ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μελέτη των εικονικών λειτουργιών του δικτύου και η εξέλιξη τους

Αλέξανδρος Τσιτσές

Επιβλέπων καθηγητής: Ιωάννης Τζήμας

Αντίρριο- Νοέμβριος 2017

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίρριο, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή
2. Ονοματεπώνυμο, Υπογραφή
3. Ονοματεπώνυμο, Υπογραφή

Αφιέρωση

Στην οικογένεια μου.

Ευχαριστίες

Για τις συμβουλές και την καθοδήγησή καθ' όλη την διάρκεια των σπουδών μου οφείλω να ευχαριστήσω τους όλους καθηγητές μου.

Επίσης θέλω να ευχαριστήσω τον καθηγητή μου κ. Ιωάννη Τζήμα για την επίβλεψη της παρούσας πτυχιακής εργασίας.

Τέλος, θέλω να ευχαριστήσω την οικογένειά μου για την στήριξή τους όλα αυτά τα χρόνια.

Περιεχόμενα

Λίστα εικόνων

Πρόλογος

Η χρήση των εικονικών μηχανών(virtual machines) που συνιστούν τον δομικό λίθο ενός εικονοποιημένου περιβάλλοντος έγινε πρώτη φορά από την IBM το 196 σε μια προσπάθεια μείωσης του κόστους του τότε πολύ ακριβού εξοπλισμού. Στόχος ήταν η ταυτόχρονη εκτέλεση εφαρμογών και διαδικασιών. Κατά την διάρκεια των δεκαετιών του ’80 και του ’90 κυριαρχούσαν τα κατανεμημένα συστήματα, οι client-server εφαρμογές και οι x86server και η εικονοποίηση πρακτικά εγκαταλείφθηκε. Λόγω των αυξανόμενων προκλήσεων που αντιμετώπιζαν οι εταιρίες όπως η περιορισμένη αξιοποίηση της υποδομής και το αυξημένο κόστος, οδήγησαν τις εταιρίες για άλλη μια φορά να στραφούν σε νέες τεχνολογίες προκειμένου να μπορέσουν να ανταπεξέλθουν στις προκλήσεις.

Η εικονοποίηση είναι μια τεχνολογία από την οποία μπορεί να ωφεληθεί οποιοσδήποτε χρησιμοποιεί υπολογιστή. Χιλιάδες οργανισμοί ανά τον κόσμο χρησιμοποιούν λύσεις εικονοποίησης για να μειώσουν το κόστος και παράλληλα να αυξήσουν την αποδοτικότητα και την ευελιξία του υφιστάμενου εξοπλισμού τους. Ουσιαστικά η εικονοποίηση επιτρέπει σε πολλαπλές εικονικές μηχανές με τα αντίστοιχα λειτουργικά συστήματα να τρέχουν ταυτόχρονα σε έναν υπολογιστή. Κάθε λειτουργικό σύστημα μοιράζεται τους διαθέσιμους πόρους στο κοινό ‘’φυσικό’’ hardware.

Εικονική μηχανή(virtual machine) είναι ουσιαστικά ένα ‘’φυσικό’’ μηχάνημα αλλά αντί για καλώδια αποτελείται από ένα σύνολο αρχείων λογισμικού. Κάθε εικονική μηχανή αντιπροσωπεύει ένα ολόκληρο σύστημα με επεξεργαστές, μνήμη, υποδομή για δικτυακή επικοινωνία, αποθηκευτικό χώρο και BIOS. Μια εικονική μηχανή τρέχει ένα ξεχωριστό λειτουργικό σύστημα και αντίστοιχες εφαρμογές, χωρίς καμία τροποποίηση όπως ένα φυσικός server.

Περίληψη

Στην παρούσα πτυχιακή εργασία παρουσιάζεται η εικονοποίηση των λειτουργιών των δικτύων. Αρχικά περιγράφονται αναλυτικά τα μέρη του NFV και όλα όσα έχει προσφέρει η εισαγωγή του στις επιχειρήσεις. Στην συνέχεια αναφέρονται οι προκλήσεις ασφαλείας που προήλθαν λόγω της εισαγωγής της εικονοποίησης και οι μέθοδοι με τις οποίες οι εταιρίες καλούνται να αντιμετωπίσουν αυτές τις προκλήσεις. Επιπλέον, γίνεται αναφορά στο SDN που είναι μια τεχνολογία που συνδέεται στενά με το NFV και αναλύονται λεπτομερώς η σχέση SDN-NFV, η SDN τεχνολογία και η ασφάλειά της. Το SDN κάνει το δίκτυο πιο ευέλικτο και ευκίνητο μέσα από τα προγραμματιστικά στοιχεία του δικτύου και εισάγει την δικτύωση με βάση την πρόθεση (Intent-based networking) που αναλύεται στην παρούσα εργασία. Ακόμα, παρουσιάζεται η μέθοδος της τμηματικής δρομολόγησης, η οποία μπορεί να χρησιμοποιηθεί μαζί με το SDN. Επιπροσθέτως, γίνεται αναφορά στο ανοικτό πρωτόκολλο επικοινωνίας Openflow και αναλύονται το πως λειτουργεί και τα δομικά του μέρη. Τέλος, παρατίθενται με λεπτομέρεια τι είναι το cloud computing και ποιες είναι οι δυνατότητές του.

Λέξεις κλειδί: Εικονοποίηση, SDN, NFV, VNF, Δικτύωση με βάση την πρόθεση, Ασφάλεια

Abstract

This thesis presents the visualization of the functions of networks. Firstly, the parts of the NFV and all that its introduction to business has offered are detailed. Following that, are the security challenges that arise from the introduction of virtualization and the methods by which companies are challenged to face these challenges. In addition, reference is made to SDN, which is a technology closely linked to the NFV, and details of SDN-NFV, SDN technology and its security are analyzed. SDN makes the network more flexible through network programming and introduces Intent-based networking that is discussed in this paper. In addition, the segment routing method, which can be used along with SDN, is presented. Additionally, reference is made to the open communication protocol "Openflow", and how its structural parts work. Finally, they detail how cloud computing works and what its capabilities are.

Key words: Virtualization, SDN, NFV, VNF, Intent-based networking, Segment Routing, Security

Εισαγωγή

Σήμερα, οι πάροχοι υπηρεσιών περιεχομένου (CSPs) αντιμετωπίζουν μια ραγδαία αύξηση κίνησης και συνδρομητών στο δίκτυό τους. Έτσι οι προκλήσεις που καλούνται να αντιμετωπίσουν είναι πολλές:

- **Αυξημένη ζήτηση**: Αναλύσεις έδειξαν ότι η κυκλοφορία δεδομένων κινητής τηλεφωνίας αυξήθηκε κατά 54% από το 2015 και έφτασε τα 60,427 petabytes, πράγμα που εκτιμάτε να αυξηθεί μέχρι το 2020 και να φτάσει τα 228,491 PB.
- **Αλλαγή σκηνικού**: Αυξανόμενη σημασία των εφαρμογών πάνω σε απλή σύνδεση και μια νέα γενιά ανταγωνιστών με νέα επιχειρηματικά μοντέλα. Για παράδειγμα, οι Hulu και Netflix είναι ευέλικτες και εύκαμπτες και μπορούν να παρέχουν υπηρεσίες επί πληρωμή πολύ πιο γρήγορα. Οι συνεχώς αυξανόμενες απαιτήσεις των καταναλωτών ανεβάζουν ολοένα και πιο ψηλά τον πήχη για τους CSPs.
- **Ανικανότητα να προσφέρουν νέες υπηρεσίες στους χρήστες γρήγορα και δυναμικά**: Οι υποδομές των σημερινών CSP δικτύων απαιτούν χειροκίνητη διαχείριση και η επεξεργασία ροής των εργασιών, με συνέπεια να μην γίνεται γρήγορη προσαρμογή και παράδοση της υπηρεσίας ή της εφαρμογής που ο καταναλωτής επιθυμεί.
- **Αυξανόμενες κεφαλαιουχικές δαπάνες (CAPEX) και τα λειτουργικά έξοδα (OPEX) και στασιμότητα ή μείωση των εσόδων**: Οι CSPs καλούνται να ερευνήσουν τις κεφαλαιουχικές δαπάνες κα τα λειτουργικά έξοδα για να μπορέσουν να ανταποκριθούν στις υψηλές απαιτήσεις των καταναλωτών τους.

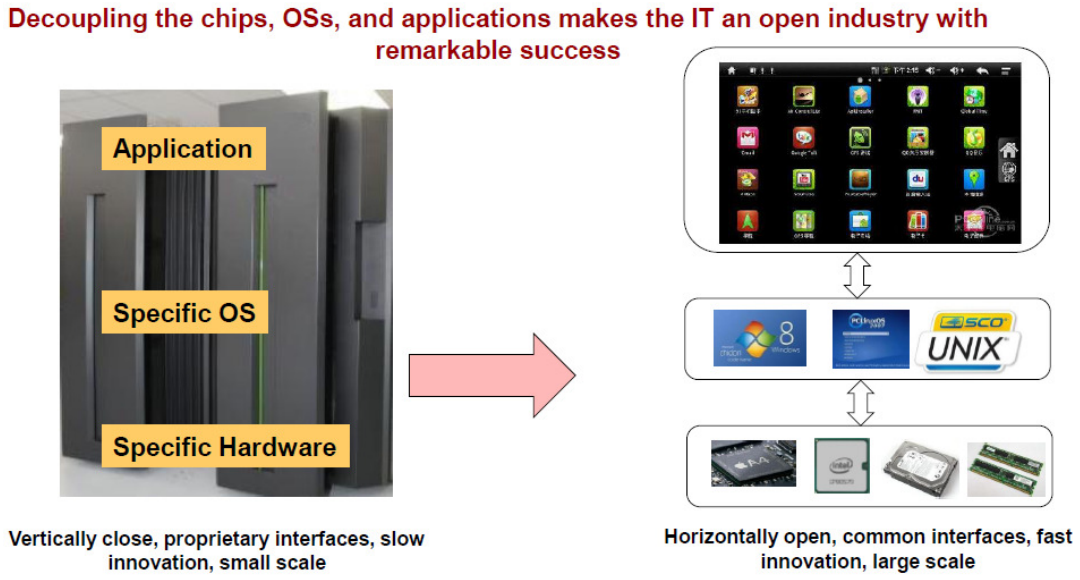
Οι CSPs δεν μπορούν να βελτιώσουν την χρήση των πόρων τους, καθώς αυτό απαιτεί να επανασχεδιάσουν τα δίκτυά τους για υψηλές τιμές κίνησης. Οι ανταγωνιστές τους, χρησιμοποιούν έναν άλλο τρόπο για να διαχειριστούν τις πολλαπλές δικτυακές εφαρμογές και να αυξήσουν την χρήση των πόρων τους, κάνοντας εικονικές τις υποδομές τους.

1. Network function virtualization (NFV)

NFV ονομάζεται η τεχνολογία που ‘’εικονοποιεί’’ τις λειτουργίες ενός κλασικού δικτύου και σχετίζεται με εφαρμογές ή υπηρεσίες προστιθέμενης αξίας, που οι CSPs χρησιμοποιούν στις υποδομές τους για να μειώσουν το κόστος και να αυξήσουν τον χρόνο διάθεσης στην αγορά. Η NFV αλλάζει τον τρόπο αρχιτεκτονικής και σχεδίασης των δικτύων. Με την NFV οι CSPs εδραιώνουν την πληθώρα των εφαρμογών, εξειδικεύοντας τον ήδη υπάρχων εξοπλισμό που χρησιμοποιούν.

Πλεονεκτήματα NFV:

- **Δημιουργούνται καινούργιες ευκαιρίες για έσοδα:** Νέες εφαρμογές που στοχεύουν συγκεκριμένες ανάγκες της αγοράς, μπορούν γρήγορα να αναπτυχθούν ταχύτατα στο επίπεδο που απαιτείται.
- **Αύξηση της ευκαμψίας και ευελιξίας:** Οι εφαρμογές και οι υπηρεσίες ενημερώνονται άμεσα και αναπτύσσονται χωρίς περιττές καθυστερήσεις.
- **Απλοποιεί το σχεδιασμό και την κλιμάκωση του δικτύου:** Νέο hardware μπορεί γρήγορα να προστεθεί επιτρέποντας στις CSPs να προσθέσουν ή να αφαιρέσουν μια κατά παραγγελία εφαρμογή χωρίς διαδικασίες ανάθεσης δημοσίων συμβάσεων.
- **Μειώνει το CAPEX και το OPEX:** Οι CSPs μπορούν να τρέχουν τα δικά τους δίκτυα πιο αποτελεσματικά με τον υψηλού επιπέδου αυτοματισμό, επαναχρησιμοποιώντας τις υπολογιστικές και αποθηκευτικές πηγές για διάφορες λειτουργίες. Το αποτέλεσμα είναι να μειώνονται οι κεφαλαιουχικές δαπάνες και τα λειτουργικά έξοδα.



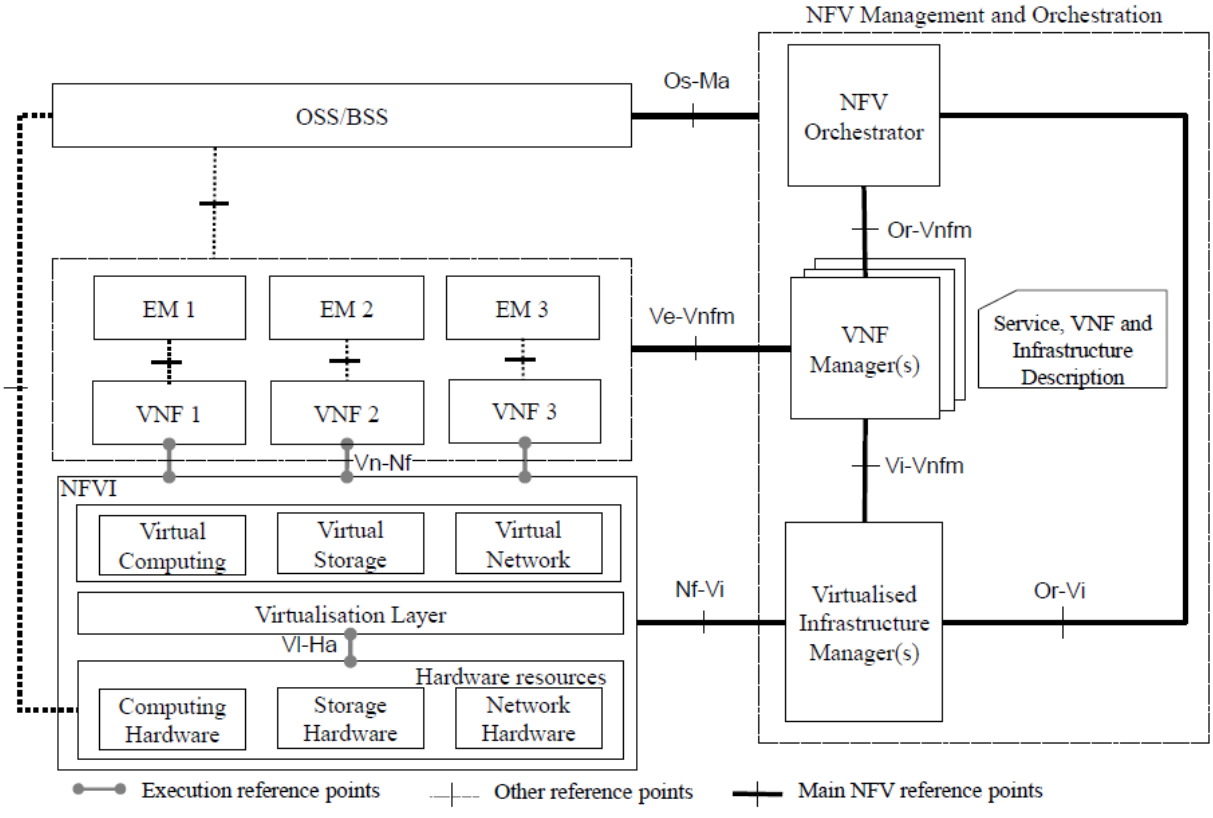
Εικόνα 1: Διαχωρισμός των εφαρμογών από το hardware

Η NFV επαναπροσδιορίζει τον τρόπο λειτουργίας των δικτύων. Ορίζει μια αρχιτεκτονική όπου οι λειτουργίες του δικτύου και οι εφαρμογές είναι ανεξάρτητες από το hardware. Αυτές οι εφαρμογές λογισμικού χρησιμοποιούν ανεξάρτητα υπολογιστικά και αποθηκευτικά στοιχεία, όπως η πλατφόρμα hardware.

1.1 ETSI NFV Framework (European Telecommunications Standards Institute)

Ο ETSI είναι αναγνωρισμένος ευρωπαϊκός οργανισμός τυποποίησης που αποτελείται από CSPs που συνεργάζονται για να καθορίσουν πρότυπα για λύσεις που χρησιμοποιούν στα δίκτυά τους. Αυτά τα πρότυπα χρησιμοποιούνται από τους πωλητές στις προσφορές τους για να καλύψουν τις απαιτήσεις.

Το ETSI NFV Industry Specification Group (ISG) έχει ορίσει ένα αρχιτεκτονικό πλαίσιο υψηλού επιπέδου για το NFV το οποίο φαίνεται στην παρακάτω εικόνα.



Εικόνα 2: Αρχιτεκτονική NFV

OSS: Operations Support Systems

BSS: Business Support Systems

EMS: Element Management System

Vn-Nf: VNF-NFV Infrastructure

Vi-Ha: Virtualization Layer-Hardware Resources

Os-Ma: OSS/BSS-NFV Management and Orchestration

Se-Ma: Service, VNF and Infrastructure Description-NFV Management and Orchestration

Ve-Vnfm: VNF/EMS-VNF Manager

Nf-Vi: NFVI-Virtualized Infrastructure Manager

Or-Vnfm: Orchestration-VNF Manager

Vi-Vnfm: Virtualized Infrastructure Manager

Or-Vi: Orchestrator-Virtualized Infrastructure Manager

Το ETSI NFV framework, αποτελείται από τρία βασικά στοιχεία:

Network Functions Virtualization Infrastructure (NFVI): Ένα υποσύστημα που αποτελείται από όλο το hardware (servers, αποθηκευτικό χώρο και δικτύωση) και από στοιχεία λογισμικού στο οποίο οι εικονικές λειτουργίες (Virtual Network Functions (VNFs)) αναπτύσσονται 'πάνω' στους φυσικούς πόρους μέσω του virtualization layer.

Management and Orchestration (MANO): Ένα υποσύστημα το οποίο περιλαμβάνει το NFV Orchestrator (NFVO), το Virtualized Infrastructure Manager (VIM) και το Virtual Network Functions Manager (VNFM).

Virtual Network Functions (VNFs): Οι VNFs είναι η εκτέλεση του λογισμικού των λειτουργιών του δικτύου, που υλοποιούνται σε μια ή πολλές εικονικές μηχανές (VMs) στο NFVI.

Το NFV Management και Orchestration παρέχει οργάνωση και διαχείριση του κύκλου ζωής των virtual software πόρων του NFVI και των VNFs, καθώς και οποιαδήποτε καθήκοντα διαχείρισης στο NFV framework.

1.2 Νέοι επιχειρηματικοί στόχοι μέσω NFV

Επιχειρηματική ευελιξία: Η δυνατότητα παροχής νέων υπηρεσιών και η ανταπόκριση στις μεταβαλλόμενες απαιτήσεις των καταναλωτών.

Καινούργιες ευκαιρίες και καινοτομίες: Με το NFV το κόστος παραγωγής μειώθηκε με αποτέλεσμα να μπορεί να υπάρξει περιθώριο λάθους κατά την δημιουργία μιας εφαρμογής δίνοντας έτσι το περιθώριο εξέλιξης σε νέες καινοτομίες.

Αύξηση του χρόνου διάθεσης στην αγορά: Μείωση του χρόνου ανάπτυξης και πιστοποίησης των εφαρμογών.

Βελτίωση των επιχειρησιακών διαδικασιών: Η εικονοποίηση επιτρέπει στις εφαρμογές να είναι ανεξάρτητες από τις υποδομές, δίνοντας την δυνατότητα αυτοματισμού, και πρωτοβουλίες διαχείρισης επιχειρηματικών διαδικασιών ανασχεδιασμού.

Βελτιστοποιημένο OPEX: Η τεχνολογία NFV μειώνει τον χειροκίνητο χειρισμό για τη δημιουργία και διαμόρφωση υπηρεσιών, μειώνοντας τα έξοδα λειτουργίας και προσφέρει αυτοματισμό υψηλού επιπέδου.

Χαμηλότερο CAPEX: Από την αυξανόμενη ζήτηση για virtualization από τις εταιρίες, έγινε καλύτερη αξιοποίηση της χωρητικότητας και αύξηση της ζήτησης, μειώνοντας τα έξοδα για επενδύσεις σε εξειδικευμένη υποδομή.

NFV-προκλήσεις

Παρόλα τα θετικά του, ο NFV θα επιφέρει επιπτώσεις στις μελλοντικές επιχειρήσεις και θα δημιουργήσει προκλήσεις για την υποστήριξη λειτουργιών του συστήματος (OOS). Για να υπάρξει μια ασφαλή μετάβαση, αυτές οι προκλήσεις μπορούν να χωριστούν σε τρείς κατηγορίες: υποδομές, λειτουργίες, υπηρεσίες.

Υποδομές-προκλήσεις

Με την αλλαγή σε NFV οι υποδομές έρχονται αντιμέτωπες με νέα στοιχεία στα δίκτυά τους, από τον κόσμο του IT και βασισμένες στα πρότυπα της βιομηχανίας. Κάποια μέρη της ήδη υπάρχουσας υποδομής θα αντικατασταθούν από εικονικές δομές-στοιχεία και θα υπάρχει ένα hybrid περιβάλλον (συνδυασμός εικονικών και φυσικών λειτουργιών του δικτύου) .

Λειτουργίες-προκλήσεις

Μια σημαντική πρόκληση, είναι η διατήρηση των πελατών και των υπηρεσιών που είναι συνδεδεμένες ήδη με τις υποδομές. Αυτό απαιτεί ενσωμάτωση στο υπάρχον OSS/BSS περιβάλλον και αυτοματισμό για να υπάρξει ευστροφία και γρηγορότερη ταχύτητα εξυπηρέτησης. Η NFV ξεχωρίζει της λειτουργίες από την υποδομή προσφέροντας νέες διαδικασίες όπως δοκιμές, επικύρωση, αποδοχή και αντιμετώπιση προβλημάτων. Ακόμα μια σημαντική πρόκληση είναι ο έλεγχος του κόστους λειτουργίας όταν εφαρμόζεται ο NFV. Παράγοντες που συμβάλλουν σε αυτό είναι:

-η πολυπλοκότητα που σχετίζεται με τη διαχείριση ενός hybrid περιβάλλοντος

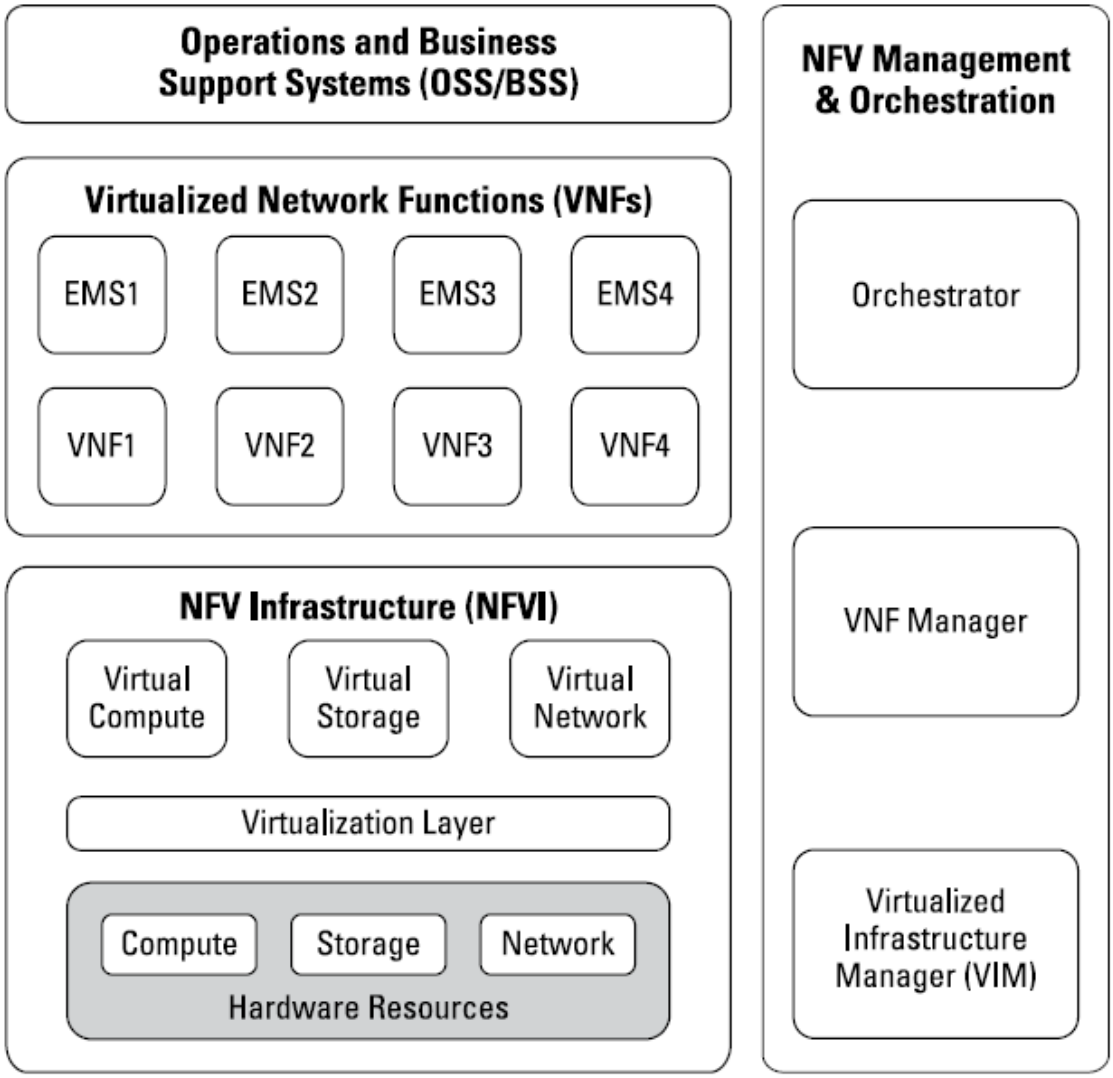
- η πολυπλοκότητα της διαχείρισης των λειτουργιών από ένα κατανεμημένο σύνολο εφαρμογών

Υπηρεσίες-προκλήσεις

Η αλλαγή σε NFV κάνει μια CSP υποδομή να είναι προγραμματιζόμενη σε πραγματικό χρόνο και να είναι αυτοματοποιημένη. Για να υπάρξει πλήρης εκμετάλλευση των επενδύσεων, οι CSPs πρέπει να επαναπροσδιορίσουν τον τρόπο που προσφέρουν τις υπηρεσίες στους πελάτες τους. Δηλαδή από ένα συγκεκριμένο αριθμό υπηρεσιών που προσφέρεται και που χρειάζεται χρόνο για να αναπτυχθεί, θα πρέπει να αλλάξει ώστε να δίνει την δυνατότητα στους καταναλωτές της να επιλέγουν τις υπηρεσίες που χρειάζονται. Επομένως οι υπηρεσίες που θα προσφέρονται θα πρέπει να είναι δυναμικές και βασισμένες στις ανάγκες των πελατών.

Hardware resources

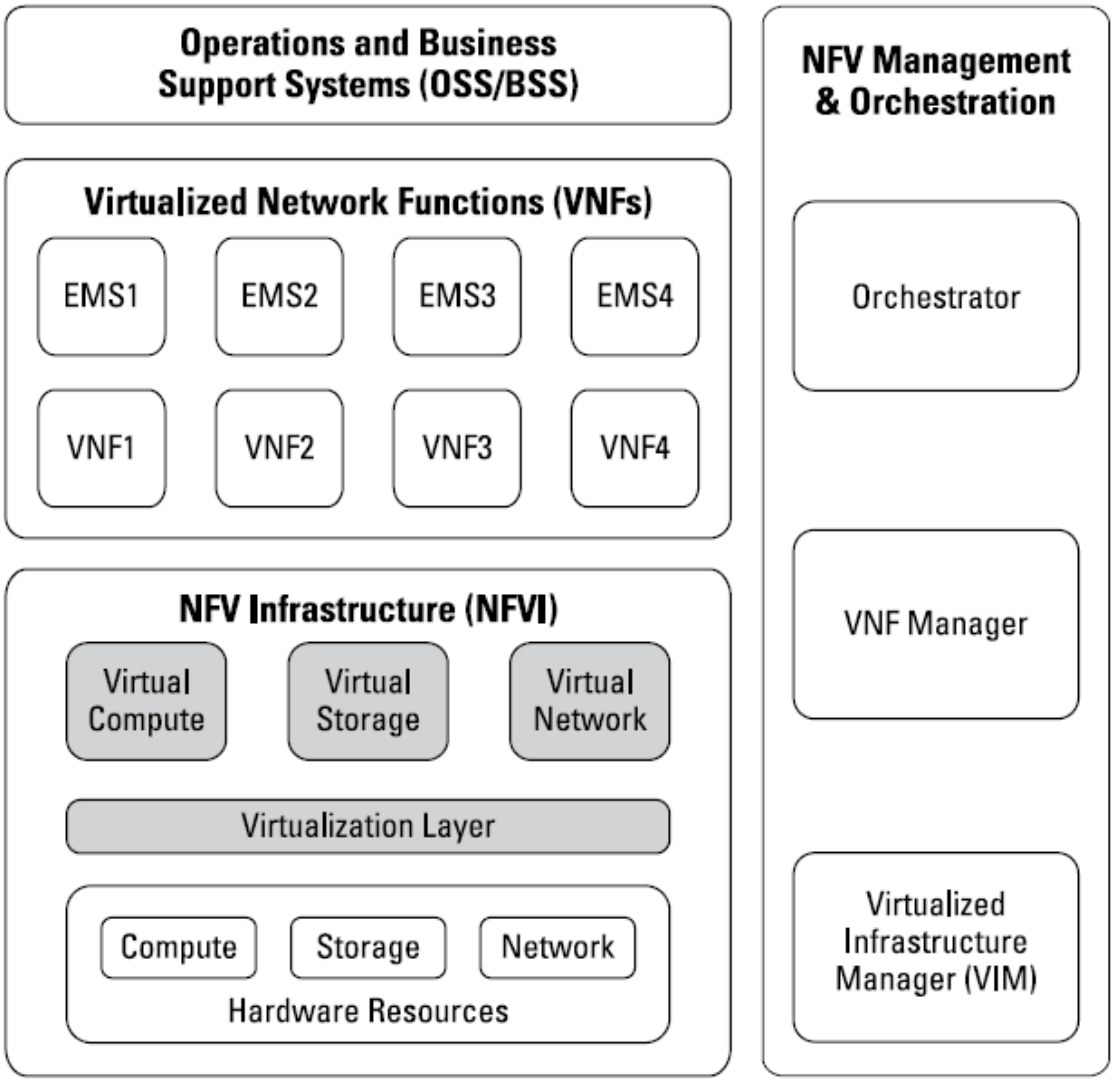
Το hardware που χρησιμοποιεί η τεχνολογία NFV περιλαμβάνει επεξεργαστική, αποθηκευτική και δικτυακή πηγή. Αυτές είναι οι πηγές που μοιράζεται (μέσω του virtualization layer)και χρησιμοποιούνται από την λειτουργία VNF για την επεξεργασία την αποθήκευση και την σύνδεση που χρειάζεται.



Εικόνα 3: Το hardware στην υποδομή NFV

Εικονικές πηγές και Virtualization layer

Ολόκληρο το hardware μετατρέπετε σε ένα ανεξάρτητο εικονικό πόρο μέσω του virtualization layer στο NFVI. Αυτοί οι εικονικοί πόροι παρουσιάζονται ως μια ανεξάρτητη οντότητα για κάθε λειτουργία VNF.



Εικόνα 4: Το εικονοποιημένο hardware και το virtualiaztion layer

Το virtualization layer (ή hypervisor) διαχωρίζει το hardware του NFVI από τις λειτουργίες VNF ώστε να μπορεί να αναπτυχθεί διαφορετικό λογισμικό στο hardware. Η βασική λειτουργία του virtualization layer είναι να αποσπά τις φυσικές πηγές (hardware) και να τις παρουσιάζει στις λειτουργίες VNF σαν ανεξάρτητες πηγές.

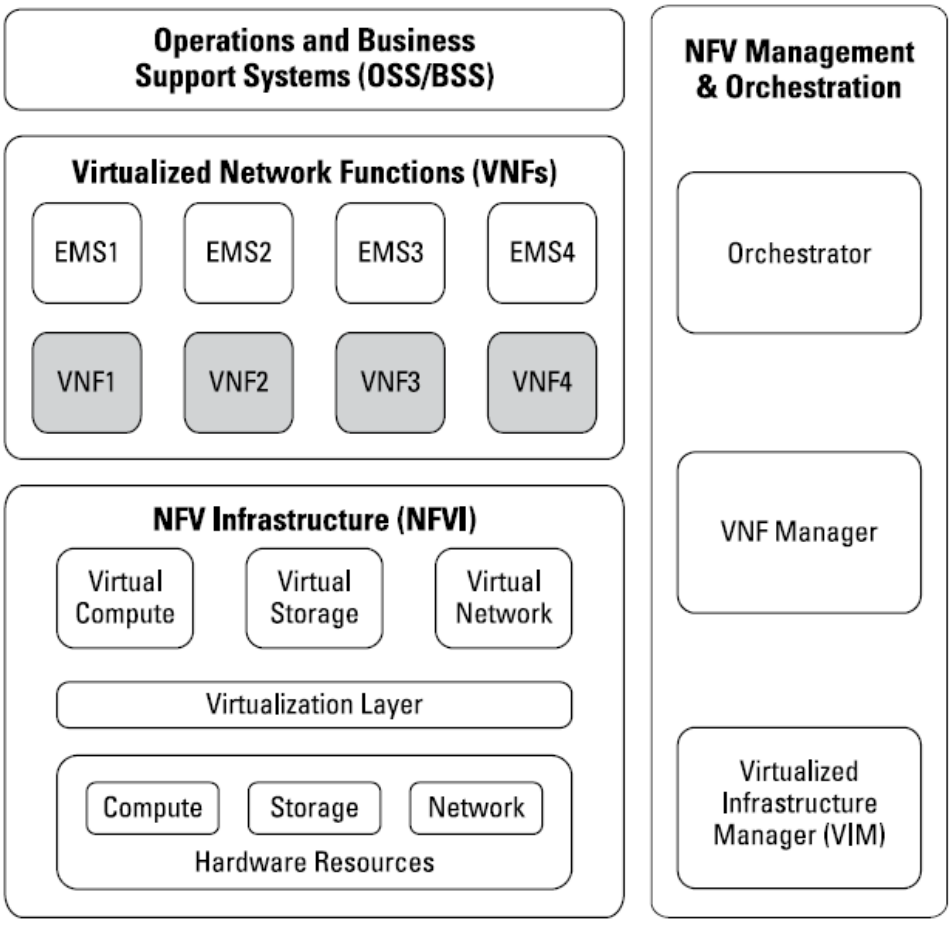
2. Μέρη του NFV: VNF και EMS

Virtual Network Functions (VNF)

Στα κλασικά δίκτυα, οι λειτουργίες του δικτύου συνήθως είναι φτιαγμένες να εφαρμόζουν το δικό τους λογισμικό. Παραδείγματα από λειτουργίες του δικτύου είναι οι routers, τα firewalls, ο Provider Edge(PE) κ.α.

Σκοπός του NFV είναι να κάνει αυτές τις λειτουργίες να είναι σαν ένα απλό λογισμικό που τρέχει πάνω στο NFVI. Οι λειτουργίες VNF είναι η εικονική έκδοση των κλασικών λειτουργιών του δικτύου. Ο διαχωρισμός του hardware από το software επιτρέπει την ανάπτυξη αυτών των λειτουργιών σε ξεχωριστό κύκλο.

Η λειτουργία VNF (virtual router, virtual switch) συνήθως δεν αλλάζει την λειτουργικότητα και τα interfaces ενός φυσικού router ή switch. Η λειτουργία VNF μπορεί να εκτελείται σε μια ή παραπάνω εικονικές μηχανές (VMs(Virtual Machines)), ή σαν μια λειτουργία σε έναν κοινόχρηστο VM.



Εικόνα 5: Οι λειτουργίες VNF στην αρχιτεκτονική αναφοράς NFV

Εκτελώντας μια λειτουργία VNF μέσα σε πολλά VMs είναι επιθυμητή η ανοχή σε σφάλματα, η εξισορρόπηση φορτίου, και η επεκτασιμότητα. Παρακάτω σημειώνονται μερικές συμβουλές που θα ήταν καλό να γνωρίζουμε όταν αναπτύσσουμε ένα VNF:

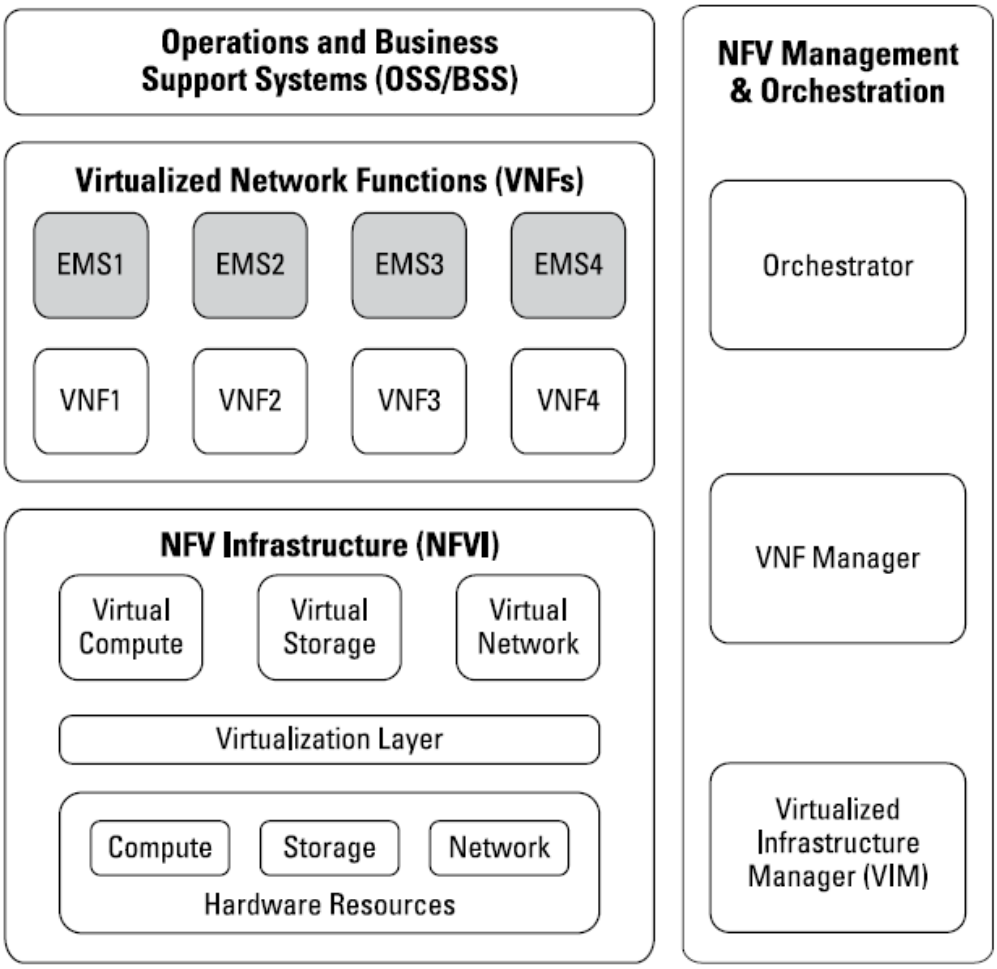
- Σχεδιασμός για διαλειτουργικότητα με διαφορετικούς hypervisors
- Εξασφάλιση ότι η διαδικασία της εικονοποίησης δεν δημιουργεί νέα κενά ασφαλείας
- Εξασφάλιση ότι η εκτέλεση του VNF δεν επηρεάζεται αρνητικά από την εικονοποίηση

2.1 Element Management System (EMS)

Ο EMS είναι ο διαχειριστής των στοιχείων του δικτύου. Βοηθά στην διαμόρφωση των στοιχείων του δικτύου. Οι λειτουργίες του είναι: η Διαχείριση Βλαβών, η Διαχείριση Διάρθρωσης, η Λογιστική Διαχείριση, η Διαχείριση Επιδόσεων και η Διαχείριση Ασφαλείας.

Ένας EMS μπορεί να διαχειρίζεται τις λειτουργίες ενός ή περισσότερων NVFs.

Ο EMS αλληλοσυνδέει τα παρακάτω:
-Τον VNF Manager για να στηρίζει την διαχείριση του κύκλου ζωής των λειτουργιών VNF
-Το OSS(Operations Support System) για να στηρίζει την ρύθμιση των παραμέτρων της εφαρμογής, και να διαχειρίζεται και να ενεργοποιεί τις υπηρεσίες των πελατών που παρέχονται από το VNF.



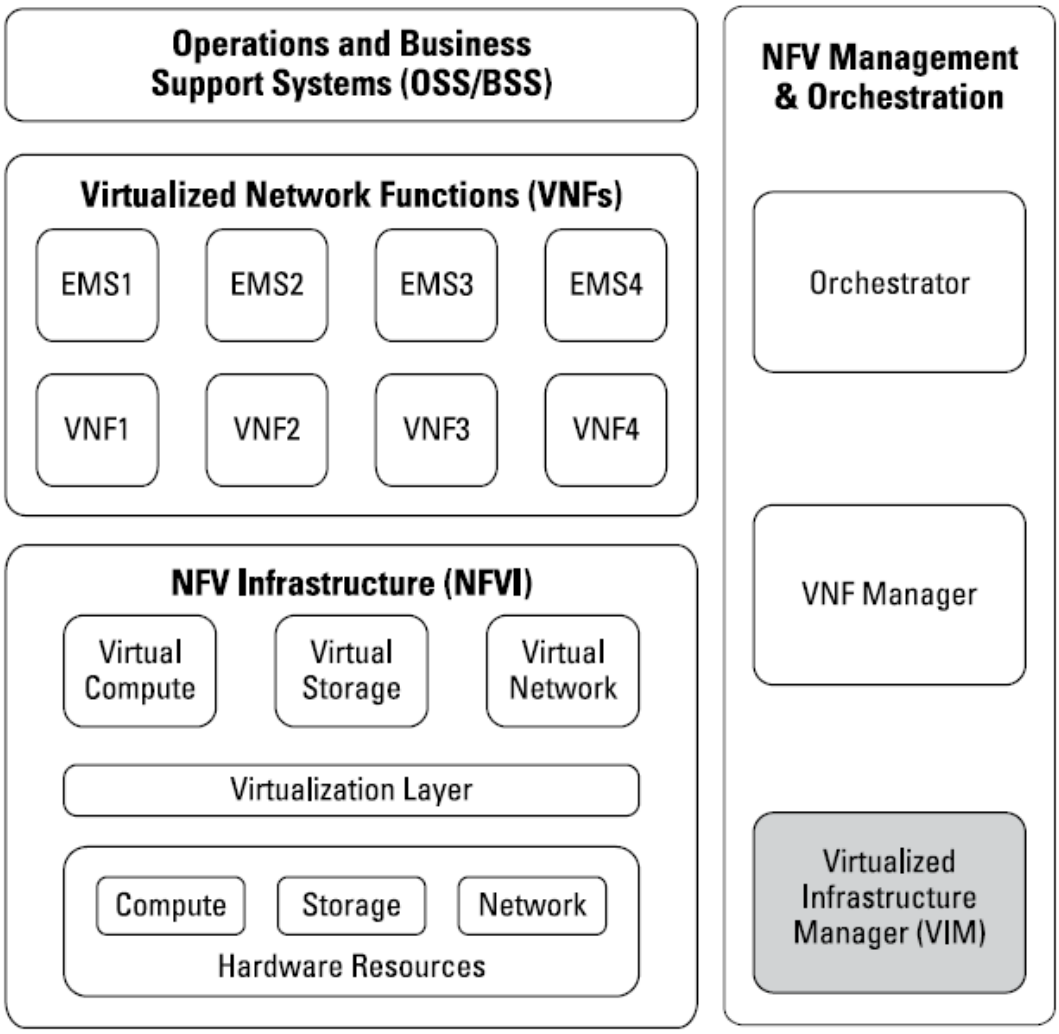
Εικόνα 6: Τα EMS στην αρχιτεκτονική αναφοράς NFV

2.2 Virtualized Infrastructure Manager (VIM)

Ο VIM είναι το σύστημα διαχείρισης που ελέγχει και διαχειρίζεται τον επεξεργαστή, τον αποθηκευτικό χώρο και τις δικτυακές πηγές του NFVI. Σε μια NFVI μπορεί να αντιστοιχεί πάνω από ένα VIM. Οι βασικές του λειτουργίες είναι:

- ✓ Διαχείριση των πόρων
  - Απογραφή Λογισμικού, συμπεριλαμβανομένων των hypervisors,και τις εικονικές (επεξεργαστικές, τις αποθηκευτικές και τις δικτυακές) πηγές
  - Κατανομή των πόρων
  - Διαχείριση των υποδομών, συμπεριλαμβανομένου της δυναμικής εκχώρησης πόρων, της διαχείρισης ενέργειας και της ανάκτησης των πόρων
- ✓ Διαχείριση της λειτουργίας
  - Διαχείριση του NFVI

- Ανάλυση των βαθύτερων αιτίων για τα ζητήματα επιδόσεων του NFVI
- Συλλογή δεδομένων για λάθη, επιδόσεις, χωρητικότητα και βελτιστοποίηση

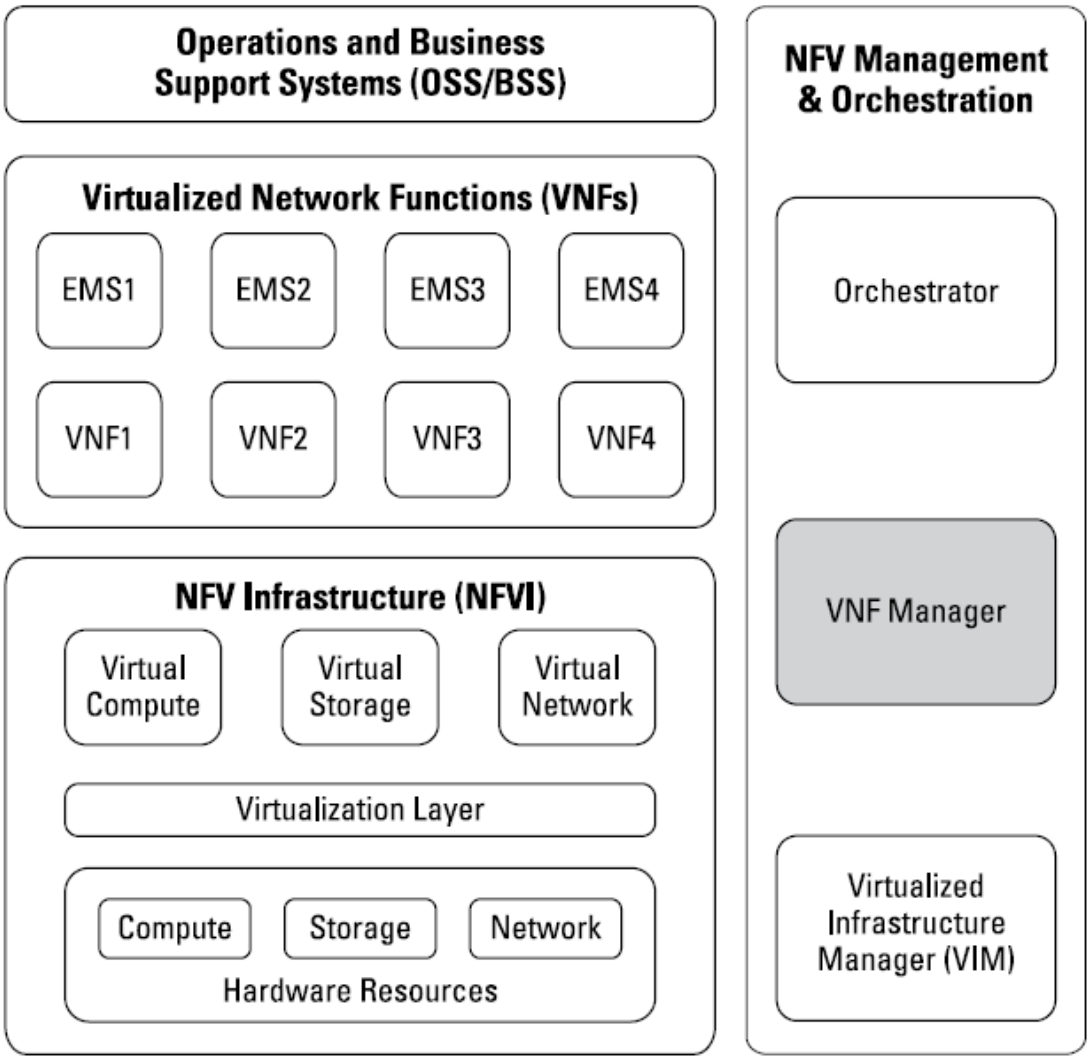


Εικόνα 7: Ο VIM στην MANO

Η διαχείριση και η κατανομή των πόρων σε ένα εικονικό περιβάλλον είναι περίπλοκη. Δεδομένου της φύσης της αρχιτεκτονικής, όλοι οι πόροι είναι μοιρασμένοι ανάμεσα σε πολλές εφαρμογές και ο VIM πρέπει να μεριμνεί για όλα τα απαιτητικά αιτήματα και περιορισμούς σε πραγματικό χρόνο.

2.3 VNF Manager

Ο Virtual Network Function Manager (VNFM) διαχειρίζεται τις λειτουργίες του εικονικού δικτύου. Στα παραδοσιακά δίκτυα η διαχείριση των λειτουργιών του δικτύου εστιάζει στη διαχείριση βλαβών (Fault Management), την διαχείριση ρυθμίσεων (Configuration Management), την διαχείριση κοστολόγησης (Accounting Management), την διαχείριση απόδοσης (Performance Management) και την διαχείριση ασφάλειας (Security Management). Με την εισαγωγή της εικονοποίησης προστέθηκαν νέες πτυχές διαχείρισης του κύκλου ζωής της λειτουργίας VNF και έγιναν βασικές λειτουργίες της διαχείρισης. Ο VNFM και ο EMS είναι στενά συνδεδεμένα και προσφέρουν υποστήριξη διαχείρισης για τη λειτουργία VNF.



Εικόνα 8: Ο VNFM στην NFV αρχιτεκτονική

Βασικός ρόλος του VNFM είναι η διαχείριση του κύκλου ζωής της λειτουργίας VNF. Ο VNFM μπορεί να εκτελέσει πολλές από τις λειτουργίες ίδιες με εκείνες ενός EMS.

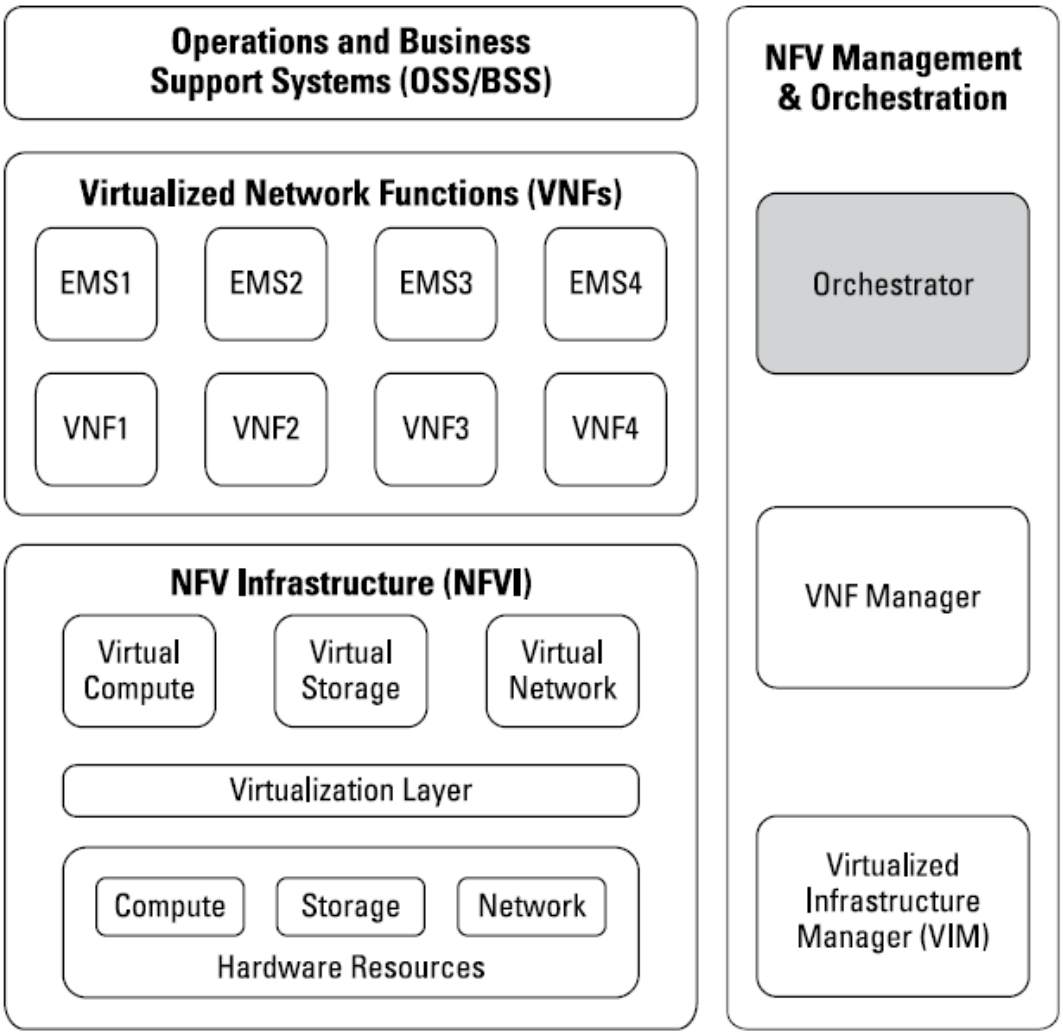
Έτσι οι κατηγορίες αρμοδιοτήτων μεταξύ του EMS και του VNFM μπορεί να διαφέρουν για κάποιες λειτουργίες του δικτύου.

- Δημιουργία μιας λειτουργίας VNF χρησιμοποιώντας προκαθορισμένα ή ήδη υπάρχοντα πρότυπα και παραμέτρους
- Αύξηση ή μείωση της λειτουργίας VNF
- Ενημέρωση και/ή αναβάθμιση των λειτουργιών VNF
- Τερματισμός της λειτουργίας VNF.

2.4 NFV Orchestration

Η NFVO είναι υπεύθυνη για την διαχείριση των υπηρεσιών του δικτύου που προέρχονται από τις λειτουργίες VNF, αλλά και για την δημιουργία end-to-end υπηρεσιών ανάμεσα στις λειτουργίες VNF. Επιπλέον είναι υπεύθυνη για το κύκλο ζωής των υπηρεσιών του δικτύου (NS (Network Services)).
Οι βασικές λειτουργίες της διαχείρισης του κύκλου ζωής των λειτουργιών VNF είναι:

- Προσδιορισμός μιας υπηρεσίας δικτύου, (εγγραφή μιας υπηρεσίας και επιβεβαίωση πως οι απαιτούμενες παράμετροι και οι σχετικοί κανόνες εγγραφήκαν σωστά)
- Δημιουργία μιας υπηρεσίας δικτύου, (Δημιουργία μιας NS χρησιμοποιώντας τις προκαθορισμένες παραμέτρους ή πρότυπα)
- Αύξηση ή μείωση μιας υπηρεσίας δικτύου, (Αύξηση ή μείωση χωρητικότητας μιας NS)
- Ενημέρωση μιας υπηρεσίας δικτύου, με βάση τις αλλαγές διαμόρφωσης
- Δημιουργία, διαγραφή, έρευνα, και ενημέρωση των κανόνων προώθησης και της ακολουθίας προώθησης
- Τερματισμός μιας υπηρεσίας δικτύου, (τερματισμός όλων των λειτουργιών VNF και αποδέσμευση των NFVI πόρων που σχετίζονται με την υπηρεσία του δικτύου, επιστρέφοντάς τους στον χώρο συγκέντρωσης πόρων (resource pool) του NFVI)



Εικόνα 9: Η NFVO στην NFV MANO

Επιπλέον η NFVO χρησιμοποιεί υπηρεσίες από άλλες λειτουργίες (όπως οι λειτουργίες του VIM για την οργάνωση των συνδέσεων μεταξύ των λειτουργιών VNF). Ομοίως, οι υπηρεσίες που παρέχονται από την NFVO μπορούν να χρησιμοποιηθούν και από άλλες λειτουργίες που είναι ταυτοποιημένες και κατάλληλα εξουσιοδοτημένες όπως (το Operations Support System (OSS) και το Business Support System (BSS)).

2.5 Συμπληρώνοντας το NFV με τον OSS μετασχηματισμό

Η δημιουργία και η παράδοση υπηρεσιών μέσα σε μια CSP γίνεται μέσω των παρακάτω στοιχείων ενός OSS (Operation Support Systems):

- Τις λειτουργίες εκπλήρωσης υπηρεσίας, που χειρίζονται το σχεδιασμό μιας υπηρεσίας , την ενεργοποίηση της υπηρεσίας, και την διαδικασία τροφοδοσίας των πόρων της
- Τις λειτουργίες ασφάλειας της υπηρεσίας, που καλύπτουν την ασφάλεια των διεργασιών (επίλυση προβλημάτων)

Για να εκμεταλλευτεί πλήρως την ευκινησία και την ευελιξία ενός εικονικού δικτύου το OSS πρέπει να γίνει:

- Αυτοματοποιημένο: Οι χειροκίνητες διεργασίες πρέπει να αυτοματοποιηθούν όπου είναι εφικτό για να γίνει η λειτουργία πιο ευέλικτη
- Βάση καταλόγου : Δομημένα και διορατικά OSS, με δυνατότητα αυτονομίας που ενδυναμώνουν τις επιχειρήσεις και τους καταναλωτές
- Βασισμένο στις προθέσεις: Αφαίρεση των ροών εργασίας για να εμφανιστεί μόνο το τελικό αποτέλεσμα
- Εστιασμένο στα δεδομένα: Αξιοποίηση των αναλύσεων για την παροχή προσφορών εξατομικευμένων υπηρεσιών

Η αλλαγή του OSS

Δύο κύριες πτυχές του NFV MANO παίζουν κύριο ρόλο στην αλλαγή του OSS και είναι οι παρακάτω:

- Αυτοματοποιημένη παροχή και διαμόρφωση: η τεχνολογία NFV έχει ευελιξία από την ικανότητά της να παρέχει υπηρεσίες με αυτοματοποιημένο τρόπο. Αυτό ενεργοποιείτε από πολλές υποκειμενικές πτυχές όπως είναι η αφαίρεση των πολύπλοκων τοπολογιών, η διαμόρφωση με βάση την πρόθεση (intent-based), κ.α. Οι προσεγγίσεις βασισμένες σε cloud μπορούν να δέσουν τα σχετικά συστήματα μεταξύ τους και να παρέχουν δυνατότητες όπως είναι ο λειτουργικός έλεγχος, η ροή τροφοδοσίας, και η βελτίωση του δικτύου για πιο αποδοτικό περιβάλλον ανάπτυξης.
- Πιο κλειστή σχέση ανάμεσα στην ασφάλεια και την ολοκλήρωση των διαδικασιών: Η αρχιτεκτονική της NFV επιτρέπει τον έλεγχο σε πραγματικό χρόνο στην κατάσταση των στοιχείων του δικτύου και της καταγραφής. Αυτή η πληροφορία είναι ανεκτίμητη για την

ολοκλήρωση της διαδικασίας, αφού δημιουργεί νέες περιπτώσεις παροχής υπηρεσιών.

Πολλές από τις υπάρχων OSS υποδομές δεν μπορούν να υποστηρίξουν αυτά τα δύο στοιχεία, διότι η σχέση μεταξύ της ολοκλήρωσης και της ασφάλειας είναι σχετικά στατική, με σημαντική καθυστέρηση στο συγχρονισμό των απαιτήσεων μεταξύ αυτών τον δύο.

3. Εικονοποίηση του κινητού δικτύου και του IP Multimedia Υποσυστήματος

Τα κινητά δίκτυα χρησιμοποιούν πολύ ιδιόκτητο υλικό (hardware) και εξειδικευμένο εξοπλισμό. Το Evolved Packet Core(EPC), που αποτελείται από διάφορα εξειδικευμένα μέρη, είναι το τελευταίο κομμάτι της αρχιτεκτονικής του δικτύου για κινητά συστήματα. Με την εικονοποίηση ορισμένων λειτουργιών του δικτύου όπως, η Serving Gateway(SGW), η Packet Gateway(PGW), και το Mobile Management Entity(MME), οι λειτουργίες μπορούν να κλιμακωθούν ανεξάρτητα, ανάλογα με τις απαιτήσεις των πόρων τους. Για παράδειγμα, μπορεί τα επίπεδα δεδομένων να χρειαστεί να αυξηθούν, αλλά όχι απαραίτητα τα επίπεδα έλεγχου.

Το IP Multimedia Subsystem (IMS) παρέχει την υπηρεσία έλεγχου των λειτουργιών για να υποστηρίξει την παροχή υπηρεσιών πολυμέσων πάνω από το EPC και άλλα IP-based δίκτυα, σταθερά και κινητά, και αποτελείται επίσης από εξειδικευμένα μέρη. Αυτές οι προσαρμοσμένες εφαρμογές μπορούν να λειτουργήσουν στους κοινούς hardware πόρους, με αποτέλεσμα να υπάρχει χαμηλότερο κόστος, υψηλή προσαρμοστικότητα, και ταχέως αναπτυσσόμενα συστήματα.

VNF Forwarding Graphs

Ένα προωθητικό γράφημα μιας λειτουργίας του δικτύου, προσδιορίζει την αλληλουχία των λειτουργιών του δικτύου, που διασχίζουν τα πακέτα στο δίκτυο. Ομοίως με τα φυσικά δίκτυα που συνδέονται με καλώδια, τα VNF Forwarding Graphs(VNF-FG) παρέχουν την λογική συνδεσιμότητα ανάμεσα στις εικονικές συσκευές. Τα VNF-FG προσφέρουν ευελιξία στην ανάπτυξη, και αναβαθμίσεις, σε σχέση με το φυσικό σχεδιασμό. Επιπλέον, αυξάνουν την ελαστικότητα που έχουν οι λειτουργίες VNF που οφείλονται στις απαιτήσεις για αλλαγή της χωρητικότητας.

Εικονοποίηση του σταθμού βάσης κινητής

Μεγάλος αριθμός radio access network(RAN) κόμβων σε κινητά δίκτυα, είναι μέρος της κεφαλαιουχικής δαπάνης και των λειτουργικών εξόδων. Οι RAN κόμβοι συμπεριλαμβανομένου και των σταθμών που συνδέονται κατευθείαν με τους συνδρομητές-κινητές συσκευές, είναι κατασκευασμένοι σε ιδιόκτητο hardware και έχουν μακριά εξέλιξη, ανάπτυξη και λειτουργικό κύκλο ζωής. Με την εικονοποίηση

τουλάχιστον ενός μέρους των RAN κόμβων, μέσα στα πρότυπα της βιομηχανίας, μπορεί να επιτευχθούν χαμηλότερα έξοδα και χαμηλότερο κόστος ενέργειας. Επιπλέον, οι βασισμένες-σε λογισμικό (software-based) εφαρμογές μπορούν να προσφέρουν δυναμική κατανομή των πόρων, καλύτερη εξισορρόπηση φορτίου και ευκολότερη διαχείριση και διαμόρφωση. Ακόμα ένα πλεονέκτημα είναι η προώθηση ενός ανταγωνιστικού περιβάλλοντος, όπου μικρότεροι, καινοτόμοι πάροχοι εφαρμογών μπορούν να συμμετέχουν σε μια ανοιχτή πλατφόρμα που παρέχεται από την NFV αρχιτεκτονική.

Εικονοποίηση του οικιακού περιβάλλοντος

Οι CSPs προσφέρουν στους πελάτες τους συνδρομητικό εξοπλισμό (CPE). Ο συνδρομητικός εξοπλισμός (routers, switches, modems) τοποθετείται είτε στο σπίτι είτε στην επιχείρηση ενός πελάτη. Η εικονοποίηση του οικιακού περιβάλλοντος παρέχει χαμηλότερα έξοδα για τον προμηθευτή, αντικαθιστώντας τους συνδρομητικούς εξοπλισμούς στα αστικά περιβάλλοντα, με χαμηλής λειτουργικότητας συσκευές πρόσβασης. Αυτές οι συσκευές μπορούν να έχουν μεγαλύτερο κύκλο ζωής, οπότε θα χρειάζονται λιγότερη συντήρηση και λιγότερες αναβαθμίσεις/ενημερώσεις. Επιπλέον, με τον τρόπο αυτό οι CSPs θα μπορούν να προσφέρουν καινούργιες υπηρεσίες χωρίς να χρειάζεται να αντικατασταθεί ο παλαιός συνδρομητικός εξοπλισμός με νέο, επιτρέποντας έτσι στον πελάτη να έχει πρόσβαση πάντα σε νέες υπηρεσίες.

Εικονοποίηση του Content Delivery Network (CDN)

Η συνεχώς αυξανόμενη ζήτηση για πλουσιότερα multimedia όπως video, streaming κτλ, δημιουργεί μεγαλύτερες προκλήσεις για το εύρος ζώνης και την χωρητικότητα στους CSPs. Η ενσωμάτωση των CDN κόμβων στα δίκτυα του χειριστή (operator networks) μπορεί να είναι μια καλή λύση για την αντιμετώπιση αυτών των προκλήσεων. Η μεταφορά δεδομένων από επεξεργαστικούς και αποθηκευτικούς κόμβους που είναι πιο κοντά στον τελικό χρήστη, αυξάνει το εύρος ζώνης και την ποιότητα του streaming. Η εικονοποίηση των CDN κόμβων προσφέρει στους παρόχους υπηρεσιών την ευελιξία να προσαρμοστούν στις νέες περιστάσεις και τις ευκαιρίες της αγοράς. Η παροχή περιεχομένου χαρακτηρίζεται από την ταχεία καινοτομία στις μορφές, τα πρωτόκολλα και τις τεχνικές συμπίεσης. Επιπροσθέτως, είναι απλούστερη η συντήρηση μέσω της χρήσης του προτύπου hardware της βιομηχανίας. Τέλος, η εικονοποίηση επιτρέπει τη δυναμική κατανομή των πόρων και την δυνατότητα αποφυγής του over-engineering.

NFV σταθερής πρόσβασης

Τα Broadband digital Subscriber Line (DSL) συνήθως χρησιμοποιούνται σε κατοικημένες περιοχές ή σε μικρομεσαίες επιχειρήσεις. Γρήγορα όμως, το DSL αντικαθιστάτε από άλλες τεχνολογίες, όπως την hybrid fiber-DSL και το VDSL2. Η NFV σταθερής πρόσβασης έρχεται αντιμέτωπη με το υψηλό κόστος και τη συμφόρηση που συχνά συνδέεται με την ευρυζωνική (broadband: δίκτυο στο οποίο τα

δεδομένα κινούνται με υψηλές ταχύτητες) πρόσβαση στο δίκτυο. Οι νέες αυτές τεχνολογίες απαιτούν εγκατάσταση νέου εξοπλισμού, που πρέπει να είναι υψηλής ενεργειακής απόδοσης και όσο το δυνατόν απλούστερες για να έχουν μεγαλύτερο κύκλο ζωής. Με την εικονοποίηση τα προβλήματα αντιμετωπίζονται μετακινώντας τη σύνθετη διαδικασία στα άκρα (head end), σε αντίθεση με τους κινητούς κόμβους. Επιπλέον, η εικονοποίηση επιτρέπει στην υποδομή να έχει πολλαπλές λειτουργίες και να προσφέρει νέα επιχειρησιακά μοντέλα. Τέλος, επιτρέπει την συνεργασία των ασύρματων στοιχείων πρόσβασης σε μια κοινή NFVI point-of-presence(PoP) ή μια πλατφόρμα.

4. NFV Security

Παρακάτω περιγράφονται μερικά από τα οφέλη για την ασφάλεια του δικτύου μετά από την εισαγωγή της εικονοποίησης στο δικτυακό περιβάλλον:

• Η κεντρική μονάδα αποθήκευσης που χρησιμοποιείται στα εικονικά περιβάλλοντα αποτρέπει την απώλεια σημαντικών δεδομένων, εάν μια συσκευή χαθεί, κλαπεί ή παραβιαστεί.

• Όταν τα VMs και οι εφαρμογές απομονωθούν σωστά, μόνο μία εφαρμογή σε ένα λειτουργικό σύστημα επηρεάζεται από την επίθεση.

• Όταν ρυθμιστεί σωστά, ένα εικονικό περιβάλλον παρέχει ευελιξία επιτρέποντας την κοινή χρήση των συστημάτων χωρίς απαραίτητα να χρειάζεται να μοιράζονται κρίσιμες πληροφορίες ανάμεσα στα συστήματα.

• Εάν μια VM έχει ‘‘μολυνθεί’’, μπορεί να επανέλθει στην προηγούμενη κατάσταση ("ασφαλές") που υπήρχε πριν από την επίθεση.

• Οι μειώσεις του hardware που προκύπτουν λόγω του virtualization βελτιώνουν την φυσική ασφάλεια, δεδομένου ότι υπάρχουν λιγότερες συσκευές και λιγότερα κέντρα δεδομένων.

• Το Desktop virtualization μπορεί να χρησιμοποιηθεί, για τον καλύτερο έλεγχο του περιβάλλοντος του χρήστη. Ένας διαχειριστής μπορεί να δημιουργήσει και να ελέγξει ένα πρότυπο (golden image) που μπορεί να σταλεί προς ‘’τα κάτω’’ στους υπολογιστές των χρηστών. Αυτή η τεχνολογία παρέχει καλύτερο έλεγχο του λειτουργικού συστήματος για να εξασφαλίζεται ότι πληροί τις οργανωτικές απαιτήσεις, καθώς και τις πολιτικές ασφάλειας.

• Η εικονοποίηση του Server μπορεί να οδηγήσει σε καλύτερη αντιμετώπιση περιστατικών, δεδομένου ότι οι servers μπορούν να επανέλθουν σε μια προηγούμενη κατάσταση, προκειμένου να εξετάσουν τι συνέβη πριν και κατά τη διάρκεια μιας επίθεσης.

• Το σύστημα πρόσβασης και ελέγχου διαχείρισης του δικτύου καθώς και ο διαχωρισμός των καθηκόντων μπορεί να βελτιωθεί, και σε ορισμένα άτομα μπορεί να ανατεθεί να ελέγχουν μόνο τα VMs εντός του δικτύου, ενώ άλλοι ασχολούνται μόνο με τα VMs στο DMZ (demilitarized zone). Μπορεί , για παράδειγμα να υπάρχουν ορισμένοι διαχειριστές που ασχολούνται μόνο με Windows servers, ενώ άλλοι ασχολούνται μόνο με Linux servers.

• Το λογισμικό του Hypervisor είναι ¨μικρό¨ και δεν είναι περίπλοκο και παρέχει μια μικρότερη επιφάνεια επίθεσης στον ίδιο τον hypervisor. Όσο μικρότερη είναι η επιφάνεια επίθεσης, τόσο λιγότερα είναι τα πιθανά τρωτά σημεία.

• Ένας τύπος επίθεσης είναι η επίθεση διπλής ενθυλάκωσης (encapsulation) σε VLAN. Αυτός ο τύπος επίθεσης εκμεταλλεύεται τον τρόπο λειτουργίας του hardware των switches. Τα περισσότερα switches εκτελούν μόνο ένα επίπεδο από-θυλάκωσης (de-encapsulation), επιτρέποντας σε έναν εισβολέα να ενσωματώσει μια κρυφή ετικέτα μέσα στο πλαίσιο. Αυτή η ετικέτα επιτρέπει την προώθηση του πλαισίου σε ένα VLAN που δεν ορίζεται από την αρχική ετικέτα. Για να αποτραπεί αυτός ο τύπος επίθεσης οι Vswitches απορρίπτουν τα διπλά πακέτα ενθυλάκωσης.

• Ένας επιτιθέμενος μπορεί να στείλει έναν μεγάλο αριθμό πλαισίων (frames) ταυτόχρονα σε ένα γνωστό VLAN, με σκοπό την υπερφόρτωση των switches. Έτσι οι switches για να μπορέσουν να διαχειριστούν την κίνηση μπορεί να μεταδώσουν κάποια πλαίσια σε άλλα VLAN. Με τον τρόπο αυτό ο επιτιθέμενος μπορεί τελικά να αποκτήσει πρόσβαση στο VLAN που θέλει. Οι Vswitches δεν επιτρέπουν στα πλαίσια να εγκαταλείψουν τον ανατεθειμένο τομέα εκπομπής τους (VLAN) και δεν είναι ευάλωτα σε αυτόν τον τύπο επίθεσης.

*ο όρος **πλαίσιο (frame)**, χρησιμοποιείται για να περιγραφεί η μορφή ενός πακέτου για μια δεδομένη τεχνολογία υλικού.

Η εικονοποίηση είναι πολύ περίπλοκη γι 'αυτό πρέπει να ρυθμιστεί σωστά για να μπορέσουν αποκτηθούν τα παραπάνω οφέλη.

4.1 Προκλήσεις για την ασφάλεια

- Η κοινή χρήση αρχείων μεταξύ των κόμβων(hosts) και των επισκεπτών δεν είναι ασφαλής.
- Η απομόνωση και η επικοινωνία ανάμεσα στα διαχωρισμένα μέρη όπως το Guest Oss και οι εφαρμογές, οι hypervisors, το hardware και τα εικονικά συστήματα διαχείρισης μερικές φορές αδυνατούν να καταστήσουν δυνατή την επικοινωνία μεταξύ του OS.
- Στην εικονοποίηση, οι πολλαπλοί servers ενοποιούνται σε ένα host, αφαιρώντας το φυσικό διαχωρισμό μεταξύ των servers, ενώ ταυτόχρονα αυξάνουν τον κίνδυνο έκθεσης που μπορεί να εξαπλωθεί από τη μία εφαρμογή στην άλλη ανάμεσα στον ίδιο host.

Τα εκτεθειμένα εικονικά στρώματα και μια επίθεση κατά του host hypervisor, μπορούν να οδηγήσουν στην έκθεση όλων των φιλοξενούμενων εικονικών μηχανών (VMs), καθώς και όλων των κοινόχρηστων φυσικών πόρων που χρησιμοποιούνται από τον εν λόγω host. Αν ο hypervisor είναι σε κίνδυνο, οποιαδήποτε συνδεδεμένη εικονική μηχανή θα είναι επίσης σε κίνδυνο. Έτσι, όταν ο hypervisor δέχεται επίθεση, ο εισβολέας αποκτά τον πλήρη έλεγχο όλων των δεδομένων που είναι στο περιβάλλον του hypervisor. Ομοίως, οι εικονικές μηχανές που δεν είναι απομονωμένες μπορούν επίσης να έχουν πλήρη πρόσβαση στους host πόρους, οπότε κάθε έκθεση οποιασδήποτε εικονικής μηχανής μπορεί να καταλήξει σε έκθεση των πόρων.

Η εικονοποίηση προσθέτει νέα στρώματα πολυπλοκότητας των υποδομών, τόσα πολλά με αποτέλεσμα η παρακολούθηση για ασυνήθιστα γεγονότα και ανωμαλίες να γίνεται περισσότερο περίπλοκη, με συνέπεια να γίνεται πιο δύσκολο να εντοπιστούν τα ζητήματα ασφάλειας, όπως οι προηγμένες ‘’επίμονες’’ απειλές.

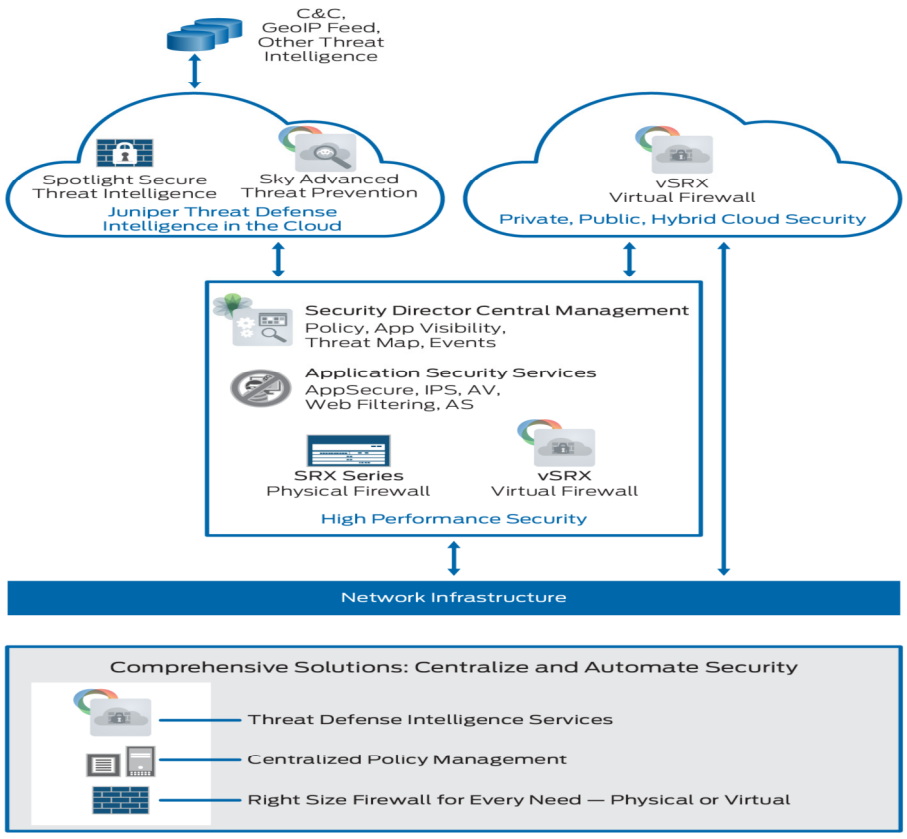
Υπάρχει επίσης μια έλλειψη ορατότητας στην κίνηση μεταξύ των εικονικών μηχανών που ποτέ δεν ‘αγγίζουν’ το φυσικό δίκτυο (κίνηση VM-to-VM), που περιπλέκει την ικανότητα να αποδοθούν πολιτικές ασφάλειας σε κάθε εικονική μηχανή και να παρακολουθούνται αυτές οι πολιτικές ασφαλείας για να διασφαλιστεί η συνεχής συμμόρφωση με τους κανονισμούς.

Η δυναμική φύση των εικονικών περιβαλλόντων παρουσιάζει επίσης νέες προκλήσεις για τα συστήματα πρόληψης εισβολών (IPS). Το Malware δημιουργήθηκε με στόχο τόσο τις φυσικές όσο και τις εικονικές μηχανές προκαλώντας την ‘μόλυνση’ μέσω του εικονικού δικτύου. Μη ανιχνεύσιμες malware επιθέσεις σε εμπιστευτικές πληροφορίες στο εικονικό περιβάλλον θέτουν επίσης προβλήματα. Άλλες απειλές για την ασφάλεια περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση, άρνηση παροχής υπηρεσιών, κτλ. Τα παραδοσιακά εργαλεία της ασφάλειας του δικτύου δεν είναι επαρκή για τα εικονικά περιβάλλοντα. Τα Firewalls πρέπει να βασίζονται σε ιδιότητες φυσικών ή δικτυακών στρωμάτων για την προστασία των servers και των

εφαρμογών που είναι ιδιαίτερα ευάλωτα σε περίπτωση παραβίασης της ασφάλειας, και τα προϊόντα ασφαλείας που έχουν σχεδιαστεί για ανεξάρτητους φυσικούς servers και σταθμούς εργασίας μπορεί να προκαλέσουν σοβαρά προβλήματα σε εικονικά περιβάλλοντα.

4.2 The Virtual Firewall: the vSRX Services Gateway (Juniper Networks)

Η vSRX Services Gateway είναι ένα φίλτρο κατάστασης (stateful firewall) που ενσωματώνεται με έναν hypervisor στον πυρήνα όπου ελέγχει και προστατεύει την κυκλοφορία στο εικονικό στρώμα, μεταξύ των εικονικών μηχανών σε ένα host, ή μεταξύ των εικονικών μηχανών σε ένα εικονικό δίκτυο. Η vSRX επιτρέπει στους διαχειριστές του δικτύου και της ασφάλειας, να προσαρμόσουν γρήγορα και αποτελεσματικά την κλίμακα του τείχους προστασίας για να ανταποκριθούν στις δυναμικές ανάγκες των εικονικών και των cloud περιβαλλόντων. Στο σχήμα 1 απεικονίζετε μια τυπική λύση εικονοποίησης από την Juniper Networks, που περιλαμβάνει την vSRX.



Εικόνα 10: Εικονοποίηση της ασφάλειας των δικτύων

Η vSRX φέρνει το Junos λειτουργικό σύστημα βασισμένο σε x86 εικονικά περιβάλλοντα, που του επιτρέπει να παραδώσει μια πλήρη, ολοκληρωμένη εικονική

λύση ασφαλείας, που περιέχει τείχος προστασίας του δικτύου(firewall), IPS, και τεχνολογίες VPN. Η vSRX επίσης ενσωματώνει ένα ολοκληρωμένο σύνολο τεχνολογιών τείχους προστασίας επόμενης γενιάς όπως: Layer 7 έλεγχο εφαρμογών, διαθεσιμότητα, βελτιστοποίηση της ροής κυκλοφορίας, web φιλτράρισμα, antivirus, anti-spam, και επιβολή ελέγχου πρόσβασης στο δικτύου. Στο Σχήμα 1 φαίνεται ότι η χρήση τόσο της πλατφόρμας SRX Series όσο και της vSRX πλατφόρμας, υπερασπίζεται τις εφαρμογές και προστατεύει τα δεδομένα καθώς κινείται σε όλη την ευρύτερη περιοχή μεταξύ των επιχειρήσεων και των cloud υπηρεσιών, και μεταξύ και εντός των συσκευών των κέντρων δεδομένων. Η vSRX μπορεί να χρησιμοποιηθεί με τον ίδιο τρόπο όπως και μια φυσική συσκευή. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για την τμηματοποίηση της κυκλοφορίας σε ένα μοντέλο παροχής υπηρεσιών cloud, ή σαν μια ειδική edge συσκευή ανά χρήστη σε μια hosted υπηρεσία, ή σε ένα εικονικό CPE για την υπηρεσία MPLS, ή απλά ως μια πιο ισχυρή εναλλακτική λύση σε ένα host-based τείχος προστασίας.

Η vSRX μπορεί να ενεργήσει ως εμπόδιο για την προστασία της περιμέτρου πρόσβασης σε ένα δίκτυο. Παρέχει υπηρεσίες ασφαλείας και διαβεβαιώνει την απομόνωση της κυκλοφορίας μέσα στον cloud, μαζί με προσαρμόσιμους firewall ελέγχους ως πρόσθετη υπηρεσία διαχείρισης.

Οι επιχειρήσεις και οι φορείς παροχής υπηρεσιών μπορούν να αξιοποιήσουν τις εικονικές επενδύσεις τους για την δημιουργία μιας περιμέτρου ασφαλείας, έχοντας ασφάλεια στους πόρους τους εντός του cloud και στους συνδρομητές της υπηρεσίας. Η vSRX επίσης υποστηρίζει το προϊόν Juniper Networks Contrail, OpenContrail, μια ποικιλία από εικονοποιημένες λειτουργίες δικτύου (NFV) περιπτώσεων χρήσεως, και τρίτων SDN λύσεων, και μπορεί να ενσωματωθεί με επόμενης γενιάς cloud orchestration εργαλεία όπως OpenStack, είτε άμεσα είτε μέσω API.

Για την καλύτερη κατανόηση της ‘’εικονοποιημένης’’ ασφαλείας θα αναλύσουμε τρείς περιπτώσεις χρήσεως:

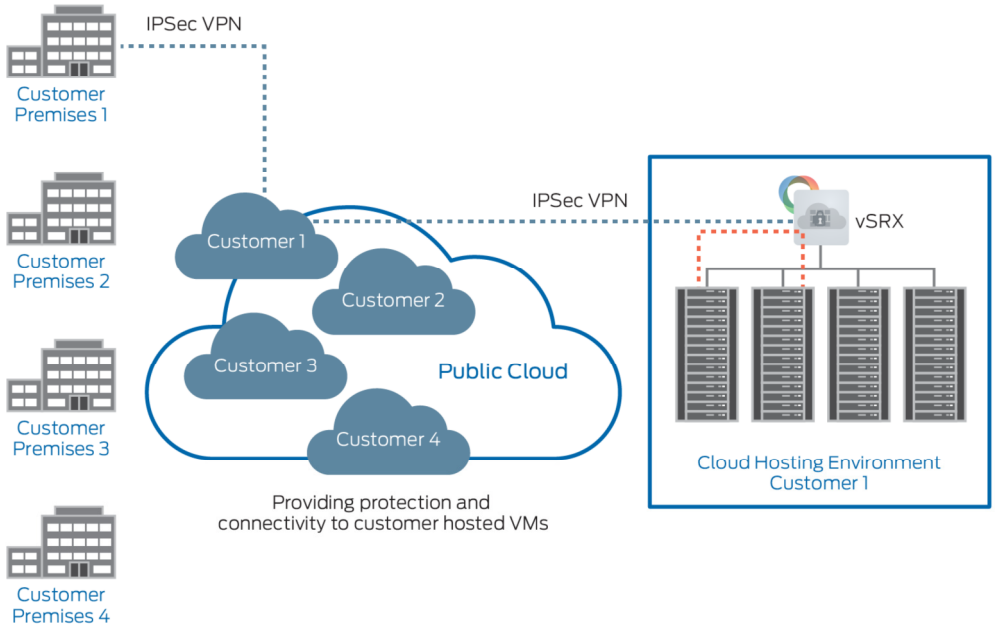
- Public Cloud Περίπτωση χρήσης (Cloud-Hosting Providers)
- Public Cloud Περίπτωση χρήσης (Managed Security Service Providers)
- Private Cloud Περίπτωση χρήσης

4.2.1 Public Cloud (Cloud-Hosting Providers)

Στην public cloud περίπτωση χρήσης, οι πάροχοι υπηρεσιών μπορούν να φιλοξενήσουν έναν μεγάλο αριθμό από VMs-σε ορισμένες περιπτώσεις άνω των 50.000 για τους πελάτες τους. Σε μια public cloud περίπτωση χρήσης, όλες οι τμηματικές ομάδες, ή χρήστες (tenants), ανήκουν σε διαφορετικές εταιρείες, έτσι ώστε κάθε μία να έχει τον δικό της τρόπο χρήσης. Ως εκ τούτου, ο πάροχος public cloud υπηρεσιών πρέπει να φιλοξενεί διαρκώς μεταβαλλόμενα μεγέθη φόρτου εργασίας, που είναι επίσης επεκτάσιμα και ελαστικά. Με την vSRX, οι πάροχοι υπηρεσιών μπορούν να παρέχουν στους πελάτες τους, την ασφάλεια που απαιτείται, τόσο στα εσωτερικά εικονικά κέντρα δεδομένων τους όσο και στα ενοικιαζόμενα(tenant) edge εικονικά δίκτυα. Σημαντικά οφέλη της vSRX είναι:

- Τμηματοποίηση πελατών
- Ασφάλεια στα άκρα του δικτύου
- Έλεγχος πρόσβασης στις εικονικές μηχανές
- Λεπτομερή έλεγχο φυσικών και εικονικών στοιχείων

Το σχήμα παρακάτω δείχνει την τοπολογία της public cloud περίπτωσης χρήσης. Περιλαμβάνει την vSRX σε συνεργασία με Junos Space προϊόντα, εικονικές συσκευές Juniper Networks Secure και προϊόντα VMware που αναπτύσσονται στην υποδομή του cloud.



Εικόνα 11: Τοπολογία δημόσιου cloud

Οι πάροχοι public cloud υπηρεσιών μπορούν να αναπτύξουν την vSRX για να προστατεύσουν τους πελάτες τους τοποθετώντας το εικονικό firewall μπροστά από το μεμονωμένο host περιβάλλον του κάθε πελάτη, διατηρώντας τα hosting περιβάλλοντα

ξεχωριστά το ένα από το άλλο. Η vSRX προσφέρει πλούσια χαρακτηρίστηκα δρομολόγησης, VPN, και μετάφραση διευθύνσεων δικτύου (NAT), επιτρέποντας στους παρόχους υπηρεσιών να συνδέσουν εύκολα χρήστες (tenants) από το public cloud στο private cloud.

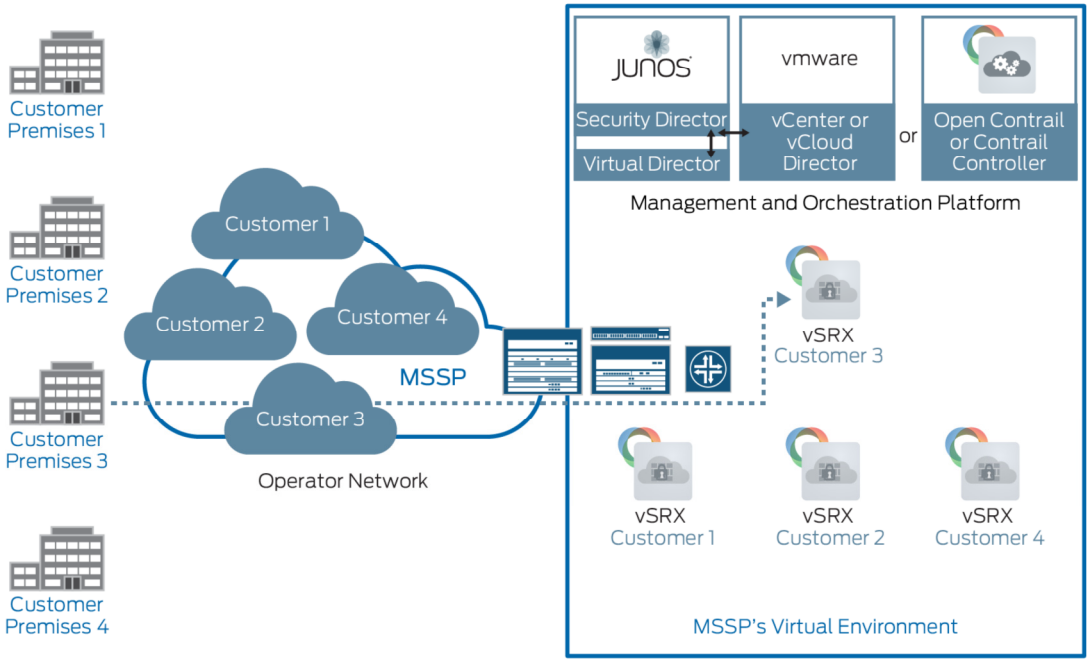
Τέλος, μια ποικιλία από διεπαφές διαχείρισης για την vSRX επιτρέπει στα VMs να είναι ασφαλή μέσω των ρυθμίσεων bootstrap και στη συνέχεια να διαχειρίζονται μέσω των CLI, J-Web, ή Junos Space Virtual Director.

4.2.2 Public Cloud Use Case (Managed Security Service Providers)

Μεγάλες εταιρίες παροχής τηλεπικοινωνιακών υπηρεσιών και οι πάροχοι διαχείρισης ασφάλειας των υπηρεσιών, προσφέρουν ολοκληρωμένες υπηρεσίες ασφαλείας στους πελάτες τους, συμπεριλαμβανομένων των firewalls και των IPsec VPNs. Οι υπηρεσίες εικονικής ασφαλείας μπορούν να αναπτυχθούν με διάφορους τρόπους σε αυτή την γενική περίπτωση χρήσης. Για την vSRX, ο πάροχος υπηρεσιών μπορεί τυπικά να εδραιώσει υπηρεσίες σε ένα εικονικό hardware στην τοποθεσία των πελατών και στη συνέχεια να προσφέρει το εικονικό firewall ως μια πλήρη υπηρεσία διαχείρισης. Η vSRX μπορεί να προσφέρει:

- Τμηματοποίηση πελατών
- Ασφάλεια
- Συμμόρφωση
- Μείωση των κεφαλαιουχικών δαπανών και των λειτουργικών εξόδων

Το σχήμα παρακάτω δείχνει τα προϊόντα λογισμικού και hardware σε μια τέτοια εκτεταμένη υπηρεσία διαχείρισης ασφάλειας του κέντρου δεδομένων.



Εικόνα 12: Δημόσιο cloud(Πάροχοι υπηρεσιών διαχείρισης της ασφάλειας)

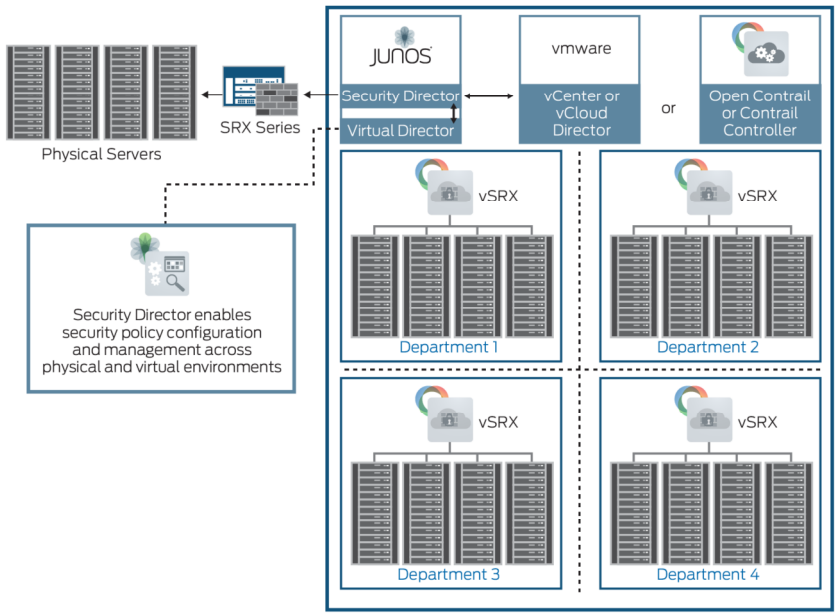
Οι πάροχοι υπηρεσιών διαχείρισης της ασφάλειας μπορούν να χρησιμοποιήσουν την vSRX για να προσφέρουν υπηρεσίες ασφαλείας στους πελάτες τους με πολλαπλές απομακρυσμένες τοποθεσίες. Αυτό συμβαίνει επειδή ένα μόνο vSRX μπορεί να χρησιμοποιηθεί για πολλαπλές απομακρυσμένες τοποθεσίες. Για παράδειγμα, ο πελάτης θα μπορούσε να έχει πολλά απομακρυσμένα καταστήματα λιανικής πώλησης, καφετέριες ή καταστήματα. Με τη χρήση της vSRX που ''κατοικεί'' στην υποδομή του φορέα παροχής υπηρεσιών, δεν είναι αναγκαίο να υπάρχουν συσκευές σε κάθε απομακρυσμένο κατάστημα ή ιστοσελίδα. Ο πάροχος υπηρεσιών ασφαλείας φιλοξενεί (host) και διαχειρίζεται την vSRX η οποία, με το συνδυασμό της εφαρμογής διαχείρισης vSRX VM και του Junos Space Security Director, επιτρέπει στον πάροχο υπηρεσιών να διαχειριστεί όλες τις φάσεις του κύκλου ζωής της πολιτικής ασφάλειας, και για τα φυσικά και για τα εικονικά στοιχεία του, από μια κοινή κεντρική πλατφόρμα. Είναι ένας από τους τρόπους όπου η εικονική ασφάλεια αλλάζει τα δίκτυα.

4.2.3 Private Cloud Use Case

Τα ιδιωτικά clouds χρησιμοποιούνται αποκλειστικά για τις ανάγκες του ιδιοκτήτη τους. Πρόκειται για κοινές λύσεις για τις μεγάλες επιχειρήσεις, τα πανεπιστήμια και τα χρηματοπιστωτικά ιδρύματα. Τα ιδιωτικά clouds επιτρέπουν στους ιδιοκτήτες τους να μεγιστοποιήσουν τους πόρους, συγκεντροποιώντας τους και μοιράζοντάς τους. Η χρήση των εικονικοποιημένων, συγκεντρωμένων πόρων σε ένα ιδιωτικό cloud μπορεί να αμφισβητήσει τις απαιτήσεις μυστικότητας , μέχρι να εφαρμοστεί η ασφάλεια για εικονικά περιβάλλοντα. Για να διατηρηθούν τα δεδομένα ιδιωτικά, και προστατευμένα, ο ιδιοκτήτης του private cloud μπορεί να τμηματοποιήσει τα εικονοποιημένα του περιβάλλοντα σε ομάδες, όπως οι επιχειρηματικές μονάδες ή τα εταιρικά τμήματα, και στη συνέχεια, να χρησιμοποιήσει την vSRX για να ασφαλίσει αυτές τις ομάδες με διαφορετικό τρόπο βάσει των εσωτερικών ή των ρυθμιστικών απαιτήσεων. Η vSRX μπορεί να παρέχει όλα τα απαραίτητα εικονικά οφέλη:

- Ασφαλή επικοινωνία μέσω δρομολόγησης, NAT, και VPNs
- Ασφάλεια στα άκρα του δικτύου
- Κράτηση και παροχή λειτουργικού διαχωρισμού
- Συμμόρφωση υποστήριξης και ρυθμιστικών αναγκών

Στο σχήμα παρακάτω φαίνεται αυτή η ιδιωτική cloud περίπτωση χρήσης, με τη χρήση εικονικοποιημένης ασφάλειας μέσω της vSRX, και των Junos Space προϊόντων, της Juniper Networks JSA Series Secure Virtual Analytics Appliance, και τα VMware προϊόντα που έχουν αναπτυχθεί στην υποδομή του cloud.



Εικόνα 13: Τοπολογία ιδιωτικού cloud

Στο σχήμα , ένας διαχειριστής του ιδιωτικού cloud μπορεί να αναπτύξει πολλαπλά vSRX για την ασφάλιση του εικονικού περιβάλλοντος, ακόμη και σε επίπεδο VM και στην άκρη (edge) του δικτύου της κάθε τμηματοποιημένης ομάδας. Η vSRX παρέχει προσαρμοσμένη ασφάλεια για εικονικά περιβάλλοντα, αυτοματισμό για λειτουργική ευκολία και αποτελεσματικότητα, και λεπτομερή έλεγχο πάνω από τα φυσικά και εικονικά στοιχεία. Με το συνδυασμό του Junos Space Security Director με το Virtual Director, οι διαχειριστές μπορούν να βελτιώσουν τη διαμόρφωση της πολιτικής, την διαχείριση και την ορατότητα στα φυσικά και εικονικά στοιχεία από μία κοινή, κεντρική πλατφόρμα.

5. Η προσέγγιση της Hewlett Packard Enterprise στην NFV

Η HPE πιστεύει πως η εξέλιξη της NFV χωρίζετε σε τέσσερα μέρη:

Διαχωρισμός: Ξεχωριστό software από το hardware. Στόχος είναι να επιτρέπετε στις εικονικές λειτουργίες (VNFs) να τρέχουν σε τυποποιημένες ανοιχτές πλατφόρμες.

Εικονοποίηση: Οι λειτουργίες του δικτύου αναπτύσσονται στους εικονικούς πόρους της υποδομής. Αυτό προσφέρει ευχρηστία, καλύτερη αποδοτικότητα του κόστους, και ικανότητα ταχύτερης κλιμάκωσης.

Cloudify: Το ευρύτερο δίκτυο λειτουργεί σαν μέρος του cloud, μαζί με τον υπολογιστικό και αποθηκευτικό χώρο. Επιτρέπει στις CSPs να πετύχουν πιο αποτελεσματική αξιοποίηση των πόρων του δικτύου, να ανταποκριθούν δυναμικά στην αλλαγή των προτύπων κίνησης και την ζήτηση των πελατών, και τέλος τους επιτρέπει την υλοποίηση υπηρεσιών μέσω του αυτοματισμού.

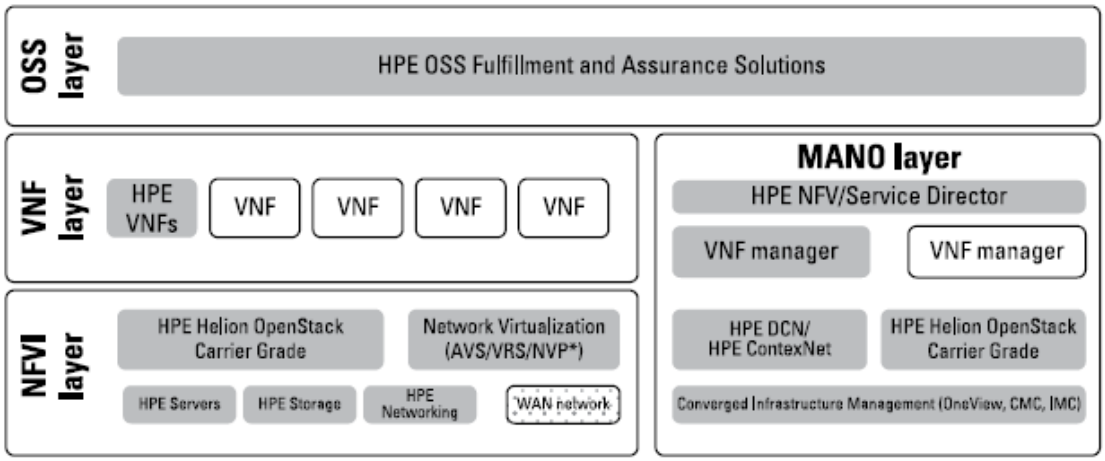
Ανάλυση: Οι παλιές λειτουργίες του δικτύου χωρίζονται σε δομικά μέρη. Οι υπηρεσίες γίνονται μικρό-υπηρεσίες. Οι δικτυακοί πόροι, οι επεξεργαστικοί πόροι και οι αποθηκευτικοί πόροι είναι κατανεμημένοι. Οι CSPs μπορούν να συνθέσουν νέες και βελτιωμένες υπηρεσίες μέσα από τα δομικά μέρη, μέσω της χρήσης serviceaware διεπαφών που παρέχουν συνεχή ενσωμάτωση με τους δικτυακούς, τους επεξεργαστικούς και τους αποθηκευτικούς πόρους.

Η HPE's πήρε την πρωτοβουλία να δημιουργήσει μια ανοιχτή πλατφόρμα και ένα ανοικτό οικοσύστημα που το ονομάζει OpenNFV. Το OpenNFV είναι ένα πρόγραμμα που παρέχει στους CSPs την δυνατότητα να φτιάξουν μια υποδομή η οποία θα μπορεί να προγραμματιστεί και θα έχει αυτοματοποιημένες λειτουργίες. Επίσης παρέχει ένα εύκολο τρόπο για τους CSPs προμηθευτές, τους προμηθευτές εξοπλισμού δικτύου, τους ανεξάρτητους πωλητές λογισμικού και τις εταιρίες ενοποίησης συστημάτων πληροφορικής (system integrators), να δοκιμάσουν και να ενσωματώσουν πολλές από τις λύσεις των προμηθευτών. Επιπλέον, σκοπός του προγράμματος OpenNFV είναι να επιταχύνει το σχεδιασμό, την δοκιμή και την ανάπτυξη των νέων cloud

υπηρεσιών και καινοτομιών, φτιαγμένες πάνω σε αξιόπιστα και υψηλής ποιότητας συστήματα, μειώνοντας έτσι τα έξοδα λειτουργίας και το ρίσκο.

5.1 HPE OpenNFV αρχιτεκτονική

Η μετάβαση σε NFV δίνει την δυνατότητα για ανάλυση του δικτύου και επιτρέπει στους CSPs να επιλέξουν διαφορετικά κομμάτια του συστήματος από διαφορετικούς προμηθευτές για να καλύψουν καλύτερα τις ανάγκες τους. Έτσι επιτρέπουν στις επιχειρήσεις να προσαρμόσουν το σύστημα τους με μεγαλύτερη ευελιξία, μικρότερο χρόνο διάθεσης στην αγορά και καλύτερη διαχείριση του κόστους, δουλεύοντας κάθε κομμάτι χωριστά με ξεχωριστό χρόνο ανάπτυξης για το καθένα. Στην πραγματικότητα όμως όταν χωρίζετε το σύστημα σε ξεχωριστά κομμάτια, προκαλούνται αλλαγές και χρειάζεται να γίνει επαναδιαμόρφωση καταναλώνοντας έτσι χρόνο και χρήμα. Για να δουλέψει ένα τέτοιο σύστημα πρέπει να είναι ανοιχτό και με αρχιτεκτονική που βασίζεται σε πρότυπα. Τα στοιχεία πρέπει να έχουν ανοιχτά interfaces με εύκολα κατανοητή αρχιτεκτονική και σαφή όρια. Η HPE OpenNFV αρχιτεκτονική αναφοράς είναι ένα προσχέδιο για το πώς τα στοιχεία του NFV μπορούν να συνδυαστούν για να δημιουργήσουν ισχυρές λύσεις για το NFV. Χρησιμοποιώντας την ETSI αρχιτεκτονική αναφοράς ως αρχικό σημείο, το OpenNFV περιέχει επεξεργαστές, κρυφή μνήμη, λειτουργικά συστήματα, αποθηκευτικό χώρο, δικτυώσεις, switching, hypervisors, ενδιάμεσο λογισμικό, διαχείριση συστημάτων, οργάνωση, εφαρμογές, και άλλα στοιχεία βελτιστοποιημένα για την επεξεργασία του NFV.



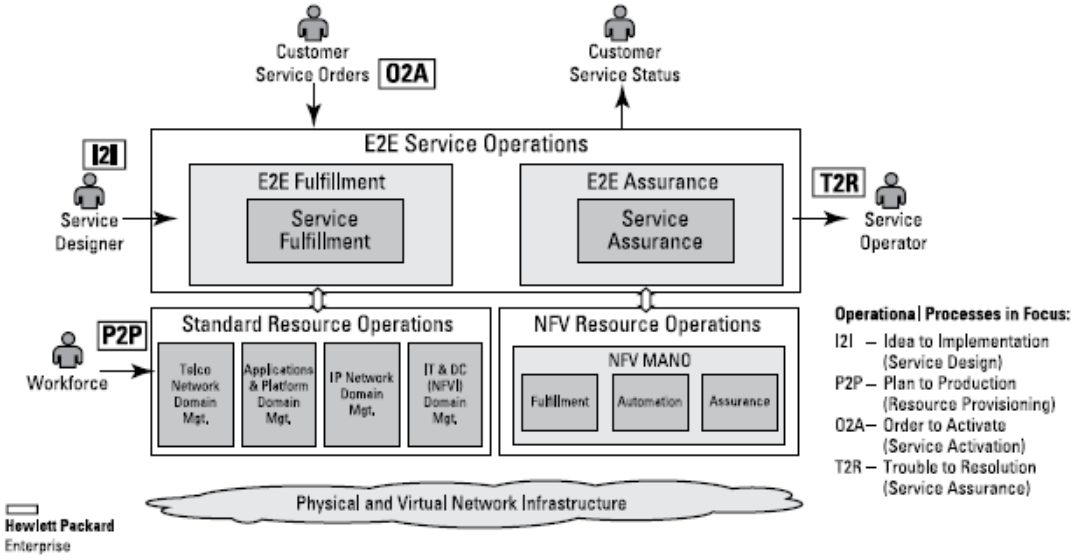
Εικόνα 14: HPE OpenNFV αρχιτεκτονική

Η αρχιτεκτονική αναφοράς είναι κλιμακωτή, και κυμαίνεται από την βάση σχεδιασμού μέχρι τις ακραίες διαμορφώσεις των επιδόσεων, που μπορεί να φιλοξενήσει ακόμα και το μεγαλύτερο σε επίπεδα κίνησης CSP δίκτυο. Η HPE παρέχει δομικά μέρη ή επιλεγμένα υποσυστήματα και στοιχεία, σύμφωνα με τις απαιτήσεις των CSPs. Επιπλέον, επειδή η αρχιτεκτονική αναφοράς είναι ανοικτή, πάντοτε υπάρχει επιλογή για να χρησιμοποιηθούν τα προτεινόμενα εξαρτήματα της

HPE ή εκείνα που προ-επιλέχθηκαν από τον CSP. Ο HPE's MANO, ο οποίος περιέχει το NFV Director και το E2E Service management capability (ικανότητα διαχείρισης) παρέχεται από τον HPE Service Director, και σχεδιάστηκε για να ενσωματώνει τις λειτουργίες του NFV με τις κλασικές λειτουργίες της υποδομής και να μπορεί να συνδέσει το 'παλιό' με το 'καινούργιο'. Αυτό δίνει την ελευθερία στους CSPs να φτιάξουν μια NFV λύση που καλύπτει τις ανάγκες τους χωρίς περιορισμούς.

Ένα νέο όραμα για το OSS

Η HPE προσφέρει μια νέα προσέγγιση στην αρχιτεκτονική του OSS για να επωφεληθεί από τα στοιχεία που προσφέρουν οι λύσεις του NFV MANO. Σκοπός είναι νέα γίνουν νέα κέντρα OSS γύρω από ένα end-to-end επίπεδο διαχείρισης υπηρεσιών, που μπορεί να δημιουργήσει υπηρεσίες σε όλη την NFV υποδομή, όπως λειτουργεί και ένα κλασικό δίκτυο. Για να γίνει αυτό υπάρχουν δυο βασικές ιδέες:



Εικόνα 15: OSS μετασχηματισμός απο την HPE

- Χρήση ενός κοινού μοντέλου πληροφοριών και δεδομένων για την περιγραφή της συμπεριφοράς και των απαιτήσεων, των εικονικών και φυσικών λειτουργιών
- Δυναμική δήλωση μιας υπηρεσίας

Αυτή η προσέγγιση αντικαθιστά την μέχρι τώρα οργάνωση (orchestration) η οποία είναι άσχημα κωδικοποιημένη. Με την νέα προσέγγιση, το OSS μπορεί να χρησιμοποιήσει αυτές τις δυναμικές δηλώσεις για να δημιουργήσει μια λίστα κατά την διάρκεια εκτέλεσης των ενεργειών, σε αντίθεση με τις διαδοχικές ροές εργασίας. Η υπηρεσία ''περιγραφής'' μπορεί να περιγράψει πως μια υπηρεσία πρέπει να συμπεριφερθεί σε μια ασυνήθιστη περίπτωση, όπως ενός σφάλματος κάποιου στοιχείου. Αυτό επιτρέπει την ''αυτό-θεραπεία'' , καθώς το OSS μπορεί να ελέγχει την κατάσταση του δικτύου και να το αναδιαμορφώνει, για να λυθεί το πρόβλημα. Οι κύριες δυνατότητες που προσφέρει η HPE μέσω του end-to-end επιπέδου διαχείρισης της υπηρεσίας είναι:

- *Ευέλικτες υπηρεσίες*: Μια προσέγγιση σχεδιασμού ενός βασικού μοντέλου που μπορεί να δημιουργεί δυναμικές υπηρεσίες και να τις ενημερώνει σε πραγματικό χρόνο. Αυτό παρέχει την δυνατότητα να εφαρμοστεί ένα βιομηχανικό σύστημα για την δημιουργία δυναμικών υπηρεσιών μεταξύ των φυσικών και των εικονικών δικτύων.
- *End-to-end ανάλυση υπηρεσίας*: Παρέχει σε πραγματικό χρόνο μακροπρόθεσμες αναλύσεις για να χρησιμοποιηθούν για τον καθορισμό αλλαγών, που πρέπει να γίνουν για την προσφορά υπηρεσιών σε πραγματικό χρόνο. Επιπλέον, αυτό βοηθά και στην ενοποίηση μεταξύ της διασφάλισης των υπηρεσιών και της ολοκλήρωσης των υπηρεσιών.
- *''Αυτό-θεραπεία''*: Ανίχνευση και διόρθωση σφαλμάτων, μέσω της χρήσης των αναλύσεων, κατά την διάρκεια των λειτουργιών ανάμεσα στην hybrid υποδομή (συνδυασμός εικονικών και φυσικών λειτουργιών του δικτύου).
- *Ευέλικτη ενσωμάτωση*: Η Διεπαφή Προγραμματισμού Εφαρμογών (API) προσφέρει σε πραγματικό χρόνο ενοποίηση με το ευρύτερο OSS οικοσύστημα.

Με την νέα OSS αρχιτεκτονική, οι CSPs έχουν μια κοντινή εικόνα για τις λειτουργίες σε ολόκληρες τις υποδομές τους (φυσικές ή εικονικές). Έτσι, θα επιτρέπετε στις ομάδες λειτουργίας να ανιχνεύουν προληπτικά προβλήματα πελατών και να επιταχύνουν την έρευνα και την επίλυση των περίπλοκων ζητημάτων.

5.2 Πρόγραμμα συνεργατών HPE OpenNFV

Στόχος είναι να δημιουργηθεί μια πλατφόρμα όπου οι CSPs θα μπορούν να επιλέξουν ελεύθερα εφαρμογές από τους προμηθευτές της επιλογής τους. Το πρόγραμμα συνεργατών της HPE OpenNFV χωρίζεται σε τρείς κατηγορίες:

- *Συνεργάτες τεχνολογίας:* Επιλογή εταιριών τεχνολογίας και προμηθευτών, συμπεριλαμβανομένου των προμηθευτών εξοπλισμού δικτύου, τους κατασκευαστές πρότυπου εξοπλισμού και των CSPs που συνεργάζονται για τις καινοτόμες τεχνολογίες, όπου ενσωματώνουν και υποστηρίζουν την HPE OpenNFV υποδομή.
- *Συνεργάτες εφαρμογών και προμηθευτές εξοπλισμού δικτύου:* Ανεξάρτητοι προμηθευτές λογισμικού διεξάγουν τεστ και πιστοποιούν τις εφαρμογές και τις τηλεπικοινωνιακές λειτουργίες τους στην HPE OpenNFV υποδομή.
- *Συνεργάτες υπηρεσιών:* Οι εταιρίες ενοποίησης συστημάτων πληροφορικής (system integrators) χρησιμοποιούν την HPE OpenNFV υποδομή σαν πλατφόρμα για τις προσφορές τους.

Εργαστήρια HPE OpenNFV

Με τον ερχομό του open-source, δηλαδή την ελεύθερη τροποποίηση ενός προϊόντος με σκοπό την βελτίωσή του, του οποίου ο σχεδιασμός είναι προσβάσιμος από όλους, είναι σημαντικό να δοκιμαστούν και μοιραστούν πληροφορίες σχετικά με τις διαφορετικές υλοποιήσεις των προμηθευτών. Για να λειτουργήσει σωστά ένα NFV οικοσύστημα, χρειάζονται εργαστήρια στα οποία πολλοί μαζί προμηθευτές θα μπορούν να δοκιμάζουν τις end-to-end λύσεις τους. Αυτά τα εργαστήρια θα προσομοιάζουν ένα κομμάτι του δικτύου, στο οποίο θα επιτρέπετε να δοκιμαστούν πράγματα πριν την παραγωγή τους. Επιπλέον, προσφέρουν μια υπηρεσία ανάπτυξης περιβάλλοντος όπου μπορεί να δοκιμαστεί η ενσωμάτωση μεταξύ των προϊόντων των προμηθευτών. Σκοπός των εργαστηρίων αυτών είναι να προσφέρουν λύσεις από διαφορετικούς προμηθευτές, οι οποίες θα είναι δοκιμασμένες και ολοκληρωμένες , εξοικονομώντας έτσι χρόνο.

6. NFV και SDN (Software-Define Networking)

Η NFV και το SDN είναι δύο τεχνολογίες οι οποίες επωφελούνται η μία από την άλλη. Το SDN εικονοποιεί τους πόρους του δικτύου για χρήση, με παρόμοιο τρόπο εικονοποίησης των αποθηκευτικών και των επεξεργαστικών πόρων με αυτόν του NFV. Μέσω της χρήσης του κοινού επιπέδου ελέγχου, το SDN μπορεί να αφαιρέσει πολύπλοκες τοπολογίες των υποδομών του δικτύου, παρέχοντας έτσι υψηλό αυτοματισμό και προγραμματισμό. Για να αναγνωρίσουμε πώς οι πόροι του SDN (SDN-enable hardware, SDN controllers, SDN applications) ταιριάζουν με την αρχιτεκτονική (ETSI) χρειάζεται πολύ δουλεία. Σε ένα CSP δίκτυο, το SDN είναι το κλειδί για την λειτουργία της NFV. Παρακάτω μερικά παραδείγματα για τον συμπληρωματικό ρόλο του SDN και της NFV:

- Για να εξασφαλίσουμε ότι η χωρητικότητα της λειτουργίας VNF έχει βελτιστοποιηθεί, είναι απαραίτητο μόνο οι κατάλληλες ροές κίνησης να κατευθύνονται προς την κατάλληλη λειτουργία VNF. Μια από τις δυνατότητες του SDN και συγκεκριμένα το Service Function Chaining(η ικανότητα να ορίζει μια λίστα μιας υπηρεσίας του δικτύου για ένα σύνολο πακέτων) είναι απαραίτητη για έναν δυναμικό έλεγχο των πακέτων κίνησης στη σωστή λειτουργία VNF.

- Ένα από τα χαρακτηρίστηκα της NFV είναι να δημιουργεί τις λειτουργίες VNF κοντά στα κέντρα δεδομένων που θα χρησιμοποιούνται. Το SDN είναι απαραίτητο για να εξασφαλίζει ότι οι παράμετροι των συνδέσεων του δικτύου και του Συμφωνητικού Παροχής Υπηρεσιών (SLAs), είναι ασφαλείς.

- Το SDN παίζει επίσης, κύριο ρόλο στην οργάνωση ενός hybrid δικτύου (εικονικό δίκτυο-φυσικό δίκτυο). Η οργάνωση των υπηρεσιών είναι μέρος του δικτύου που διαχειρίζεται την δημιουργία και την παράδοση των υπηρεσιών. Το SDN

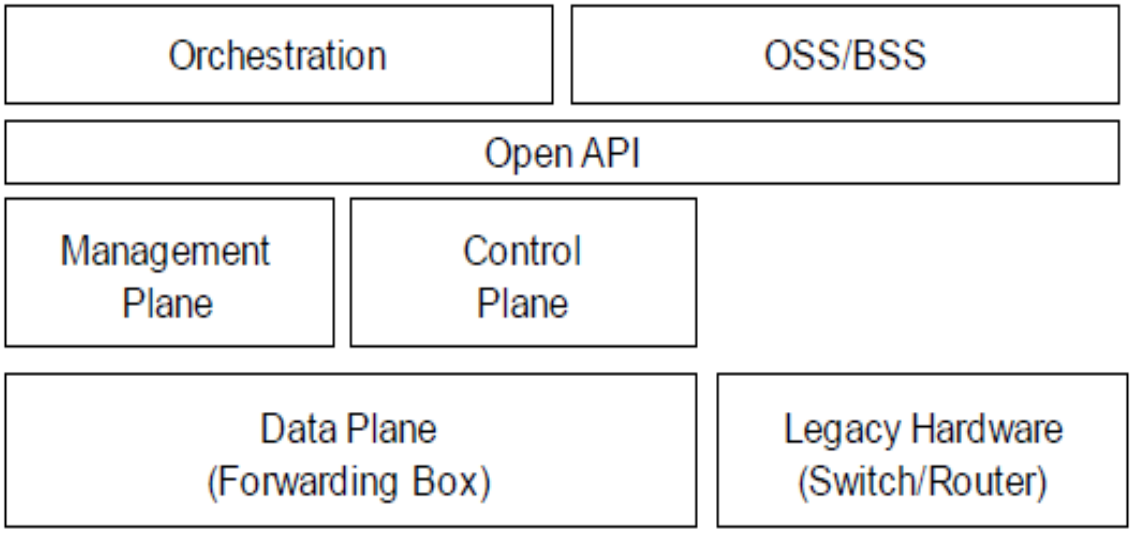
παρέχει ένα ενιαίο σημείο διαμόρφωσης και διαχείρισης για τα υποκείμενα ετερογενή στοιχεία του δικτύου.

6.1 Πλάνο της Verizon για SDN-NFV δίκτυα

- Διαχωρισμός του control plane και του data plane
- Εικονοποίηση των λειτουργιών του δικτύου
- Προγραμματιστικός έλεγχος του δικτύου
- Προγραμματιστικός έλεγχος των υπολογιστικών πόρων χρησιμοποιώντας ενορχήστρωση/οργάνωση (orchestration)
- Διαμόρφωση πρότυπων πρωτοκόλλων
- Ένας μηχανισμός για την διαχείριση και την κατανομή των hardware πόρων
- Αυτοματοποιημένος έλεγχος, ανάπτυξη και επιχειρηματικές διαδικασίες
- Αυτοματοποιημένη οργάνωση των πόρων για να ανταποκριθούν στις ανάγκες της εφαρμογής/λειτουργίας

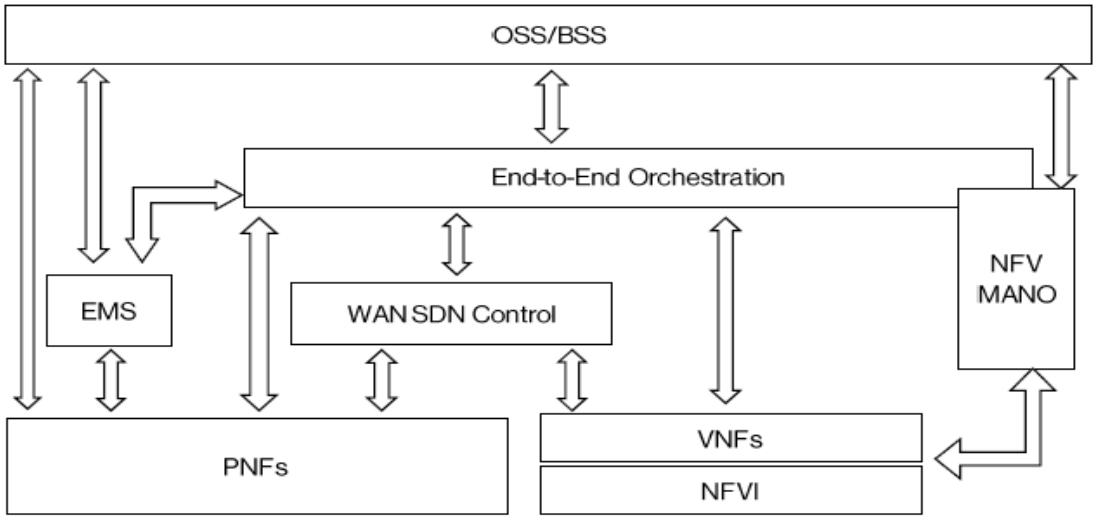
6.2 Software Defined Networking (SDN)

Συνήθως, η διεπαφή(interface) μεταξύ του control plane και του data plane είναι κλειστή και βρίσκεται στο εσωτερικό των router και των switch με αποτέλεσμα να μην μπορεί κάποιος να αλλάξει εύκολα τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται σε ένα δίκτυο. Η βασική ιδέα της αρχιτεκτονικής SDN είναι η αποσύνδεση του control plane από το data plane και η δημιουργία μιας ανοιχτής διεπαφής μεταξύ τους. Το control plane τρέχει εξωτερικά από τους δρομολογητές πάνω από ένα λειτουργικό σύστημα, το οποίο διαχειρίζεται τους πίνακες προώθησης των routers και των switches ενός δικτύου. Με αυτή την προσέγγιση γίνεται πολύ πιο εύκολο να εφαρμόσει κανείς καινοτόμες τεχνικές δρομολόγησης και διαχείρισης της κίνησης μιας και ένα νέο πρωτόκολλο δρομολόγησης μπορεί να εφαρμοστεί πολύ γρήγορα, απλά με τη χρήση νέου λογισμικού, πάνω από το λειτουργικό σύστημα, χωρίς να χρειάζονται αλλαγές στους routers και τους switches. Οι SDN Controllers εκθέτουν αφηρημένη τοπολογία και δεδομένα στα γειτονικά συστήματα, απλοποιώντας την οργάνωση των end-to-end υπηρεσιών και οδηγούν στην εισαγωγή καινοτόμων εφαρμογών που βασίζονται στον προγραμματισμό του δικτύου.



Εικόνα 16: Διαχωρισμός του Control και Data plane

6.2.1 End-to-end Orchestration



Εικόνα 17: Αρχιτεκτονική διαχείρισης και ελέγχου υψηλού επιπέδου

NFV MANO: Διαχειρίζεται την NFVI και είναι υπεύθυνο για τον κύκλο ζωής των λειτουργιών VNF. Βασικές λειτουργίες είναι:

- Κατανομή και απαλλαγή των NFVI πόρων (επεξεργαστής, αποθηκευτικός χώρος, συνδεσιμότητα δικτύου, μνήμη)
- Διαχείριση του δικτύου μεταξύ των εικονικών μηχανών και των λειτουργιών VNF (Data Center SDN Control)
- Συγκεκριμενοποίηση, κλιμάκωση, θεραπεία, ενημέρωση και διαγραφή των λειτουργιών VNF
- Παρακολούθηση των κινδύνων και των επιδόσεων που σχετίζονται με το NFVI

WAN SDN Control: Εκπροσωπεί ένα ή περισσότερα SDN Controllers που διαχειρίζονται την συνδεσιμότητα των υπηρεσιών μεταξύ των domains των προμηθευτών και των πολλαπλών τεχνολογιών. Μπορεί να διαχειριστεί την συνδεσιμότητα μεταξύ των παλαιότερων και νεώτερων φυσικών δικτύων, αλλά μπορεί και να διαχειριστεί της εικονικές λειτουργίες, όπως είναι οι εικονικοί Provider Edge routers (vPE)

End-to-end Orchestration (EEO): Υπεύθυνο για την κατανομή, την εμφάνιση και την ενεργοποίηση των λειτουργιών του δικτύου που χρειάζονται για μια end-to-end υπηρεσία. Οι διεπαφές (interfaces) του είναι:

- Με το NFV MANO, για αίτημα δημιουργίας λειτουργιών VNF
- Με το WAN SDN, για αίτημα συνδεσιμότητας μέσω του WAN
- Με τις φυσικές λειτουργίες του δικτύου (PNFs) και τις εικονικές λειτουργίες του δικτύου (VNFs), για την παροχή και την ενεργοποίηση μιας υπηρεσίας

Η EEO και ο NFV MANO αλληλεπικαλύπτονται. Από τον ορισμό του ETSI NFV για το MANO υπάρχει μια λειτουργία που ονομάζεται Network Service Orchestration(NSO) η οποία είναι υπεύθυνη για το υποσύνολο των λειτουργιών, που απαιτούνται για την end-to-end οργάνωση όπως γίνεται από την EEO.

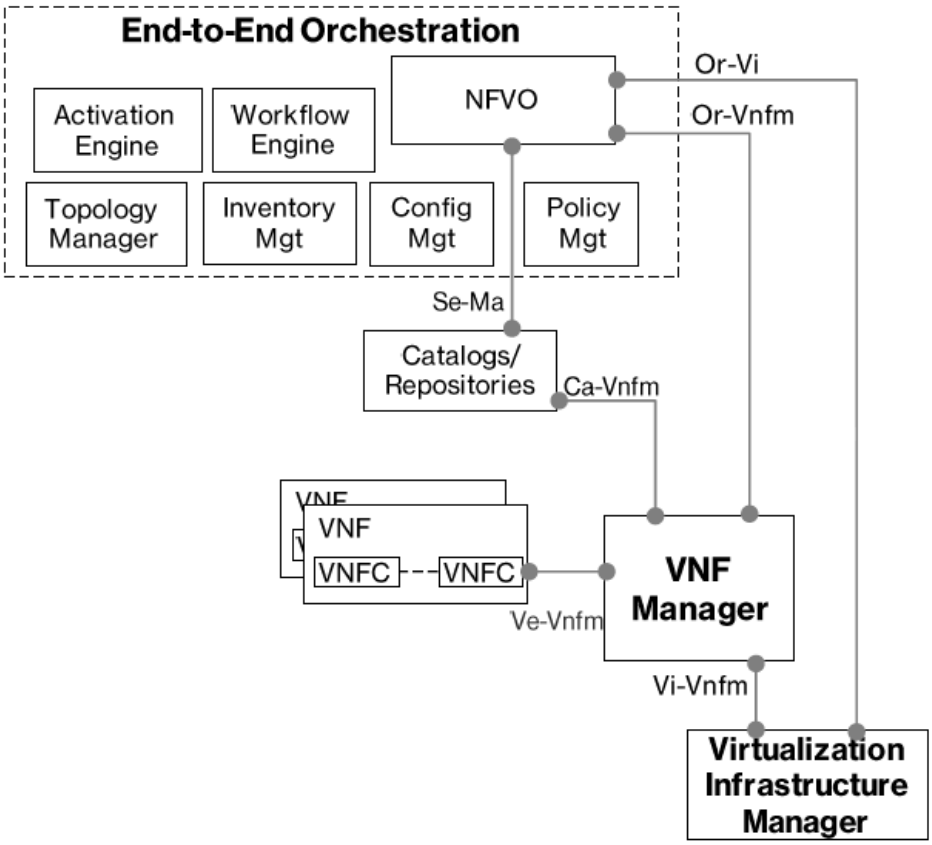
Υπάρχει μια βασική διαφορά του NFV MANO και του WAN SDN Control. Ο NFV MANO γνωρίζει εάν κάποια λειτουργία του δικτύου είναι εικονική χωρίς να γνωρίζει τι κάνει. Από την άλλη ο WAN SDN Control γνωρίζει τι κάνουν οι λειτουργίες του δικτύου χωρίς να γνωρίζει εάν αυτή είναι εικονοποιημένη.

Συνεργασία με παλιά συστήματα

Στα δίκτυα, οι υπηρεσίες διαχειρίζονται μέσω του OSS και του BSS συστήματος που ενδέχεται να υπάρχει διεπαφή (interface) με το Element Management Systems (EMS) για την διαμόρφωση των στοιχείων του δικτύου. Εξαιτίας της τυποποίησης των πρωτοκόλλων ελέγχου και των μοντέλων δεδομένων, ο EMS σταδιακά θα αντικατασταθεί, από νέα συστήματα που θα λειτουργούν σε όλους τους προμηθευτές και τα domain, όπως είναι οι SDN Controllers και συστήματα διαχείρισης των λειτουργιών VNF.

6.2.2 VNF Descriptors

Στις υπάρχουσες φυσικές λειτουργίες των δικτύων, τα εσωτερικά μέρη του λογισμικού της λειτουργίας PNF,είναι κρυμμένα από τον χειριστή και διαχειρίζονται από τον προμηθευτή του εξοπλισμού. Στην NFVI τα μέρη της επικοινωνίας είναι εκτεθειμένα και υποστηρίζονται από την NFVI, επομένως τα εικονικά links της λειτουργίας VNF πρέπει να οριστούν σαν μέρος του VNF Descriptor για να εξασφαλιστεί η σωστή λειτουργία των λειτουργιών VNF. Ο VNF Descriptor(VNFD) είναι ένα πρότυπο ανάπτυξης το οποίο περιγράφει μια λειτουργία VNF από την άποψη της ανάπτυξης και των απαιτήσεων της λειτουργικής συμπεριφοράς. Επίσης, ο VNFD περιέχει συνδεσιμότητα , διαπαφές (interfaces), και KPIs απαιτήσεις, που μπορούν να χρησιμοποιηθούν από τα λειτουργικά μέρη του NFV MANO για να καθιερώσει κατάλληλα Virtual Links μέσα στην NFVI ανάμεσα σε VNFC περιπτώσεις, ή ανάμεσα σε VNF περιπτώσεις και την endpoint διεπαφή σε άλλες εικονικές λειτουργίες. Τα VNFDs χρησιμοποιούνται από τον VNFM για να εκτελέσει τις λειτουργίες διαχείρισης του κύκλου ζωής στους VIM και τις λειτουργίες VNF, με τις Vi-Vnfm και Ve-Vnfm διεπαφές που φαίνονται και στο παρακάτω σχήμα.



Εικόνα 18: Ve-Vnfm και Vi-Vnfm διεπαφές

Εκτός από τους τύπους δεδομένων, τα αρχεία του descriptor είναι σημαντικά για μια end-to-end αρχιτεκτονική. Οι τύποι δεδομένων, περιγράφουν πώς να διαχειριστείς μια λειτουργία ή υπηρεσία, από την άποψη τροφοδοσίας και παρακολούθησης. Τα αρχεία

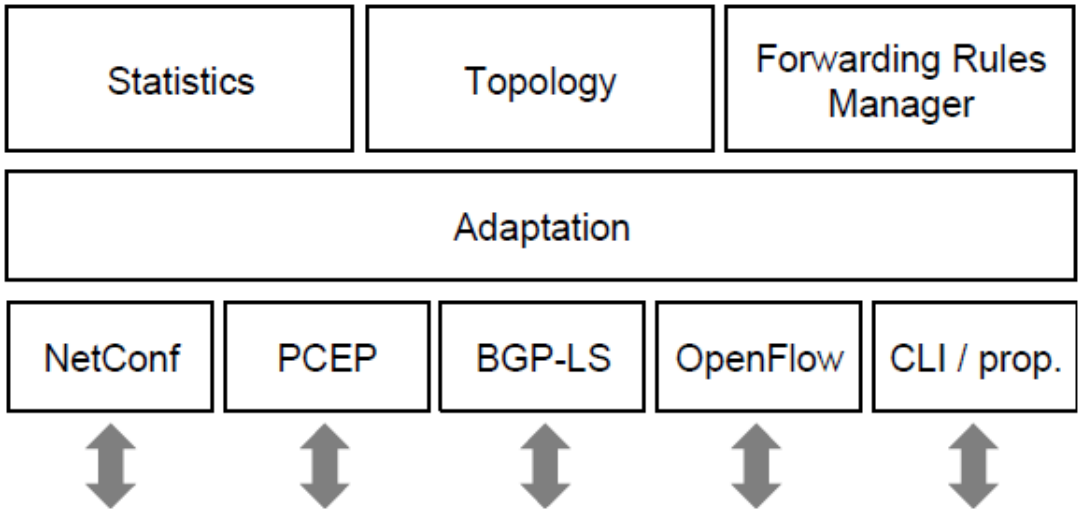
του descriptor περιγράφουν πώς να φτιάξεις, να κλιμακώσεις, να θεραπεύσεις, και να αναβαθμίσεις μια VNF ή/και μια υπηρεσία δικτύου (Network Service). Τα descriptor αρχεία δημιουργούνται από τον ‘’αρχιτέκτων’’ της υπηρεσίας του δικτύου ή αλλιώς τον σχεδιαστή της VNF. Τέλος, τα descriptor αρχεία κρατάνε μόνο την πληροφορία που απαιτείται σε κάθε επίπεδο της διαδικασίας οργάνωσης. Ο VNFM χρησιμοποιεί τον VNFD για να εκτελέσει τις λειτουργίες διαχείρισης του κύκλου ζωής (αναβάθμιση, κλιμάκωση, θεραπεία, τερματισμός) χρησιμοποιώντας το πρότυπο VNFD.

6.2.3 WAN SDN Controller

Οι Data Center SDN λύσεις είναι καλά ορισμένες, με καλά οριοθετημένες λύσεις που ικανοποιούν την επεκτασιμότητα (scalability). Οι WAN SDN λύσεις αναδύονται σαν τις επόμενες κύριες εφαρμογές του SDN και έχει ανακοινωθεί ένας μεγάλος αριθμός αναπτύξεων. Ένας WAN SDN Controller πρέπει να επιτύχει τους ακόλουθους στόχους:

- Βόρεια διεπαφή προγραμματισμού εφαρμογών (Northbound API): Επιτρέπει στις εφαρμογές και τα συστήματα οργάνωσης να προγραμματίσουν το δίκτυο και να αιτηθούν υπηρεσίες από αυτό. Επίσης η διεπαφή προσφέρει ‘’αφαίρεση’’ (abstraction) στο δίκτυο. Με τον όρο αφαίρεση (abstraction) εννοούμε την απόκρυψη κάποιον λεπτομερειών προκειμένου να μειωθεί η πολυπλοκότητα και να αυξηθεί η αποδοτικότητα.
- Μοντέλο με γνώμονα το στρώμα προσαρμογής (Adaptation Layer) που επιτρέπει στις υπηρεσίες του δικτύου να βοηθούν την κίνηση προς τον βορρά* και τον νότο*.
- Έλεγχος πολλαπλών στρωμάτων και πολλαπλών προμηθευτών
- Αυτοματοποιημένη διαχείριση των end-to-end υπηρεσιών
- Βελτιστοποίηση των πόρων
- Εύρεση και διόρθωση των τοπολογιών
- Συλλογή και επεξεργασία των στατιστικών
- Παροχή μιας διεπαφής ελέγχου για κλασικούς/hybrid μηχανισμούς ελέγχου

*(Σαν η «προς βορρά» διεπαφή ορίζεται η επικοινωνία των εφαρμογών με τον controller και σαν η «προς νότο» διεπαφή ορίζεται η επικοινωνία μεταξύ του controller και των συσκευών .)



Εικόνα 19: Λειτουργίες του WAN SDN Controller

6.3 Αξιοπιστία

Με την εικονοποίηση, το hardware και το software ανήκουν σε διαφορετικούς προμηθευτές και διάφορα στοιχεία των λειτουργιών VNF ‘’κατοικούν’’ σε διαφορετικούς servers, συνδεδεμένα μέσω του δικτύου από switches, από έναν ακόμη διαφορετικό προμηθευτή.

Εφεδρικό Σενάριο

Παράδειγμα ενός fail-over σεναρίου. Ένα VNFC που παρέχει την λειτουργικότητα του ελέγχου δεδομένων (data plane), θα υλοποιηθεί με 1+1 διαμόρφωση. Αυτό σημαίνει ότι κατά την υλοποίηση της λειτουργίας VNF, δύο αντίγραφα του VNFC δημιουργούνται, όπου το ένα είναι ενεργό και το άλλο σε αναμονή. Και τα δύο VNFCs μπορούν να έχουν πρόσβαση σε μια κοινή βάση δεδομένων όπου η πληροφορίες είναι αποθηκευμένες, ή το ενεργοποιημένο VNFC μπορεί να ενημερώνει το VNFC που είναι σε αναμονή όποτε αλλάζει κάτι. Σε κάθε περίπτωση και σε οποιοδήποτε χρόνο το VNFC που είναι σε αναμονή μπορεί να συνεχίσει, αν το ενεργοποιημένο σταματήσει να λειτουργεί. Για να υπάρχει έλεγχος τυχόν σφαλμάτων τα VNFCs στέλνουν ένα παλμό κάθε 10ms. Όταν το VNFC σε αναμονή δεν λάβει τρείς παλμούς, τότε αυτομάτως μπαίνει σε λειτουργία, με την όλη διαδικασία να διαρκεί 50ms. Σε αυτό το σημείο το VNFC είναι εκτεθειμένο, αφού δεν υπάρχει πλέον κάποιο άλλο σε αναμονή. Η αντικατάσταση γίνεται από τον VNFM, ο οποίος λαμβάνει σφάλματα από το VNFC που σταμάτησε να λειτουργεί, αλλά και από το πλέον ενεργοποιημένο VNFC. Επιπλέον, λαμβάνει σφάλματα και από τον VIM που εντόπισε και αυτός το σφάλμα, καθώς και από άλλα στοιχεία που εντόπισαν το σφάλμα. Έτσι, ο VNFM συνεργάζεται με τον VIM και δημιουργούν ένα νέο VNFC.

Παράγοντες που επηρεάζουν την αξιοπιστία

- Αποτυχίες του server και του hypervisor
- Αποτυχίες του δικτύου
- Αξιοπιστία της λειτουργίας VNF (software bugs)
- Συστήματα διαχείρισης και έλεγχου`
- Ο χρόνος αντικατάστασης του VNFC
- Καθυστέρηση ανάμεσα στα VNFCs
- Αποτυχία των domains

Δομημένη διαδικασία

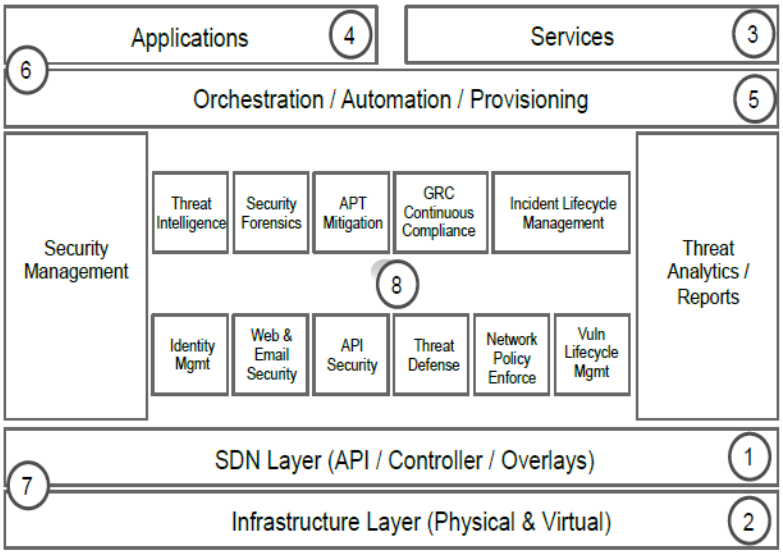
Τα παρακάτω βήματα θα μπορούσαν να βοηθήσουν ένα διαχειριστή να δομήσει μια διαδικασία για την καλύτερη αξιοπιστία της NFV:

1. Προσδιορισμός της ευρωστίας της υποδομής
    - Αναμενόμενα ποσοστά αποτυχίας των server και του hypervisor
    - Αναμενόμενα ποσοστά αποτυχίας των συνδέσεων του δικτύου
    - Αναμενόμενη καθυστέρηση ενός πλήρως ‘γεμισμένου’ δικτύου
    - Υπάρχουν συνδέσεις που μπορούν να ρίξουν περισσότερους από έναν server κάθε φορά;
2. Πρόσβαση και τεστ της αξιοπιστίας των σημαντικότερων συστημάτων ελέγχου
    - Αναμενόμενη διαθεσιμότητα των VNFM, VIM, SDN Controllers
3. Βασισμένοι στα ποσοστά αποτυχίας και την διαθεσιμότητα στα συστήματα ελέγχου, οι προμηθευτές μπορούν να εκτιμήσουν την θεωρητική διαθεσιμότητα των λύσεών τους.
4. Τεστ:
    - Εκτέλεση μιας λειτουργίας VNF σε πραγματική υποδομή. Εισαγωγή σφαλμάτων για να διαπιστωθεί αν όλες οι εφεδρικές διαδικασίες λειτουργούν σωστά
    - Εκτέλεση του δικτύου για αρκετό χρονικό διάστημα για να διαπιστωθεί αν τα υποτιθέμενα ποσοστά διαθεσιμότητας αντέχουν

7. SDN Security

Οι εφαρμογές γράφτηκαν για να είναι ανθεκτικές σε θέματα ασφαλείας όπως είναι η σωστή απόρριψη των πακέτων όταν βρεθεί μια DDOS επίθεση. Το σχήμα παρακάτω περιγράφει τα επίπεδα ασφαλείας που χρησιμοποιούνται για το κάθε στρώμα της αρχιτεκτονικής.

1. Securing Controller
2. Securing Infrastructure
3. Securing Network Services
4. Securing Application
5. Securing Management & Orchestration
6. Securing API
7. Securing Communication
8. Security Technologies



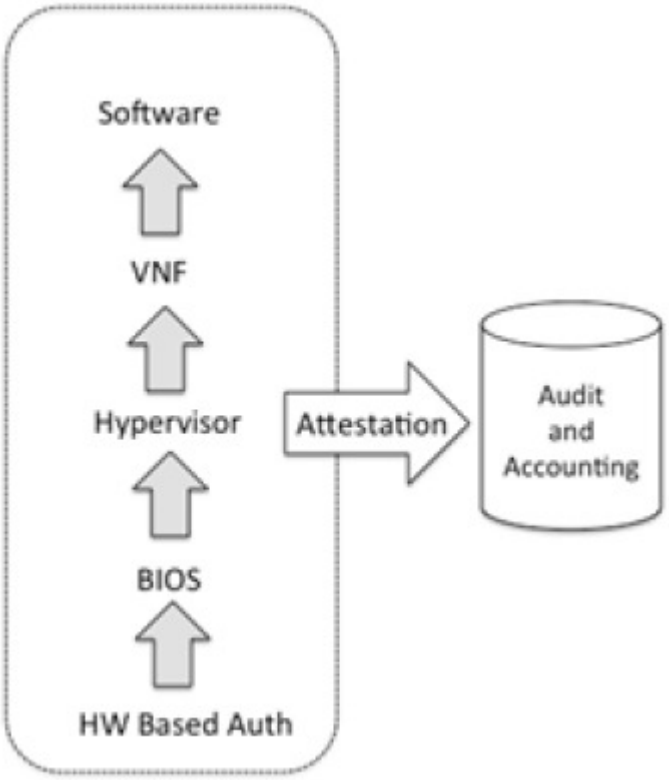
Εικόνα 20: Πολλαπλά στρώματα ασφαλείας για την προστασία του SDN

Στο παραπάνω σχήμα, φαίνεται η διαδικασία ασφάλισης των αιτημάτων της εφαρμογής στο δίκτυο, και η επεξεργασία του προγραμματισμού (κώδικα) του δικτύου για να παραδοθεί ένα αποτέλεσμα. Υπάρχουν 8 επίπεδα απειλών που σχετίζονται με την ασφάλεια παροχής μιας υπηρεσίας σε ένα δίκτυο.

7.1 Domain Security

Η επιφάνεια της επίθεσης για ένα εικονικό στοιχείο SDN υποδομής είναι διαφορετική από ένα ειδικό στοιχείο του δικτύου. Ο φόρτος εργασίας δεν είναι πλέον δεμένος σε έναν συγκεκριμένο server αλλά έχει την δυνατότητα να τρέχει σε οποιοδήποτε server.

Οι Hardware-based Root-of-Trust υπηρεσίες μπορούν να χρησιμοποιηθούν για να εξασφαλίσουν την ακεραιότητα ενός υπολογιστικού server (compute server), μετρώντας και επικυρώνοντας υλικολογισμικά (firmware) και λογισμικά μέρη (software) πριν την εκτέλεση τους. Μόνο τα επικυρωμένα μέρη μπορούν να εκτελεστούν. Κάθε προσπάθεια για εισαγωγή μη-εξουσιοδοτημένης αλλαγής δια μέσου φυσικής (ή μακρινής) πρόσβασης μπορεί να έχει σαν αποτέλεσμα έναν συναγερμό, και όλες οι προσπάθειες για μη-εξουσιοδοτημένα υλικολογισμικά (firmware) και λογισμικά (software) θα αποτύχουν.



Εικόνα 21: "Αλυσίδα εμπιστοσύνης"

Server UEFI BIOS

Σε server επίπεδο, υπάρχει ένας αριθμός από UEFI BIOS ρυθμίσεις οι οποίες πρέπει να διαμορφωθούν για να βοηθήσουν την ασφάλεια ενάντιας μη-εξουσιοδοτημένων αλλαγών ή ενημερώσεων. Οι BIOS ρυθμίσεις και ικανότητες κατασκευάζονται ειδικά, έτσι ώστε όπου είναι διαθέσιμες οι ακόλουθες ρυθμίσεις θα πρέπει να διαμορφωθούν:

- Κωδικός Επόπτη (Supervisor)- Περιορίζει την μη-εξουσιοδοτημένη πρόσβαση στις ρυθμίσεις όπως ημερομηνία και ώρα, σειρά εκκίνησης και προτεραιότητας, και ρυθμίσεις δικτύου.
- Κλείδωμα BIOS ρυθμίσεων- Αποτρέπει αλλαγές στις ρυθμίσεις BIOS χωρίς το κωδικό του Supervisor.
- Κλείδωμα BIOS ενημερώσεων- Αποτρέπει τις BIOS αναβαθμίσεις / υποβαθμίσεις, και την πιθανή επαναφορά του BIOS στις εργοστασιακές ρυθμίσεις .
- Απενεργοποίηση κάθε αχρησιμοποίητης θύρας και συσκευής- Οποιεσδήποτε NICs, USB θύρες, WIFI,Bluetooth, κτλ.
- Κλείδωμα της σειράς εκκίνησης- Αποτροπή εκκίνησης από μη-εξουσιοδοτημένες πηγές.
- Απενεργοποίηση της λίστας συσκευών εκκίνησης- Για την αποτροπή επιλογής, συσκευής εκκίνησης από την κονσόλα.

- Επαλήθευση όλων των BIOS υλικολογισμικών (firmware) στοιχείων κατά την εκκίνηση- Χρήση του UEFI Secure Boot για επιβεβαίωση υπογραφών όλων των UEFI BIOS firmware στοιχείων πριν φορτωθούν.

Επικοινωνία του δικτύου

Η ασφάλεια της κίνησης του δικτύου είναι πολύ σημαντική. Η επικοινωνία μεταξύ των υπηρεσιών του OpenStack στους κόμβους διαχειριστή (Keystone, Glance, Cinder), καθώς και η πρόσβαση στη βάση δεδομένων του δικτύου, η σειρά μηνυμάτων, και η κίνηση μεταξύ των ‘’ενοικιαζόμενων’’ δικτύων στα ιδιωτικά δίκτυα, είναι μερικά από τα σημαντικά μέρη της ασφάλειας της κίνησης του δικτύου. Οι τύποι της κίνησης που πρέπει να προστατευτούν είναι:

1. Μηνύματα: Μερικές υπηρεσίες του OpenStack επικοινωνούν μεταξύ τους χρησιμοποιώντας έναν μεσίτη (broker) μηνυμάτων και ουρά. Η επικοινωνία με τον μεσίτη θα πρέπει να είναι ασφαλής χρησιμοποιώντας TLS (Transport Layer Security) για την αποτροπή υποκλοπών ή πλαστοπροσωπίας στο δίκτυο.
2. Βάση δεδομένων: Οι υπηρεσίες του OpenStack χρησιμοποιούν υποκείμενες βάσεις δεδομένων για συνεχή αποθήκευση δεδομένων και metadata. Αυτές οι επικοινωνίες πρέπει να ρυθμιστούν ώστε να χρησιμοποιούν την TLS και client X.509 πιστοποιητικά για την αποτροπή υποκλοπών ή χακάρισμα του κωδικού ή/και πλαστοπροσωπίας.
3. Libvirt: Πρόσβαση σε ολόκληρο το δίκτυο μέσω αυτής της λειτουργίας που χρειάζεται κατά την διάρκεια των live διαδικασιών μετάβασης. Αν είναι ενεργοποιημένη, αυτή η επικοινωνία πρέπει επίσης να ρυθμιστεί ώστε να μπορεί να χρησιμοποιήσει το TLS ή/και το Kerberos ή τα client X.509 πιστοποιητικά.
4. Τελικά σημεία API: Κάποιες υπηρεσίες του OpenStack επικοινωνούν μεταξύ τους χρησιμοποιώντας εσωτερικά HTTP τελικά σημεία. Όλα τα OpenStack API τελικά σημεία πρέπει να ρυθμιστούν για να χρησιμοποιούν το TLS για την προστασία των δεδομένων τους.
5. Χρήστες (tenants) και projects: Η εσωτερική κίνηση των χρηστών είναι συνήθως απομονωμένη μέσω ενός τούνελ ενθυλάκωσης (VxLAN,VLAN,GRE). Τα Security Groups πρέπει να χρησιμοποιούνται για να περιορίζουν την πρόσβαση στο δίκτυο μέσα ή έξω από την ενοικιαζόμενη λειτουργία VNF σε συγκεκριμένες θύρες ή σε άλλες λειτουργίες VNF στο ίδιο project.
6. Κόμβος δια-υπολογιστή και δια-VNF προστασία κίνησης: Σε ορισμένα σενάρια ανάπτυξης, μπορεί να απαιτείται να παραχθεί εμπιστευτικότητα και ακέραιη προστασία σε όλη την κίνηση ανάμεσα στους υπολογιστικούς κόμβους, και σε κάποια σενάρια προστασίας όλης της κίνησης ανάμεσα στις λειτουργίες VNF. Υπάρχει συνεχής προσπάθεια από το OpenStack και την

ETSI NFV να επεκτείνει το VPNaaS για την αντιμετώπιση τέτοιων περιπτώσεων χρήσης.

7.2 Παρακολούθηση και διαχείριση ασφάλειας δικτύου

Μερικά από τα μέτρα ασφάλειας που μπορούν να εφαρμοστούν στο δίκτυο είναι η ζωντανή παρακολούθηση της ασφάλειας του δικτύου, η ανάλυση της συμπεριφοράς του δικτύου σε πραγματικό χρόνο, η εισχώρηση, η ανίχνευση και η προστασία του δικτύου και τα εξωτερικά firewalls. Η παρακολούθηση της ασφάλειας του δικτύου, επιτρέπει στον προμηθευτή και/ή στον χρήστη να παρακολουθεί ζωντανά την κίνηση ανάμεσα στις λειτουργίες VNF, καθώς και την διαχείριση, τον χειρισμό και τον έλεγχο δεδομένων ώστε να αποκτήσει ορατότητα μέσα στα δυναμικά εικονικά δίκτυα.

Η παρακολούθηση της ασφάλειας μπορεί να απαιτήσει ασφαλή παράδοση της πολιτικής παρακολούθησης μέσω ενός Πράκτορα Παρακολούθησης της Ασφάλειας (Security Monitoring Agent) [τρέχει σαν μέρος ενός VM ή Container] στην πλατφόρμα, και εκθέτοντας με ασφάλεια την κυκλοφορία ανά πολιτική σε κατάλληλες μηχανές ανάλυσης της κίνησης του δικτύου. Το Sflow, το Netflow/IPFIX και άλλες μορφές πακέτων μπορούν να χρησιμοποιηθούν μαζί με την παρακολούθηση μετα-δεδομένων (metadata) σε συγκεκριμένες μηχανές ανάλυσης.

Η διαχείριση της ασφάλειας περιλαμβάνει τη διαχείριση του κύκλου ζωής της ασφάλειας, η οποία περιλαμβάνει τον σχεδιασμό και την εφαρμογή της ασφάλειας. Αυτό εξασφαλίζει ότι οι πολιτικές ασφαλείας έχουν σχεδιαστεί με συνέπεια και ότι παρέχονται στις εικονικές, και τις φυσικές λειτουργίες ασφαλείας.

7.2.1 Ασφάλεια δεδομένων

Ένας αριθμός από νότια APIs και πρωτόκολλων χρησιμοποιούνται από τον ελεγκτή για την επικοινωνία στο δίκτυο, όπως είναι το Openflow (OF), το Open vSwitch το Database Management Protocol (OVSDB), το Cisco onePK κ.α. Κάθε ένα από αυτά εφαρμόζει τον δικό του τρόπο ασφάλειας για την επικοινωνία, αλλά λόγω του ότι είναι καινούργια μπορεί να μην έχουν αναπτυχθεί με την πλήρη απαραίτητη ασφάλεια. Η ικανότητα χρήσης των APIs για την δημιουργία φιλικότερης διαχείρισης των διεπαφών προς τον χρήστη αυξάνουν την επιφάνεια επίθεσης στις υποδομές του δικτύου σημαντικά, γιατί η ασφάλεια δεν περιορίζεται πλέον στο δικτυακό εξοπλισμό του προμηθευτή.

Τα συστήματα SDN συνήθως χρησιμοποιούν γενικού σκοπού (x86) συστήματα και TLS για να ασφαλίσουν το επίπεδο ελέγχου(control plane), αλλά οι περίοδοι με

μεγάλη διάρκεια ζωής μπορούν να κάνουν τον έλεγχο των δεδομένων ευάλωτο στις επιθέσεις. Το πρωτόκολλο ελέγχου κίνησης πρέπει να διαχωρίζετε από τις κύριες ροές δεδομένων, είτε μέσω των μέτρων ασφαλείας του δικτύου είτε εκτός ζώνης του δικτύου. Οι οργανισμοί θα πρέπει να έχουν σαν παράγοντα την διαθεσιμότητα επιλογών ασφαλείας όταν επιλέγουν ελεγκτές. Η χρήση του TLS για την πιστοποίηση των ελεγκτών και των τελικών σημείων θα βοηθήσει στην αποτροπή υποκλοπών και πλαστογραφιών στην επικοινωνία των νότιων συνδέσεων.

7.2.2 Ασφάλεια ελεγκτή

Ο SDN ελεγκτής (controller) είναι επίσης στόχος των χάκερ. Η ισχυρή κεντρική οργάνωση που παρέχεται από τον SDN ελεγκτή, επίσης αντιπροσωπεύει ένα ενιαίο σημείο αποτυχίας που είναι υψηλός στόχος των χάκερ. Τα στοιχεία του δικτύου είναι ανοικτά σε εντολές από τον ελεγκτή και αυτός μπορεί να είναι ένας τρόπος επίθεσης. Δηλαδή, οι επιτιθέμενοι μπορούν να προσπαθήσουν να πάρουν τον έλεγχο του δικτύου απλά προσποιούμενοι ότι είναι ο SDN ελεγκτής ή ‘’σπάζοντας’’ τον ίδιο τον ελεγκτή. Υπάρχουν επίσης νέοι τύποι DDoS επιθέσεων που προσπαθούν να εκμεταλλευτούν πιθανά όρια κλιμάκωσης μιας SDN υποδομής, βρίσκοντας την αυτοματοποιημένη διαδικασία που λαμβάνει μεγάλα ποσοστά από τους κύκλους της CPU.

Η πρόσβαση στον SDN ελεγκτή θα πρέπει να ελέγχετε για την αποφυγή μη-εξουσιοδοτημένης δραστηριότητας. Οι διαχειριστές θα πρέπει να δημιουργούν πολιτικές ελέγχου πρόσβασης με βάση το ρόλο [role-based access control (RBAC)] καθώς και διαδρομές ελέγχου, για να μην γίνονται μη-εξουσιοδοτημένες αλλαγές στους ελεγκτές. Μιας μεγάλης διαθεσιμότητας αρχιτεκτονικής ελεγκτή θα μπορούσε σε κάποιο βαθμό να περιορίσει τις DDoS επιθέσεις με την χρήση εφεδρικών χειριστών για να αντικαταστήσουν τις απώλειες των άλλων ελεγκτών. Ως κεντρικό σημείο αποφάσεων του δικτύου, είναι σημαντικό να ασφαλιστεί ο SDN ελεγκτής εντός της αρχιτεκτονικής. Απαιτείτε ισχυρός έλεγχος πρόσβασης, παράλληλα με τον διαχωρισμό της ζώνης εμπιστοσύνης. Η προστασία από τις DDoS επιθέσεις, τα anti-virus και άλλες τεχνικές πρόληψης και μείωσης των απειλών είναι απαραίτητες.

7.2.3 Ασφάλεια εφαρμογών (northbound)

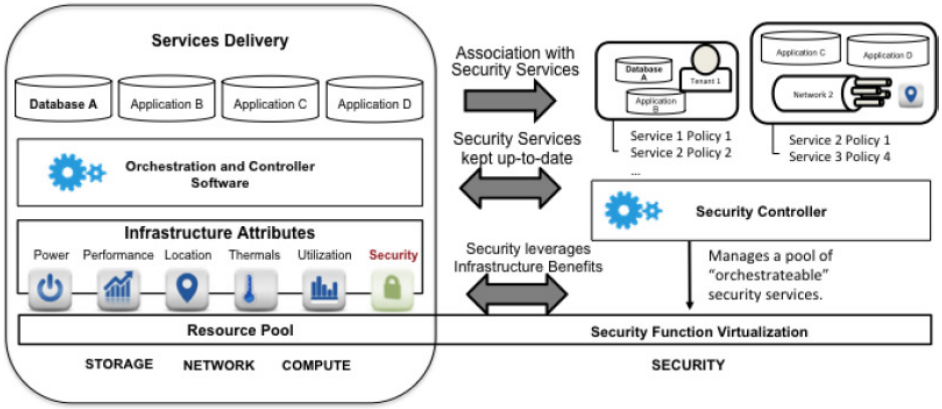
Τα ‘’βόρεια’’ πρωτόκολλα και τα APIs είναι επίσης στόχος επίθεσης και υπάρχουν πολλά που μπορεί να επιλέξει ένας χάκερ. Τα APIs χρησιμοποιούν Java, JSON και Python, κ.α., και οι επιτιθέμενοι μπορούν να αποκτήσουν τον έλεγχο της SDN υποδομής με την εκμετάλλευση των τρωτών σημείων σε οποιοδήποτε από αυτά. Η ασφάλεια είναι επομένως απαραίτητη, αλλιώς οι πολιτικές του SDN θα μπορούσαν να δημιουργηθούν από τον επιτιθέμενο προκειμένου να πάρει τον έλεγχο. Αφήνοντας ένα προεπιλεγμένο κωδικό πρόσβασης στις APIs επιτρέπει στον χάκερ να τον

μαντέψει εύκολα και στη συνέχεια να δημιουργήσει πακέτα και να τα προωθήσει στη διεπαφή διαχείρισης ελεγκτή για να προσδιορίσει τη δομή του δικτύου SDN ή ακόμη και να στήσει ένα δικό του. Η πιο κοινή πρόκληση είναι να εξασφαλιστεί ότι υπάρχει ένας μηχανισμός για τον έλεγχο πρόσβασης σε μια εφαρμογή στο επίπεδο ελέγχου, ώστε να αποτραπεί το χακάρισμα αυτής της επικυρωμένης εφαρμογής. Η χρήση TLS ή SSH για την ασφάλεια των επικοινωνιών στα '' βόρεια'' θεωρείται η καλύτερη λύση. Άλλη μια βοήθεια για την ασφάλεια είναι να σιγουρευτούμε ότι οι βόρειες εφαρμογές είναι ασφαλώς κωδικοποιημένες. Αυτό σημαίνει ότι οι μέθοδοι πιστοποίησης και κρυπτογράφησης, πρέπει να εφαρμόζονται σε όλες τις επικοινωνίες ανάμεσα στις εφαρμογές και τις υπηρεσίες αιτημάτων SDN, αλλά και στον ελεγκτή που εξυπηρετεί αυτές τις αιτήσεις. Οι τελικοί χρήστες θα πρέπει να αξιοποιήσουν τις σχετικές δυνατότητες του SDN να εισαγάγει νέες δυνατότητες ασφαλείας σε όλο το δίκτυο. Θα πρέπει να δώσουν μεγάλη προσοχή στην ρύθμιση παραμέτρων ασφαλείας που προστατεύει τον ελεγκτή και την επικοινωνία μεταξύ του ελεγκτή και των εφαρμογών στην βόρεια πλευρά του API.

7.3 SDN Security Controller

Η SDN-NFV αρχιτεκτονική μπορεί να ωφεληθεί από την προσθήκη ενός χειριστή ασφαλείας (security controller). Τα πλεονεκτήματα είναι:

- Οργάνωση (Orchestration) για τις υπηρεσίες ασφαλείας ανάμεσα σε όλα τα εικονικά κέντρα δεδομένων
- Διαχείριση και οργάνωση των κατανεμημένων λύσεων ασφαλείας
- Δεν απαιτούνται αλλαγές στο δίκτυο ή στο φόρτο εργασίας των εικονικών μηχανών (VMs)
- Μη-αποδιοργανωτική παράδοση της ασφάλειας στο φόρτο εργασίας των VMs
- Συνεχή ενσωμάτωση με τις εικονικές πλατφόρμες
- Αυτόματος συγχρονισμός



Εικόνα 22: SDN Security Controller

Η ολοκληρωμένη πολιτική ασφαλείας και η δυνατότητα ορατότητας του δικτύου, οδηγούν στο επιθυμητό επίπεδο αυτοματισμού που προκύπτει από την SDN / NFV αρχιτεκτονική. Ένα κεντρικό πλαίσιο ελέγχου ασφαλείας παρέχει την δυνατότητα της κατανεμημένης υποδομής ασφαλείας, της προσθήκης υπηρεσιών που βασίζονται στην πολιτική των ροών εργασίας, και την δυνατότητα επεκτασιμότητας, ώστε να μπορούν να προστεθούν οργανωτές (orchestrators) και λειτουργίες VNF, με την απαραίτητη προστασία και αποκατάσταση που είναι επεκτάσιμη σε όλα τα διανεμημένα κέντρα δεδομένων και τις διανεμημένες NFV / SDN αρχιτεκτονικές.

8. Intent-based Networking

Το SDN κάνει το δίκτυο πιο ευέλικτο και ευκίνητο, μέσα από τα προγραμματιστικά στοιχεία του δικτύου. Ο προγραμματισμός αυτός πρέπει να γίνει με ένα πρότυπο τρόπο. Ως εκ τούτου, η τυποποίηση του πρωτοκόλλου του 'Νότου' που διατάζει άμεσα ένα στοιχείο του δικτύου να προωθήσει κίνηση είναι σημαντική. Έτσι μέσω του πρωτόκολλου του 'βορρά', διαφορετικές εφαρμογές λένε σε έναν ελεγκτή SDN το **τι και πώς** θέλουν να επιτευχτεί κάτι από το δίκτυο. Δηλαδή, η εφαρμογή δεν έχει να πει μόνο την πρόθεσή της (**το τι**), αλλά πρέπει να πει και τον τρόπο για να το επιτύχει **(το ΠΩΣ).**

Ένα απλό παράδειγμα για το **πώς** και το **τι** στα κλασικά δίκτυα, είναι η προσπάθεια να στείλει η κίνηση από το σημείο Α στο σημείο Β μεταξύ των δρομολογητών ενός συγκεκριμένου προμηθευτή.

• **Τι:** Είναι η πρόθεση για την αποστολή της κυκλοφορίας από το Α στο Β

• **Πως:** Είναι η ρύθμιση ορισμένων παραμέτρων (για παράδειγμα, χρησιμοποιώντας ορισμένες εντολές CLI από κάποιους προμηθευτές) για ορισμένες μεταφορές (MPLS, οπτική).

Είναι σαφές ότι στην περίπτωση αυτή, τόσο το **τι** όσο και το **πώς** θα χρειαζόντουσαν για να ρυθμιστεί η κίνηση με επιτυχία. Είναι προφανές, επίσης, ότι ο χρήστης πρέπει να καταλάβει το CLI ενός συγκεκριμένου προμηθευτή για να μπορέσει να ρυθμίσει ένα τέτοιο σενάριο. Μπορεί όμως ο χρήστης να έχει καταλάβει και να γνωρίζει ένα διαφορετικό παλαιότερο από το υπάρχον σύνολο CLI, αν ο προμηθευτής ή ο εξοπλισμός δικτύωσης έχει αλλάξει με νεότερο. Αυτό δεν είναι ένα αρκετά ευέλικτο περιβάλλον. Το SDN, όμως, επιτρέπει την αφαίρεση που δεν είναι διαθέσιμη σε κανονικά περιβάλλοντα δικτύωσης. Το υψηλότερο επίπεδο των εν λόγω αφαιρέσεων επιτυγχάνεται όταν μια εφαρμογή στο SDN καθορίζει μόνο την πρόθεση, αλλά όχι τον τρόπο για να επιτευχθεί το επιθυμητό αποτέλεσμα.

Η δικτύωση με βάση την πρόθεση έχει γίνει πρόσφατα το επίκεντρο της ομάδας εργασίας του 'Βορρά' στο Open Networking Foundation (ONF) και γενικά αναφέρεται ως δικτύωση που βασίζεται στη πρόθεση [Intent-based Networking

(IBN)]. Η ομάδα εργασίας έχει σχηματιστεί για την τυποποίηση των μοντέλων και των διεπαφών με βάση την IBN. (Άλλοι οργανισμοί τυποποίησης εργάζονται επίσης για την τυποποίηση IBN με τον ένα ή τον άλλο τρόπο.) Με την IBN, ο χρήστης ή η εφαρμογή πρέπει να καθορίσει μόνο την πρόθεση. Για παράδειγμα:

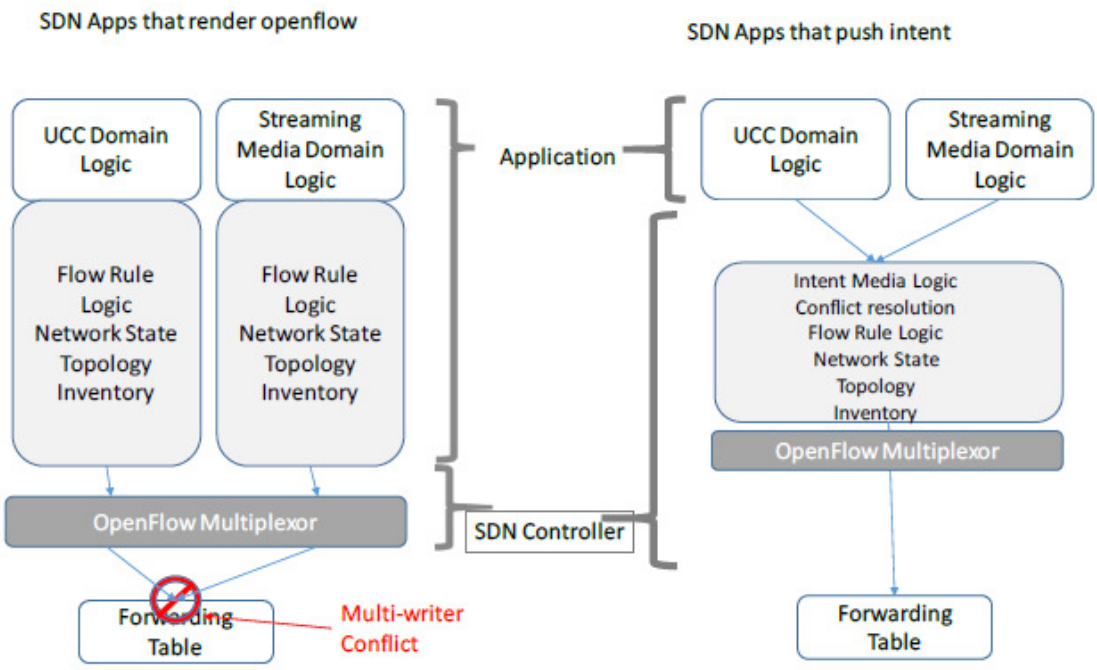
• Χρειάζομαι μια διαδρομή από το Α στο Β με την μικρότερη καθυστέρηση.

• Χρειάζομαι ένα εύρος ζώνης των 40 MB από το χρόνο Α στο Β, αλλιώς 100 MB.

• Εάν το Jitter αυξηθεί στο σύνδεσμο, αλλάξτε τη διαδρομή σε μονοπάτι Χ και μόλις αυτό γίνει κανονικό επανέφερε το πίσω στην αρχική διαδρομή.

Ο ελεγκτής SDN, ο οποίος είναι αρκετά ευφυής, παίρνει αυτές τις εντολές και τις μεταφράζει σε εντολές χαμηλού επίπεδου υποδομών και σε ενέργειες. Αυτό αφαιρεί την πίεση από την εφαρμογή για να κατανοήσουν τις υποκείμενες λεπτομέρειες των υποδομών χαμηλού επιπέδου και ανοίγει νέα μονοπάτια για τους προγραμματιστές εφαρμογών.

Το παρακάτω διάγραμμα συγκρίνει τα κύρια στοιχεία και τη φύση των εργασιών ανάπτυξης ανάμεσα σε ένα σύστημα όπου μια εφαρμογή SDN ή υπηρεσία SDN παράγει άμεσα χαμηλό επίπεδο προγραμματισμού της συσκευής, όπως η χρήση openflow, και ένα σύστημα όπου η εφαρμογή απλά σπρώχνει την ‘’πρόθεση’’ στην μηχανή που παρέχει μια υπηρεσία πρόθεσης για τους κανόνες της συσκευής. Σε αυτό το παράδειγμα δύο διαφορετικές μορφές media streaming έχουν αρχικά δύο διαφορετικές εφαρμογές SDN να πιέζουν τους κανόνες του openflow. Το ένα είναι για την διαδραστική επικοινωνία ήχου και βίντεο, και το άλλο είναι για streaming ταινίες. Υπάρχει μεγάλη αλληλοεπικάλυψη μεταξύ των κανόνων μεταγωγής που απαιτούνται για τις διαδραστικές ροές και τις ροές streaming. Αυτό μπορεί εύκολα να γενικευθεί έτσι ώστε ένα ενιαίο σύνολο της λογικής της ροής να μπορεί να υποστηρίξει και τις δύο απαιτήσεις. Ωστόσο, επειδή πρόκειται για δύο διαφορετικές εφαρμογές, το καθένα έχει ένα σύνολο παρόμοιων, ή ακόμη και τελείως διαφορετικών λογικών για την άμεση δημιουργία κανόνων συσκευής. Επιπλέον, και οι δύο από αυτές τις εφαρμογές πιστεύουν ότι τους ανήκουν αποκλειστικά οι πίνακες ροής στα switches, με αποτέλεσμα να κάνουν ασύμφωνες αλλαγές, προκαλώντας βλάβη στο σύστημα. Στο μοντέλο βασισμένο στην ‘’πρόθεση’’ η κοινή λογική ωθείται προς την πρόθεση της μηχανής. Τώρα, οι προγραμματιστές των δύο εφαρμογών γράφουν πολύ λιγότερο κώδικα, και δεν ασχολούνται με οποιαδήποτε από την πολυπλοκότητα του χαμηλού επιπέδου προγραμματισμού της συσκευής. Επιπλέον, με τη χρήση ενός κοινού συστήματος για την απόδοση οδηγιών χαμηλού επιπέδου, οι προγραμματιστές αποφεύγουν εντελώς το πρόβλημα των πολλών ‘συγγραφέων’ και έχουν έναν ενιαίο διαχειριστή ενός συνεκτικού πίνακα ροής.



Εικόνα 23: Σύγριση SDN εφαρμογών

8.1 Πλεονεκτήματα του intent-based networking

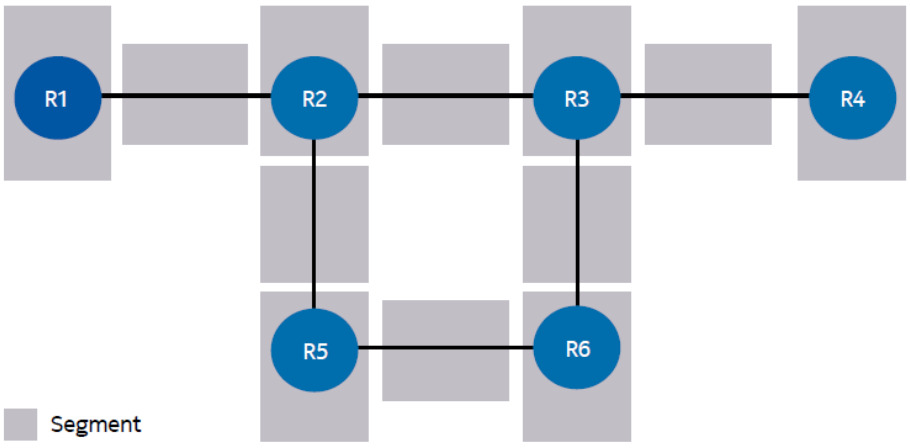
- Κλιμακωτό: Η IBN είναι πιο επεκτάσιμη σε σύγκριση με τα ‘’μη-πρόθυμα’’ πρωτόκολλα. Καθώς ο προγραμματιστής της εφαρμογής δεν χρειάζεται να γνωρίζει το περιβάλλον με τις υποδομές, η ευελιξία για αναβάθμιση της εφαρμογής θα αυξηθεί σημαντικά. Επίσης, η εισαγωγή νέων εφαρμογών γίνεται γρήγορα, αφού ο προγραμματιστής της εφαρμογής πρέπει να επικεντρωθεί περισσότερο στις εφαρμογές, αντί να κατανοήσει το πώς οι εφαρμογές λειτουργούν μαζί με την υποδομή.
- Φορητό: Μια εφαρμογή που αναπτύχθηκε για ένα περιβάλλον SDN μπορεί εύκολα να μεταφερθεί και σε άλλο περιβάλλον SDN χωρίς ο προγραμματιστής της εφαρμογής να εμπλακεί. Αυτό σημαίνει επίσης ότι μια εφαρμογή που αναπτύχθηκε για έναν ελεγκτή SDN μπορεί να τρέξει και σε έναν ελεγκτή ενός άλλου προμηθευτή.
- Συναφής: Η IBN θα φέρει συνοχή και θα αφαιρέσει τις συγκρούσεις από τις πολλαπλές εφαρμογές. Στο παρελθόν, υπήρχε πάντα πρόβλημα, όταν πολλαπλές εφαρμογές έδιναν εντολές σε έναν ελεγκτή SDN. Υπήρχε πάντα ο κίνδυνος της σύγκρουσης, δεδομένου ότι δεν ήταν δυνατόν να αποκωδικοποιήσει τις αλλαγές χαμηλού επιπέδου που πολλαπλές εφαρμογές προκαλούσαν στο δίκτυο, με αποτέλεσμα ο ελεγκτής να μην μπορεί να κατανοήσει την πρόθεση των εφαρμογών.
- Εξάλειψη του ‘’αποκλειστικού πωλητή/παρόχου’’ ως εμπόδιο για την επιλογή, την ευελιξία και την καινοτομία
- Δυνατότητα «εγγραφής μια φορά (write once)» για την ενσωμάτωση του φόρτου εργασίας και των εφαρμογών με τις υποδομές.

- Δυνατότητα συνδυασμού των καλύτερων εφαρμογών υπηρεσιών του δικτύου από ένα ευρύ οικοσύστημα από ανεξάρτητους προμηθευτές λογισμικού.
- Δυνατότητα σύγκρισης διαφορετικών εφαρμογών για τα επιθυμητά χαρακτηριστικά και επιλογή των προμηθευτών, των πρωτοκόλλων, των διασυνδέσεων, κλπ που βασίζονται σε εμπειρικά δεδομένα.

9. Segment Routing (SR)/ (Τμηματική δρομολόγηση) *Cisco*

Η τμηματική δρομολόγηση χρησιμοποιεί τις κοινές τεχνολογίες ελέγχου δεδομένων, όπως είναι το MPLS, και απαιτεί μόνο μικρές αλλαγές στα υπάρχοντα πρωτόκολλα δρομολόγησης. Η τμηματική δρομολόγηση είναι πλήρως τεκμηριωμένη από την IETF, με την συνεισφορά των προμηθευτών και των διαχειριστών. Η βασική προϋπόθεση επικεντρώνεται στην έννοια του source routing(δρομολόγηση πηγής), όπου η πηγή, ή η είσοδος του κόμβου, καθοδηγεί το πακέτο για τον δρόμο που θα πάρει, συμπεριλαμβανομένου και τον δρόμο που θα ακολουθήσει. Δηλαδή, το πακέτο εκτός από τα δεδομένα που περιέχει, περιέχει και το δρομολόγιο που θα ακολουθήσει για να φτάσει στον προορισμό του.

Στη τμηματική δρομολόγηση, ένας κόμβος κατευθύνει το πακέτο μέσω μιας ταξινομημένης λίστας οδηγιών που ονομάζονται "τμήματα". Ένα τμήμα μπορεί να αντιπροσωπεύει οποιαδήποτε εντολή, και βασίζεται είτε σε μια τοπολογία είτε σε μια υπηρεσία. Όπως και με τις άλλες τεχνικές δρομολόγησης της πηγής, οι πλήρεις οδηγίες για τη διαδρομή μέσω του δικτύου εφαρμόζονται στον κόμβο της πηγής και ενσωματώνονται στην κεφαλίδα των πακέτων.



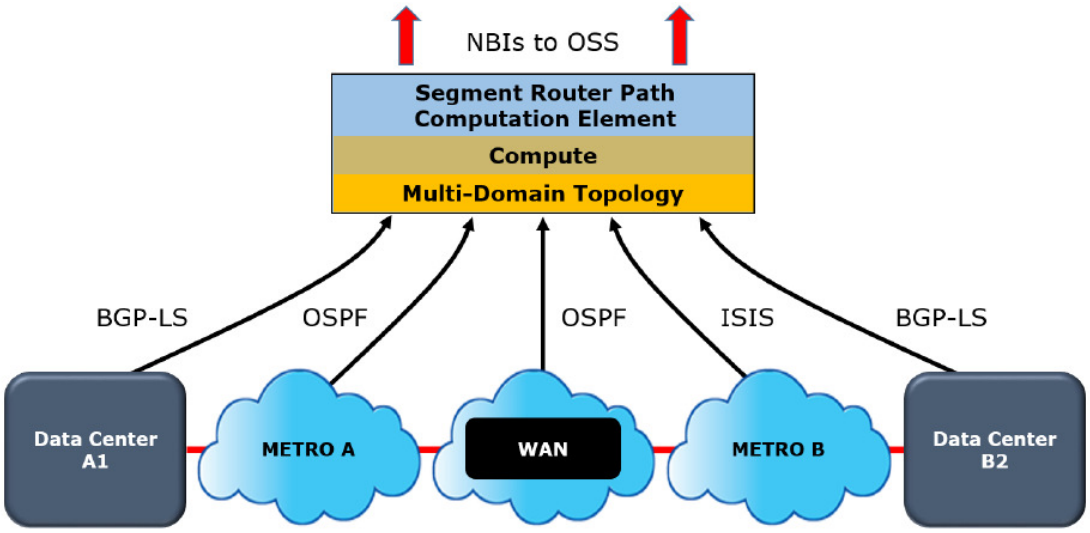
Εικόνα 24: Αναπαράσταση της SR domain σε τμήματα

Η τμηματική δρομολόγηση είναι μια μέθοδος που προωθεί τα πακέτα στο δίκτυο με βάση το πρότυπο δρομολόγησης προέλευσης. Οι οδηγίες εφαρμόζονται στα πακέτα ως μια διατεταγμένη στοίβα ετικετών. Κάθε δρομολογητής επεξεργάζεται το τμήμα στην κορυφή της στοίβας, κατόπιν αφαιρεί το κορυφαίο τμήμα και στέλνει το πακέτο σύμφωνα με τις οδηγίες. Στο επόμενο hop, ο νέος δρομολογητής επεξεργάζεται το

νέο κορυφαίο τμήμα, το αφαιρεί από τη στοίβα και στέλνει το πακέτο προς το δρόμο του. Αυτή η διαδικασία ακολουθείται μέχρι να αφαιρεθούν όλα τα τμήματα ώστε τα πακέτα φτάσουν στον προορισμό τους. Η τμηματική δρομολόγηση αξιοποιεί και άλλα πρωτόκολλα εσωτερικής πύλης, όπως το IS-IS, το OSPF, και το MPLS για πιο αποτελεσματική και πιο ευέλικτη προώθηση. Επιπλέον, είναι ένας ταχύτερος και πιο αποτελεσματικός τρόπος για την προώθηση της κίνησης σε ένα MPLS δίκτυο.

Ένα πλεονέκτημα της χρήσης της τμηματικής δρομολόγησης με το SDN είναι ότι υπάρχουν σημαντικές βελτιώσεις στους χρόνους σύγκλισης, λόγω της περιορισμένης ποσότητας των πληροφοριών κατάστασης που πρέπει να διανέμονται από τους ελεγκτές SDN, αφού με τη τμηματική δρομολόγηση, δημιουργούνται μέσω του δρομολογητή εισόδου όλες οι απαιτούμενες πληροφορίες κατάστασης στην κεφαλίδα του πακέτου. Ένα άλλο πλεονέκτημα της χρήσης της τμηματικής δρομολόγησης είναι η διαλειτουργικότητα μεταξύ των πωλητών και των domain, καθώς και με τα υπάρχοντα δίκτυα. Οι προγραμματιστές της τμηματικής δρομολόγησης αποφάσισαν σκόπιμα να προγραμματίσουν με βάση γνωστά πρωτόκολλα και να μην καθορίσουν ένα νέο πρωτόκολλο επιπέδου ελέγχου. Επίσης επέλεξαν να ορίσουν την τμηματική δρομολόγηση σε MPLS δίκτυα, τα οποία αναπτύσσονται ευρέως από τους παρόχους σε όλο τον κόσμο. Η χρήση του MPLS σε συνδυασμό με τα υπάρχοντα πρωτόκολλα, όπως το BGP, το PCE, το NETCONF / YANG, κλπ., σημαίνει ότι η τμηματική δρομολόγηση μπορεί εύκολα να εισαχθεί και να λειτουργήσει με τα υπάρχοντα δίκτυα.

Επιπλέον, ο συνδυασμός της τμηματικής δρομολόγησης με το PCE επιτρέπει την δημιουργία μονοπατιών ανάμεσα σε πολλαπλά domains, καθορίζοντας διαδρομές από μητροπολιτικά δίκτυα σε δίκτυα κορμού αλλά και την σύνδεση των κέντρων δεδομένων με το WAN. Τέλος, κάποιες τεχνικές δρομολόγησης πηγής συνδέονται στενά με το SDN που βασίζεται στο OpenFlow, με αποτέλεσμα οι τεχνικές αυτές να περιορίζονται και να λειτουργούν μόνο όπου υπάρχει το OpenFlow στο δίκτυο. Με την τμηματική δρομολόγηση όπως ορίζεται από την IETF, αυτός ο περιορισμός δεν υπάρχει.



Εικόνα 25: Κεντρικός έλεγχος με PCE

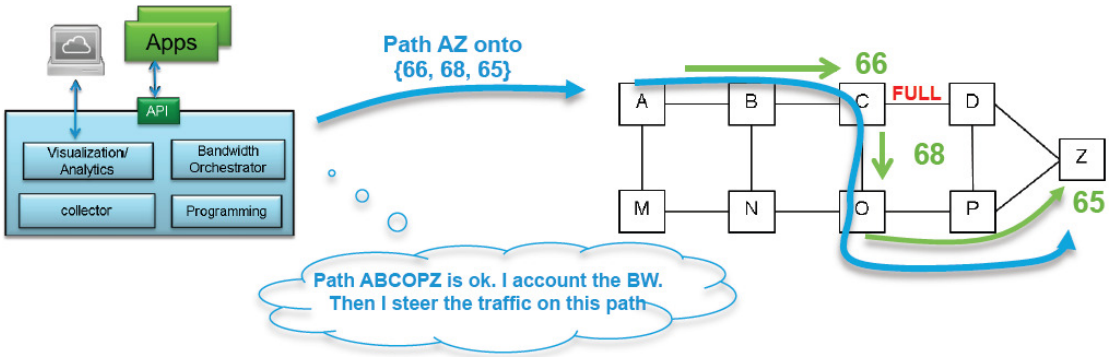
Multi- Protocol Label Switching (MPLS)

Το Multi- Protocol Label Switching (MPLS) είναι ένα πρωτόκολλο που εφαρμόζεται μεταξύ του επιπέδου 2 & 3. Το MPLS προωθεί τα πακέτα εισάγοντας (pushing) και αφαιρώντας (popping) ετικέτες στο δίκτυο. Οι ετικέτες(labels) παρέχουν μια ταχύτερη διέλευση για το πακέτο, καθώς είναι αυτοματοποιημένες για την επιλογή της βέλτιστης διαδρομής μέσα στο δίκτυο, εξοικονομώντας πολύ χρόνο. Έτσι το MPLS χρησιμοποιεί διαφορετικούς τύπους δρομολογητών για να προωθήσει τα δεδομένα μέσω του δικτύου. Οι δρομολογητές που ωθούν και απωθούν τις ετικέτες είναι γνωστοί ως Label Edge Routers (LER) ή ως δρομολογητές εισόδου / εξόδου. Οι LERs διατηρούν έναν πίνακα δρομολόγησης γνωστό ως Forwarding Equivalence Class (FEC). Οι δρομολογητές που προωθούν τα πακέτα με τις ετικέτες είναι γνωστά ως Label Switching Routers (LSR). Οι LSRs διατηρούν έναν πίνακα δρομολόγησης που είναι γνωστός ως Forwarding Information Base (FIB). Η διαδρομή που λαμβάνεται από τα πακέτα μέσω του δικτύου MPLS είναι γνωστή ως Label Switched Path (LSP).

Το MPLS χρησιμοποιεί δύο πρόσθετα πρωτόκολλα στα δίκτυά του:

• Label Distribution Protocol (LDP): Χρησιμοποιείται με το Interior Gateway Protocols (IGP), όπως είναι το OSPF και το IS-IS.

• Resource Reservation Protocol (RSVP): Χρησιμοποιείται για το MPLS Traffic Engineering (TE)



Εικόνα 26: MPLS

9.1 Segment Routing for Traffic Engineering

Η τμηματική δρομολόγηση για Traffic Engineering* πραγματοποιείται μέσω ενός TE τούνελ μεταξύ της πηγής και του προορισμού. Η τμηματική δρομολόγηση για TE χρησιμοποιεί την έννοια της δρομολόγησης της πηγής, όπου η πηγή υπολογίζει τη διαδρομή και κωδικοποιείται στην κεφαλίδα πακέτου ως ένα τμήμα. Κάθε τμήμα είναι ένα end-to-end μονοπάτι από την πηγή προς τον προορισμό, και καθοδηγεί τους δρομολογητές στον κορμό του δικτύου του παρόχου για να ακολουθήσουν την καθορισμένη διαδρομή αντί της συντομότερης διαδρομής που υπολογίζεται από το Interior gateway protocol (IGP). Ο προορισμός δεν γνωρίζει την παρουσία του TE τούνελ. Έτσι η τμηματική δρομολόγηση χρησιμοποιεί μια ενιαία πηγή και ανακουφίζει τους υπόλοιπους δρομολογητές από το καθήκον του υπολογισμού της απαιτούμενης διαδρομής διαμέσου του δικτύου.

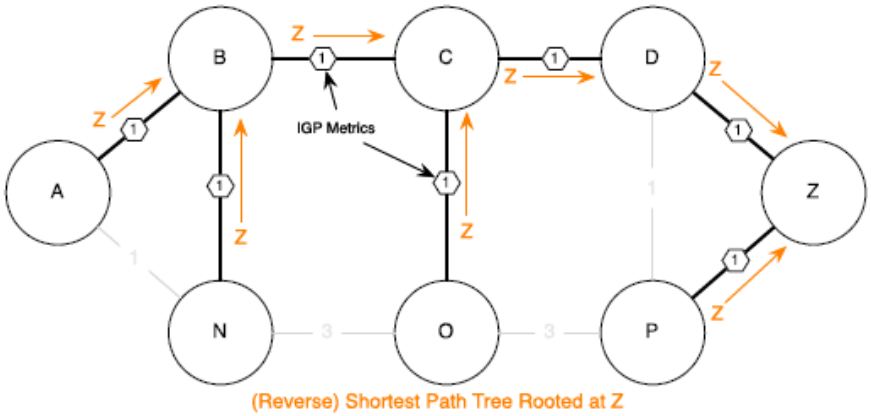
*(**Traffic engineering**: είναι η διαδικασία καταμερισμού της κίνησης μέσα στο δίκτυο, ώστε να ικανοποιηθούν οι απαιτήσεις των εφαρμογών).

Η τμηματική δρομολόγηση χρησιμοποιεί το εύρος ζώνης του δικτύου πιο αποτελεσματικά από τα παραδοσιακά δίκτυα MPLS και προσφέρει χαμηλότερο latency.

Σε σχέση με τα παραδοσιακά δίκτυα MPLS, ένα τμήμα προστίθεται στη θέση της ετικέτας MPLS. Ενώ κάθε ετικέτα MPLS επισημαίνει μόνο ένα κόμβο στον κορμό του δικτύου, το τμήμα επισημαίνει ολόκληρη την διαδρομή από την πηγή έως τον προορισμό. Έτσι η τμηματική δρομολόγηση μειώνει τον αριθμό των ετικετών που απαιτείται στο δίκτυο. Κάθε τμήμα περιέχει πολλαπλά αναγνωριστικά (32-bit) τμήματα που κατευθύνουν τα δεδομένα κατά μήκος μιας καθορισμένης διαδρομής. Υπάρχουν δύο είδη τμηματικών SID:

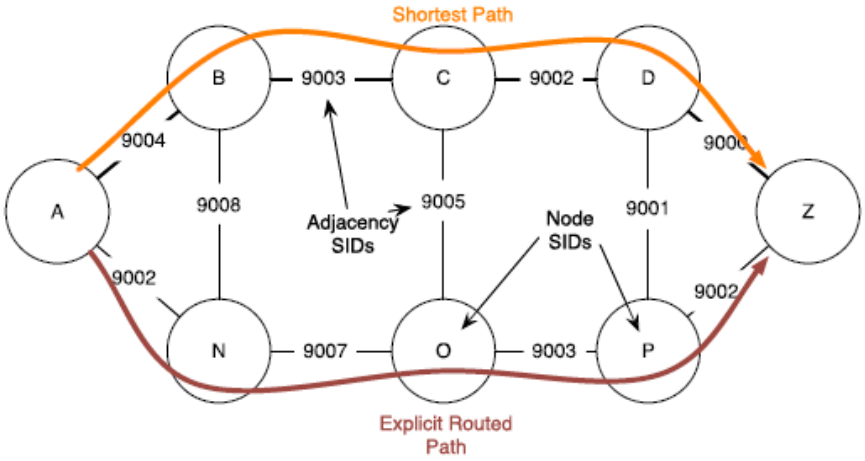
- **Local SIDs - Prefix SID**: Ένα τμήμα ID που περιέχει ένα πρόθεμα IP διεύθυνσης υπολογισμένο από το IGP στο δίκτυο κορμού του παρόχου. Τα

προθεματικά SIDs είναι παγκοσμίως μοναδικά. Ένας SID κόμβος είναι μια ειδική μορφή προθέματος SID που περιέχει τη loopback διεύθυνση του κόμβου ως πρόθεμα.



Εικόνα 27: Prefix SID

- **Global SIDs - Adjacency SID**: Μια γειτνίαση SID είναι μια σύνδεση μεταξύ δύο δρομολογητών. Δεδομένου ότι η γειτνίαση SID είναι σχετική με ένα συγκεκριμένο router, είναι τοπικά μοναδική. Χρησιμοποιείται για να προσδιορίσει μια συγκεκριμένη γειτνίαση μεταξύ δύο κόμβων.



Εικόνα 28: Adjacency Sid

9.2 Καθοδήγηση της κίνησης για τα Segment Routing Tunnels

Στατική δρομολόγηση

Οι στατικές δρομολογήσεις μπορούν να χρησιμοποιήσουν ένα SR τούνελ ως διεπαφή του επόμενου-hop. Και το πρόθεμα IPv4 και το πρόθεμα IPv6 μπορούν να δρομολογούνται μέσω του τούνελ.

Αναγγελία αυτόματης δρομολόγησης (Autoroute Announcement)

Το SR τούνελ μπορεί να ‘’διαφημίζεται’’ σε ένα IGP ως το επόμενο hop ρυθμίζοντας την αναγγελία αυτόματης δρομολόγησης στη πηγή του δρομολογητή. Το IGP στη συνέχεια εγκαθιστά διαδρομές στην Routing Information Base (RIB) για συντομότερα μονοπάτια που αφορούν τον προορισμό του τούνελ. Η αναγγελία αυτόματης δρομολόγησης του IPv4 προθέματος μπορεί να πραγματοποιηθεί μέσω του OSPF ή του IS-IS. Η αναγγελία αυτόματης δρομολόγησης του προθέματος IPv6 μπορεί να πραγματοποιηθεί μόνο μέσω του IS-IS.

Ανίχνευση Βρόχου

Η αποτυχία ενός συνδέσμου σε μια διαδρομή μπορεί ακούσια να προκαλέσει loop σε ένα πακέτο, αν το εναλλακτικό hop του τρέχον δρομολογητή είναι να εισάγει ένα νέο ενδιάμεσο μονοπάτι που οδηγεί πίσω στο τρέχον δρομολογητή ή σε έναν άλλο δρομολογητή που εμφανίζεται νωρίτερα στη διαδρομή. Όταν η SR έχει διαμορφωθεί με την κατάσταση αναγγελίας αυτόματης δρομολόγησης (autoroute announce) στον δρομολογητή της πηγής, οι βρόχοι ανιχνεύονται και ακυρώνονται στο μονοπάτι της τμηματικής δρομολόγησης.

Προορισμός αυτόματης δρομολόγησης (Autoroute)

Το χαρακτηριστικό του προορισμού αυτόματης δρομολόγησης επιτρέπει την προσθήκη διαδρομών για συγκεκριμένα προθέματα απευθείας στο RIB, με ένα κόστος διαδρομής που ταιριάζει με το υπολογισμένο κόστος της IGP στο τούνελ προορισμού.

Pseudowire Preferred Path

Ένα στατικά ρυθμισμένο τμήμα δρομολόγησης μπορεί να χρησιμοποιηθεί ως προτιμώμενος δρόμος για μια pseudowire VPLS / VPWS.

Επιλογή τούνελ

Η τμηματική δρομολόγηση παρέχει τους ακόλουθους τύπους μηχανισμών επιλογής τούνελ:

• **Πολιτική με βάση την επιλογή σήραγγας (PBTS):** Η επιλογή τούνελ μπορεί να πραγματοποιηθεί με βάση την αξία της κλάσης του τούνελ [Tunnel Class (TC)] των

εξερχόμενων πακέτων MPLS. Οι κλάσεις των τούνελ διαμορφώνονται σε κάθε τούνελ βάσης. Τα τούνελ χωρίς διαμορφωμένη κλάση έχουν ανατεθεί σε μια προκαθορισμένη κατηγορία 0.

• **Επιλογή τούνελ προωθητικής κλάσης:** Η τμηματική δρομολόγηση επιτρέπει την επιλογή του τούνελ με βάση τη προωθητική κλάση. Προωθητική κλάση είναι ένας μηχανισμός χαρτογράφησης μιας συγκεκριμένης κλάσης κυκλοφορίας, σε ένα συγκεκριμένο τούνελ μέσα από ένα σύνολο παράλληλων τούνελ.

Εξισορρόπηση φορτίου για την τμηματική δρομολόγηση

Τα SR τούνελ υποστηρίζουν την εξισορρόπηση φορτίου για τις ακόλουθες ρυθμίσεις:

• Πακέτα TE Links: Διεπαφές που ομαδοποιούνται για να σχηματίσουν πακέτα συνδέσμων, για την εξισορρόπηση φορτίου της κίνησης μεταξύ των διεπαφών.

• Ίσο κόστος πολλαπλά μονοπάτια (ECMPs): Εάν το τμηματικό μονοπάτι TE LSP διασχίσει ένα ή περισσότερα προθεματικά SIDs που έχουν ECMPs, η κίνηση LSP εξισορροπείται μεταξύ των διαδρομών ECMP για κάθε πέρασμα των προθεματικών SIDs από την πηγή ή οποιοδήποτε μέσο σημείο κατά μήκος της διαδρομής.

• Πολλαπλά Τούνελ: Εάν υπάρχουν πολλαπλά παράλληλα τούνελ μεταξύ της πηγής και του προορισμού, τα τούνελ εξισορροπούν το φορτίο.

9.3 Segment Routing Tunnel Reoptimitization

Η Επανα-βελτίωση του τούνελ τμηματικής δρομολόγησης ενεργοποιείται όταν η πηγή βρίσκει μια πιο βέλτιστη διαδρομή από αυτήν που χρησιμοποιείται ήδη από το αρχικό LSP. Όταν παρουσιαστεί βλάβη κατά μήκος του LSP, η πηγή μπορεί να εναλλάξει τα μονοπάτια ενεργοποιώντας εκ νέου την βελτιστοποίηση (Reoptimization). Όταν ο δρομολογητής της πηγής ανιχνεύσει σφάλμα σε ένα προστατευμένο LSP, ενεργοποιείται ένα 5λεπτο χρονόμετρο αναδρομολόγησης . Εάν η πηγή εξακολουθεί να χρησιμοποιεί το σπασμένο μονοπάτι, όταν λήξει ο χρόνος, το τούνελ ‘πέφτει’ και οι υπηρεσίες μεταφέρονται σε άλλο μονοπάτι.

Η επανα-βελτιστοποίηση είναι ένας κρυφός διακόπτης πάνω από το μηχανισμό που μπορεί να προκύψει στις ακόλουθες περιπτώσεις.

• Τροποποίηση του μονοπατιού (hop) από την αρχική TE LSP

• Αποσύνδεση ενός μονοπατιού της τοπολογίας

• Έλλειψη του SID στη βάση δεδομένων SID

• Όταν γίνεται διαθέσιμη καλύτερη επιλογή διαδρομής με χαμηλότερη τιμή δείκτη

9.3.1 Segment Routing Tunnel Protection

Τα τούνελ τμηματικής δρομολόγησης προστατεύονται με οποιονδήποτε από τους παρακάτω τρόπους.

• 1: 1 προστασία διαδρομής: Σε αυτήν την περίπτωση, ένα backup LSP έχει ρυθμιστεί για κάθε αρχικό LSP.

• Γρήγορη επανα-δρομολόγηση (FRR) τοπικής προστασίας: Η FRR επιτρέπει την ενεργοποίηση προ-ρυθμισμένων backup μονοπατιών μέσα σε 50 ms από την αποτυχίας μιας διαδρομής.

Σε κάθε μονοπάτι τμηματικής δρομολόγησης, κάθε δρομολογητής (κόμβος) λειτουργεί ως ένα Σημείο Τοπικής Επισκευής (PLR) για τον εντοπισμό και την επισκευή του σφάλματος του αρχικού LSP.

> ***Τα FRRs δεν μπορούν να προστατεύσουν τις αποτυχίες ενός συγκεκριμένου κόμβου SID. Σε αυτή την περίπτωση η 1: 1 διαδρομή προστασίας θα πρέπει να ενεργοποιηθεί.

• Τοπική προστασία γρήγορης επαναδρομολόγησης IP (FRR): Τα IP FRRs είναι ειδικές μορφές FFR όπου ένα IGP (όπως OSPF ή IS-IS) υπολογίζει και να ενεργοποιεί το backup μονοπάτι, σε περίπτωση αποτυχίας μιας σύνδεσης.

Όταν μια απροστάτευτη γειτνίαση SID αποτύχει, το IGP πυροδοτεί την άμεση απόσυρση της SID από το δίκτυο, και την ακύρωση του LSP. Όταν μια προστατευόμενη γειτνίαση SID αποτύχει, η αποτυχημένη SID και οι συναφείς πληροφορίες προώθησης διατηρούνται για περίπου 5-15 λεπτά για να επιτρέψει στην πηγή του τούνελ να ανιχνεύσει και να αντιδράσει στην αποτυχία της LSP.

• TE backup μονοπάτια για FFR τοπική προστασία: Το MPLS TE παρέχει την σύνδεση ή / και την προστασία του κόμβου σε κάθε δρομολογητή (κόμβο) υπολογίζοντας ένα backup τούνελ προς την κατεύθυνση του επόμενου hop ή στο next-to next hop. Τέτοιες backup διαδρομές είναι ανώτερες από τα IGP-μονοπάτια, επειδή παρέχουν 100% σύνδεση, κόμβο, και την Shared Risk Link Groups (SRLG) προστασία σε οποιαδήποτε τοπολογία.

• Προστασία του τούνελ μονοπατιού: Η προστασία του τούνελ μονοπατιού είναι η συγκεκριμενοποίηση ενός ή περισσοτέρων standby LSPs για την προστασία από την αποτυχία της αρχικής LSP ενός τούνελ τμηματικής δρομολόγησης. Η προστασία του μονοπατιού έχει σχεδιαστεί για να ελαχιστοποιεί την απώλεια κίνησης, όταν η αρχική LSP αποτύχει. Ωστόσο, θα διακοπεί η κυκλοφορία μέχρι να ολοκληρωθεί η παρακάτω ακολουθία:

1. Το σφάλμα ανιχνεύεται από έναν PLR δρομολογητή(router).
2. Ο PLR δρομολογητής αποσύρει τη δημοσίευση του συνδέσμου, και την ενημέρωση της τοπολογίας.
3. Το σφάλμα διαδίδεται στη πηγή του δρομολογητή μέσα από μια ενημερωμένη τοπολογία.
4. Η πηγή του δρομολογητή μεταβαίνει στο δευτερεύον προ-τροφοδοτούμενο μονοπάτι.

9.4 Πλεονεκτήματα εναλλαγής σε τμηματική δρομολόγηση

• Έτοιμο για SDN: Η τμηματική δρομολόγηση δημιουργήθηκε για το SDN και αποτελεί το θεμέλιο για την Application Engineered Routing (AER). Η τμηματική δρομολόγηση προετοιμάζει τα δίκτυα για επιχειρηματικά μοντέλα, όπου οι εφαρμογές μπορούν να κατευθύνουν την συμπεριφορά του δικτύου. Η τμηματική δρομολόγηση παρέχει τη σωστή ισορροπία μεταξύ της κατανεμημένης ευφυΐας και της κεντρικής βελτιστοποίησης και προγραμματισμού.

• Ελάχιστη διαμόρφωση: Η τμηματική δρομολόγηση για Traffic Engineering απαιτεί ελάχιστη διαμόρφωση του δρομολογητή της πηγής.

• Εξισορρόπηση φορτίου: Σε αντίθεση με το RSVP-TE, η εξισορρόπηση φορτίου μπορεί να γίνει για την τμηματική δρομολόγηση με την παρουσία του ίσου κόστους πολλαπλών μονοπατιών (ECMPs).

• Υποστηρίζει Fast Reroute (FFR): Σε περίπτωση αποτυχίας της σύνδεσης ή ενός κόμβου σε ένα δίκτυο, ο MPLS χρησιμοποιεί τον FFR μηχανισμό για σύγκλιση. Με την τμηματική δρομολόγηση που χρησιμοποιείται για το TE, ο χρόνος σύγκλισης είναι λιγότερος απο 50ms. (Ως χρόνος σύγκλισης (convergence time), ορίζεται ο χρόνος που περνά μέχρι όλοι οι δρομολογητές να συμφωνήσουν σχετικά με την τοπολογία του δικτύου, από τη στιγμή που θα προκύψει μια αλλαγή)

• Ανάπτυξη Plug-and-Play: Τα τούνελ τμηματικής δρομολόγησης είναι διαλειτουργικά με το υπάρχον MPLS επίπεδο δεδομένων και επίπεδο ελέγχου και μπορούν να εφαρμοστούν σε μια υπάρχουσα εγκατάσταση.

10. Διεπαφές *(Interfaces)* SDN-NFV

- Vi-Ha (Virtualization Layer – Hardware Resources)

Ενώνει το virtualization layer με τους hardware πόρους για να δημιουργήσει ένα περιβάλλον εκτέλεσης για τις λειτουργίες VNF και για να συλλέξει πληροφορίες για την κατάσταση των hardware πόρων και για την διαχείριση των λειτουργιών VNF χωρίς να εξαρτώνται από οποιαδήποτε hardware πλατφόρμα.

- Vn-Nf (VNF – NFVI)

Αυτή η διεπαφή αντιπροσωπεύει το περιβάλλον εκτέλεσης που παρέχεται από την NFVI για τη λειτουργία VNF. Δεν λαμβάνει κάποιο συγκεκριμένο πρωτόκολλο ελέγχου και εγγυάται ανεξάρτητο κύκλο ζωής του hardware, εκτέλεση και φορητότητα των απαιτήσεων της λειτουργίας VNF. Η Vn-Nf διεπαφή παρέχει ένα ‘’περίβλημα’’ εικονικής μηχανής που ενώνεται με τον hypervisor και παρέχει ολοκληρωμένες δικτυακές υπηρεσίες στις λειτουργίες VNF. Επιπλέον συνδέει τα παρακάτω:

  - Τα VNFCs με άλλα VNFCs ανάμεσα στην ίδια ή σε διαφορετική λειτουργία VNF.
  - Τα VNFCs με τον αποθηκευτικό χώρο.
  - Τις VNFs με PNFs και εξωτερικά τελικά σημεία.

- Nf-Vi (NFVI – VIM)

Αυτή είναι η διεπαφή ανάμεσα στην διαχείριση και την οργάνωση του τομέα (domain) της δικτυακής υποδομής και των λειτουργιών διαχείρισης και οργάνωσης στο VIM. Η οργάνωση και η διαχείριση της NFVI γίνεται αυστηρά μέσω του Nf-Vi και περιέχει τα παρακάτω:

  - Συγκεκριμένη εργασία των εικονικών πόρων σε απόκριση των αιτημάτων της κατανομής πόρων.
  - Προώθηση της κατάστασης των πληροφοριών των εικονικών πόρων.
  - Διαμόρφωση των hardware πόρων και αλλαγή των πληροφοριών της κατάστασης.

- Or-Vi (NFVO – VIM)

Αυτή η διεπαφή χρησιμοποιείται για τις ανταλλαγές ανάμεσα στον NFV Orchestrator και τον VIM για την αίτηση πόρων και για συγκεκριμενοποιήσεις του VNFC, αλλά και για τον VIM για την αναφορά των χαρακτηριστικών, της διαθεσιμότητας, και της κατάστασης των υποδομών του δικτύου.

  - Κράτηση των πόρων και/ή κατανομή των αιτημάτων από τον NFVO
  - Διαμόρφωση των εικονικών hardware πόρων και ανταλλαγή της κατάστασης των πληροφοριών:
    - Κράτηση/ελευθέρωση NFVI πόρων

- Κατανομή/ελευθέρωση/ενημέρωση NFVI πόρων
- Πρόσθεση/αφαίρεση/ενημέρωση της εικόνας του VNF software
- Προώθηση των πληροφοριών διαμόρφωσης, των συμβάντων, των αποτελεσμάτων των μετρήσεων, και των αρχείων χρήσης όσον αφορά τους NFVI πόρους στον NFVO.

Η Or-Vi διεπαφή υποστηρίζει τις παρακάτω λειτουργίες:

- ✓ Διαχείριση της εικόνας του VNF software
- ✓ Διαχείριση του καταλόγου των εικονικών πόρων
- ✓ Διαχείριση της χωρητικότητας των εικονικών πόρων
- ✓ Διαχείριση των εικονικών πόρων
- ✓ Διαχείριση της εκτέλεσης των εικονικών πόρων
- ✓ Διαχείριση των σφαλμάτων των εικονικών πόρων
- ✓ Διεπαφή διαχείρισης πολιτικής
- ✓ Διεπαφή διαχείρισης NFP

- Vi-Vnfm (VIM – VNFM)

Αυτή η διεπαφή χρησιμοποιείται από τον VNFM για αίτηση ή/και για τον VIM για την αναφορά των χαρακτηριστικών, της διαθεσιμότητας, και την κατάσταση των πόρων της υποδομής

- Κατανομή των αιτημάτων πόρων από τον VNFM
- Διαμόρφωση των εικονικών hardware πόρων και αλλαγή της κατάστασης πληροφοριών
  - Κράτηση των NFVI πόρων και ανάκτηση πληροφοριών
  - Κατανομή/ελευθέρωση των NFVI πόρων
  - Ανταλλαγές των πληροφοριών διαμόρφωσης ανάμεσα στα σημεία αναφοράς, και τα σημεία προώθησης στον VNFM για πληροφορίες, για τις οποίες ο VNFM έχει εγγραφεί (π.χ. συμβάντα, αποτελέσματα μετρήσεων και αρχεία χρήσης όσον αφορά τους πόρους NFVI που χρησιμοποιούνται από τη λειτουργία VNF)

Η Vi – Vnfm διεπαφή υποστηρίζει της παρακάτω λειτουργίες:

- ✓ Διαχείριση εικόνας του VNF software
- ✓ Διαχείριση καταλόγου εικονικών πόρων
- ✓ Διαχείριση εικονικών πόρων
- ✓ Διαχείριση εκτέλεσης εικονικών πόρων
- ✓ Διαχείριση σφαλμάτων εικονικών πόρων

- Ve - Vnfm(VNF/EM – VNFM)

Αυτή η διεπαφή χρησιμοποιείται για ανταλλαγές ανάμεσα στην λειτουργία VNF, το EMS και τον VNFM. Αυτή η διεπαφή μπορεί να χωριστεί σε δύο διεπαφές:

- Ve-Vnfm-em, σημείο αναφοράς ανάμεσα στο EMS και το VNFM.
- Ve-Vnfm-vnf, σημείο αναφοράς ανάμεσα στην λειτουργία VNF και το VNFM.

Αυτά τα σημεία αναφοράς χρησιμοποιούνται για ανταλλαγές ανάμεσα στο VNF/EM και τον VNFM και χρειάζεται να υποστηρίζουν τα παρακάτω:

- Αιτήματα για διαχείριση του κύκλου ζωής της λειτουργίας VNF
- Ανταλλαγή των πληροφοριών διαχείρισης
- Η ανταλλαγή της κατάστασης των πληροφοριών είναι απαραίτητη για την διαχείριση του κύκλου ζωής των υπηρεσιών του δικτύου.

Η Ve-Vnfm διεπαφή υποστηρίζει τις παρακάτω λειτουργίες:

- Διαμόρφωση της λειτουργίας VNF
- Διαχείριση εκτέλεσης της λειτουργίας VNF
- Διαχείριση σφαλμάτων της λειτουργίας VNF

- Or-Vnfm (NFVO – VNFM)

  Αυτή η διεπαφή χρησιμοποιείται για ανταλλαγές ανάμεσα στον NFVO και τον VNFM και πρέπει να υποστηρίζει τα παρακάτω:

  - Αιτήματα που σχετίζονται με τους πόρους π.χ. εξουσιοδότηση, επικύρωση, κράτηση, και κατανομή των VNFMs.
  - Αποστολή πληροφοριών διαμόρφωσης στον διαχειριστή της λειτουργίας VNF, ώστε η λειτουργία VNF να μπορεί να διαμορφωθεί κατάλληλα, για να λειτουργήσει εντός του VNF Forwarding Graph στην υπηρεσία του δικτύου.
  - Συλλογή πληροφοριών κατάστασης από την λειτουργία VNF απαραίτητη για την διαχείριση του κύκλου ζωής της υπηρεσίας του δικτύου.
  - Ο ETSI έχει ορίσει τις παρακάτω ενέργειες που πρέπει να υποστηρίζονται από αυτή την διεπαφή:
    - Εξουσιοδότηση/επικύρωση/κράτηση/ελευθέρωση των NFVI πόρων για την λειτουργία VNF
    - Κατανομή/ελευθέρωση αιτημάτων των NFVI πόρων για τη λειτουργία VNF.
    - Δημιουργία της λειτουργίας VNF
    - Ανάκτηση της λειτουργίας VNF (π.χ. ανάκτηση πληροφορίας)
    - Ενημέρωση της λειτουργίας VNF (π.χ. ενημέρωση διαμόρφωσης)
    - Κλιμάκωση της λειτουργίας VNF
    - Τερματισμός της λειτουργίας VNF
    - Ανάκτηση πακέτων της λειτουργίας VNF

Επιπλέον αυτή η διεπαφή υποστηρίζει την προώθηση των συμβάντων, και άλλες πληροφορίες κατάστασης για τη λειτουργία VNF που μπορούν να επηρεάσουν την υπηρεσία του δικτύου.

Η Or-Vnfm διεπαφή υποστηρίζει τις παρακάτω λειτουργίες:

- Διαχείριση πακέτων της λειτουργίας VNF
- Πραγματοποίηση της λειτουργίας του κύκλου ζωής της VNF
- Διαχείριση του κύκλου ζωής της λειτουργίας VNF
- Ειδοποίηση αλλαγής του κύκλου ζωής της λειτουργίας VNF
- Διαχείριση εκτέλεσης της λειτουργίας VNF
- Διαχείριση σφαλμάτων της λειτουργίας VNF
- Διαχείριση των εικονικών πόρων
- Διαχείριση πολιτικής της διεπαφής

- Se-Ma (catalogs/Repositories και Orchestration)

Οι υπηρεσίες, η λειτουργία VNF και η περιγραφή των σχημάτων των υποδομών παρέχουν πληροφορίες σχετικά με το πρότυπο ανάπτυξης λειτουργίας VNF, το VNF Forwarding Graph, τις πληροφορίες σχετικά με τις υπηρεσίες και τα πρότυπα πληροφοριών των NFV υποδομών. Αυτά τα πρότυπα/περιγραφές χρησιμοποιούνται ανάμεσα στην διαχείριση και την οργάνωση της NFV. Τα λειτουργικά τμήματα της διαχείρισης και της οργάνωσης της NFV χειρίζονται τις πληροφορίες που υπάρχουν στα πρότυπα/περιγραφές και μπορεί να εκθέσουν πληροφορίες των εφαρμοστέων λειτουργικών τμημάτων, όπως απαιτείται.

- Re-Sa (Repositories και Service Assurance)

Αυτή η διεπαφή χρησιμοποιείται από την διασφάλιση των υπηρεσιών για την πρόσβαση στην υπηρεσία ασφάλειας δεδομένων.

- Ca-Vnfm (Catalogs και VNFM)

Αυτή η διεπαφή χρησιμοποιείται από το VNFM για την διαχείριση του κύκλου ζωής των λειτουργιών VNF.

- Os-Ma (OSS/BSS – NFVM & Orchestration)

Το Os-Ma σημείο αναφοράς χρησιμοποιείται για ‘’ανταλλαγές’’ ανάμεσα στον NFVO και το υπάρχον OSS/BSS σύστημα. Το Os-Ma-nfvo σημείο αναφοράς που προέρχεται από το Os-Ma πρέπει να υποστηρίζει τα παρακάτω:

- Το Network Service Descriptor και τη διαχείριση των πακέτων της λειτουργίας VNF
- Τη διαχείρισης του κύκλου ζωής της εικονικής υπηρεσίας δικτύου
  - Συγκεκριμενοποίηση της εικονικής υπηρεσίας δικτύου
  - Ενημέρωση της εικονικής υπηρεσίας του δικτύου

- Ανάκτηση της εικονικής υπηρεσίας του δικτύου
- Κλιμάκωση της εικονικής υπηρεσίας του δικτύου
- Τερματισμός της εικονικής υπηρεσίας του δικτύου

❖ Τη διαχείριση του κύκλου ζωής της λειτουργίας VNF: Ο NFVO πιστοποιεί τον VNFM και προωθεί τα αιτήματα

❖ Τη διαχείριση και/ή την εφαρμογή της πολιτικής για τις εικονικές υπηρεσίες του δικτύου, τις λειτουργίες VNF και τους πόρους NFVI (για έλεγχο εξουσιοδότησης/πρόσβασης, κράτηση/τοποθέτηση/κατανομή πόρων κτλ.)

❖ Αναζήτηση πληροφοριών για τις εικονικές υπηρεσίες του δικτύου και των λειτουργιών VNF από το OSS/BSS.

❖ Προώθηση των συμβάντων, των αρχείων υπολογισμών και χρήσης, και των αποτελεσμάτων μέτρησης επιδόσεων όσον αφορά τις εικονικές υπηρεσίες του δικτύου, τις λειτουργίες VNF και τους πόρους NFVI στο OSS/BSS, καθώς και πληροφορίες σχετικά με τις ενώσεις μεταξύ αυτών των διεπαφών και των NFVI πόρων πχ. ο αριθμός των εικονικών μηχανών που χρησιμοποιούνται από κάποια λειτουργία VNF.

Η Os-Ma διεπαφή υποστηρίζει τις παρακάτω λειτουργίες:

- Διεπαφές των Υπηρεσιών Δικτύου
- Διαχείριση των πακέτων της λειτουργίας VNF
- Διαχείριση της εικόνας του VNF software
- Διαχείριση του κύκλου ζωής της λειτουργίας VNF
- Γνωστοποίηση αλλαγών του κύκλου ζωής της λειτουργίας VNF
- Διεπαφή διαχείρισης της πολιτικής

Όλες οι παρακάτω διεπαφές δεν έχουν οριστεί ακόμα από το ETSI αλλά είναι πιθανόν οριστούν στο μέλλον.

- Or-Sa (NFVO – Service Assurance)
- Or-EMS (NFVO – Element Management Systems)
- Ve-Sa (Virtual Element – Service Assurance)
- Vnfm- Sa(VNFM – Service Assurance)
- Vi-Sa (VIM – Service Assurance)
- Nfvi-Sa (Network Function – Service Assurance)
- Or-Nf (Orchestrator – Network function)
- Or-Sdnc (Orchestrator – SDN Controller)
- Sdnc-Nf (SDN Controller – Network Function)
- Vi-Sdnc (VIM to SDN Controller)
- Sdnc-Net (SDN Controller- Networks)
- Dsc-Nf (Domain Specific Controller – Network Functions)
- Sdnc-Sa (SDN Controller – Service Assurance)
- Cf-N (Collection Function – NFVI)

- Cf-Sa (Collection Function – Service Assurance)

11. OpenFlow: Τι είναι;

Το OpenFlow είναι ένα ανοικτό πρωτόκολλο επικοινωνίας που δρα στο Layer 2 του μοντέλου του OSI και παρέχει πρόσβαση στο επίπεδο προώθησης ενός router ή ενός switch στο δίκτυο. Το OpenFlow επιτρέπει στη διαδρομή των πακέτων δεδομένων εντός του δικτύου των switches, να καθοριστεί από το λογισμικό που εκτελείται σε τουλάχιστον δύο routers. Το OpenFlow έχει σχεδιαστεί για τη διαχείριση της κυκλοφορίας του δικτύου μεταξύ των switches και των routers που μπορεί να είναι διαφορετικά μοντέλα και από διαφορετικούς προμηθευτές. Επιπλέον, χωρίζει τον προγραμματισμό των switches και των routers από το hardware, ώστε να μην χρειάζεται να γίνει καμία ρύθμιση παραμέτρων του hardware και όλο το σύνολο ελέγχου να μπορεί να επιτευχθεί με ευελιξία μέσω του λογισμικού. Με την πάροδο του χρόνου, πολλά SDN πρωτόκολλα πιθανόν να προκύψουν, αλλά προς το παρόν, το OpenFlow είναι η συνήθης SDN γλώσσα που χρησιμοποιούμε. Σε ένα SDN με ένα κεντρικό επίπεδο ελέγχου (control plane), το πρωτόκολλο OpenFlow μεταφέρει το μήνυμα μεταξύ των SDN ελεγκτών και της σχετικής υποδομής δικτύου, φέρνοντας τις εφαρμογές του δικτύου σε λειτουργία. Μέχρι στιγμής, οι πωλητές και οι επιχειρήσεις έχουν επιτύχει ταχεία πρόοδο στην ανάπτυξη των OpenFlow προϊόντων και στο σχεδιασμό στρατηγικών για το δικτύου.

Πώς λειτουργεί;

Σε έναν κλασικό router ή switch, η γρήγορη προώθηση πακέτων (data path) και οι υψηλού επιπέδου αποφάσεις δρομολόγησης (control path) γίνονται με την ίδια συσκευή. Ένα OpenFlow Switch χωρίζει αυτές τις δύο λειτουργίες. Το τμήμα διαδρομής δεδομένων (data path) εξακολουθεί να βρίσκεται στο switch, ενώ οι αποφάσεις δρομολόγησης υψηλού επιπέδου εκτελούνται σε ένα ξεχωριστό ελεγκτή(controller), συνήθως σε έναν τυπικό διακομιστή(server). Το Switch OpenFlow και ο ελεγκτής επικοινωνούν μέσω του πρωτοκόλλου OpenFlow, το οποίο καθορίζει τα μηνύματα, όπως τα πακέτα που λαμβάνονται, το ‘πέταγμα’ των πακέτων, την τροποποίηση forwarding table , και την συλλογή στατιστικών.

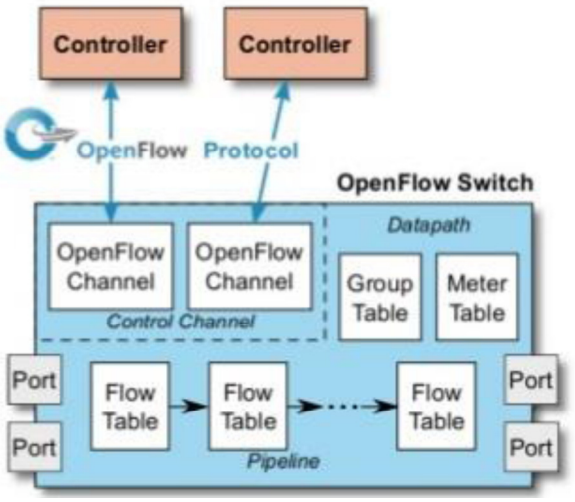
Το μονοπάτι δεδομένων(data path) ενός OpenFlow Switch παρουσιάζει ένα καθαρό πίνακα ροής. Κάθε καταχώρηση στο πίνακα ροής περιέχει ένα σύνολο πεδίων πακέτου για να ταιριάζει, και μια ενέργεια (όπως send-out-port, modify-field, ή drop). Όταν το OpenFlow Switch λαμβάνει ένα πακέτο που δεν έχει ‘δει’ ποτέ πριν, και για το οποίο δεν έχει εγγραφές ροής που ταιριάζουν, στέλνει αυτό το πακέτο στον ελεγκτή. Ο ελεγκτής παίρνει μια απόφαση σχετικά με το πώς να χειριστεί αυτό το πακέτο. Μπορεί να ‘πετάξει’ το πακέτο, ή να προσθέσει μια καταχώρηση ροής κατευθύνοντας το switch για το πώς να προωθήσει παρόμοια πακέτα στο μέλλον.

11.1 Δομικά μέρη Openflow

Τα βασικά δομικά μέρη του Openflow πρωτοκόλλου είναι τα παρακάτω:

- Openflow controller
- Οι Openflow μεταγωγείς που αποτελούνται από:

I. Πόρτες
II. Το ασφαλές κανάλι Openflow
III. Πίνακες ροών



Εικόνα 29: Δομή Openflow

Openflow controller

Το Openflow αποτελεί το μέσω επικοινωνίας μεταξύ ενός controller και του δικτυακού εξοπλισμού μέσω ενός καναλιού. Ένας controller που χρησιμοποιεί το openflow έχει την δυνατότητα να αποστέλλει μηνύματα στο δίκτυο μέσω ενός καναλιού επικοινωνίας ,χωρίς το ίδιο το πρωτόκολλο να μπορεί να καθορίσει την δομή του , ακόμη και παράλληλα με κάποιο άλλο πρωτόκολλο.

Openflow μεταγωγέας

Ένας openflow μεταγωγέας αποτελεί τον εξοπλισμό ο οποίος έχει την δυνατότητα να προσπελάσει τα μηνύματα που του αποστέλλονται από τον controller και αφορούν την διαχείριση των πακέτων. Η διαχείριση βασίζεται σε ένα σύνολο πινάκων, τους flow πίνακες ,τους group πίνακες και τους meter πίνακες. Οι πίνακες αυτοί συμπληρώνονται βάση των μηνυμάτων που λαμβάνονται από τον controller.

Οι μεταγωγείς αποτελούνται από δύο κατηγορίες:

- Openflow-only μεταγωγείς: οι οποίοι έχουν την δυνατότητα να διαχειριστούν πακέτα μόνο βάση του openflow πρωτοκόλλου
- Υβριδικοί μεταγωγείς: οι οποίοι αποτελούν υβριδικό εξοπλισμό με την δυνατότητα να υποστηρίξουν τόσο την openflow μεταγωγή όσο και την παραδοσιακή μεταγωγή με την χρήση του Ethernet πρωτοκόλλου.

Οι πόρτες σε έναν Openflow μεταγωγέα λειτουργούν με παρόμοιο τρόπο όπως σε κάθε μεταγωγέα. Τα πακέτα εισέρχονται σε μία πόρτα εισόδου , επεξεργάζονται από τον μεταγωγέα και μεταφέρονται σε μία πόρτα εξόδου. Παρόμοια , μία πόρτα μπορεί να προστεθεί, να αλλάξει ή να αφαιρεθεί. Καθώς μπορεί να υπάρχουν εγγραφές σε openflow πίνακες που κατευθύνουν πακέτα σε πόρτες που έχουν αφαιρεθεί , είναι σημαντικό να ενημερώνεται ο controller για κάθε αλλαγή στην κατάσταση των πορτών ώστε αντίστοιχα να ενημερώνονται και οι πίνακες.

Το Openflow ορίζει τρία είδη πορτών τα οποία θα πρέπει όλα να υποστηρίζονται από έναν openflow μεταγωγέα:

I. Φυσική πόρτα: Μία φυσική πόρτα αναφέρεται σε μία πόρτα του δικτυακού εξοπλισμού. Όταν στο υλικό υποστηρίζονται περισσότεροι του ενός εικονοποιημένου μεταγωγέα , μία openflow φυσική πόρτα αποτελεί ένα μέρος μίας πόρτας του εξοπλισμού αντίστοιχα με την λειτουργία των VLANs
II. Λογική πόρτα: Οι λογικές πόρτες δεν αντιστοιχούν στις φυσικές του εξοπλισμού. Αντίστοιχα με οποιοδήποτε λογική διεπαφή οποιουδήποτε δικτυακού εξοπλισμού μπορούν να αναφέρονται σε tunnel , loopback κλπ διεπαφές. Το πως αντιστοιχίζονται σε φυσικές πόρτες είναι ανεξάρτητο με το Openflow. Το openflow τις αντιμετωπίζει παρόμοια με τις φυσικές.
III. Κλειστές (reserved) πόρτες: Αποτελεί ειδική κατηγορία πορτών όπου χρησιμοποιούνται για εσωτερική διαχείριση πακέτων. Χωρίζονται σε 5 ‘’υποχρεωτικές’’ πόρτες:
    - ALL: αναφέρεται σε όλες τις πόρτες που μπορούν να χρησιμοποιηθούν σαν εξωτερικές πόρτες. Δηλαδή όλες οι πόρτες εκτός της εισερχόμενης πόρτας και των πορτών που έχουν αποκλειστεί από την προώθηση πακέτων
    - CONTROLLER: είναι η πόρτα όπου ο switch επικοινωνεί μέσω του ασφαλούς καναλιού με τον controller.
    - TABLE: είναι η εισερχόμενη πόρτα σε ένα pipeline
    - IN_PORT: είναι μία εισερχόμενη και μια εξερχόμενη πόρτα ταυτόχρονα. Χρησιμοποιείται όταν κάποιο πακέτο πρέπει να επιστρέψει από την πόρτα που προήλθε
    - ANY: μπορεί να αποτελέσει μια εισερχόμενη , μια εξερχόμενη ή μια οποιαδήποτε πόρτα. Χρησιμοποιείται όταν το Openflow απαιτεί περιγραφή πόρτας και δεν υπάρχει αντίστοιχη κατηγορία.

Παράλληλα υπάρχουν και οι ‘’προαιρετικές’’ πόρτες:

- LOCAL: οι εσωτερικές και οι εξωτερικές πόρτες του εξοπλισμού για την διαχείριση του μεταγωγέα
- NORMAL: Αφορούν τους υβριδικούς μεταγωγείς και αναφέρονται στις εξερχόμενες πόρτες κατά την μετάβαση από Openflow στην κανονική λειτουργία του εξοπλισμού
- FLOOD: παρόμοιες με τις NORMAL πόρτες, αφορούν τους υβριδικούς μεταγωγείς. Χρησιμοποιούνται για όταν τα πακέτα πρέπει να αποσταλούν σε όλες τις πόρτες (flooded) μέσω της κανονικής λειτουργίας του εξοπλισμού.

Ασφαλές κανάλι

Για την επικοινωνία μεταξύ του controller και του εξοπλισμού απαιτείται ένα κανάλι όπου θα μεταφέρονται όλα τα μηνύματα και τα πακέτα που αφορούν την λειτουργία του δικτύου. Το κανάλι δημιουργείται μέσω της TCP σύνδεσης. Παρόλο που δεν απαιτείται να είναι κρυπτογραφημένη η επικοινωνία συνήθως κρυπτογραφείται μέσω του TLS πρωτοκόλλου.

Με την δημιουργία της TCP επικοινωνίας , ο controller και ο μεταγωγέας διαπραγματεύονται την έκδοση του openflow που θα χρησιμοποιήσουν. Κάθε πλευρά αναφέρει την νεότερη έκδοση που υποστηρίζει και χρησιμοποιείται η νεότερη που υποστηρίζουν και οι δύο πλευρές. Χρησιμοποιείται η διαδικασία ECHO REQUEST /REPLY για τον έλεγχο της ποιότητας της σύνδεσης.

Σε περίπτωση που δεν υποστηρίζεται καμία κοινή έκδοση , αποστέλλεται μήνυμα σφάλματος και η σύνδεση τερματίζει. Αντίστοιχα σε περίπτωση αποσύνδεσης , ο μεταγωγέας εισέρχεται σε μία από τις παρακάτω καταστάσεις:

- Fail Secure Mode: όπου δεν πραγματοποιούνται προσπάθειες επικοινωνίας με τον controller από την πλευρά του μεταγωγέα. Χρησιμοποιεί τις εγγραφές στους υπάρχοντες πίνακες για την διαχείριση των πακέτων μέχρι να λήξει η ισχύ τους.
- Fail Standalone Mode: Ο μεταγωγέας επανέρχεται στην κανονική του λειτουργία μία επιλογή που αφορά αποκλειστικά τους υβριδικούς μεταγωγείς

Εφόσον επανασυνδεθεί ο εξοπλισμός με τον controller , είτε ο εξοπλισμός μπορεί να ζητήσει την ανανέωση των υπαρχόντων εγγραφών ,είτε ο ίδιος ο controller να διαγράψει και να ανανεώσει τις εγγραφές ,καθώς η διατήρηση τους εγκυμονεί κινδύνους για την λειτουργία του δικτύου.

Η αξιοπιστία της αποστολής και λήψης των Openflow μηνυμάτων βασίζεται αποκλειστικά στον μηχανισμό TLS και στην TCP σύνδεση καθώς δεν υφίσταται κάποια λειτουργία επιβεβαίωσης λήψης καθώς και ούτε διατήρησης της σωστής σειράς.

Openflow πίνακες

Στόχος της ανταλλαγής μηνυμάτων μεταξύ του Controller και του switch είναι η δημιουργία openflow πινάκων, όπου βάση των εγγραφών τους θα διαχειρίζονται τα πακέτα οι switches.

12. Cloud Computing

Τι είναι το cloud computing;

Το cloud computing είναι η αποθήκευση και η πρόσβαση σε δεδομένα και προγράμματα μέσω του Internet αντί του σκληρού δίσκου ενός υπολογιστή. Ο όρος σύννεφο(cloud) είναι μόνο μια μεταφορά για τον κόσμο του διαδικτύου. Με πολύ απλά λόγια το «cloud computing» είναι μία δομή, με την οποία μας δίνεται η δυνατότητα να έχουμε πρόσβαση και να χρησιμοποιούμε web εφαρμογές χωρίς να τις διαθέτουμε στον υπολογιστή μας ή σε κάποια άλλη συσκευή που είναι διασυνδεδεμένη με το ίντερνετ. Σε αυτή τη δομή η εφαρμογή βρίσκεται σε ένα server και εμείς τη χρησιμοποιούμε χωρίς να χρειάζεται να την εγκαταστήσουμε στον υπολογιστή μας.

Πλεονεκτήματα cloud computing

•Οικονομία. Αυτό είναι από τα πιο βασικά πλεονεκτήματα του cloud computing. Το κόστος που μπορεί να έχει ένα λογισμικό ίσως να είναι απαγορευτικό για μία μικρή εταιρία. Με το «cloud» τα δεδομένα αυτά αλλάζουν καθώς η εταιρία δεν πληρώνει την εφαρμογή αλλά πληρώνει την χρήση της. Συνήθως σε cloud δίκτυα υπάρχουν πολλές δυνατότητες και «πακέτα» για την πληρωμή της χρήσης κάποιας εφαρμογής.

•Μεγάλος αποθηκευτικός χώρος. Η αποθήκευση των διαφόρων πληροφοριών είναι θέμα υψίστης σημασίας. Με το cloud computing έχουμε συνήθως όσο αποθηκευτικό χώρο θα χρειαστούμε.

•Πρόσβαση από οποιαδήποτε συσκευή διαθέτει σύνδεση στο ίντερνετ.

•Πολύ μεγάλη ευελιξία.

Μειονεκτήματα του cloud computing

- Ασφάλεια δεδομένων: Στο παρελθόν έχουν γίνει επιθέσεις από χακερς οι οποίοι πολλές φορές έχουν καταφέρει να διαγράψουν ή να αλλάξουν δεδομένα. Παρόλες τις μεθόδους ασφαλείας που προσφέρουν οι πάροχοι οι επιθέσεις είναι δύσκολο να αποφθεχθούν
- Αυξημένη πολυπλοκότητα: Αυτό συμβαίνει όταν έχουμε μία εφαρμογή αποθηκευμένη κάπου τοπικά, σε ένα δικό μας web server και προσπαθούμε να την κάνουμε να επικοινωνήσει με μία άλλη στο cloud. Τα πράγματα εκεί γίνονται αρκετά περίπλοκα και πολλές φορές η λύση εκτός ότι δεν είναι προφανής , αποτυγχάνει
- Κόστος μεταβίβασης: Η χρονική καθυστέρηση για την αλλαγή μιας φυσικής εφαρμογής σε ηλεκτρονική μορφή αποτελεί σημαντικό πρόβλημα και μπορεί να συντελέσει ακόμα και στο να μην γίνει η χρήση του cloud
- Σύνδεση στον ίντερνετ: Σε περίπτωση που δεν υπάρχει ίντερνετ (πχ. λόγω τεχνικού προβλήματος) ο χρήστης δεν έχει την δυνατότητα χρήσης του Cloud

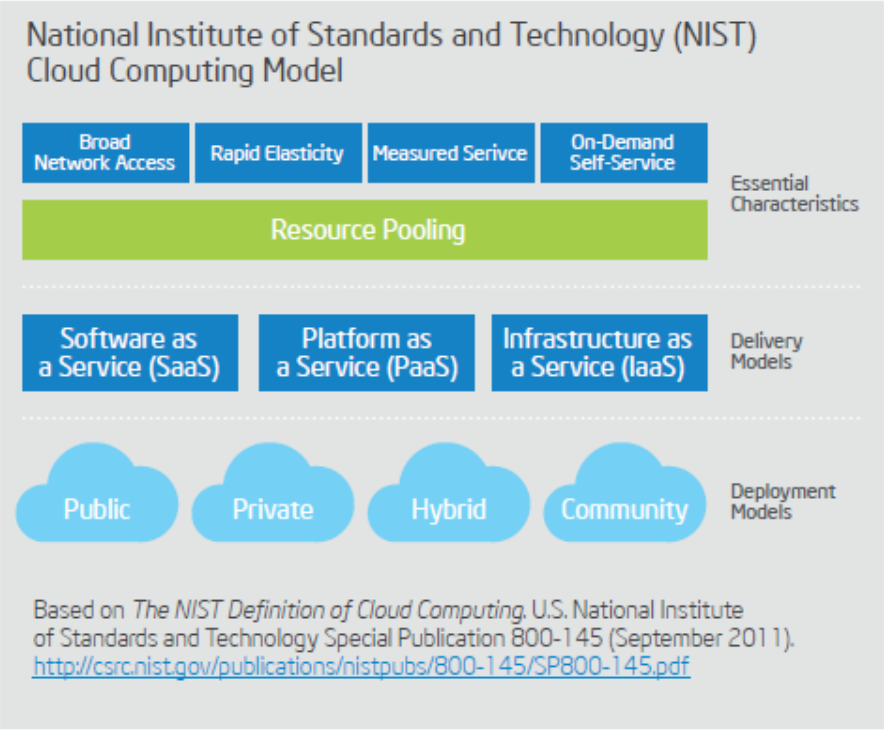
Ο όρος «Virtualization» στο cloud computing

Η τεχνολογία virtualization είναι η κινητήριος δύναμη του cloud computing. Στην τεχνολογία αυτή μπορούμε να χωρίσουμε ένα φυσικό hardware, ένα webserver , σε πολλά κομμάτια που το κάθε ένα τρέχει το δικό του λειτουργικό. Έτσι επιτυγχάνεται άριστη λειτουργικότητα , ταχύτητα και απόλυτη αξιοποίηση των πόρων του συστήματος. Αυτά τα κομμάτια είναι σαν εικονικοί servers και ονομάζονται εικονικές μηχανές (VMs). Ο cloud συνδέεται με την έννοια του virtualization γιατί ουσιαστικά είναι ένα σύνολο συνδεδεμένων εικονικών μηχανών. Αυτός είναι ο λόγος που τα cloud δίκτυα έχουν τόσες πολλές δυνατότητες και επεκτασιμότητα διότι μοιράζονται τους πόρους των διάφορων συνδεδεμένων εικονικών μηχανών.

Δυνατότητες υψηλής απόδοσης του Cloud

Ορισμός του Cloud Computing σύμφωνα με το US NIST

Το Cloud Computing είναι ένα μοντέλο που επιτρέπει την εύκολη, on-demand (τη στιγμή που ζητείται) πρόσβαση μέσω δικτύου σε ένα “κοινό ταμείο” από παραμετροποιήσιμους υπολογιστικούς πόρους (π.χ. Δίκτυα, servers, αποθηκευτικό χώρο, εφαρμογές και υπηρεσίες) οι οποίοι μπορούν πολύ εύκολα να παρακολουθηθούν και να αποδοθούν με πολύ μικρή παρέμβαση της διαχείρισης, ή αλληλεπίδρασης από τον πάροχο των υπηρεσιών.



Εικόνα 30: Cloud computing (NIST)

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) προσδιορίζει αρκετά από τα βασικά χαρακτηριστικά της υψηλής απόδοσης του ιδιωτικού cloud:

• Αυτοεξυπηρέτηση κατά παραγγελία - Οι χρήστες μπορούν αυτόματα να έχουν τους δικούς τους υπολογιστικούς πόρους που χρειάζονται, χωρίς να απαιτείται ανθρώπινη παρέμβαση, συνήθως μέσω μιας διαδραστικής πύλης που τους επιτρέπει να διαμορφώσουν και να διαχειρίζονται αυτές τις υπηρεσίες.

• Ευρεία πρόσβαση στο δίκτυο - Οι πόροι είναι διαθέσιμοι μέσω του δικτύου και μπορούν να προσεγγιστούν από πολλές συσκευές, συμπεριλαμβανομένων των έξυπνων τηλεφώνων, τα tablets, τους φορητούς υπολογιστές κτλ.

• Ταχεία ελαστικότητα - Οι πόροι μπορούν να είναι γρήγοροι και ελαστικοί ή να μειώνονται ανάλογα με τη ζήτηση. Η κλιμάκωση είναι αυτόματη για τους χρήστες.

• Μέτρηση χρήσης υπηρεσίας - Η χρήση μιας υπηρεσίας μετράται και μπορεί να παρακολουθείται, να ελέγχεται και να αναφέρεται για διαύγεια.

• Συγκέντρωση, τοποθεσία-διαφάνεια πόρων για πολλαπλούς χρήστες – Επεξεργαστικοί πόροι, αποθηκευτικοί πόροι και πόροι δικτύωσης συγκεντρώνονται για να εξυπηρετούν πολλαπλές ομάδες χρηστών (ενοικιαστές) με διαφορετικούς φυσικούς και εικονικούς πόρους που μπορούν να ανατεθούν δυναμικά και να ανακαθοριστούν σύμφωνα με τη ζήτηση των χρηστών. Επειδή οι χρήστες γενικά δεν

έχουν τον έλεγχο της ακριβούς θέσης των πόρων, υπάρχει μια αίσθηση ανεξαρτησίας της τοποθεσίας, ωστόσο η τοποθεσία μπορεί να καθορίζεται σε υψηλότερο επίπεδο αφαιρετικότητας (χώρα, κράτος, κέντρο δεδομένων).

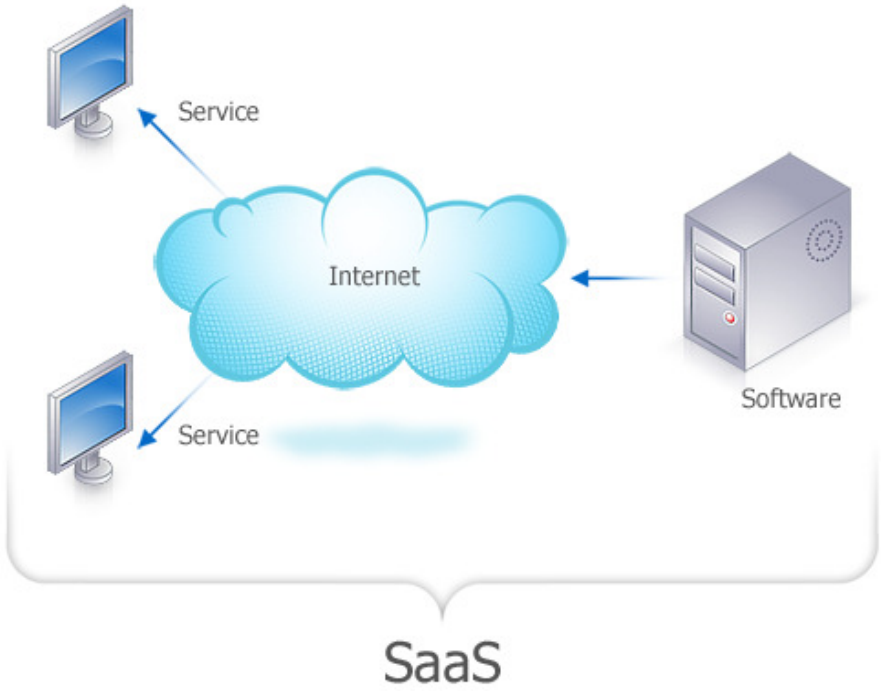
Εκτός από αυτές τις δυνατότητες, το NIST ορίζει επίσης τα στρώματα παροχής υπηρεσιών και τα μοντέλα ανάπτυξης. Τα μοντέλα ανάπτυξης περιλαμβάνουν ιδιωτικά, δημόσια, κοινοτικά (community) και υβριδικά clouds. Τα επίπεδα υπηρεσιών για καθένα από αυτά τα μοντέλα παράδοσης περιλαμβάνουν:

Infrastructure as a service (IaaS)

Η υποδομή σαν υπηρεσία (IaaS) παρέχει στους χρήστες φυσικούς υπολογιστικούς πόρους, τοποθεσία, διαμέριση δεδομένων, κλιμάκωση, ασφάλεια, δημιουργία αντιγράφων ασφαλείας κλπ.. Η IaaS επιτρέπει στους χρήστες να αυτοεξυπηρετούνται από αυτούς τους πόρους προκειμένου να τρέξουν πλατφόρμες και εφαρμογές. Σε αυτό το μοντέλο, ο χρήστης του cloud επικαλύπτει και συντηρεί τα λειτουργικά συστήματα και το λογισμικό της εφαρμογής. Οι πάροχοι των cloud συνήθως χρεώνουν τις υπηρεσίες IaaS με βάση την υπολογιστική χρησιμότητα: το κόστος αντικατοπτρίζει το ποσό των πόρων που διατίθενται και καταναλώνονται.

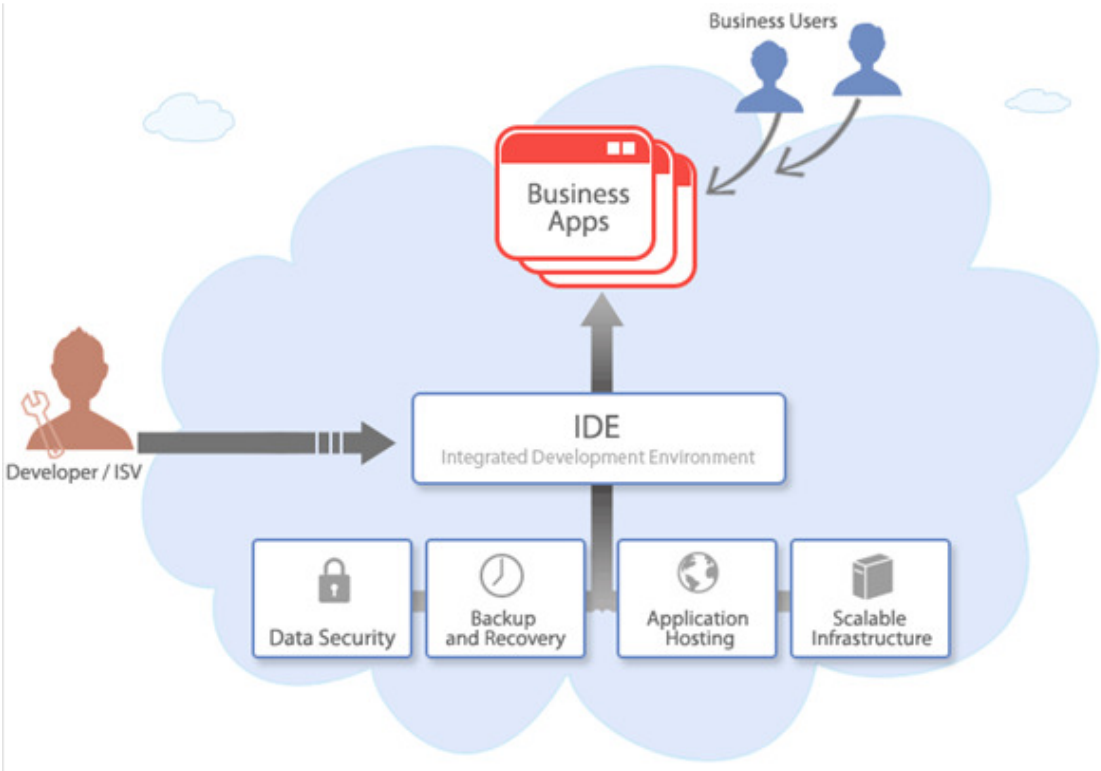
Software as Service (SasS)

Σε αυτό τον τύπο υπάρχει ένα application το οποίο βρίσκεται σε ένα cloud server και ο χρήστης μπορεί να έχει πρόσβαση σε αυτό μέσω μίας απλή σύνδεσης στο ίντερνετ. Το software αυτό ανήκει σε κάποιον κατασκευή και ο χρήστης το πληρώνει ανάλογα με την χρήση που του κάνει και τους πόρους που χρειάζεται. Το βασικό πλεονέκτημα του μοντέλου «software as service» είναι ότι ο κατασκευαστής αναλαμβάνει τα έξοδα συντήρησης του software καθώς και τη φιλοξενία του σε κάποιον cloud server. Ο χρήστης πληρώνει μόνο την χρήση που κάνει (αν και υπάρχουν και cloud applications που είναι δωρεάν). Επίσης το μοντέλο SasS είναι δημιουργημένο με βασικό γνώμονα τη σωστή λειτουργία του software με χρήση του browser. Όσον αφορά την ασφάλεια των διαφόρων εφαρμογών, συνήθως χρησιμοποιείται SSL (Secure Sockets Layer) το οποίο είναι παγκοσμίως αναγνωρισμένο. Έτσι , οι χρήστες μπορούν με ασφάλεια να χρησιμοποιήσουν το cloud application.



Εικόνα 31: SaaS

Platform as Service (PaaS)



Εικόνα 32: PaaS

Αυτό το μοντέλο μοιάζει πολύ με το προηγούμενο. Το βασικό του στοιχείο είναι ότι παρέχει την πλατφόρμα την οποία χρησιμοποιεί ένας χρήστης για να δημιουργήσει

κάτι, χρησιμοποιώντας γλώσσες προγραμματισμού, υπηρεσίες, βιβλιοθήκες και άλλα εργαλεία προγραμματισμού, χωρίς να εγκαταστήσει τίποτα. Το «platform as service» μοντέλο χρησιμοποιείται πιο πολύ για δημιουργία web interfaces, web εφαρμογών κλπ. Ένα σημαντικό πρόβλημα που υπάρχει με αυτό το μοντέλο είναι ότι αυτή η εφαρμογή που δημιουργούμε βασίζεται σε ένα συγκεκριμένο framework και υπάρχει πιθανότητα αν θελήσουμε να την μεταφέρουμε σε άλλο παροχέα cloud υπηρεσιών αυτή να μη λειτουργεί σωστά.

Μοντέλα παράδοσης του cloud

Public Cloud

Αυτό το μοντέλο δημιουργείται από εκατοντάδες web servers που τρέχουν και πάρα πολλά datacenters σε διάφορα σημεία του πλανήτη. Αυτό έχει ως αποτέλεσμα να μπορεί κάποιος να χρησιμοποιήσει μία υπηρεσία διαλέγοντας την τοποθεσία που θα βρίσκεται η εφαρμογή. Κοινώς διαλέγει το datacenter που είναι πιο κοντά του. Εταιρίες που προσφέρουν το public cloud είναι οι: Google, Amazon, Rackspace κλπ. Αυτή η public εφαρμογή του cloud υποστηρίζεται από εταιρίες πολύ εύρωστες οικονομικά διότι η ανάπτυξη και συντήρηση των webserver και datacenter παγκοσμίως κοστίζει πολλά χρήματα. Οι πάροχοι cloud υπηρεσιών προσφέρουν υπηρεσίες σε πολλαπλές επιχειρήσεις, ακαδημαϊκά ιδρύματα, κυβερνητικούς οργανισμούς και άλλους οργανισμούς με πρόσβαση μέσω του ίντερνετ.

Private Cloud

Αυτό το είδος της cloud τεχνολογίας εφαρμόζεται μέσα σε οργανισμούς-εταιρίες όπου δημιουργείται ένα cloud δίκτυο το οποίο όμως βρίσκεται στα όρια του οργανισμού αυτού. Τα ιδιωτικά clouds μπορούν να λειτουργούν εντός ή εκτός των εγκαταστάσεων και βρίσκονται πίσω από το τείχος προστασίας της εταιρείας. Το δίκτυο αυτό δημιουργείται κατά παραγγελία με βάση τις ανάγκες του οργανισμού.

Hybrid Cloud

Τα υβριδικά clouds συνδυάζουν δύο μοντέλα παράδοσης (για παράδειγμα, ιδιωτικά και δημόσια) και παραμένουν μοναδικά ως οντότητες αλλά δεσμεύονται μαζί από την τεχνολογία που επιτρέπει φορητότητα στα δεδομένα και την εφαρμογή. Το Cloudbursting είναι ένα παράδειγμα ενός τρόπου όπου οι επιχειρήσεις χρησιμοποιούν υβριδικά σύννεφα για να εξισορροπήσουν τα φορτία κατά τη διάρκεια περιόδων αιχμής ζήτησης.

Community Cloud

Η υποδομή του Cloud παρέχεται μόνο για αποκλειστική χρήση από μια συγκεκριμένη κοινότητα χρηστών, από οργανισμούς με κοινές απαιτήσεις πληροφορικής όπως είναι η ασφάλεια, η πολιτική και η συμμόρφωση.

Επίλογος

Στην παρούσα εργασία παρουσιάστηκαν ο τρόπος λειτουργίας και η δομή του NFV και πολλές από τις τεχνολογίες που εισήλθαν με την εικονοποίηση. Η τεχνολογία προχωρά με τεράστιους ρυθμούς επομένως αυτές οι τεχνολογίες αλλάζουν για να βελτιωθεί η απόδοση τους ή αντικαθίστανται από άλλες.

13. Ακρωνύμια

AER - Application Engineered Routing

API - Application Programming Interface

BGP - Border Gateway Protocol

BIOS - Basic Input/Output System

BSS - Business support system

CAPEX - Capital expenditures

CLI - Command Line Interface

CPE - Customer Premise Equipment

DDoS - Distributed Denial of Service

DMZ - Demilitarized zone

ECMP - Equal-Cost Multi-Path routing

EMS - Element Management System

ETSI - European Telecommunications Standards Institute

FEC - Forwarding Equivalence Class

FIB - Forwarding information base

FRR - Fast Reroute

HPE - Hewlett Packard Enterprise

IaaS - Infrastructure as a Service

IBN - Intent-Based Networking

IETF - Internet Engineering Task Force

IGP - Interior Gateway Protocol

IPS - Intrusion Prevention System

IPSec - IP Security

IS-IS - Intermediate System to Intermediate System --routing protocol

KPI - Key Performance Indicator

LDP - Label Distribution Protocol

LER - Label Edge Router

LSP - Label Switched Path

LSR - Link-state routing protocol

MPLS - MultiProtocol Labeling Switching

NETCONF - Network Configuration Protocol

NFV - Network functions virtualization

NIC - Network Interface Card

NIST - National Institute of Standards and Technology

OPEX - Operating expenses

OSPF - Open Shortest Path First --routing protocol

OSS - Operations support system

PaaS - Platform as Service

PBTS - Policy-based tunnel selection

PCE - Path computation element

PLR - Point of Local Repair

PNF - Physical network function

RAN - Radio Access Network

RIB - Routing information base

RSVP - Resource Reservation Protocol

SasS - Software as Service

SDN - Software Defined Networking

SID - System identification number

SLA - Service Level Agreement

SR - Segment Routing

SRLG - Shared Risk Link Groups

TC - Tunnel Class

TE - Traffic Engineering

TLS - Transport Layer Security

UEFI - Unified Extensible Firmware Interface

VIM - Virtual Infrastructure Management

VM - Virtual Machine

VNF - Virtual network function

VNFC - VNF Component

VNF-FG - VNF Forwarding Graph

VPLS - Virtual Private LAN Service

VPN - Virtual Private Network

VPN - Virtual Private Network

WAN - Wide Area Network

14. Πηγές

NFV:

1) Network Functions Virtualization For Dummies®, Hewlett Packard Enterprise Special Edition
2) NFV Infrastructure: Competitive Dynamics and Solution Assessments
3) Network Functions Virtualization! Challenges and solutions strategic WHITE PAPER
4) Cloud Computing for Telecom Network Function Virtualization (NfV)HUAWEI TECHNOLOGIES CO., LTD.

NFV SECURITY:

1) Providing security in NFV challenges and opportunities strategic WHITE PAPER | NFV INSIGHTS SERIES
2) **http://resources.infosecinstitute.com/virtualization-security-2/**
3) **https://www.juniper.net/techpubs/en_US/learn-about/LA_SecurityVirtualization.pdf**
4) **https://www.sdxcentral.com/articles/news/ericsson-offers-nfvi-platform-modular-components/2016/11/**
5) **http://www.telecomasia.net/content/ericsson-unveils-verified-nfv-infra-solution**
6) Learn About Security Virtualization 2016 by Juniper Networks

INTENT-BASED NETWORKING:

1) SDN-NFV Reference Architecture, Verizon Network Infrastructure Planning
2) **http://resources.solarwinds.com/intent-based-networking-not-an-option-but-a-must-for-sdn/**

SDN SECURITY:

1) SDN-NFV Reference Architecture, Verizon Network Infrastructure Planning
2) **http://www.computerweekly.com/feature/How-to-secure-the-SDN-infrastructure**

Segment routing:

1) Introduction to Segment Routing: Cisco ASR 9000 Series Aggregation Services Router Segment Routing Configuration Guide
2) Making networks sdn-ready with segment routing, HEAVY READING JANUARY 2017 , Cisco
3) SDN-NFV Reference Architecture, Verizon Network Infrastructure Planning

Openflow:

1) OpenFlow Switch Specification Version 1.3.0 (Wire Protocol 0x04) June 25, 2012 : **https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf**

Cloud Computing:

1) Intel IT Center Planning Guide | Virtualization and Cloud Computing
2) **http://www.pcmag.com/article2/0,2817,2372163,00.asp**
3) **https://www.ibm.com/blogs/cloud-computing/2014/02/how-does-cloud-computing-work/**
4) **http://www.moneycrashers.com/cloud-computing-basics/**
5) **https://www.ibm.com/blogs/cloud-computing/2014/02/cloud-computing-basics/**
6) Cloud Computing FOR DUMmIES
7) **https://en.wikipedia.org/wiki/Cloud_computing#Infrastructure_as_a_service_.28IaaS.29**
8) Link φωτογραφίας: **http://c.teamwox.com/articles/2010/4/SaaS_pic.png**
9) Link φωτογραφίας: http://www.zoho.com/creator/images/subpages/paas.gif