίες, και οι εταιρείες μπορεί να υποστούν βαριά πρόστιμα αν αδυνατούν να αποδείξουν ότι έλαβαν όλα τα αναγκαία μέτρα για την αποφυγή των επεισοδίων. Επιπλέον η βιομηχανική κατασκοπεία, μπορεί να οδηγήσει σε απρόβλεπτες δαπάνες, και η απώλεια του ανταγωνιστικού πλεονεκτήματος . Είναι ζωτικής σημασίας για τις επιχειρήσεις να να επιβάλουν όλα τα αναγκαία μέτρα ασφαλείας για τη μείωση του ρίσκου .

Κεφάλαιο 2

Software Defined Networks

2.1 Τα δίκτυα σήμερα - σύντομη ιστορία

Η δικτύωση των υπολογιστών είναι ένας μηχανισμός που επιτρέπει στους υπολογιστές να ανταλλάσσουν δεδομένα μεταξύ τους. Τα δίκτυα είναι ολοένα και πιο σημαντικά στη ζωή μας. Ξεκινώντας από τη δεκαετία του '40 και στοχεύοντας τη στρατιωτική και ακαδημαϊκή συνεργασία, τα δίκτυα μπορούν να βρεθούν παντού σήμερα.

Ο Γιώργος Stibitz [35] δημιούργησε την πρώτη απομακρυσμένη διαχείριση υπολογιστή στα Bell Labs. Το επόμενο ορόσημο ήταν το ημιαυτόματο περιβάλλον των επιχειρήσεων της έρευνας που δημιουργήθηκε από την IBM και μια αεροπορική εταιρεία για να γίνει το πρώτο ηλεκτρονικό σύστημα κρατήσεων (1960). Το επόμενο ορόσημο ήταν το ARPANET το 1965 όπου δύο υπολογιστές συνδέονταν, ένα στην Καλιφόρνια και ένα στο MIT χρησιμοποιώντας τηλεφωνικές γραμμές

Η εισαγωγή του TCP ήταν το επόμενο ορόσημο το 1974 που βοήθησε στη δημιουργία και την ανάπτυξη του Διαδικτύου.

Η επόμενη εξέλιξη στα δίκτυα είναι, το SDN και το NFV.

2.2 Τα δίκτυα σήμερα - περιορισμοί [1]

Τα δίκτυα σήμερα έχουν λάβει πολλές σύνθετες και διαφορετικές μορφές. Το ίδιο το Διαδίκτυο αποτελείται από εκατομμύρια μεμονωμένα ιδιωτικά μικρότερα δίκτυα. Οι διαχειριστές των δικτύων, [Σχήμα 2.1] πρέπει να προσθέτουν, αφαιρούν δυνατότητες από τον εξοπλισμό του δικτύου, να προσθέτουν νέο εξοπλισμό και ούτω καθεξής. Αυτό γίνεται, σήμερα, για κάθε εξοπλισμό δικτύου ξεχωριστά, κυρίως με την αντιγραφή των εντολών (με πολύ λίγες εξαιρέσεις) για κάθε στοιχείο του δικτύου. Είναι εύκολο να καταλάβουμε ότι αυτή η προσέγγιση δεν είναι επεκτάσιμη. Κατά τη διάρκεια των ετών εταιρείες, όπως η Cisco, έχουν παράξει κάποιες ιδιόκτητες λύσεις για να ανταποκριθούν στα προβλήματα αυτά.

Για παράδειγμα, η Cisco έχει ένα πρωτόκολλο για τη διάδοση των VLANs. Αυτό δημιουργεί πρόσθετες σκέψεις, όπως: Όλος ο εξοπλισμός του δικτύου πρέπει να αγοραστεί από έναν μόνο προμηθευτή, διαλειτουργικότητα, όλες οι συσκευές από τον προμηθευτεί μπορεί να μην υποστηρίζουν το πρωτόκολλο, και το πρωτόκολλο λύνει ένα πολύ μικρό μέρος του προβλήματος.

Στο παραπάνω παράδειγμα βλέπουμε άλλο ένα σημαντικό μειονέκτημα των δικτύων σήμερα, την εξάρτηση από τον προμηθευτή.

Όταν οι προμηθευτές θέλουν να αναπτύξουν νέες υπηρεσίες για να ανταποκριθούν στις απαιτήσεις των επιχειρήσεων, η ικανότητά τους εμποδίζεται από το κύκλο ανάπτυξης του προϊόντος

Επίσης οι εταιρείες προτιμούν να αγοράζουν εξοπλισμό από έναν μοναδικό προμηθευτή για πολλούς λόγους, όπως: interoberability, ο χρόνος που απαιτείται για να μάθουν το νέο προιόν, λογιστική υποστήριξη και συντήρηση των γραμμών .

Επιπλέον, τα δίκτυα σήμερα δεν έχουν σχεδιαστεί για την έκρηξη της εποχής της πληροφορίας και είναι αδύνατο να ανταποκριθούν στις σύγχρονες απαιτήσεις της αγοράς.

Για παράδειγμα, για να προστεθεί ή να μετακινηθεί οποιαδήποτε συσκευή, πρέπει να γίνουν αλλαγές σε switches, routers, Firewalls, ACL, VLANs, QoS, στα πρωτόκολλα, ενώ έχοντας

πάντα υπόψη θέματα διαλειτουργικότητας μεταξύ των συσκευών και των εκδόσεων του λογισμικού.

Επιπλέον, οποιαδήποτε πιθανή διακοπή της υπηρεσίας κοστίζει σε χρήμα και σε πολύτιμη φήμη. Για τους λόγους αυτούς, τα δίκτυα δεν μεταβάλλονται συχνά.

Ακόμη, σε ένα σύνθετο και διαρκώς μεταβαλλόμενο περιβάλλον , οι διαχειριστές δικτύου αγωνίζονται να ανταποκριθούν στις απαιτήσεις των επιχειρήσεων και να εφαρμόζουν αποτελεσματικά την πολιτική διχτύου. Με την έκρηξη του Bring Your Own Device (BYOD), οι διαχειριστές ξαφνικά πρέπει να διαχειρίζονται πολλές διαφορετικές συσκευές, με διαφορετικά επίπεδα διαβάθμισης ασφαλείας

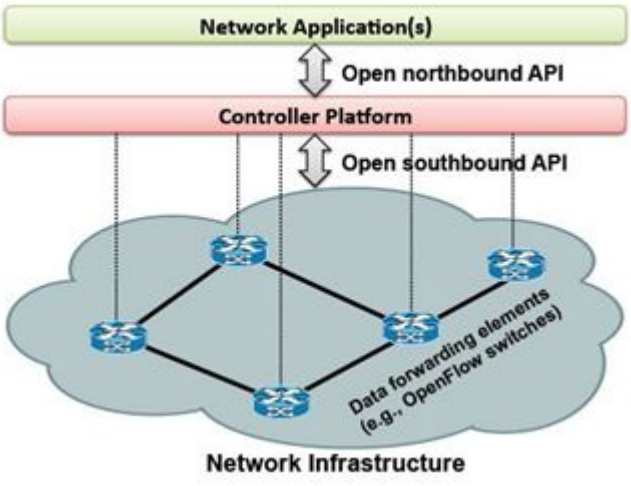
Αυτό έδωσε αφορμή για τη κατασκευή συστημάτων διαχείρισης κινητών συσκευών (MDM) και εξαγορές $1 billion ,όπως η εταιρεία Μεράκι από τη Cisco. Όπως υποδηλώνει το όνομα, τα MDM χρησιμοποιούνται για τη διαχείριση των κινητών συσκευών και συμβάλει στην εφαρμογή των πολιτικών σε όλο το δίκτυο. Η πολυπλοκότητα καθιστά την όλη διαδικασία αργή, και επιρρεπής σε σφάλματα.

Αυτό είναι πολύ πιο εύκολο να γίνει σε SDN δίκτυα παρά σε συμβατικά δίκτυα.

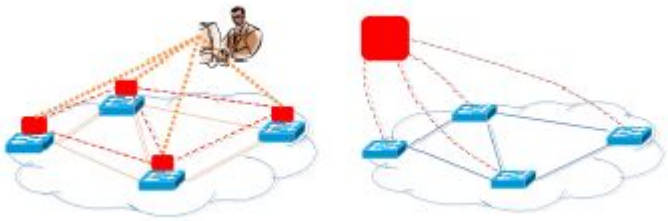
2.3 Software Defined Networks

Η SDN τεχνολογία δικτύωσης αποσυνδέει τα επίπεδα ελέγχου και δεδομένων του δικτύου. Στο SDN το υλικό χειρίζεται την προώθηση της κυκλοφορίας σύμφωνα με τους κανόνες που καθορίζονται από τον ελεγκτή. Ο ελεγκτής επικοινωνεί με όλες τις συσκευές του δικτύου χρησιμοποιώντας ένα πρωτόκολλο ή πρότυπο. OpenFlow [3], είναι το πρότυπο που χρησιμοποιείται πιο συχνά σήμερα.

Στο Σχήμα 2.1 και 2.2 βλέπουμε την αφαίρετικότητα που παρέχεται στο δίκτυο χρησιμοποιώντας την τεχνολογία SDN και την ικανότητα να ελέγχετε το δίκτυο από ένα σημείο ελέγχου υψηλού επιπέδου.



Σχήμα 2.1 Απλοποιημένη άποψη SDN δικτύου



Σχήμα. 2.2 Διαχειρισμός συσκευών δικτύου πριν και μετά το SDN

2.4 Ελεγκτές:

2.4 .1 Επισκόπηση:

Ένας ελεγκτής SDN είναι μια μηχανή που "κρατά" όλη η λογική για την ροή της κυκλοφορίας στο δίκτυο. Ο ελεγκτής είναι η καρδιά του δικτύου.

Ένας ελεγκτής συνήθως χρησιμοποιεί τα API νότια για να επικοινωνούν με τους δρομολογητές και τους διακόπτες (όπως OpenFlow) και API βόρεια όπως REST API για την επικοινωνία με τις εφαρμογές. Αυτή η αφαίρεση επιτρέπει την ευελιξία τόσο για τους προμηθευτές υλικού και τους προγραμματιστές.

Μέχρι το 2014 ο εξοπλισμός που υποστιρίζει το OpenFlow προτόκολλο, είναι σπάνιο να βρεθεί στα δίκτυα παραγωγής και είναι αρκετά δαπανηρός. Πρόσθετα νότια APIs , όπως η

διασύνδεση με το σύστημα δρομολόγησης (i2rs) έχει αναπτυχθεί για να αξιοποιήσει τα παραδοσιακά πρωτόκολλα όπως το OSPF, και MPLS [2].

Είναι σημαντικό να σημειωθεί εδώ ότι OpenFlow και SDN δεν είναι το ίδιο αλλά σε φόρουμ και συζητήσεις στο διαδίκτυο μερικές φορές το SDN και το OpenFlow χρησιμοποιείται αλληλένδετα.

2.4.2 Ελεγκτές-σύντομη ιστορία [4]:

Category	Pre-SDN	SDN
Data plane programming	NetScript ,SwitchWare	OpenFlow
Decoupling Control and Data Planes	4D ,RCP,Tempest	NOX, Ethane
Network Virtualization	Tempest, VINI ,Geni	Open vSwitch, Mininet FlowVisor
Network OS	Cisco IOS, JUNOS	NOX

Πίνακας 2.1: Διάφορα έργα στο παρελθόν που έδωσαν τις βάσεις για το SDN / NFV

Το SDN είναι έντονα επηρεασμένο από τις προηγούμενες προσπάθειες για να παρέχει λειτουργικότητα όπως τη αποσύνδεση του ελέγχου και του επίπεδου των δεδομένων, το virtualization του δίκτυου. Προ-SDN προσπάθειες, δεν υποστηρίζουν δίκτυα SDN και ως εκ τούτου δεν κληρονομούν τα οφέλη ότι μπορεί να αποκτηθεί με τη χρήση των δικτύων SDN.

Οι προσπάθειες για την εφαρμογή λογισμικού δικτύωσης σε commodity εξοπλισμό τρέχει πίσω στο '80, όπου οι hackers υλικού και άλλους λάτρεις έκαναν προσπάθειες να τρέξουν τα προτόκολλα δικτύου σε υπολογιστές αλλά ό, τι τρέχει στο υλικό είναι πολύ πιο γρήγορο από ό,τι στο λογισμικό. (Υλικό που έχει σχεδιαστεί για ένα συγκεκριμένο σκοπό, όπως η εφαρμογή ειδικών ολοκληρωμένων κυκλωμάτων.)

Μόνο η πρόσφατη προόδους στο υλικό, επέτρεψε στα πρωτόκολλα δικτύου να τρέχουν πάνω σε λογισμικό αποτελεσματικά

2.4.3 Ελεγκτές - Λειτουργικότητα:

Όταν ένας εξοπλισμός του δικτύου λαμβάνει ένα πακέτο ελέγχετε στον αντίστοιχο πίνακα για να παρθούν αποφάσεις προώθησης. Όταν δεν υπάρχει αντιστοιχία στον πίνακα που ελέγχεται το πακέτο προωθείται στον ελεγκτή. Ο ελεγκτής αποφασίζει τότε ποια είναι η αναγκαία δράση για το συγκεκριμένο πακέτο και στέλνει πίσω στο διακόπτη, την απαραίτητη λογική για το πακέτο και για τα επόμενα πακέτα. Ο διακόπτης θα ακολουθήσει αυτή τη λογική για ένα συγκεκριμένο χρονικό διάστημα (δηλαδή 30 δευτερόλεπτα) πριν το να στείλει ξανά στο ελεγκτή. Είναι δυνατόν να εκχωρήθεί προληπτικά λογική στον εξοπλισμό του δικτύου.
Η επικοινωνία μεταξύ του εξοπλισμού του δικτύου και τον ελεγκτή πραγματοποιείται μέσω κρυπτογραφημένου καναλιού (TLS).
Το OpenFlow επιτρέπει τον έλεγχο των ροών. Κάθε ροή δημιουργείτε από τον ελεγκτή και η κάθε ροή αποθηκεύεται στον πίνακα ροών. Στο Flow-Based έλεγχο αποθηκεύεται μία ροή σε κάθε εγγραφή του πίνακα ενώ στο συγκεντρωτικό μια εγγραφή καλύπτει ένα σύνολο από ροές.

2.4.4 Ελεγκτές - Ταχύτητα και Ανοχή σφαλμάτων:

Το πρώτο πακέτο της ροής πρέπει να πάει στον ελεγκτή, ο ελεγκτής λαμβάνει την απόφαση και το πακέτο πηγαίνει πίσω στο διακόπτη πριν διαβιβαστεί. Αυτή η διαδικασία διαρκεί 10 των χιλιοστών του δευτερολέπτου σε ιδανικές συνθήκες. (Δηλαδή δεν υπάρχει συμφόρηση)
Τα επόμενα πακέτα, αφού η λογική είναι εγκατεστημένο στο διακόπτη μπορεί να διαβιβαστεί σε λιγότερο από 1 ms. Αυτό ονομάζεται ο χρόνος προετοιμασίας της ροής.
Ως εκ τούτου, η τοποθέτηση των ελεγκτών του δικτύου σε στρατηγικό σημείο είναι απαραίτητη για να εξασφαλιστεί η επικοινωνία ελάχιστης καθυστέρησης μεταξύ διακόπτη και των ελεγκτών.
Έχοντας πολλαπλούς ελεγκτές και τοποθετώντας τους στα σωστά σημεία στο δίκτυο διασφαλίζεται μικρό χρονικό διάστημα επικοινωνίας μεταξύ διακοπτών και ελεγκτών Επίσης διασφαλίζεται ότι δεν υπάρχει μόνο ένα σημείο αποτυχίας το οποίο ενισχύει την ασφάλεια

και την διαθεσιμότητα του δικτύου.

Ελεγκτές όπως Onix [5] και HyperFlow [6] προσπαθούν να διατηρήσουν ένα λογικά συγκεντρωμένο αλλά φυσικά διανεμημένο επίπεδο ελέγχου, ενώ ο Kandoo [7] χρησιμοποιεί μια υβριδική προσέγγιση που μπορεί να αξιοποιήσει τους τοπικούς ελεγκτές για θέσεις εργασίας σε τοπικό επίπεδο και παγκόσμιο ελεγκτή για τις θέσεις εργασίας που απαιτούν ευρεία γνώση του δικτύου

Όταν θέλουμε να επιλέξουμε τι ελεγκτή να χρησιμοποιήσουμε [Table.2] διάφοροι παράγοντες έχουν σημασία όπως:

τι γλώσσες προγραμματισμού γνωρίζουμε, τη στήριξη της κοινότητας, τη καμπύλη εκμάθησης. Για αυτή την διπλωματική χρησιμοποιήθηκε ο ελεγκτής POX, ο οποίος είναι ανοικτού κώδικα ελεγκτής που αναπτύχθηκε από Nicira (αποκτήθηκε από την VMware). Οφέλη από τη χρήση POX περιλαμβάνουν: εύκολος στην εκμάθηση, εύκολη εγκατάσταση, τρέχει σε όλα τα λειτουργικά συστήματα, και καλό για μαθησιακούς σκοπούς.

2.4.5 Τύποι ελενγκτών

Controller	Implementation	Open Source	Developer
POX	Python	Yes	Nicira
NOX	Python/C++	Yes	Nicira
Maestro	Java	Yes	Rice university
Trema	Ruby/C	Yes	NEC
Floodlight	Java	Yes	BigSwitch
OpenDaylight	Java	Yes	Linux

Πίνακας 2.2: Ελενγκτές

2.5 Ενδιαφέρουσες εφαρμογές- κυκλοφορίας δεδεομένων

ElasticTree [8] Είναι ένα πρωτόκολλο δρομολόγησης που σχεδιάστηκε από το Στάνφορντ και την HP. Η εφαρμογή εκμεταλλεύεται το γεγονός οτι γνωρίζει όλο το δίκτυο

χρησιμοποιώντας το OpenFlow και συγκεκριμένα τον ελεγκτή NOX και προσπαθεί να μειώσει τους λογαριασμούς ηλεκτρισμού των κέντρων δεδομένων. Ο λογαριασμός ηλεκτρικού ρεύματος των κέντρων δεδομένων απαρτίζει ένα μεγάλο ποσοστό του OpEx.

Η αποτελεσματικότητα των υποδομών (DCIE) [9], είναι το ποσοστό της αξίας που προέρχεται από τη διαίρεση της τεχνολογίας των πληροφοριών παραγωγής ηλεκτρικού ρεύματος με συνολική ισχύ εγκατάστασης . ElasticTree μειώνει την ηλεκτρική ενέργεια από την παρακολούθηση του φόρτου της κίνησης στους συνδέσμους και τον εξοπλισμό του δικτύου, καθώς και με το κλείσιμο του εξοπλισμού που δεν χρειάζεται, διατηρώντας παράλληλα ένα περιθώριο ασφαλείας για αναπάντεχη υπερβολική ζήτηση της κυκλοφορίας ή για πιθανές βλάβες του εξοπλισμού. Το ποσοστό των δαπανών για ηλεκτρική ενέργεια, που αφορά δίκτυα και δικτυακό εξοπλισμό σε ένα κέντρο δεδομένων είναι μέχρι και 20%. Με το κλείσιμο του μη απαραίτητου εξοπλισμό, το ElasticTree χρησιμοποιεί ένα υποσύνολο του προηγούμενου Fat Tree με αποτέλεσμα έως και 38% εξοικονόμηση στο λογαριασό του ρεύματος Απλά για τα κέντρα δεδομένων στις ΗΠΑ η εξοικονόμηση εκτιμάτε ότι μπορεί να είναι περίπου 1 δισ KWhr ετησίως.

2.6 Το μέλλον των SDN

Ας εξετάσουμε τώρα το μέλλον της SDN σε αριθμούς. Το SDN εμφανίστηκε για πρώτη φορά το 2007 και μέχρι το 2012,οι εταιρείες SDN που εξαγοράστικαν ισούνται με 1,5 δισεκατομμύρια δολάρια ενω υπάρχουν περισσότερα από 225 SDN εταιρείες. Η συνολική αγορά SDN αναμένεται να φθάσει τα $ 35 δισεκατομμύρια μέχρι το 2018. [36]

Κεφάλαιο 3

Network Functions Virtualization

3.1 Εισαγωγή-Σύντομη Ιστορία του NFV

3.2 Οφέλη από NFV

3.3 Εικονική δικτύωση και τεμαχισμός Δικτύων.

3.4 NFV adoption survey

3.1 Εισαγωγή-Σύντομη Ιστορία του NFV [13]

Το NFV δημιουργήθηκε το 2012 από την AT & T, η BT, η China Mobile και η Deutsche Telekom μαζί με Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) ως τις προδιαγραφές του Ομίλου Βιομηχανίας. Ορισμός NFV είναι: «κάθε υπηρεσία που μπορεί να παραχθεί σε ιδιόκτητες εφαρμογές μπορεί να τρέξει σε εικονικές μηχανές". Λειτουργίες δικτύου που τρέχουν σε hardware μπορεί τώρα να τρέχουν εικονικά. Λειτουργίες όπως firewalls, load balancers, το DNS, caching, NAT

3.2 Οφέλη από NFV [14] [17] [18]

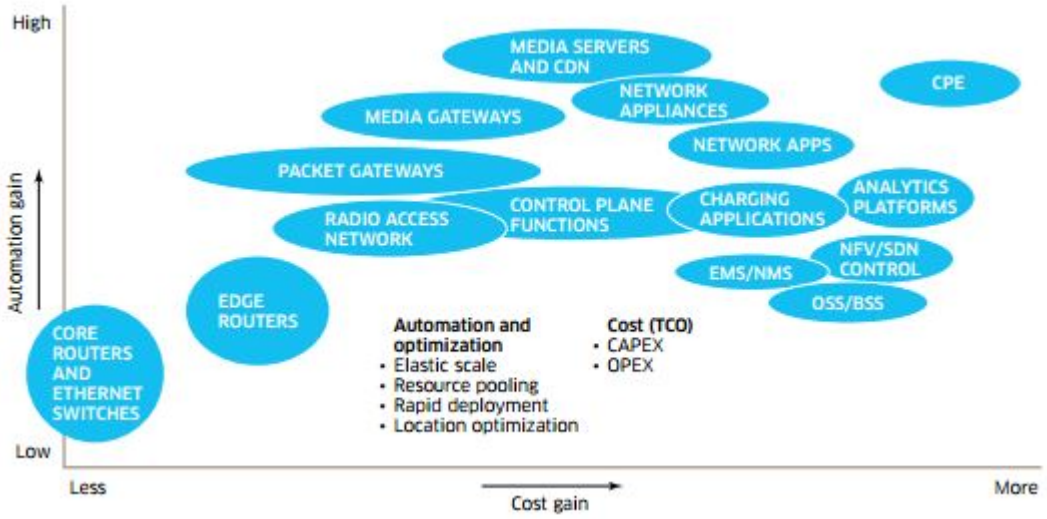
Η ανάπτυξη του NFV καθοδηγείται κυρίως από τεράστια μείωση χρόνου και κόστους κατά την ανάπτυξη και τη συντήρηση των λειτουργιών του δικτύου. SDN και NFV επιτρέπουν στους χρήστες να βελτιστοποιήσουν τη χρήση πόρων του δικτύου, και να δημιουργήσουν δυναμικά εικονικά δίχτυα .

Τα οφέλη του NFV:

Μείωση capital expenses: μειώνεται η ανάγκη πρόβλεψης για μελλοντική ανάπτυξη. Αντ 'αυτού ένα pay as you grow μοντέλο χρησιμοποιείται

Μείωση των λειτουργικών εξόδων: μειωμένες απαιτήσεις σε χώρο, ενέργεια για μηχανήματα και ψύξη των μηχανημάτων.

Επιτάχυνση του χρόνου διάθεσης στην αγορά: Μειώνει το χρόνο για να αναπτυχθούν νέες υπηρεσίες δικτύου και να αναβαθμίσουν γρήγορα σύμφωνα με τις ταχέων μεταβαλλόμενες απαιτήσεις της αγοράς.

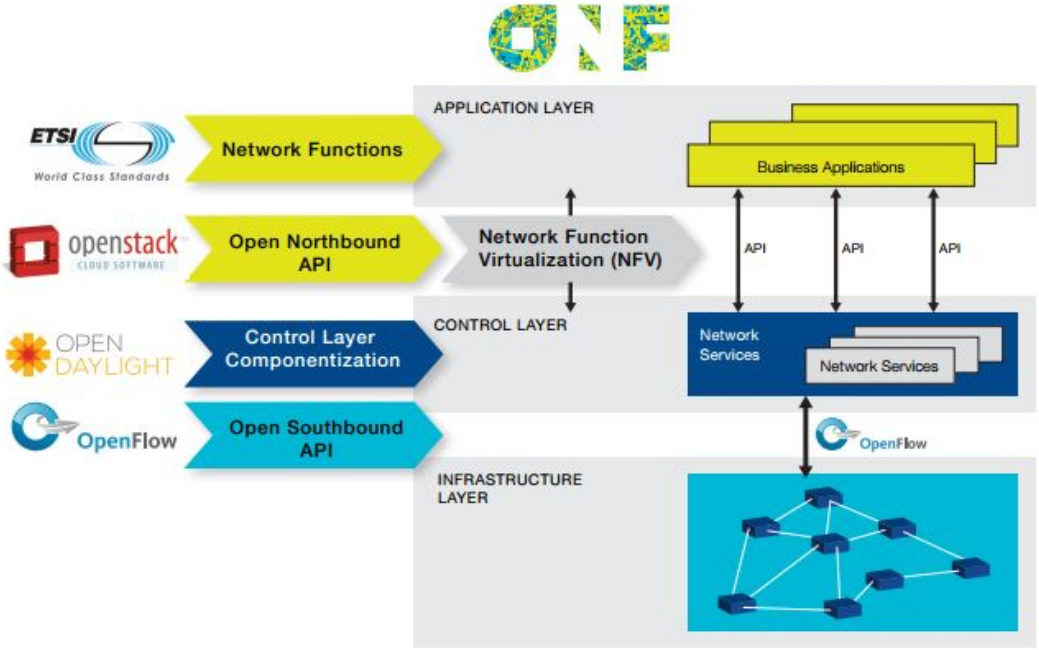


Σχήμα. 3.1 Αυτοματοποίηση και κέρδος [11]

Είναι προφανές ότι όπια λύση ανακαλύψουμε για να αυτοματοποιήσουμε τις λειτουργίες δικτύου, πάντα θα χρειαζόμαστε την βασική υποδομή για να τρέξουμε τις εφαρμογές μας πάνω (bare metal). Ο βαθμός αυτοματοποίησης που μπορεί να επιτευχθεί ποικίλλει ανάλογα με τον τύπο του πόρου. Όπως φαίνεται στο διάγραμμα 3.1 οι συσκευές Customer Premises Equipment (CPE) μπορούν να αυτοματοποιηθούν πολύ παρέχοντας σημαντικά οφέλη κόστους για τους πάροχους των ευρηζωνικών υπηρεσιών.

Στην αρχή του SDN (2009), το SDN και NFV ήταν το ίδιο και το αυτό. Το 2012 η διαφορά μεταξύ του SDN και NFV έγινε πιο εμφανής και οδήγησε στη δημιουργία NFV. Όταν αναφερόμαστε σε SDN εννοούμε συνήθως διακόπτες που υποστιρίζουν OpenFlow που μπορούν να ελέγχονται από έναν ελεγκτή. NFV είναι υπηρεσίες όπως το NAT, firewall που εκτελείται σε λογισμικό και παρέχει δεδομένα στον ελεγκτή για να λάβει τις απαραίτητες αποφάσεις.

3.3 Εικονική δικτύωση και τεμαχισμός Δικτύων.



Σχ. 3.2 SDN και NFV μαζί στο δίκτυο [12]

3.3.1 Εφαρμογές Εικονική δικτύωση [4]

Υπάρχουν πολλά οφέλη και πιθανές εφαρμογές από τη χρήση εικονικών δικτύων και από τον τεμαχισμό των πόρων του δικτύου όπως:

Πειραματισμός πάνω στα δίκτυα παραγωγής - πειραματική υποδομή μπορεί να τρέξει παράλληλα με την παραγωγή

Ανάπτυξη υπηρεσιών, ανεξάρτητα από το υλικό και τον προμηθευτή

Δυναμική Κλιμάκωση των πόρων - είναι δυνατή η εκχώρηση από ένα σύνολο πόρων

3.3.2 Γιατί να τεμαχιστεί το δίκτυο [4]

Τμήματα με διαφορετικές ανάγκες

Πολλαπλοί πελάτες-ενοικιαστές σε κέντρο δεδομένων

Πειραματισμός

Ενοικίαση κομματιών του δικτύου σε άλλους πάροχους

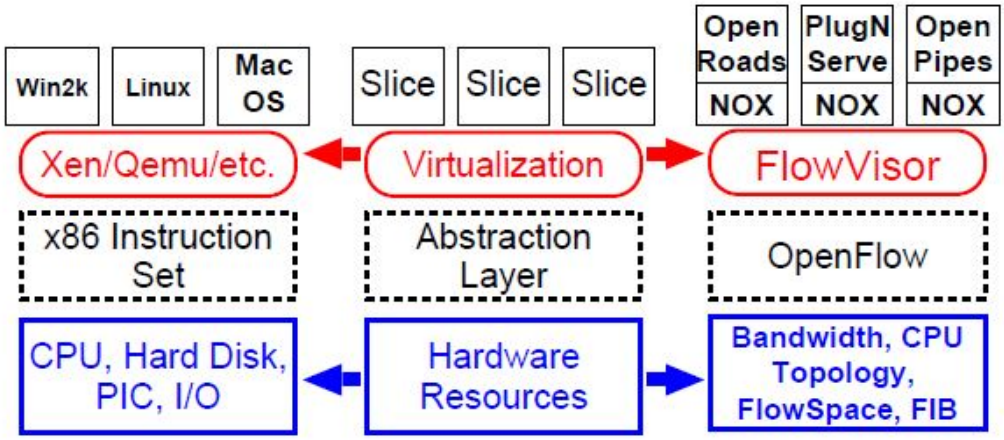
Οι εταιρείες που προσφέρουν υπηρεσίες PaaS και IaaS όπως το Microsoft Azure και AWS ήδη χρησιμοποιούν αυτές τις τεχνολογίες για να επιτρέψουν σε πολλαπλούς ενοικιαστές να χρησιμοποιούν τα κέντρα δεδομένων τους. Κάθε πελάτης μπορεί να σχεδιάσει και να χρησιμοποιήσει το δικό του εικονικό δίκτυο.

Επιπλέον, για να δοκιμάστούν νέες πειραματικές υπηρεσίες σήμερα, θα πρέπει να δημιουργηθεί ένα νέο δίκτυο παρόμοιο με το δίκτυο παραγωγής για τη δοκιμή των νέων υπηρεσιών.

Εναλλακτικά μπορεί να χρησιμοποιηθεί προσομοίωση που επίσης κοστίζει αρκετά και τα αποτελέσματα δεν είναι απολύτως αντιπροσωπευτικά με τη συμπεριφορά που θα είχε η νέα υπηρεσία στο production δίκτυο. Μερικές φορές η χρήση προσομοίωσης δεν είναι εφικτή.

Ο τεμαχισμός του δικτύου περιλαμβάνει τον τεμαχισμό του εύρους ζώνης, την τοπολογία, την κυκλοφορία, πίνακες προώθησης κ.ο.κ.

Υπάρχουν πολυάριθμες λύσεις για τον τεμαχισμό του δικτύου [Πίνακας 3]. Εκτός από FlowVisor [26], OpenVirtex [24] ενεργεί ως πληρεξούσιος μεταξύ του λειτουργικού συστήματος του δικτύου και τις συσκευές προώθησης. AutoSlice [25] είναι μια άλλη λύση που επιτρέπει σε πολλαπλούς ελεγκτές για τη διαχείριση εικονικού δικτύου SDN τους.



Σχ. 3.3 τεμαχισμός του δικτύου χρησιμοποιώντας FlowVisor

Solution	Multiple Controllers	Slicing
FlowVisor [26]	Yes, one per slide	Virtual flow tables per slice
AutoSlice [25]	Yes, one per slide	VLAN tags
OpenVirteX [24]	Yes, one per slide	Virtual flow tables per slice
Splendid Isolation [23]	Single controller	Compiler time VLAN

Πίνακας 3.1: Λύσεις τεμαχσμού του δικτύου

3.4 NFV adoption survey[16]

Σύμφωνα με μια έρευνα που έγινε απο την HP, τον Ιανουάριο του 2014 οι προτεραιότητες των CIOs και CTOs των παρόχων υπηρεσιών σε παγκόσμιο επίπεδο είναι οι εξής:

Απαντώντας στην ερώτηση:

"Πότε τα NFV θα είναι ένας σημαντικός παίκτης στην αγορά των Παρόχων Υπηρεσιών";

Σχεδόν οι μισοί από τους συμμετέχοντες αναμένουν ότι NFV θα είναι ένας σημαντικός παίκτης στα επόμενα 2-3 χρόνια, ενώ ένα επιπλέον 36% μέσα στα επόμενα 1-2 χρόνια.

Απαντώντας στην ερώτηση «Ο πιο σημαντικός λόγος που θα χρησιμοποιούσατε NFV στην επιχείρηση";

21% δήλωσε ότι τα νέα έσοδα είναι ο κύριος λόγος, που ακολουθείται από 15% για τη μείωση του κόστους επένδυσης, το 13% για τη μείωση των λειτουργικών εξόδων και, τέλος, 13% για την αύξηση της ευελιξίας και της κλιμάκωσης

Απαντώντας στην ερώτηση «Η πιο σημαντική τεχνική πρόκληση» .26% πιστεύει ότι η διαλειτουργικότητα και φορητότητα είναι η μεγαλύτερη τεχνική πρόκληση που ακολουθείται από 18% ότι η διασφάλιση των επιδόσεων είναι μια άλλη σημαντική πρόκληση.

Κεφάλαιο 4

OpenStack [19] [20] [21] [22]

4.1 Επισκόπηση:

OpenStack είναι ένα σύνολο εργαλείων λογισμικού για την οικοδόμηση και τη διαχείριση πλατφόρμων πληροφορικής για δημόσια και ιδιωτικά clouds. OpenStack είναι ένα λειτουργικό σύστημα για το σύννεφο. Το έργο ξεκίνησε από την εταιρεία Rackspace και την NASA και από τότε υποστηρίζεται από 190 μεγάλες εταιρείες όπως η Dell, HP, IBM και χιλιάδες άτομα.

OpenStack είναι γραμμένο κυρίως σε Python και διανέμεται υπό την άδεια Apache.

4.2 Λειτουργικότητα:

Το OpenStack "δημιουργεί" δεξαμενές πόρων, καθώς και δεξαμενές εφαρμογών που επικοινωνούν με τους πόρους αυτούς μέσω API. Dashboards και άλλες διαχειριστικές λειτουργίες χρησιμοποιούν επίσης API για να ανάψουν εικονικές μηχανές, τη δημιουργία εικονικών δικτύων κλπ.

OpenStack είναι μια αφηρημένη έννοια, ένα στρώμα ελέγχου που εκτελείται πάνω από διαφορετικά Hypervisors που τρέχουν στο κέντρο δεδομένων.

Για παράδειγμα, ένα κέντρο δεδομένων μπορεί να έχει πολλαπλούς servers από διαφορετικούς πωλητές, και εικονικές μηχανές που χρησιμοποιούν Hypervisors όπως KVM, XEN, η VMware, Hype-V. Αυτά τα Hypervisors απο διαφορετικούς πωλητές, ελέγχονται χρησιμοποιώντας διαφορετικές εντολές και λειτουργούν με διαφορετικό τρόπο, που δημιουργεί πολυπλοκότητα και προβλήματα διαλειτουργικότητας.
Το Openstack είναι επίσης ένα εργαλείο που βοηθά στη δημιουργία δικτύων με υψηλότερη διαθεσιμότητα και ανοχή σφαλμάτων περιβάλλοντα ακόμα και μεταξύ διαφορετικών κέντρων δεδομένων.

4.3 Τα Συστατικά του OpenStack:

Nova: Η κύρια μηχανή, ο ελεγκτής. Χρησιμοποιείται για την ανάπτυξη και τη διατήρηση εικονικών μηχανών

Swift: Το σύστημα αποθήκευσης. Αυτόματη επιλέγει πού θα αποθηκεύονται τα δεδομένα, φροντίζει για back ups και καθιστά εύκολη την κλιμάκωση.

Neutron: παρέχει τις δυνατότητες δικτύωσης.

Horizon: Το ταμπλό του OpenStack, αφού OpenStack είναι ανοιχτού κώδικα καθένας μπορεί να δημιουργήσει ένα ταμπλό προσαρμοσμένο στις ανάγκες του.

Κεφάλαιο 5

Ασφάλεια

5.1 Εισαγωγή

Οι SDN αρχιτεκτονικές μοιράζονται πολλούς παρόμοιους τύπους επιθέσεων με τα συμβατικά δίκτυα αλλά αντιμετωπίζουν και άλλες διαφορετικές απειλές. Οι απειλές αυτές μπορούν να στοχεύσουν τους ελεγκτές και τα μονοπάτια μεταξύ ελεγκτών και διακοπτών.

Θα πρέπει να λαμβάνεται ειδική μέριμνα για σκλήρυνση των ελεγκτών, καθώς είναι πολύ ελκυστικοί στόχοι για τους επιτιθέμενους.

Όλη η επικοινωνία μεταξύ των διακοπτών και των ελεγκτών είναι κρυπτογραφημένη με τη χρήση TLS. [3]

5.2 Επιθέσεις εναντίον στο SDN

5.2.1 Denial of Service

Denial of Service μπορεί να συμβεί εναντίων κόμβων αλλά επίσης και εναντίων των μονοπατιών μεταξύ των ελεγκτών και τον διακοπτών.

Ακόμα ένας τρόπος να πραγματοποιηθεί αυτή η επίθεση είναι η αποστολή πολλών τυχαία

δημιουργημένων πακέτων και αφού το κάθε πακέτο δεν θα ταιριάζει σε καμία ροή μέσα στους πίνακες του διακόπτη, θα προωθούνται όλα στον ελεγκτή

Επιπλέον, αν ένας εισβολέας καταφέρει να γεμίσει με δεδομένα ή να διακόψει τη γραμμή μεταξύ του ελεγκτή και του διακόπτη και αν δεν υπάρχει αρκετό εύρος ζώνης ή επιπλέον συνδέσεις μεταξύ του ελεγκτή και του διακόπτη, ο διακόπτης θα χάσει την επικοινωνία με τον ελεγκτή και ολόκληρο το τμήμα του δικτύου πίσω από τον ελεγκτή θα πάει κάτω.

5.2.2 Αναγνώριση

Πριν από τη εκτέλεση μιας επίθεσης ένας εισβολέας προσπαθεί να μάθει όλες τις πληροφορίες που μπορεί σχετικά με το δίκτυο ώστε να μπορεί να εκμεταλλευτεί αυτήν την πληροφορία αργότερα σε μια εξειδικευμένη επίθεση

Στο SDN, ένας εισβολέας που κάνει αναγνωρίσεις, εν δύναμη επιδιώκει να μάθει τους κανόνες ροής που εγκαταστάθηκαν στον διακόπτη και που στέλλονται τα πακέτα για μια συγκεκριμένη ροή.

Η επίθεση αυτή χρησιμοποιεί ανάλυση χρονισμού. Όπως προαναφέρθηκε, κάθε πακέτο που διαβιβάζονται στον ελεγκτή εμφανίζει πολύ υψηλότερο RTT.

5.2.3 Διοικητική σταθμοί

Ο επιτιθέμενος θα επιδιώξει να αναλάβει τον έλεγχο των διοικητικών σταθμών (που έχουν πρόσβαση στους ελενγκτές), γιατί τότε μπορεί να ελέγξει το δίκτυο. Αυτή η απειλή αυτή δεν είναι ειδική σε SDN, αλλά στο SDN η κατάλυψη του διοιητικού σταθμού σημαίνει το συνολικό έλεγχο του δικτύου.

Είναι ζωτικής σημασίας η σκλήρυνση των σταθμών ελέγχου και η χρήση out-of-bound σύνδεσης για την επικοινωνία του διακόπτη ελεγκτή.

5.3 Αξιοποίηση των SDN για εφαρμογές ασφάλειας

Πολλά από τα έργα που δημιουργήθηκαν προσπαθούν να αξιοποιήσουν τη δύναμη των SDN για την παροχή καλύτερων λύσεων ασφάλειας. Οι περισσότερες λύσεις που προτάθηκαν ευκολήνουν τη διοίκηση και είναι λιγότερο επιρρεπείς σε σφάλματα διαμόρφωσης ή σε αντικρουόμενους κανόνες ασφαλείας

Μερικές από τις λύσεις ασφάλειας SDN στοχεύουν: στον αποτελεσματικό έλεγχο της πρόσβασης, στη γρήγορη ανίχνευση και τον μετριασμό των επιθέσεων DDOS, την παρακολούθηση της υποδομής καιθώς και τη δημιουργία fine-grain πολιτικών ασφαλείας.

Παρακάτω παρατίθενται μερικά ενδιαφέροντα έργα SDN.

5.3.1 Ενεργός Ασφαλεία [34]

Για να συνειδητοποιήσουμε ότι μια επίθεση είναι υπό εξέλιξη στα συμβατικά δίκτυα, βλέπουμε είτε οπτικά σήματα, όπως τα αρχεία καταγραφής (από τους servers ή firewalls), ή έχουμε κάποιο συναγερμό από κάποιο συστήματος αποτροπής εισβολών.

Ένας περιορισμός στα συμβατικά συστήματα, είναι ότι η θέση τους στο δίκτυο, τους επιτρέπει να συλλέγουν πληροφορίες μόνο από ένα τμήμα του δικτύου. Τα στοιχεία ασφαλείας σήμερα λειτουργούν ξεχωριστά, και ως εκ τούτου δεν επιτρέπουν μια πλήρη εικόνα της ασφάλειας του δικτύου να σχηματιστεί. Firewalls, IPS / IDS, Digital Forensics tools συλλέγουν πληροφορίες και μπορούν να αποσταλούν σε μια κεντρική μονάδα διαχείρισης και ανάλυσης πληροφοριών (SIEM) για να δημιουργηθεί μια πλήρη εικόνα του δικτύου και είτε χειροκίνητα είτε αυτόματα να αποφασιστούν οι ενέργειες που πρέπει να ληφθούν όταν το δίκτυο είναι υπό επίθεση.

Η Ενεργός Ασφαλείας [34] οδηγεί την προσέγγιση αυτή ένα βήμα παραπέρα με τη συλλογή του περιεχομένου της μνήμης κατά τη διάρκεια της επίθεσης που είναι πιθανό να καθαρίστεί μετά από την επίθεση από τον εισβολέα. Με την εξαγωγή του περιεχομένου της μνήμης κατά τη διάρκεια της επίθεσης, μπορούμε να ελέγξουμε ποια αρχεία είναι ανοιχτά, ποιες υποδοχές δίκτυου χρησιμοποιούνται. κ.ο.κ. Το πιο σημαντικό είναι ότι τα κρυπτο κλειδιά μπορούν να συλληφθούν και αυτό μας επιτρέπει την αποκρυπτογραφήση των συνδέσεων των κανάλιων επικοινωνίας που χρησιμοποιήθηκαν από τον εισβολέα στην επίθεση. Επιπλέον ο

κακόβουλος κώδικας μπορεί να μεταφερθεί σε ένα guarantined σύστημα για περαιτέρω μελέτη.

5.3.2 OpenFlow-Random host mutation (OF-RHM) [33]

Ένα στατικό δίκτυο επιτρέπει στον εισβολέα να μελετήσει το δίκτυο σε βάθος και να αναλύσει τις αδυναμίες που μπορούν να αξιοποιηθούν σε μια επίθεση. Στη συνέχεια, χρησιμοποιώντας ένα κόμβο που έχει καταληφθεί μπορεί να επιτεθεί περαιτέρω σε άλλους κόμβους στο δίκτυο.

Το OpenFlow-Random host mutation προστατεύει συστήματα από επιθέσεις, παρέχοντάς τους εικονικές διευθύνσεις IP οι οποίες μεταφράζονται σε πραγματικές διεύθυνσεις IP από τον ελεγκτή. Εικονική διευθύνσεις IP αλλάζουν συνεχώς και κατά συνέπεια δεν επιτρέπει στον εισβολέα να έχει μια ολοκληρωμένη εικόνα του δικτύου, δημιουργώντας ένα "Moving Target Defence". Η τεχνική αυτή είναι παρόμοια με την frequence hoping που χρησιμοποιείται στη στρατιωτική επικοινωνία. [30]

Στο OF-RHM ο ελεγκτής εκτελεί τις ακόλουθες εργασίες:

συντονίζει την αλλαγή των διευθύνσεων σε όλους τους διακόπτες, ελέγχει για διαθέσιμες διευθύνσεις IP , προσδιορίζει την βέλτιστη σειρά νέων εικονικών διευθύνσεων και της αναθέτει σε κόμβους, καθώς και NAT, DNS.

Η λειτουργία φένεται καλύερα στο σχήμα 5.3

Παρά το γεγονός ότι το RHM ήταν δυνατό σε συμβατικά δίκτυα, ήταν πάρα πολύ δαπανηρό και πρόσθετε μεγάλη πολυπλοκότητα στο δίκτυο.

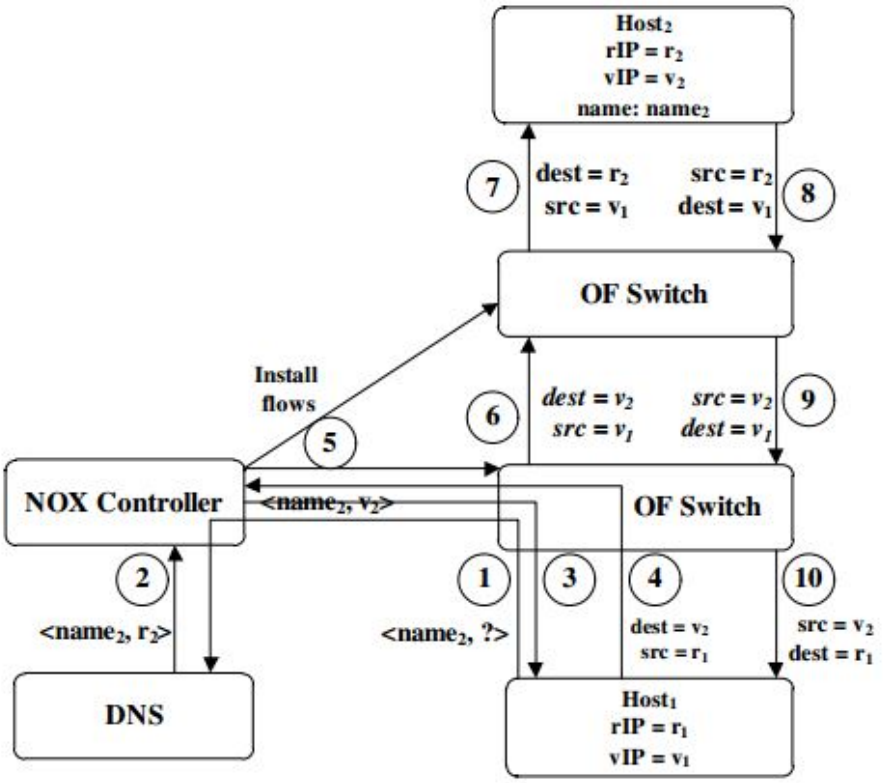


Fig. 5.1 Random Host Mutation Flow

5.3.3 FortNox [32]

FortNox είναι μια επέκταση του NOX ελεγκτή, και έχει ως στόχο να ενισχύσει το NOX με τη δυνατότητα να επιβάλλει περιορισμούς στις ροές του δικτύου.

Το FortNox ενσωματώνει μια μηχανή ανίχνευσης σύγκρουσης κανόνων ροής. Το ForNox αποφασίζει να αποδεχθεί ή να απορρίψει ροές ανάλογα με το αν η αίτηση εισαγωγής έρχεται από μια υψηλότερη άδεια ασφάλειας.

Αξιολογώντας έναν υποψήφιο κανόνα ροής έναντι 1000 άλλων κανόνων ροής παίρνει 7 ms, το οποίο είναι αρκετά γρήγορ.

Το FortNox εγκαταστεί κανόνες κάποιας πολιτικής, με την έκφραση

Αφήστε http κυκλοφορίας στο web server

Φόρμα <οπουδήποτε> -> Θύρα διακομιστή 80 προς τα εμπρός

5.4 Ασφάλεια as a Service (SaaS) [41], [42]

SaaS είναι ένα επιχειρηματικό μοντέλο, το οποίο οι πάροχοι μπορούν να πωλούν ως συνδρομή. Οι υπηρεσίες ασφαλείας των παρόχων είναι συνήθως πιο αποτελεσματική και σε χαμηλότερες τιμή από ό, τι οι περισσότεροι μικροί οργανισμοί μπορούν να αντέξουν οικονομικά από μόνοι τους. Οι υπηρεσίες αυτές μπορούν να περιλαμβάνουν: Firewall, Anti-Virus, DPI, IPS και άλλα.

Τα οφέλη για τις επιχειρήσεις μπορεί να περιλαμβάνουν

Constant virus definition updates

Grater security expertise

Overall cost reductions.

Κεφάλαιο 6

Home Gateway / Set Top Boxes

6.1 Επισκόπηση

6.2 Οφέλη NFV για τα δίκτυα του σπιτιού

6.3 Χαρακτηριστικά / υπηρεσίες που μπορεί να μετακινηθούν στο σύννεφο

6.1 Επισκόπηση [37]

Residential Gateway, Customer Premises Equipment (CPE) είναι ο εξοπλισμός που συναντιέται πιο συχνά στα σπίτια σήμερα για την παροχή υπηρεσιών διαδικτύου.

Ο όρος CPE, αναφέρεται συνήθως στις λιγότερο ακριβές συσκευές με μικρές ικανότητες. Επιτρέπουν τη σύνδεση των δικτύων του σπιτιού LAN / s με το WAN (συνήθως το Internet) μέσω μιας υπηρεσίας παροχής Internet (ISP). WAN σύνδεση παρέχεται συνήθως μέσω των γραμμών τηλεφώνου, καλωδιακής γραμμής, γραμμές οπτικών ινών, ή δορυφορικής σύνδεσης. Μερικές από τις τυπικές λειτουργίες των πυλών είναι NAT, DHCP, παρέχουν δυνατότητες firewall, Internet πρωτόκολλο δρομολόγησης, ασύρματη συνδεσιμότητα, και μόντεμ.

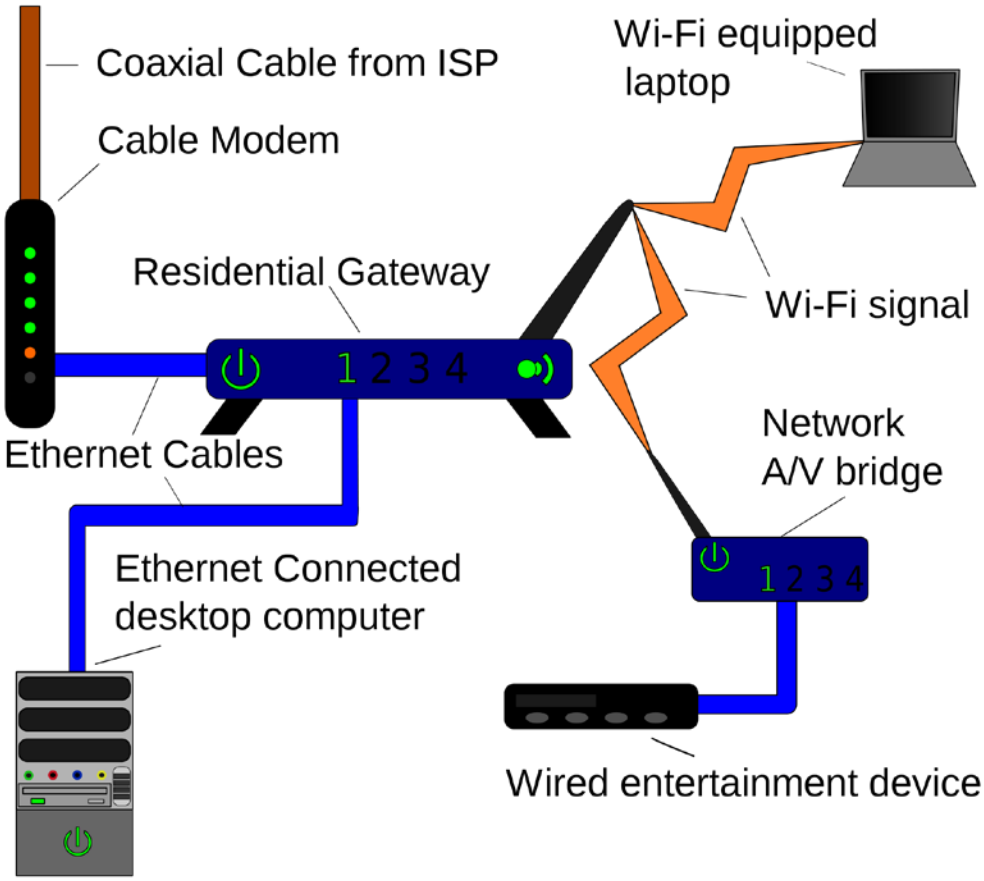
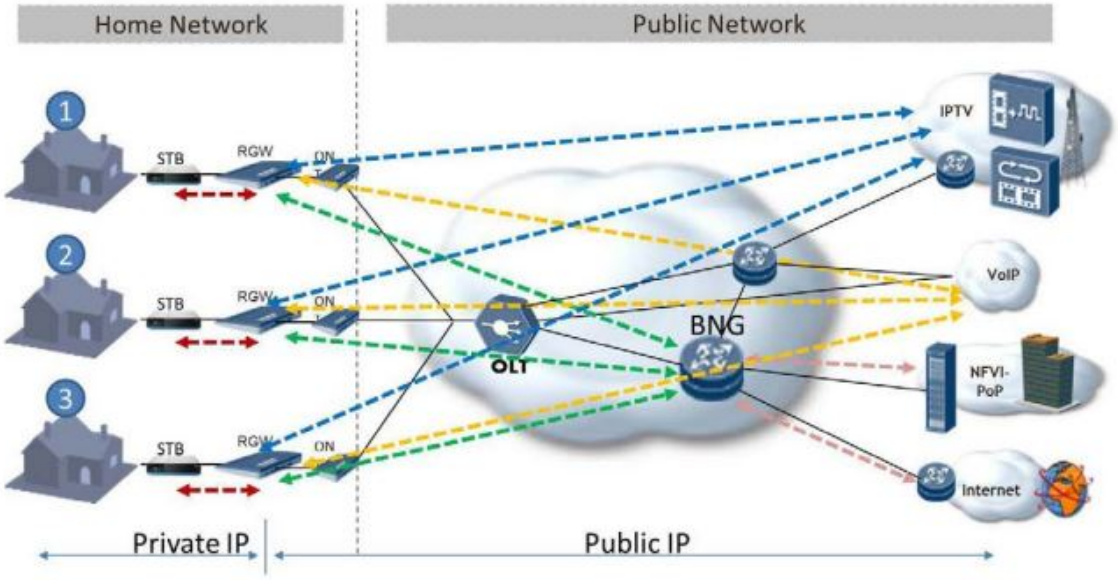


Fig. 6.1 Τυπικό σενάριο Home Gateway. Πύλη και μόντεμ είναι συνήθως στο ίδιο κουτί.

Set-Top Box (STB) [39] είναι μια συσκευή που περιέχει μια είσοδο δέκτη και συνδέεται με μια τηλεόραση. Ένα STB ανά τηλεόραση είναι απαραίτητο. Η πηγή του σήματος μπορεί να προέλθει από Ethernet, καλωδιο ή δορυφορική. Υβριδικά κουτιά μπορούν να λαμβάνουν σήματα από Ethernet (για παράδειγμα για τα κανάλια HD) και από τον αέρα για το υπόλοιπο των καναλιών, μειώνοντας έτσι την ανάγκη για το εύρος ζώνης υψηλής ταχύτητας. Ορισμένα STB έχουν τοπική μνήμη για αποθήκευση μαγνητοσκοπημένων τηλεοπτικών σειρών.

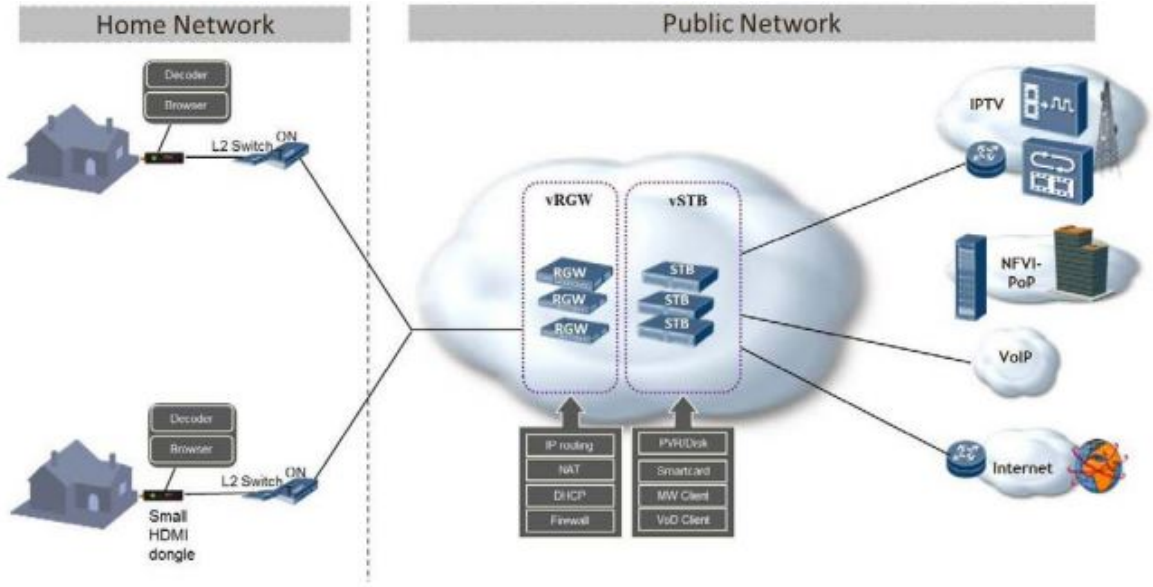


Σχ. 6.2: Τυπικό σενάριο όπου STB και HG διαμένουν στις εγκαταστάσεις του πελάτη.

6.2 Οφέλη NFV για τα δίκτυα του σπιτιού [38] [40]

Υπάρχουν αρκετές λειτουργίες στο οικιακό δίκτυο που μπορεί να γίνουν vritualized και συνοψίζονται παρακάτω. Αυτές οι λειτουργίες μπορούν πλέον να διαμένουν στο σύννεφο (Εικόνα 6.3) και παρέχουν διάφορα οφέλη για τους παρόχους και τους χρήστες. (όπως αναφέρεται στην παράγραφο 3.2)

Επιπλέον, επιτρέπει στους παρόχους την παροχή πρόσθετων υπηρεσιών, χαμηλότερες τιμές για τις υφιστάμενες υπηρεσίες, και να χρησιμοποιούν διαφορετικές δομές τιμολόγησης.



Σχήμα. 6.3: STB και εικονικές πύλες στο σύννεφο

Πρόσθετα οφέλη για τη χρήση των λειτουργιών NFV για το σπίτι περιλαμβάνουν:

Μικρότερο χρόνο εισαγωγής νέων υπηρεσιών στην αγορά αφού οι νέες υπηρεσίες εγκαθίστανται από τον πάροχο στο cloud χωρίς την αγορά και διανομή νέων HomeGateways. Επίσης οι ενημερώσεις γίνονται επίσης αυτόματα από τον πάροχο.

Ακόμη αποφεύγεται η εγκατάσταση νέου εξοπλισμού. Οι ISPs, τώρα, πρέπει να αντικαθιστούν τα HomeGateways τους κάθε λίγα χρόνια, καθώς εμφανίζονται νέες τεχνολογίες και νέα χαρακτηριστικά.

Δεδομένου ότι οι πάροχοι υπηρεσιών Διαδικτύου αλλάζουν τις παλιές πύλες τους με νέες, σε κάθε δεδομένη στιγμή υπάρχουν HomeGateways από διάφορους προμηθευτές στο δίκτυο που δημιουργεί πολύπλοκη υλικοτεχνική υποστήριξη.

Επίσης όταν τα HomeGateways είναι στο cloud υπάρχουν πρόσθετες δυνατότητες για τη συντήρηση και τη διάγνωση προβλημάτων

Άλλο πλεονέκτημα είναι η παροχή API για να χρησιμοποιηθεί από τις υπηρεσίες τρίτων.

Παρ 'όλα τα οφέλη που προκύπτουν από αυτό το μοντέλο, υπάρχουν και κάποια μειονεκτήματα : [40]

Η ταχύτητα λήψης μπορεί να χρειαστεί να είναι 25Mbps + εάν οι πολλά άτομα στο σπίτι και χρησιμοποιούν HD streaming media.

Για την απλοποίηση των λειτουργιών αποκωδικοποίησης ορισμένες λειτουργίες χρησιμοποιούν το VDI το οποίο είναι πιο υπολογιστικά δαπανηρό στην πλευρά του διακομιστή από ένα απλό HTTP request.

Θέματα που πρέπει να ληφθούν υπόψη όταν χρησιμοποιείτε το πιο πάνω μοντέλο [40]

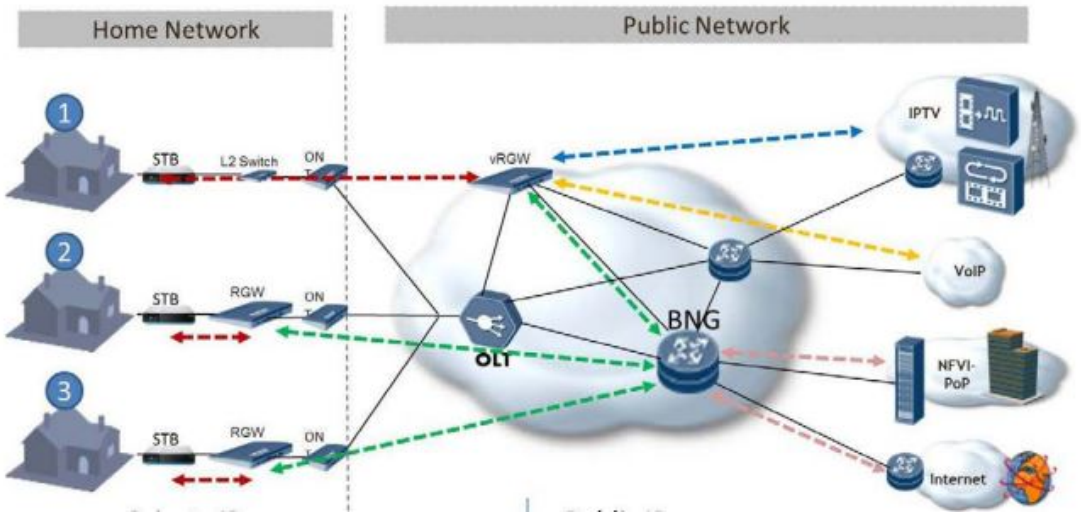
Στην περίπτωση που υπάρχει ένας DHCP server για τις εσωτερικές διευθύνσεις IP, κάποιο επίπεδο ενορχήστρωσης απαιτείται για να βεβαιωθούμε ότι ανά πελάτη οι απαιτούμενες λειτουργίες ικανοποιούνται.

Η λειτουργία των STB είναι ευαίσθητη στη απόδοση και η καθυστέρηση πρέπει να περιορίζεται στο ελάχιστο.

Τα θέματα ασφαλείας είναι μεγάλα και ο προμηθευτής πρέπει να εγγυηθεί την πλήρη απομόνωση μεταξύ των χρηστών, ίσως με τεμαχισμό VM και με κρυπτογράφηση των δεδομένον.

Αναμένετε ότι το περισσότερο traffic θα αποτελείτε από streaming media.

Επιπλέον, οι πάροχοι υπηρεσιών Διαδικτύου θέλουν να εγκαταστσούν προοδευτικά νέες υπηρεσίες στο δίκτυό τους, άρα πρέπει να υποστηρίζετε συνύπαρξη συμβατικών Home Gateway με εικονικές Home Gateway και εικονικά Set Top Box. (Εικ 6.4)



Σχ. 6.4: Συνύπαρξη των εικονικών και συμβατικών πυλών.

6.3 Χαρακτηριστικά / υπηρεσίες που μπορεί να μετακινηθούν στο σύννεφο [40]

Home Gateways:

Συνδεσιμότητα:

Διακομιστή DHCP για να παρέχει διευθύνσεις IP σε συσκευές LAN:
Δρομολογητές BRAS παρέχουν, στα συμβατικά δίκτυα, διευθύνσεις IP για την εξωτερική διεύθηνση του HomeGayeway. Τώρα υπάρχει η δυνατότητα η πύλη NFV να παρέχει IPs για το εσωτερικό δίκτυο για κάθε χρήστη και την αφαίρεση του διακομιστή DHCP από τα HomeGayeways

NAT υπηρεσία. Για να μεταφράζονται οι ιδιωτικές διευθύνσεις του σπιτιού σε δημόσιες διεύθυνσης IP. Αφού το κουτί NFV θα παρέχει τις ιδιωτικές διευθύνσεις IP, θα πρέπει επίσης να είναι υπεύθυνο για τις μεταφράσεις NAT.

PPPoE client (ή άλλο σχετικό πρωτόκολλο που χρησιμοποιείτε σήμερα), για τη σύνδεση του HG με τον BRAS. Μια νέα μέθοδος για έλεγχο της ταυτότητας του συνδρομητή χρειάζεται

Εφαρμογή Συγκεκριμένη συμπεριφορά δρομολόγησης, για καλύτερο QoS.
Το NFV στο σύνεφφο θα είναι μια πολύ πιο ισχυρή μηχανή από τα φθηνά οικιακά κουτιά και θα διαθέτει επαρκείς πόρους για την εκτέλεση υπηρεσιών QoS.

Ασφάλεια:

Κεντρικό Firewall, Antivirus, IPS και ακόμη DPI, με αυξημένη λειτουργικότητα από ένα μικρό Home Gateway μπορεί να προσφέρει.

Γονικός Έλεγχος

NAT

Προώθηση θύρας

Site to Site VPNs

Διοίκηση:

Αυξημένη Στατιστικά και Διαγνωστικά

Παρόμοια τεχνολογία με πρωτόκολλο UPnP, αλλά με αυξημένη ασφάλεια.

Στατιστική

STB

Media Streaming: Στα συμβατικά δίκτυα, ένα STB ανά / τηλεόραση, τώρα οι χρήστες έχουν τη δυνατότητα να κάνουν streaming μέσω HTTP.

Mutliple οθόνες: Χρησιμοποιώντας το STB μπορεί να παρακολουθήσετε 1 κανάλι, ενώ τώρα πολλαπλές οθόνες μπορούν να προβληθούν στον ίδιο χρόνο.

Video on Demand.

Βιντεοσκόπηση στο σύννεφο.

Διαφορετικές αναλύσεις και κωδικοποίησης . Αν οι συνδρομητές γραμμών, αντιμετωπίζουν κάποια προβλήματα, ή το εύρος ζώνης είναι χαμηλό, οι διαχειριστές μπορούν να χρησιμοποιήσουν διαφορετικές αναλύσεις ή / και κωδικοποίησης ως προσωρινή λύση.

Κεφάλαιο 7

Επίδειξη DHCP snooping

7.1 Επισκόπηση

DHCP snooping είναι διάφορες τεχνικές που εφαρμόζονται σε Layer 2 υλικό για να εξασφαλιστεί η άμβλυνση των διαφορετικών επιθέσεων L2.

Υποκλοπή DHCP μετριάζει τις επιθέσεις, όπως: DHCP rouge attack, ARP spoofing.

7.2 Πώς λειτουργεί [44] [45]

Ο Διαχειριστής επιλέγει αξιόπιστες και μη αξιόπιστες πόρτες στο διακόπτη. Οι αξιόπιστες πόρτες αφήνουν DHCP servers να ενωθούν πάνω. Μηνύματα DHCP σε μή αξιόπιστες πόρτες πετάγονται.

user@switch> **show dhcp snooping binding**

DHCP Snooping Information:

MAC address IP address Lease (seconds) Type VLAN Interface

00:05:85:3A:82:77 192.0.2.17 600 dynamic employee ge-0/0/1.0

00:05:85:3A:82:79 192.0.2.18 653 dynamic employee ge-0/0/1.0

00:05:85:3A:82:80 192.0.2.19 720 dynamic employee ge-0/0/2.0

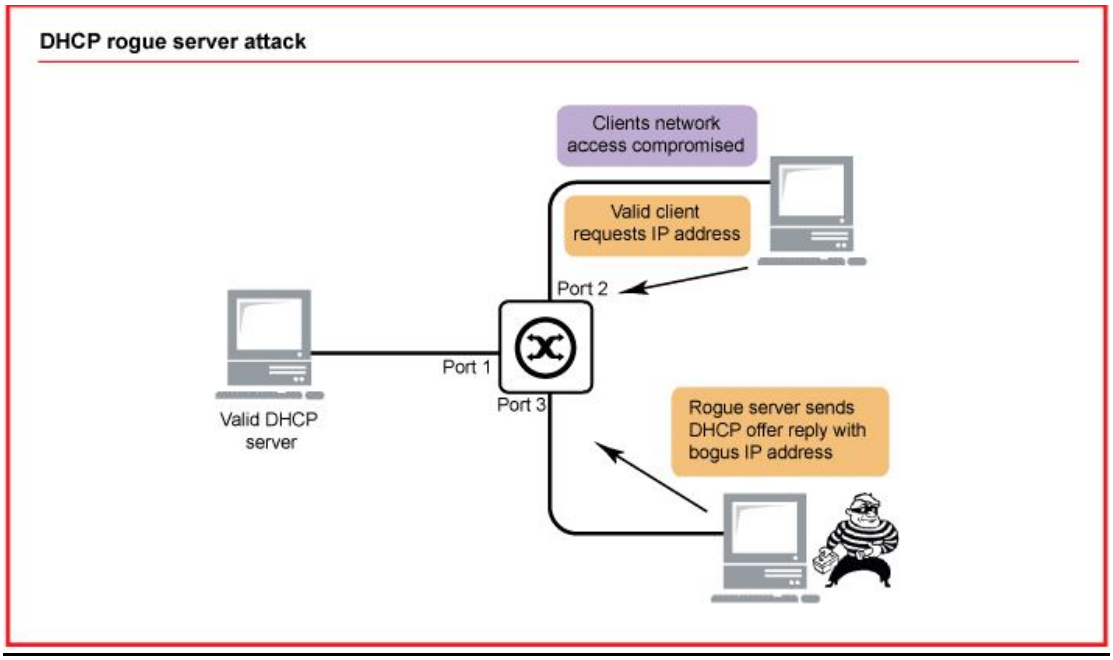


Fig. 7.2: DHCP masquerade attack.

7.3 DHCP masquerade attack [43]

Η επίθεση εκμεταλλεύεται την έλλειψη εξουσιοδότησης μεταξύ του διακομιστή DHCP και

των πελάτων DHCP. Όταν ένας πελάτης ξεκινά ένα DHCP discovery (broadcast) ο πρώτος DHCP server που απαντά έχει περισσότερες πιθανότητες να προσφέρει τις πληροφορίες του από μια άλλη προσφορά που θα έρθει αργότερα.

Ένας εισβολέας μπορεί να εκμεταλλευτεί αυτή την έλλειψη εξουσιοδότησης και να προσφέρει τη δική του διεύθυνση IP ως το Default Gateway του δικτύου. Οι πελάτες που δέχονται αυτές τις DHCP πληροφορίες στέλνουν όλες τα δεδομένα στη προεπιλεγμένη πύλη που είναι ο επιτιθέμενος. Ο επιτιθέμενος μπορεί έτσι να διαβάσει όλα τα μη κρυπτογραφημένα δεδομένα που στέλνονται. Στη συνέχεια ο επιτιθέμενος στέλνει τα δεδομένα στο πραγματικό τους προορισμό, καθώς και τις απαντήσεις πίσω στον αποστολέα. Με αυτό το τρόπο ο αποστολέας χωρίς τεχνικές γνώσεις δύσκολα καταλαβαίνει ότι είναι θύμα της επίθεσης αυτής. Ο επιτιθέμενος μπορεί να προκαλέσει DOS όποτε θέλει.

Η πιθανότητας επιτυχίας αυτής της επίθεσης είναι μεγάλη γιατί συνήθως οι επιτιθέμενοι είναι γεωγραφικά πιο κοντά στο θύμα από το πραγματικό διακομιστή DHCP.

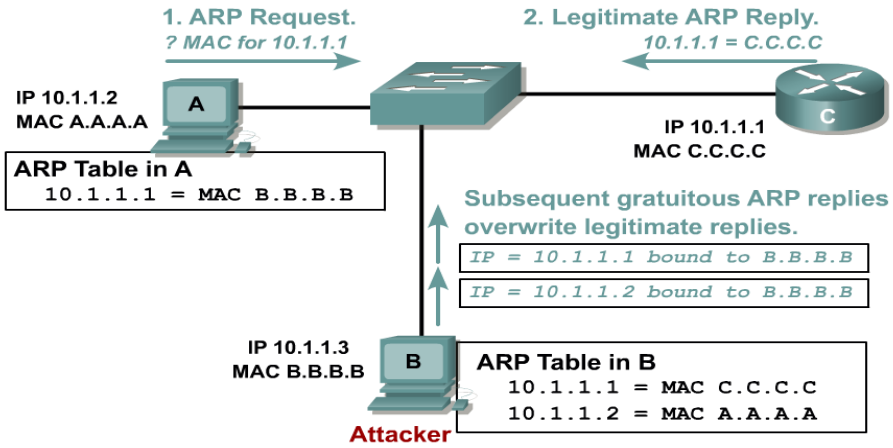


Fig. 7.3: ARP spoofing attack.

7.4 ARP spoofing [44]

ARP spoofing ή ARP poisoning είναι ένας άλλος τρόπος για να γίνει MITM. Σε αυτή την επίθεση, οι επιτιθέμενοι δημιουργούν πλαστά μηνύματα ARP και προσπαθούν να

συσχετίσουν τη διεύθηνση IP τους με το MAC address του Default Gateway. Αυτό είναι εφικτό λόγω της φύσης του ARP που είναι stateless και χωρίς μηχανισμούς ελέγχου ταυτότητας.

Το ARP spoofing μπορεί να αντιμετωπιστεί με διάφορες τεχνικές όπως DHCP spoofing detection software, Intrusion Prevention Systems καθώς και με κρυπτογράφηση όλων των δεδομένων.

7.5 Επίδειξη DHCP spoofing

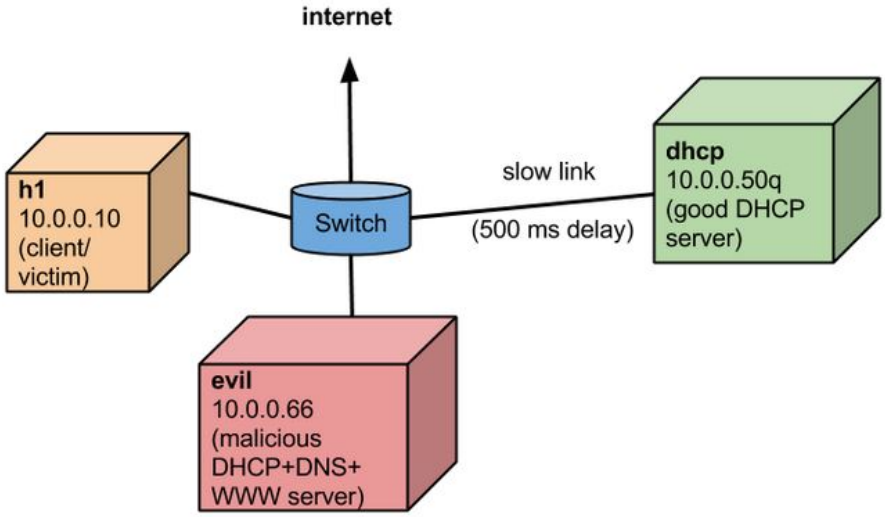


Fig. 7.3: DHCP masquerade σενάριο επίθεσης.

Επίδειξη της επίθεσης γίνεται σε προσομοιωμένο περιβάλλον δικτύου χρησιμοποιώντας Mininet [48] προσομοιωτή δικτύου, Open V Switch[49], και τον ελεγκτής POX, όλα εκ των οποίων είναι ανοιχτού κώδικα.

Έχουμε μετριάσει την επίθεση προσθέτοντας λογική στο λογισμικό Switch που διατίθεται μαζί με τον ελεγκτή POX.

Για την προσομοίωση της επίθεση μας χρησιμοποιήσαμε ένα σενάριο που δημιουργήθηκε από το Στάνφορντ [47]. Το σενάριο είναι το εξής

Όταν η h1 πόρτα υποβάλλει αίτηση DHCP προωθείται τόσο στο κανονικό DHCP όσο και στο κακό DHCP, αλλά το κακό ανταποκρίνεται πρώτα επειδή ο έγκυρος DHCP συνδέεται μέσω μιας πιο αργής σύνδεσης. Το κακό παρέχει το δικό του IP ως έγκυρου διακομιστή DNS,

δημιουργώντας ένα MITM.

Ο κώδικας για την επίθεση, και ένα βίντεο επίδειξης δημιουργήθηκε από το Standford[47].

Εμείς γράψαμε τον κώδικα για την αντιμετώπιση αυτής τις επίθεσης.

7.6 Αντιμετώπιση DHCP masquerade attack

Ο κώδικας του L2 DHCP snooping mitigation βρίσκεται στο Παράρτημα Α

Περιγραφή των δομών που χρησιμοποιήθηκαν

Έναν πίνακα ARP που κατέχει τις αντιστοιχίσεις μεταξύ MAC και διευθύνσεις IP

Ένας πίνακας με αντιστοιχίσεις Mac στο Port που έχει τις διεύθυνσης MAC που αντιστοιχούν σε κάθε θύρα

Ένας πίνακας TrustedTable που έχει όλες τις θύρες που έχουν επιλεχτεί ως αξιόπιστες από τον διαχειριστή

Ένα πίνακα Snooping που κρατά τα πεδία που μπορούν να εξεταστούν για κάθε πακέτο. Τα πεδία περιλαμβάνουν τη διεύθυνση MAC, διεύθυνση IP, το χρόνο μίσθωσης, VLAN αριθμό, Interface

Η ακόλουθη λογική ελέγχεται για κάθε πακέτο που έρχεται στο διακόπτη

Συνάρτηση Handle_PacketIn

1.Πιάσε το ID του διακόπτη που είναι ενωμένος με τον ελεγκτή γιατί πολλοί διακόπτες μπορεί να είναι συνδεδεμένοι με τον ελεγκτή. Αν είναι νέος διακόπτης, δημιούργησε ένα νέο ArpTable για τον διακόπτη αυτό. Επίσης δημιούργησε ένα νέο TrustedTable

2.Πιάσε τον αριθμό της πόρτας του διακόπτη που ήρθε το πακέτο μέσα

3. Ο διαχειριστής καθορίζει της αξιόπιστες πόρτες του διακόπτη.

Στη συνέχεια το πακέτο ελέγχεται αν είναι του τύπου Ethernet L2

Έπειτα ελέγχεται και προστίθεται στο snooping table το VLAN , Interface και το MAC address

Έπειτα ελέγχεται αν το πακέτο είναι του τύπου IPv4 και φυλάγεται το source IP

Μετά ελέγχεται αν το πακέτο περιέχει DHCP traffic και αν είναι DHCP αν είναι DHCP offer. Αν είναι DHCP offer τότε ελέγχεται εναντίων στο TrustedTable πίνακα. Άν η πόρτα έιναι αξιόπιστη τότε το πακέτο στέλνετε στο προορισμό του αλλιώς πετάγεται και καταγράφετε το περιστατικό

Έπειτα ενημερώνετε ο MAC to Port πίνακας.

Κεφάλαιο 8

Συμπεράσματα

8.1 Συζήτηση - Συμπεράσματα

Ολοκληρώνοντας την εργασία αυτή, στο Κεφάλαιο 8 παρουσιάζονται τα γενικά συμπεράσματα καθώς γίνεται αναφορά σε μελλοντικά σχέδια που αφορούν περαιτέρω βελτιστοποιήσεις του αλγόριθμου DHCP snooping στα SDN δίχτυα.
Η παρούσα διπλωματική εργασία είχε στόχο την γενική ανασκόπηση των δικτύων SDN, καθώς και της τεχνολογίας NFV και πώς μπορούν αυτές οι τεχνολογίες να φέρουν μεγάλα οφέλη. Μελετήθηκε επίσης η εφαρμογή αυτών των λύσεων στο οικιακό περιβάλλον και συγκεκριμένα στο πως οι υπηρεσίες αυτές μπορούν να χρησιμοποιηθούν από τους παρόχους υπηρεσιών διαδικτύου για να παρέχουν περισσότερα οφέλη και δυνατότητες στους πελάτες. Επίσης η παρούσα διπλωματική εργασία είχε στόχο τη κατασκευή του αλγορίθμου DHCP snooping σε δίκτυα SDN.

8.2 Μελλοντική Εργασία

Μια εισήγηση ως προς μελλοντική δουλειά που μπορεί να γίνει πάνω στη συγκεκριμένη διπλωματική είναι ένα επιπλέον χαρακτηριστικά στο DHCP snooping αλγόριθμο και η δημιουργία μια ολοκληρωμένης λύσης ασφαλείας που θα παρέχει περισσότερες πληροφορίες για τον επιτιθέμενο και την επίθεση. Για παράδειγμα, αν έχι εντοπιστεί η επίθεση τότε όλη η κυκλοφορία από τον επιτιθέμενο προωθήτε σε ένα σύστημα ανάλυσης που μαζεύει και αναλύει περισσότερες πληροφορίες για τη φύση του επιτιθέμενου και την επίθεση, χωρίς επιτιθέμενος να το γνωρίζει.

Βιβλιογραφία

[1] Wikipedia, “Software Defined Networks” 2014

[2] “What is SDN controller” [Online].

Available: https://www.sdncentral.com/sdn-controllers/

[3] “OpenFlow Switch Specification” Open Networking Foundation [Online].

Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.1.pdf

[4] Coursera “Software Defined Networks”

2013[Online] https://www.coursera.org/course/sdn

[5]”Onix: A Distributed Control Platform for Large-scale Production Networks”

[Online] Available: http://yuba.stanford.edu/~casado/onix-osdi.pdf

[6]”HyperFlow: A Distributed Control Plane for OpenFlow” [Online]

Available: http://www.cse.iitd.ac.in/~siy107537/csl374/a5/files/Tootoonchian.pdf

[7]”Kandoo: A Framework for Efficient and Scalable Offloading of Control Applications” [Online]

Available: http://conferences.sigcomm.org/sigcomm/2012/paper/hotsdn/p19.pdf

[8]”ElasticTree: Saving Energy in Data Center Networks” 2010 [Online] Available:

https://www.usenix.org/legacy/event/nsdi10/tech/full_papers/heller.pdf

[9]”Data center infrastructure efficiency”[Online]

Available: Data_center_infrastructure_efficiency

[10]”Hedera: Dynamic Flow Scheduling for Data Center Networks”[Online]

Available:http://bnrg.cs.berkeley.edu/~randy/Courses/CS294.S13/7.3.pdf

Available: http://bnrg.cs.berkeley.edu/~randy/Courses/CS294.S13/7.3.pdf

[11] Fig3.1 [Online]

Available: http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2013/9377-network-functions-virtualization-challenges-solutions.pdf

[12] ”OpenFlow-enabled SDN and Network Functions Virtualization” [Online]

Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-sdn-nvf-solution.pdf

[13]”Network Functions Virtualization explained” [Online]

Available: http://wikibon.org/wiki/v/Network_Function_Virtualization_or_NFV_Explained

[14] [Online] Available: http://www.opendaylight.org/resources/about-sdn 2

[15] “What is Network Functions Virtualization” [Online]

Available: https://www.sdncentral.com/whats-network-functions-virtualization-nfv/

[16] ”NFV priorities

for service provider CIOs“ [Online]

Available: http://www.hp.com/hpinfo/newsroom/press_kits/2014/MWC/HP_FactSheet_NFVPriorities.pdf

[17] “NFV Unbound, Christos Kolias | OpenDaylight Summit 2014“ [Online]

Available: https://www.youtube.com/watch?v=3Lmq_3ZhO_Q

[18]”NFV use cases” [Online]

Available: http://portal.etsi.org/NFV/NFV_White_Paper.pdf http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

[19]”What is OpenStack” [Online]

Available:http://opensource.com/resources/what-is-openstack

[20]”OpenStack Basics” [Online]

Available:https://www.youtube.com/watch?v=c1GFoY4btpo

[21]”The operating system of the cloud”[Online]

Available:http://www.rackspace.com/cloud/openstack/

[22]”OpenStack” [Online] Available:http://www.openstack.org/

[23] “Splendid Isolation: Language-Based Security for SDN” [Online]

Available:http://conferences.sigcomm.org/sigcomm/2012/paper/hotsdn/p79.pdf

[24] [Online]

Available: https://www.usenix.org/system/files/conference/ons2014/ons2014-paper-al_shabibi.pdf

[25] [Online]

Available: http://conferences.sigcomm.org/co-next/2012/eproceedings/student/p3.pdf

[26] [Online]

Available: http://archive.openflow.org/downloads/technicalreports/openflow-tr-2009-1-flowvisor.pdf

[27]”Security Analysis of the Open Networking Foundation (ONF) OpenFlow Switch Specification“ [Online] Available: http://tools.ietf.org/pdf/draft-mrw-sdnsec-openflow-analysis-02.pdf

[28]”OpenFlow Vulnerability Assessment” in Proceeding of the second ACM SIGCOMM workshop on Hot topics in software defined networking.

[29]Attacking Software-Defined Networks:A First Feasibility Study [Online] Available: http://conferences.sigcomm.org/sigcomm/2013/papers/hotsdn/p165.pdf

[30] “Frequency hopping” [Online] Available: https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

[31]”” [Online] Available: http://web.engr.illinois.edu/~caesar/papers/veriflow-nsdi-2013.pdf

[32]”FortNox” [Online] Available: http://www.csl.sri.com/users/vinod/papers/fortnox.pdf

[33]”OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking“ [Online] Available: http://conferences.sigcomm.org/sigcomm/2012/paper/hotsdn/p127.pdf

[34]”Active Security” [Online] Available: http://conferences.sigcomm.org/hotnets/2013/papers/hotnets-final119.pdf

[35]”Geoge Stibitz. First remote controlled computer” [Online]

Available: https://en.wikipedia.org/wiki/George_Stibitz

[36]”SDN market size” [Online]

Available: https://www.sdncentral.com/market/sdn-market-sizing/2013/04/

[37]”Residential Gateway Wikipedia” [Online] Available: https://en.wikipedia.org/wiki/Residential_gateway

[38]”SDN home gateway scenario slide47 ” [Online]

Available: http://www.iaria.org/conferences2013/filesAFIN13/NetWare%202013-SDN%20and%20Architectures%20v1.2-%20August%2025,%202013.pdf

[39]”Set Top Boxes” [Online] Available: https://en.wikipedia.org/wiki/Set-top_box

[40]”NFV uses cases” [Online]

Available: http://www.etsi.org/deliver/etsi_gs/nfv/001_099/001/01.01.01_60/gs_nfv001v010101p.pdf

[41]”Firewall as a Service. OpenStack” [Online] Available:

http://docs.openstack.org/api/openstack-network/2.0/content/fwaas_ext.html

[42]”SaaS Wikipedia” [Online] Available:

https://en.wikipedia.org/wiki/Security_as_a_service

[43]”Roque DHCP” [Online] Available: http://seclists.org/vuln-dev/2002/Sep/99

[44]”DHCP snooping” [Online] Available:

http://packetpushers.net/five-things-to-know-about-dhcp-snooping/

[45]”DHCP snooping” [Online] Available:

http://www.juniper.net/documentation/en_US/junos12.3/topics/concept/port-security-dhcp-snooping.html

[46]”ARP spoofing” [Online] Available: https://en.wikipedia.org/wiki/ARP_spoofing

[47] ”DHCP masquerade attack” [Online]

Available: https://github.com/mininet/mininet/wiki/Dhcp-masquerade-attack

[48]”Mininet network Simulator ” [Online] Available: http://mininet.org/

[49]”Open Virtual Switch” [Online] Available: http://openvswitch.org/

[50]”Open Virtual Switch” [Online] Available:

http://www.noxrepo.org/pox/about-pox/

Παράρτημα Α

Function PacketIn that checks every incoming packet of the switch

```
 def _handle_PacketIn (self, event):

    # Change to get the PID for the switch connected to the controller
    dpid = event.connection.dpid
    inport = event.port



    packet = event.parsed

    if dpid not in self.arpTable:
       # New switch -- create an empty table
       self.arpTable[dpid] = {}
       print "new arp Table created"
    if dpid not in self.trustedTable:
       # New trusted port for dhcp traffic manual 1,2
       self.trustedTable[dpid] = {1,2}
       print "new trusted port    '{0}'".format(self.trustedTable[dpid])

    dhcp = packet.find('dhcp')

 # Manually allowing only 10 hosts to connect to the switch.
    if inport < 11:
       ethernet = packet.find('ethernet')

       #checking for ethernet traffic
```

```
        if ethernet is not None:

            # Checking for VLAN Tags
            if packet.type == ethernet.VLAN_TYPE:
              vlan = packet.find('vlan')
              if vlan.id not in self.s["VLAN"]:
                self.s["VLAN"].append(vlan.id)

            if inport not in self.s["Interface"]:
                self.s["Interface"].append(inport)

            if ethernet.src not in self.s["MAC_address"]:
                self.s["MAC_address"].append(ethernet.src)



            ip = packet.find('ipv4')
            if dhcp is not None:
                # We dont want to save request that have src IP 0.0.0.0
                if dhcp.op != 1:
                    self.s["IP_address"].append(ip.srcip)
            else:
                 if ip is not None:
                     self.s["IP_address"].append(ip.srcip)


                      # This routine checks if any DHCP offers are sent in a non trusted
ports and rejects them
        if dhcp is None:
            test = 0;
        else:
```

```
            # print "This is a dhcp packet '{0}'".format(dhcp)
            if dhcp.op == 2:
                print "This is an offer from the server"
                if inport in self.trustedTable[dpid]:
                    print "valid DHCP offer"
                else:
                    print "ALERT! Rogue DHCP in port '{0}'".format(inport)
                    # Halt the event, or forward it to a honeypot
                    return


        if isinstance(packet.next, ipv4):
            # print "packet ,packet.next, packet.next.next ,packet.next.next.next, packet.next.srcip'{0}','{1}','{2}', '{3}', '{4}'".format(packet ,packet.next, packet.next.next ,packet.next.next.next, packet.next.srcip )


            # Learn or update port/MAC info
            if packet.next.srcip in self.arpTable[dpid]:
                if self.arpTable[dpid][packet.next.srcip] != (inport, packet.src):
                    print "Re learned"

            else:

            self.arpTable[dpid][packet.next.srcip] = Entry(inport, packet.src)
```