ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εικονικοποίηση του Evolved Packet Core (EPC) σε Υπολογιστικό Νέφος

Ιωάννης - Κωνσταντίνος - Σαββίδης

Επιβλέπων: **Ευστάθιος Χατζηευθυμιάδης,** Αναπληρωτής Καθηγητής

ΑΘΗΝΑ

ΝΟΕΜΒΡΙΟΣ 2015

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εικονικοποίηση του Evolved Packet Core (EPC) σε Υπολογιστικό Νέφος

Ιωάννης Κ. Σαββίδης
Α.Μ.: 1115200800248

ΕΠΙΒΛΕΠΟΝΤΕΣ: Ευστάθιος Χατζηευθυμιάδης, Αναπληρωτής Καθηγητής

ΠΕΡΙΛΗΨΗ

Στη παρούσα πτυχιακή εργασία θα αποπειραθούμε να μελετήσουμε τους μηχανισμούς/περιορισμούς ασφαλείας ανα χρήστη στις υπηρεσίες τεχνολογιών cloud computing (υπολογιστικής νέφους) καθώς και την εικονικοποίηση του Evolved Packet Core (EPC) σε υπολογιστικό νέφος.

Χάριν πληρότητας, θα χωριστεί σε τέσσερις ενότητες. Η πρώτη ενότητα θα περιλαμβάνει μια εισαγωγή στην οποία θα περιγράφονται βασικές έννοιες σχετικές με το αντικείμενο, καθώς και παραδοχές που κάναμε καθ'όλη τη διάρκεια της εκπόνησης της εργασίας αυτής.

Η δεύτερη ενότητα θα περιλαμβάνει μια γενική εισαγωγή στη τεχνολογία cloud, και κάποιες θεμελιώδεις αρχές που εδραιώθηκαν από το ETSI για την χρήση cloud σε EPC περιβάλλον.

Στην τρίτη ενότητα, θα επιχειρήσουμε να σχεδιάσουμε μια αρχιτεκτονική cloud, η οποία θα περιγράφει τη πορεία ενός πακέτου δεδομένων από ένα σταθερό σημείο σε ένα άλλο σταθερό σημείο και εκεί παρεμβάλλεται το cloud. Θα περιγράψουμε μια αρχιτεκτονική, η οποία μπορεί να εγγυηθεί πως ότι μπαίνει μέσα στο cloud κρυπτογραφημένο, θα μπορεί να βγαίνει κιόλας πάλι κρυπτογραφημένο.

Στην τέταρτη και τελευταία ενότητα, θα παρουσιάσουμε κάποια συμπεράσματα στα οποία καταλήξαμε κατόπιν της έρευνας και της παρουσίασης που προηγήθηκε.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Cloud στις Τηλεπικοινωνίες

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: μηχανισμοί/περιορισμοί ασφαλείας, cloud, EPC, κρυπτογραφία

ABSTRACT

On this thesis paper, we will make an attempt to study the security mechanisms/constraints per subscriber on the cloud computing services as well as the virtualization of Evolved Packet Core (EPC) in cloud computing.

Just to make this presentation complete, this paper will be divided into four parts. The first part will include an introduction, in which basic subject-related concepts will be described, as well as admissions that were made while writing this paper.

The second part will include a general introduction to the concept of cloud technology and some fundamental principles for using cloud in a EPC environment, as those were established by ETSI.

On the third part, we will attempt to design a cloud architecture, which will describe the course of a data package from one endpoint to another endpoint and in between those endpoints there will be the cloud. We will try to describe an architecture, that will be able to guarantee that whatever package enters the cloud encrypted, leaves the cloud still being encrypted

On the fourth and final part, we will present the conclusions that we've drawn from this research and presentation that took place before.

SUBJECT AREA: Cloud for Telecommunications

KEYWORDS: security mechanisms/constraints, cloud, EPC, cryptography

ΕΥΧΑΡΙΣΤΙΕΣ

Στον κ. Ευστάθιο Χατζηευθυμιάδη, για την αποτελεσματική επικοινωνία μαζί του, σε κάθε στάδιο της εκπόνησης της, καθώς την παροχή χρήσιμου υλικού για την τελειοποίηση της.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΠΡΟΛΟΓΟΣ

- Η παρούσα εργασία εκπονήθηκε στα πλαίσια της πτυχιακής μου εργασίας ως φοιτητή στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών κατά το εαρινό εξάμηνο 2014 - 2015.
- Το μάθημα αυτό είναι παρμένο από το πρόγραμμα σπουδών του Τμήματος Πληροφορικής και Τηλεπικοινωνιών της Σχολής Θετικών Επιστημών, η οποία εντάσσεται στο Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (Ε.Κ.Π.Α.)
- Επιβλέπων καθηγητής της εργασίας αυτής ήταν ο αναπληρωτής καθηγητής Ευστάθιος Χατζηευθυμιάδης,

1. ΚΥΡΙΩΣ ΘΕΜΑ

1.1 Εισαγωγή - Παραδοχές

1.1.1 Εισαγωγή

Το γενικό πλαίσιο στο οποίο εντάσσεται η παρούσα εργασία είναι αυτό της επιστήμης των δικτύων τηλεπικοινωνιών. Θεμελιώδεις έννοιες σε αυτό το αντικείμενο, θεωρούνται οι κάτωθι:

- Πρωτόκολλα μεταφοράς δεδομένων: βασικοί κανόνες με τους οποίους ένα πακέτο δεδομένων κινείται εντός δικτύου
- Δρομολόγηση/προώθηση πακέτων: Η διαδικασία της κίνησης ενός πακέτου δεδομένων εντός του δικτύου
- Υπηρεσίες δικτύου: ο τρόπος παροχής υπηρεσιών εντός των πλαισίων του δικτύου.
- Εικονικές μηχανές (Virtual machines): Οι εφαρμογές εκείνες πάνω στις οποίες μπορούν να λειτουργήσουν ακόμη και ολόκληρα λειτουργικά συστήματα, χωρίς να επιβαρύνεται η επεξεργαστική ισχύς του εκάστοτε υπολογιστή.

1.1.2 Παραδοχές

Οι περιπτώσεις χρήσης που περιγράφονται (Use Cases) είναι βάσει των προτύπων που μας δίνονται από το ETSI και είναι διαθέσιμα και στην επίσημη σελίδα του.

1.2 Cloud Computing (Υπολογιστική Νέφους)

Το ΥΝ αποτελεί ένα νέο δεδομένο στην εποχή που διανύουμε, καθώς αποτελεί βάση για νέες εφαρμογές που αναπτύσσονται, και οι οποίες συντελούν στη πρόοδο της επιστήμης των Τηλεπικοινωνιών. Αυτό πραγματοποιείται συνοπτικά μέσω συσκευών οι οποίες ενεργοποιούνται διαδικτυακά (internet-enabled devices), και οι οποίες επιτρέπουν να λειτουργούν («τρέχουν») επάνω τους εφαρμογές λογισμικού. Το υπολογιστικό νέφος (ή πιο απλά νέφος) οργανώνεται σε 3 σημαντικές κατηγορίες βάσει του επιπέδου ασφαλείας του: το δημόσιο (public), το ιδιωτικό (private) και το υβριδικό (hybrid)

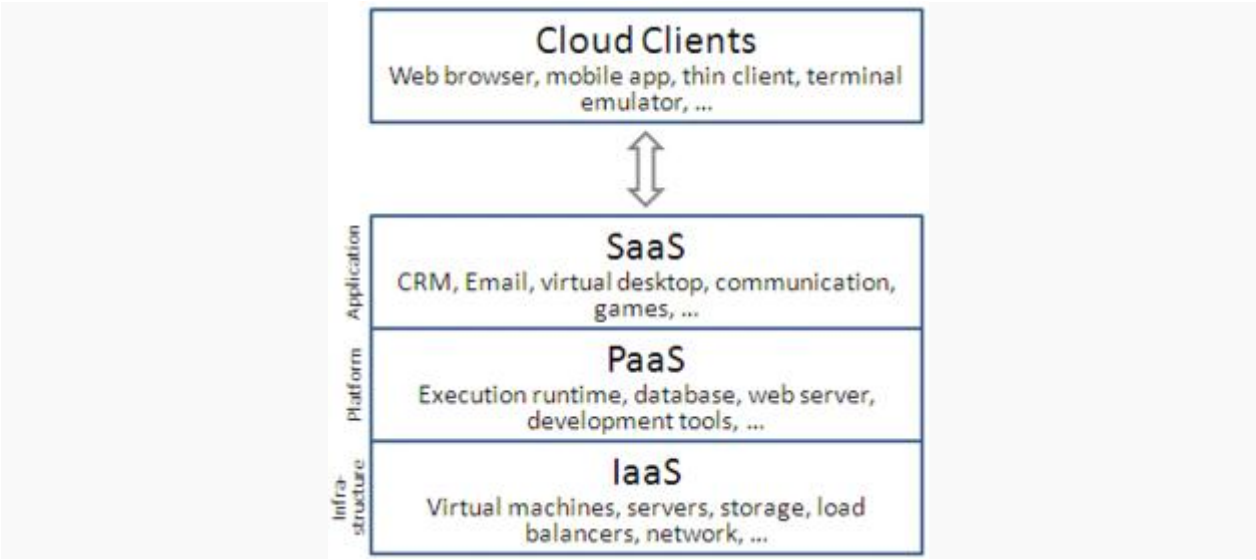
Το ΥΝ βασίζεται στον διαμοιρασμό πόρων για να πετύχει συνοχή και οικονομία σε περιπτώσεις κλιμάκωσης. Είναι παρόμοιο με μια δημόσια υπηρεσία ενός δικτύου. Στα θεμέλια του ΥΝ υπάρχει η ευρύτερη έννοια της σύγκλισης υποδομών αλλά και των διαμοιραζόμενων υπηρεσιών.

Ακόμη, εστιάζει στο να μεγιστοποιήσει την αποτελεσματικότητα των διαμοιραζόμενων πόρων. Οι πόροι αυτοί συνήθως δεν διαμοιράζονται απλώς από πολλαπλούς χρήστες, αλλά επαναδεσμεύονται δυναμικά ανάλογα με τις απαιτήσεις των χρηστών. Η προσέγγιση αυτή πρέπει να είναι σε θέση να μεγιστοποιήσει την υπολογιστική ισχύ, και έτσι να μειώσει την περιβαλλοντική ζημία. Και αυτό διότι θα απαιτείται λιγότερο ρεύμα, λιγότερος χώρος στοίβας, λιγότερη χρήση air condition για μια σειρά από λειτουργείες. Με τη βοήθεια του ΥΝ, πολλοί χρήστες μπορούν να έχουν πρόσβαση σε έναν εξυπηρετητή, για να αντλήσουν και να ανανεώσουν τα δεδομένα τους, δίχως να χρειάζεται να πληρώσουν άδειες για διαφορετικές εφαρμογές.

Ο όρος «μετάβαση στο ΥΝ» επίσης αναφέρεται στην μετάβαση μιας οργάνωσης από το **CAPEX (Capital expenditure)** μοντέλο (αγορά ενός αποκλειστικού hardware και απόσβεση του σε βάθος χρόνου) στο **OPEX (Operating expenditure)** μοντέλο (χρήση μιας διαμοιραζόμενης ΥΝ υποδομής και πληρωμή κάθε φορά που κάποιος τη χρησιμοποιεί).

Θιασώτες του ΥΝ, υποστηρίζουν πως με τη χρήση του, υπάρχουν πολλά πλεονεκτήματα στον κόσμο των εταιρειών και των επιχειρήσεων. Αρχικά, οι εταιρείες γλυτώνουν το κόστος των υποδομών. Έτσι, εστιάζουν περισσότερο σε έργα τα οποία τις ξεχωρίζουν από τις υπόλοιπες, παρά στις υποδομή αυτές καθεαυτές. Επίσης, σημαντικό πλεονέκτημα είναι ότι οι επιχειρήσεις έχουν τη δυνατότητα να κάνουν τις

εφαρμογές τους γρηγορότερα διαθέσιμες προς χρήση, με βελτιωμένη διαχειρισιμότητα και λιγότερη συντήρηση. Ακόμη, παρέχει στο IT την δυνατότητα να κινείται ταχύτατα και να προσαρμόζει τους πόρους για να καλύψει την κυμαινόμενη και απρόβλεπτη επιχειρηματική απαίτηση.
Παρόλα αυτά, παρουσιάζεται το εξής κρίσιμο σημείο, που προβληματίζει πολλούς. Οι πάροχοι ΥΝ συχνά χρησιμοποιούν ένα μοντέλο χρέωσης σύμφωνα με τη χρήση. Αυτό μπορεί να οδηγήσει σε υπερβολικά υψηλές χρεώσεις, αν οι διαχειριστές δεν δεχτούν το μοντέλο κοστολόγησης των υπηρεσιών του ΥΝ.
Η παρούσα διαθεσιμότητα των δικτύων υψηλής χωρητικότητας, φτηνών υπολογιστών και αποθηκευτικών μέσων, σε συνδυασμό με την ευρεία αποδοχή της οπτικοποίησης υλικού, της υπηρεσιοστραφούς αρχιτεκτονικής, της αυτονομιστικής υπολογιστικής και της χρηστικής υπολογιστικής (autonomic and utility computing), έχει οδηγήσει σε ανάπτυξη στο πεδίο του ΥΝ. Οι εταιρείες μπορούν να κλιμακώνονται όσο αυξάνονται οι υπολογιστικές απαιτήσεις και μετά να αποκλιμακώνονται όσο μειώνονται οι απαιτήσεις.
Αξίζει να σημειωθεί ότι χρήστες υπηρεσιών ΥΝ, αυξάνονται 50% ανά έτος.
Ενώ η υπηρεσιοστραφής αρχιτεκτονική που υιοθετείται στο ΥΝ πρεσβεύει το γνωμικό “everything as a service” («τα πάντα ως υπηρεσία», χρησιμοποιώντας το απλό ακρωνύμιο aas δηλαδή as a service) οι πάροχοι του ΥΝ προσφέρουν τις υπηρεσίες τους σύμφωνα με διαφορετικά μοντέλα, τα οποία δημιουργούν μια στοίβα: infrastructure-, platform- και software-as-a-service. Αυτό ερμηνεύεται και παρουσιάζεται σχηματικά παρακάτω:



Σχήμα 1: Η στοίβα διαφορετικών as a service μοντέλων σε αλληλεπίδραση με τους χρήστες-πελάτες του cloud

Είδαμε, λοιπόν, ποιες κατηγορίες μοντέλων υπηρεσιών του ΥΝ υπάρχουν. Ας δούμε τώρα ξεχωριστά τη κάθε κατηγορία.

1.2.1 Υποδομή ως υπηρεσία (Infrastructure-as-a-Service, IaaS)

Στο πιο βασικό μοντέλο υπηρεσιών ΥΝ, σύμφωνα με την IETF (Internet Engineering Task Force), οι πάροχοι του IaaS προσφέρουν υπολογιστές (είτε φυσικές συσκευές είτε εικονικές μηχανές, που είναι και το πιο συνηθισμένο), καθώς και άλλους πόρους.
Ένας hypervisor (όπως οι Xen, Oracle VirtualBox, VMware ESX/ESXi, Hyper-V) τρέχει τις εικονικές μηχανές σαν φιλοξενούμενους. Κοινοπραξίες hypervisors εντός του λειτουργικού του ΥΝ μπορούν να υποστηρίξουν μεγάλους αριθμούς από εικονικές μηχανές και έχουν την δυνατότητα να κλιμακώσουν προς τα πάνω ή προς τα κάτω τις υπηρεσίες ανάλογα με τις ποικίλες απαιτήσεις των πελατών. Τα IaaS ΥΝ συχνά

προσφέρουν επιπρόσθετους πόρους, όπως βιβλιοθήκη για εικόνες δίσκων εικονικών μηχανών, χώρο για αποθήκευση raw blocks, αρχείων ή αντικειμένων, firewalls, εξισορροπητές φόρτου (load balancers), διευθύνσεις IP, εικονικών τοπικών δικτύων (VLANs) και πακέτα λογισμικού. Οι πάροχοι IaaS- ΥΝ προσφέρουν αυτούς τους πόρους κατόπιν απαίτησης από τις δεξαμενές εξοπλισμού που είναι εγκατεστημένες στα κέντρα δεδομένων. Για ευρυζωνική συνδεσιμότητα, οι πελάτες μπορούν να χρησιμοποιήσουν είτε το διαδίκτυο είτε νέφος παρόχου.
Για να αναπτύξουν τις εφαρμογές τους, οι χρήστες εγκαθιστούν εικόνες λειτουργικών συστημάτων και το λογισμικό της εφαρμογής τους στην υποδομή του ΥΝ. Σε αυτό το μοντέλο, ο χρήστης χρησιμοποιεί συμπληρώματα και διατηρεί τα λειτουργικά και το λογισμικό της εφαρμογής του. Οι πάροχοι του ΥΝ τυπικά χρεώνουν τις IaaS υπηρεσίες σε μια βάση υπολογιστικής χρησιμότητας: το κόστος αντανακλά τη ποσότητα των πόρων που δεσμεύονται και καταναλώνονται.

1.2.2 Πλατφόρμα ως υπηρεσία (Platform-as-a-Service, PaaS)

Στα PaaS μοντέλα, οι πάροχοι του ΥΝ προσφέρουν μια υπολογιστική πλατφόρμα, που τυπικά περιλαμβάνει λειτουργικό σύστημα, περιβάλλον εκτέλεσης γλώσσας προγραμματισμού, βάση δεδομένων, και web server. Οι προγραμματιστές εφαρμογών μπορούν να αναπτύξουν και να «τρέξουν» τις λύσεις λογισμικού τους σε μια ΥΝ πλατφόρμα, χωρίς το κόστος και τη πολυπλοκότητα του να αγοράζουν και να διαχειρίζονται το υποκείμενο λογισμικό και τα επίπεδα λογισμικού.
Με κάποια PaaS προσφορές όπως το Microsoft Azure και το Google App Engine, οι υποκείμενοι πόροι υπολογιστή και αποθήκευσης κλιμακώνονται αυτόματα για να συμφωνήσουν με τις απαιτήσεις της εφαρμογής. Έτσι, ο χρήστης του ΥΝ δεν θα χρειάζεται να δεσμεύει ο ίδιος πόρους. Κάτι το οποίο προτάθηκε επίσης από μια αρχιτεκτονική, η οποία στοχεύει στην εγγυήσεις πραγματικού χρόνου σε περιβάλλοντα ΥΝ. Ακόμα, το PaaS μπορεί να παρέχει πιο συγκεκριμένους τύπους εφαρμογών, όπως για παράδειγμα τη κωδικοποίηση πολυμέσων.
Κάποιοι πάροχοι ενσωμάτωσης και διαχείρισης δεδομένων έχουν επίσης δεχτεί εξειδικευμένες εφαρμογές του PaaS ως μοντέλα μεταφοράς για λύσεις σε θέματα δεδομένων.
Παραδείγματα αυτών περιλαμβάνουν το iPaaS (Integration Platform as a Service), το οποίο και επιτρέπει στους πελάτες να προγραμματίσουν, εκτελούν και να διαχειρίζονται ροές ενσωμάτωσης. Σε αυτό το μοντέλο, οι πελάτες οδηγούν την ανάπτυξη και εξάπλωση των ενσωματώσεων, χωρίς εγκατάσταση ή διαχείριση ενδιάμεσου υλικού ή υλικού γενικότερα.
Το dPaaS (data Platform as a Service) προσφέρει προιόντα ενσωμάτωσης και διαχείρισης δεδομένων σαν μια πλήρως διαχειριζόμενη συσκευή. Κάτω από το dPaaS, ο πάροχος PaaS, όχι ο πελάτης , είναι αυτός ο οποίος διαχειρίζεται τον προγραμματισμό και την εκτέλεση των λύσεων δεδομένων (data solutions) χτίζοντας προσαρμοσμένες εφαρμογές δεδομένων για τον πελάτη. Οι χρήστες του dPaaS διατηρούν τη διαφάνεια και τον έλεγχο των δεδομένων μέσω εργαλείων οπτικοποίησης δεδομένων.

1.2.3 Λογισμικό ως υπηρεσία (Software as a Service, SaaS)

Στο Software-as-a-Service μοντέλο, οι χρήστες αποκτούν πρόσβαση σε λογισμικό και βάσεις δεδομένων εφαρμογών. Οι πάροχοι του ΥΝ διαχειρίζονται την υποδομή και τις πλατφόρμες που τρέχουν τις εφαρμογές. Το SaaS κάποιες φορές αναφέρεται ως

«λογισμικό κατ'απαίτηση» (on demand software) και συνήθως χρεώνεται βάσει χρήσης ή χρησιμοποιώντας κόστος εγγραφής.
Στο SaaS μοντέλο, οι πάροχοι ΥΝ εγκαθιστούν και λειτουργούν λογισμικό εφαρμογών στο ΥΝ και οι χρήστες του ΥΝ αποκτούν πρόσβαση στο λογισμικό μέσω πελατών ΥΝ. Οι χρήστες δεν διαχειρίζονται την υποδομή και τη πλατφόρμα όπου τρέχει η εφαρμογή. Αυτό ακυρώνει την ανάγκη να εγκατασταθεί και να τρέξει η εφαρμογή στον υπολογιστή του ίδιου του χρήστη, κάτι που απλοποιεί την συντήρηση και την υποστήριξη.
Οι εφαρμογές του ΥΝ διαφέρουν από άλλες εφαρμογές ως προς την δυνατότητα κλιμάκωσης τους, η οποία μπορεί να επιτευχθεί μέσω κλωνοποίησης εργασιών σε πολλαπλές εικονικές μηχανές (virtual machines) κατά τη στιγμή της εκτέλεσης για να συμβαδίσει με τις μεταβαλλόμενες απαιτήσεις φόρτου. Οι εξισορροπητές φόρτου (load balancers) διαμοιράζουν το φόρτο σε ένα σετ εικονικών μηχανών. Η διεργασία είναι αόρατη στον χρήστη, που βλέπει απλώς ένα σημείο πρόσβασης. Προκειμένου να στεγάσει ένα μεγάλο αριθμό από χρήστες του ΥΝ, οι εφαρμογές του ΥΝ. μπορούν να είναι πολυχρηστικές (multi tenant), δηλαδή κάθε μηχανή μπορεί να εξυπηρετεί άνω της μιας ένωσης χρηστών ΥΝ.
Το μοντέλο χρέωσης για τις εφαρμογές του SaaS είναι τυπικά ένα μηνιαίο ή ετήσιο ποσό ανά χρήστη, έτσι ώστε οι τιμές να είναι προσαρμόσιμες και κλιμακούμενες εάν προστίθενται ή αφαιρούνται ανά πάσα στιγμή. Υποστηρικτές του ισχυρίζονται ότι το SaaS δίνει σε μια επιχείρηση τη δυνατότητα να μειώσει τα λειτουργικά κόστη μέσω της χρήσης (αξιοποίησης) εξωτερικού (μη ιδιόκτητου) υλικού (hardware outsourcing) καθώς και της συντήρησης και υποστήριξης λογισμικού του παρόχου του ΥΝ. Αυτό επιτρέπει στην επιχείρηση να επαναπροσδιορίσει τα λειτουργικά κόστη του IT μακριά από έξοδα προσωπικού και υλικού/λογισμικού, προς επίτευξη άλλων στόχων.
Επιπρόσθετα, με τις εφαρμογές κεντρικοποιημένες, οι ενημερώσεις μπορούν να γίνουν χωρίς να χρειάζεται οι χρήστες να εγκαταστήσουν νέο λογισμικό. Ένα αρνητικό στοιχείο του SaaS εμφανίζεται με την αποθήκευση δεδομένων των χρηστών στον server του παρόχου του ΥΝ. Ως εκ τούτου, δύναται να υπάρχει άνευ αδείας πρόσβαση στα δεδομένα αυτά. Για αυτό το λόγο, οι χρήστες υιοθετούν όλο και περισσότερο έξυπνα συστήματα διαχείρισης κλειδιού τρίτων (third-party key management) προκειμένου να διασφαλίσουν τα δεδομένα τους.

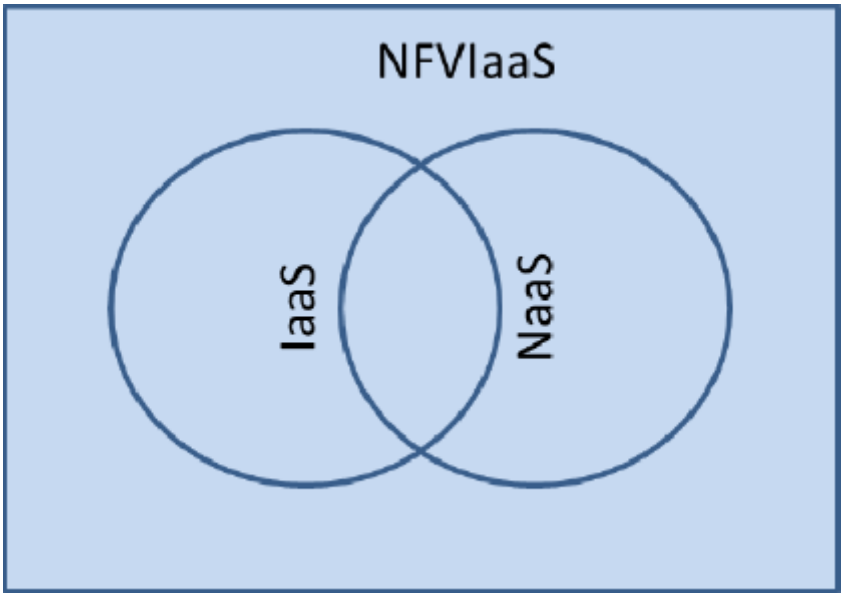
1.3 NFV (Εικονικοποίηση Δικτυακών Λειτουργιών) και περιπτώσεις χρήσης του (Use Cases)

Το NFV ορίζεται ως μια αρχή αρχιτεκτονικής δικτύου, το οποίο προτείνει τη χρήση τεχνολογιών που σχετίζονται με την εικονικοποίηση του IT για να κάνει εικονικοποίηση ολόκληρων κλάσεων λειτουργιών κόμβων δικτύου σε δομικά blocks, που μπορούν να είναι απλά ή αλυσιδωτά συνδεδεμένα με σκοπό τη δημιουργία υπηρεσιών επικοινωνίας.
Γενικά, το NFV βασίζεται στις τεχνικές εικονικοποίησης διακομιστή που χρησιμοποιούνται παραδοσιακά (όπως αυτές του enterprise IT). Ταυτόχρονα όμως διαφέρει από αυτές. Μια εικονικοποιημένη λειτουργία δικτύου (VNF, virtualized network function) μπορεί να αποτελείται από μια η περισσότερες εικονικές μηχανές, οι οποίες να τρέχουν διαφορετικά μεταξύ τους λογισμικά και διεργασίες, ένα επίπεδο πάνω από τους εξυπηρετητές, τους μεταγωγείς (switches) και αποθηκευτικούς χώρους βιομηχανικών προδιαγραφών ή ακόμα και ΥΝ computing υποδομές. Κάτι τέτοιο εξοικονομεί χρήματα, τα οποία υπό διαφορετικές συνθήκες, θα επενδυόνταν στην αγορά υλικού για κάθε μια λειτουργία δικτύου (network function).
Για παράδειγμα, μια εικονικοποιημένη λειτουργία συνοριακού ελεγκτή συνόδου (ΣΕΣ) μπορεί να αναπτυχθεί για να προστατέψει ένα δίκτυο, χωρίς το τυπικό κόστος και τη πολυπλοκότητα της απόκτησης και εγκατάστασης φυσικών μονάδων.

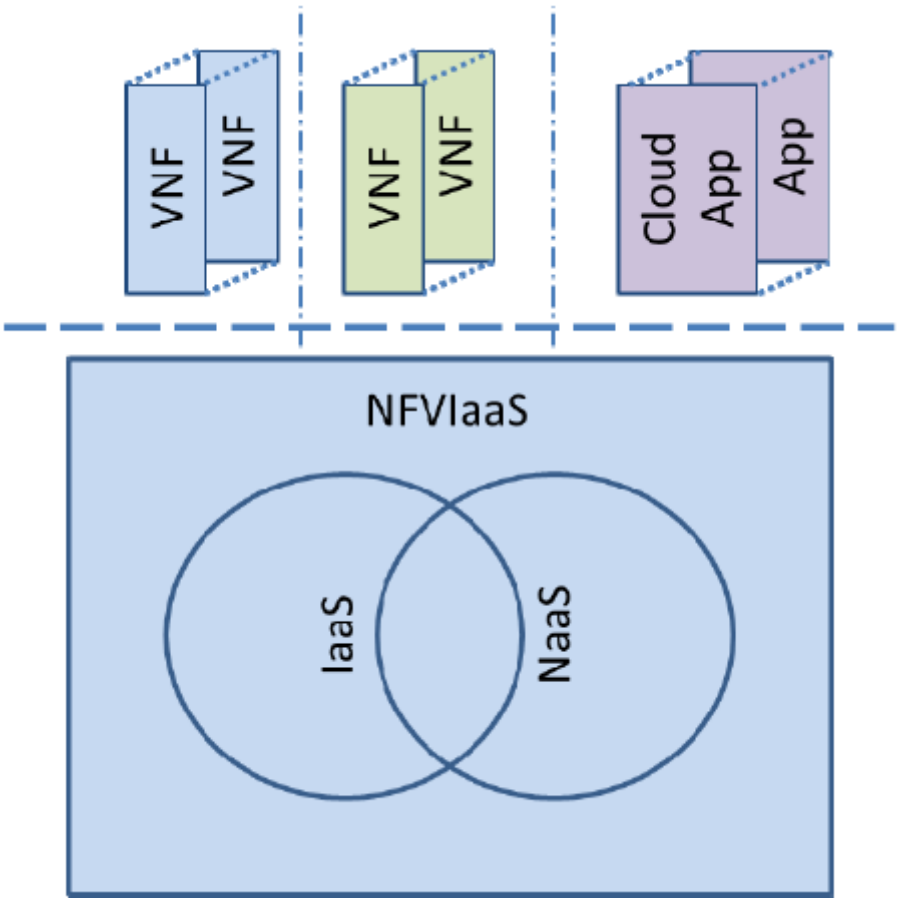
Σε αυτό το σημείο, θα μελετήσουμε τις περιπτώσεις χρήσης του NFV (use cases). Θα εστιάσουμε σε εκείνες, που αφενός μεν σχετίζονται άμεσα με την ασφάλεια δεδομένων του χρήστη των υπηρεσιών ΥΝ, αφετέρου δε μπορούν να προταθούν λύσεις για τα θέματα ασφαλείας που (όπως θα δούμε και στη συνέχεια) ανακύπτουν κατά περίπτωση.

Ας σημειωθεί, ότι τα ακόλουθα σχήματα που χρησιμοποιούνται, είναι παρμένα από το επίσημο αρχείο του ETSI με τίτλο «ETSI Group Specifications for NFV 1.1.1 (10-2013)»

1.3.1 Εικονικοποίηση της Υποδομής των Δικτυακών Λειτουργιών Ως Υπηρεσία (NFVIaaS)

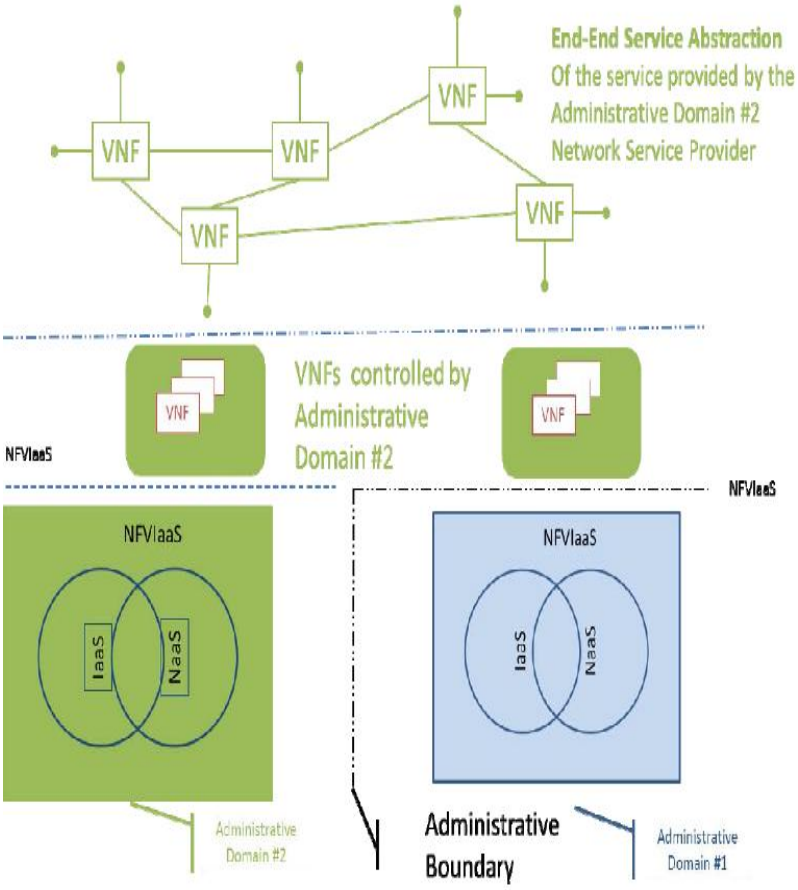


Σχήμα 2: Χαρτογράφηση του IaaS – NaaS



Σχήμα 3: Πολυχρηστική υποστήριξη του NFVIaaS

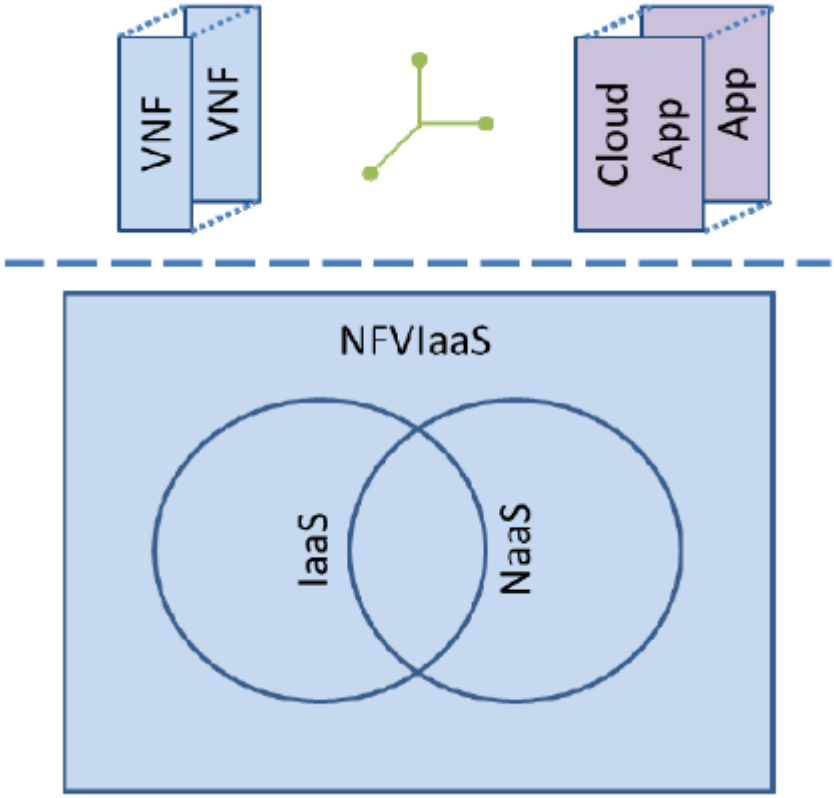
Στο Σχήμα 2, βλέπουμε πως τα μοντέλα Υποδομή-ως-υπηρεσία και Δίκτυο-ως-υπηρεσία παρουσιάζουν κοινά σημεία εντός των πλαισίων της εικονικοποίησης-της-υποδομής-των-δικτυακών-λειτουργιών-ως-υπηρεσία (NFVIaaS). Στο δε Σχήμα 3, παρατηρούμε ότι επάνω σε αυτή την υποδομή, βασίζονται εικονικοποιημένες δικτυακές λειτουργίες (virtualized network functions, VNFs), καθώς και άλλες εφαρμογές του ΥΝ.



Σχήμα 4: Εικονικοποιημένη δικτυακή λειτουργία ελεγχόμενη από διοικητικό τομέα

Οι VNFs όμως ελέγχονται από κάποιον διοικητικό τομέα, όπως παρουσιάζεται στο παραπάνω σχήμα. Ο τομέας αυτός βρίσκεται στο ακριβώς από πάνω επίπεδο από το NFVIaaS, και αντιστοιχεί ένας σε κάθε σετ VNFs.

1.3.1.1 Στόχοι εικονικοποίησης (virtualization targets)



Σχήμα 5: NFVIaaS στη πλήρη του μορφή

Οι ανάγκες που παρουσιάζονται και πρέπει να καλυφθούν είναι αρκετά σημαντικές. Πρώτα από όλα, να μπορεί να γίνει το NFVaaS διαθέσιμο εντός της χωρητικότητας που του δίνεται, αλλά να ικανοποιήσει και άλλους περιορισμούς, έτσι ώστε, αυτή η εμπορική προσφορά να μπορέσει να οδηγήσει στην ανάπτυξη της NFV υποδομής. Επίσης, να μπορεί να τρέξει μια VNF σταθερά στην NFV υποδομή ενός άλλου παρόχου υπηρεσίων μαζί με τη δική του NFV υποδομή για βελτίωση της ανθεκτικότητας. Ακόμη σημαντικό θα ήταν, να μπορεί να τρέξει μια VNF σταθερά στην NFV υποδομή ενός άλλου παρόχου υπηρεσιών προκειμένου να βελτιώσει την εμπειρία του πελάτη, ελαττώνοντας την καθυστέρηση. Επιπροσθέτως, να μπορεί να τρέξει μια VNF σταθερά στην NFV υποδομή ενός άλλου παρόχου υπηρεσιών προκειμένου να συμμορφωθεί με τις κανονιστικές απαιτήσεις.
Επομένως οι στόχοι εικονικοποίησης πρέπει να είναι οι ακόλουθοι:
Πρώτος στόχος, πρέπει να είναι η περιγραφή των μεταδεδομένων των τύπων των NFVI πόρων, η οποία μπορεί να γίνει διαθέσιμη μέσω του NFVIaaS. Επίσης, πρέπει να υπάρξουν μηχανισμοί για να υποστηρίξουν ανάκαμψη από σφάλματα κατά μήκος των NFV υποδομών, τα οποία διαχειρίζονται διαφορετικές περιοχές και διαφορετικοί μηχανισμοί για να επικυρώσουν την ανεξαρτησία της NFV υποδομής την οποία διαχειρίζονται διαφορετικές διοικητικές περιοχές. Ακόμη να υφίστανται μηχανισμοί για να μετράται η περίοδος αδράνειας σε συγκεκριμένες διατάξεις καθώς και εργαλεία σχεδιασμού για πρόβλεψη αναμενόμενης περιόδου αδράνειας σε σχεδιασμένη διάταξη. Σημαντικό είναι επίση να υπάρξουν μηχανισμοί που αναγνωρίζουν και περιορίζουν τις τοποθεσίες όπου η πληροφορία αποθηκεύεται και επεξεργάζεται.

1.3.1.2 Συνύπαρξη των εικονικοποιημένων (VNFs) και των μη εικονικοποιημένων δικτυακών λειτουργιών

Οι VNFs από πολλαπλούς παρόχους υπηρεσιών μπορούν να συνυπάρξουν εντός της ίδιας NFV υποδομής. Η NFV υποδομή θα παρέχει την ανάλογη απομόνωση μεταξύ των

πόρων που δεσμεύονται στους διαφορετικούς παρόχους υπηρεσιών. Σφάλματα σε VNF στιγμιότυπα ή απαιτήσεις σε πόρους από έναν πάροχο υπηρεσιών δε θα έπρεπε να επιτρέπεται να υποβαθμίζει τη λειτουργία των VNF σταθερών σε άλλους παρόχους υπηρεσιών.
Έτσι θα υπάρχει η ανάγκη να υλοποιηθούν μηχανισμοί προώθησης πακέτων όπως οι IP και Ethernet προκειμένου να **διασυνδεθούν με VNF σταθερές στην υποδομή άλλου Παρόχου Υπηρεσιών, να διαχειριστούν VNF σταθερές στην υποδομή ενός άλλου Παρόχου Υπηρεσιών και να συνδεθούν σε άλλους χρήστες, οι οποίοι είναι συνδεδεμένοι στο δίκτυο πρόσβασης ενός άλλου Παρόχου Υπηρεσιών.**

1.3.1.3 Προβλήματα/θέματα που προκύπτουν

Ας δούμε ποια προβλήματα/θέματα πρέπει να αντιμετωπιστούν. Πρώτα από όλα, η ανάγκη να υποστηριχθεί μέτρηση παραμέτρων σχετικών με τη συμφωνία επιπέδου παροχής υπηρεσίας σε μια προσφορά NFVIaaS μεταξύ Παρόχων Υπηρεσιών. Επιπροσθέτως, η ανάγκη να υποστηρίζει ειδοποίηση σε περίπτωση σφάλματος και διαγνωστικές υπηρεσίες σε μια εμπορική προσφορά NFVIaaS μεταξύ Παρόχων Υπηρεσιών.

1.3.2 Εικονική δικτυακή λειτουργία ως υπηρεσία (VNFaaS)

1.3.2.1 Πλεονεκτήματα του VNFaaS

Σημαντικά πλεονεκτήματα παρατηρούνται στο VNFaaS. Πρώτα από όλα, το μικρό αποτύπωμα εργαλείων λογισμικού για να αποκτήσει πρόσβαση στην υπηρεσία μια επιχείρηση, βοηθάει στην μικρότερη επιβάρυνση της RAM όταν τα εργαλεία αυτά χρησιμοποιούνται. Επίσης, η αποτελεσματική χρήση των αδειών λογισμικού είναι ένα σημαντικό πλεονέκτημα, που γλυτώνει χρόνο και σαφώς χρήμα. Ακόμα, η κεντρικοποιημένη διαχείριση και τα κεντρικοποιημένα δεδομένα εν γένει, βοηθούν και συνεισφέρουν στον καλύτερο έλεγχο και τη διαχείριση των δεδομένων. Τέλος, η εξοικονόμιση χρημάτων αποτελεί ένα γενικό προτέρημα της χρήσης του VNFaaS, αφού όπως διαπιστώνουμε, με τη χρήση αυτής έχουμε μικρότερη επιβάρυνση του συστήματος και επέκταση της διάρκειας ζωής του υλικού πάνω στο οποίο το σύστημα βασίζεται.

1.3.2.2 Στόχοι εικονικοποίησης

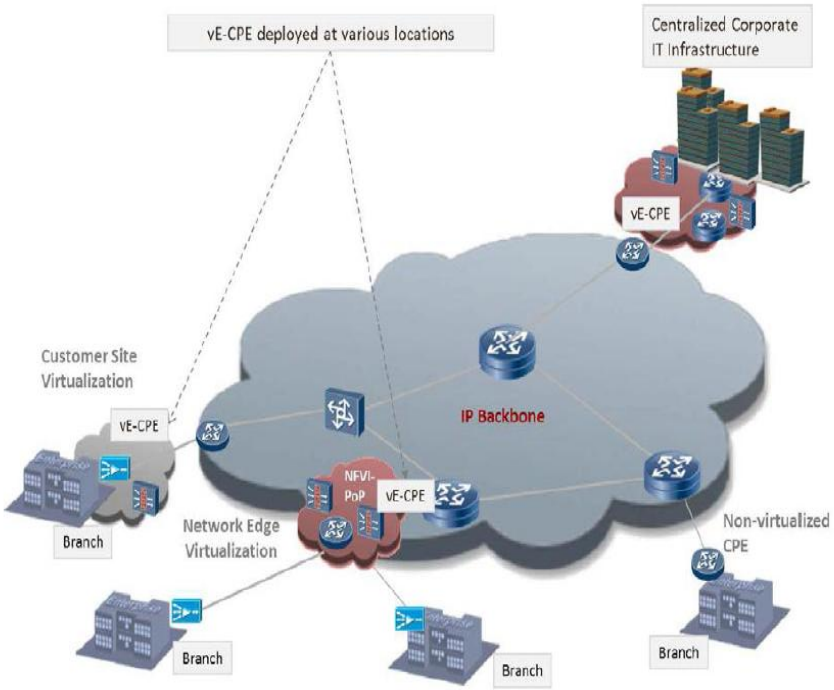
Σχήμα 6: Το δίκτυο κορμού του παρόχου υπηρεσιών

Εικονικοποίηση της επιχείρησης μπορεί να περιλαμβάνει είτε **εικονικοποίηση των CPE (εξοπλισμός χρήστη) λειτουργιών (vE-CPE) στο ΥΝ του παρόχου υπηρεσιών, είτε εικονικοποίηση των PE (άκρο παρόχου) λειτουργιών (vPE) όπου οι λειτουργίες των εικονικών υπηρεσιών δικτύου και των PE που προσανατολίζονται προς το δίκτυο κορμού μπορούν να εκτελεστούν στο υ.ν. του παρόχου.**

Οι PE δρομολογητές (routers) διαμοιράζονται σε έναν μεγάλο αριθμό πελατών, ενώ ένας CPE δρομολογητής χρησιμοποιείται αποκλειστικά από έναν μόνο πελάτη. Έτσι, μεγαλύτερη εξοικονόμιση σε κλιμάκωση μπορεί να κερδιθεί από εικονικοποίηση του PE δρομολογητή παρά από αυτή του CPE δρομολογητή.

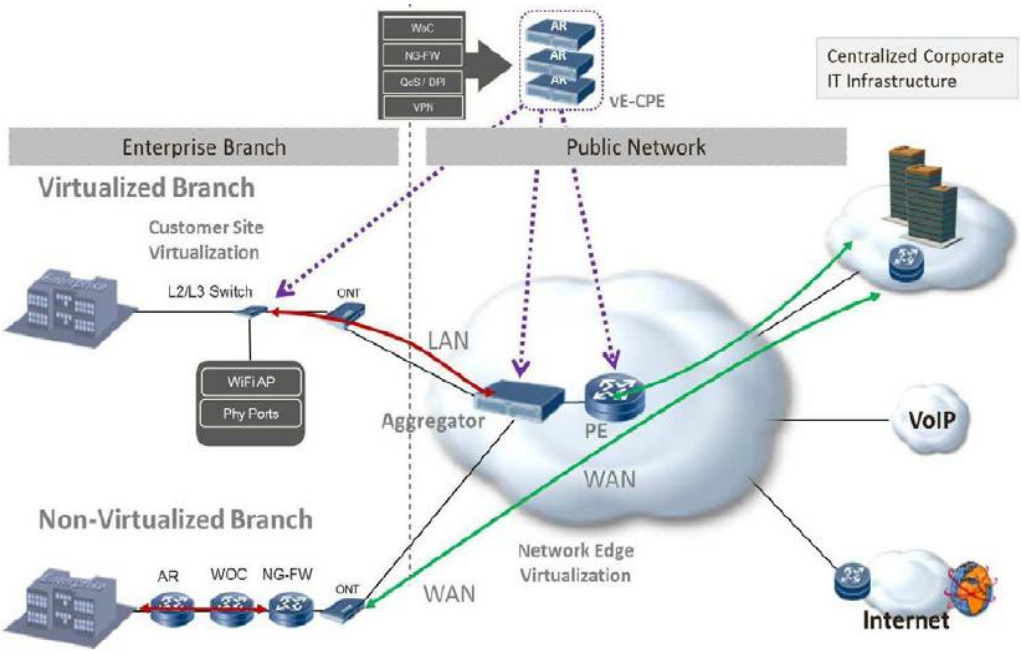
Εικονικοποίηση του CPE (vE-CPE)

Η vE-CPE πρόταση ενισχύει το δίκτυο επιχειρήσεων αντικαθιστώντας συσκευές με συμβατές ως προς το NFV εικονικοποιημένες λύσεις, που βρίσκονται είτε στο επιχειρηματικό ΥΝ ή στον πάροχο του NFV πλαισίου. Υπηρεσίες που παρέχονται σε αυτή τη πρόταση δύνανται να περιλαμβάνουν ένα δρομολογή που παρέχει έλεγχο ποιότητας υπηρεσίας και άλλες προηγμένες υπηρεσίες όπως, ανίχνευση και προστασία επιπέδου 7 από εισβολή και άλλα. Στο σχήμα που ακολουθεί βλέπουμε παραδείγματα διαφορετικών τοποθεσιών ανάπτυξης του vE-CPE.



Σχήμα 7: Παραδείγματα τοποθεσίας vE-CPE

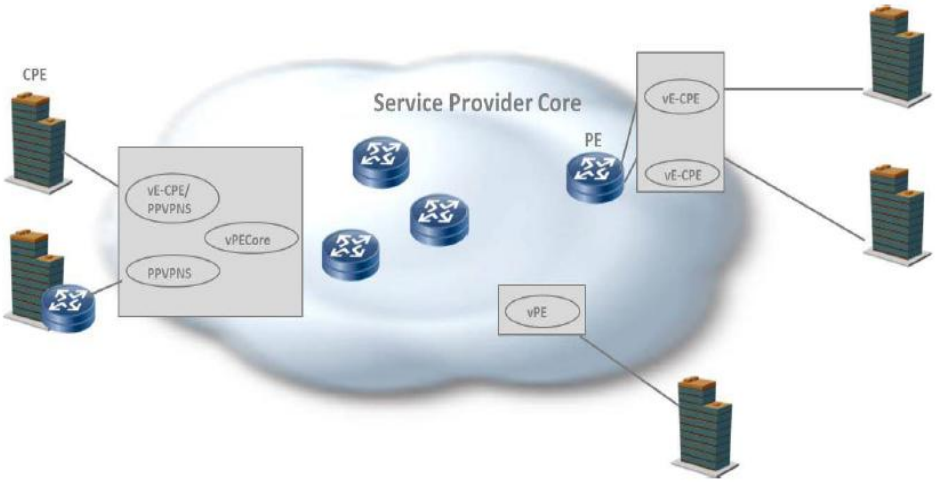
Στη συνέχεια (Σχήμα 8) βλέπουμε σε ποια σημεία διαφέρουν μια εικονικοποιημένη διακλάδωση EPC και μια μη-εικονικοποιημένη EPC διακλάδωση. Κάτι το οποίο εύκολα παρατηρούμε σαν διαφορά είναι ο τρόπος με τον οποίο επικοινωνούν με το δημόσιο δίκτυο. Η μεν εικονικοποιημένη διακλάδωση, επικοινωνεί μέσω ενός L2/L3 μεταγωγέα και του οπτικού τερματικού δικτύου (optical network terminal) μόνο, και επειδή προέρχεται από ένα τοπικό δίκτυο (LAN, Local Area Network), όταν πρέπει να επικοινωνήσει με την IT υποδομή θα πρέπει το κάνει μέσω ενός συναθροιστή και του οπτικού τερματικού δικτύου. Η δε μη-εικονικοποιημένη διακλάδωση ενώ δεν χρησιμοποιεί συναθροιστή και οπτικό τερματικό δικτύου για να επικοινωνήσει με το IT υποδομή (είναι σε WAN και τα δύο), χρησιμοποιεί δρομολογητή πρόσβασης επιχείρησης (access router) και ελεγκτή βελτιστοποίησης του WAN μιας επιχείρησης (WAN Organization Controller)



Σχήμα 8: Μη-εικονικοποιημένο CPE and vCPE

Εικονικοποίηση του PE

Εικονικοποίηση των κύριων δρομολογητών μπορεί να μην είναι δυνατή λόγω υψηλών απαιτήσεων σε ρυθμοαπόδοση, αλλά η εικονικοποίηση του PE δρομολογητή είναι πιο πιθανή, με επιπρόσθετα οφέλη από τη παροχή ικανότητας κλιμάκωσης, από VPN υπηρεσίες που προβλέπονται από τον πάροχο μέσω της δυναμικής αλλαγής της δέσμευσης των εικονικών πόρων (Σχήμα 1.9).



Σχήμα 9: Εικονικοποίηση του CPE, εικονικές υπηρεσίες δικτύου και PE λειτουργίες που προσανατολίζονται προς το δίκτυο κορμού

Οι δικτυακές λειτουργίες που δύναται να χρησιμοποιηθούν τυπικά είναι στη παρακάτω λίστα:

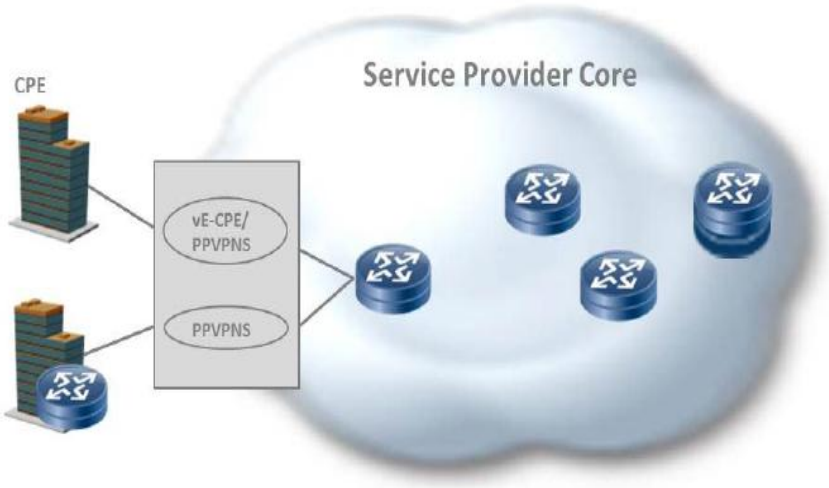
1. **Δρομολογητής πρόσβασης επιχείρησης ή εξοπλισμού χρήστη (AR – Enterprise Access Router/Enterprise CPE)**
2. **Δρομολογητής άκρου παρόχου (PE – Provider Edge Router)**
3. **Τείχος προστασίας της επιχείρησης (FW – Enterprise Firewall)**
4. **NG-FW – Enterprise NG-FW**

5. **Ελεγκτής βελτιστοποίησης του WAN μιας επιχείρησης (WOC – Enterprise WAN Optimization Controller)**
6. **Αναλυτική Εξερεύνηση Πακέτου (DPI – Deep Packet Inspection) (συσκευή ή λειτουργία)**
7. **Σύστημα αποτροπής εισβολής (IPS – Intrusion Prevention System) και άλλες συσκευές ασφαλείας**
8. **Παρακολούθηση απόδοσης δικτύου (Network Performance Monitoring)**

1.3.2.3 Συνύπαρξη των εικονικοποιημένων και των μη-εικονικοποιημένων λειτουργιών

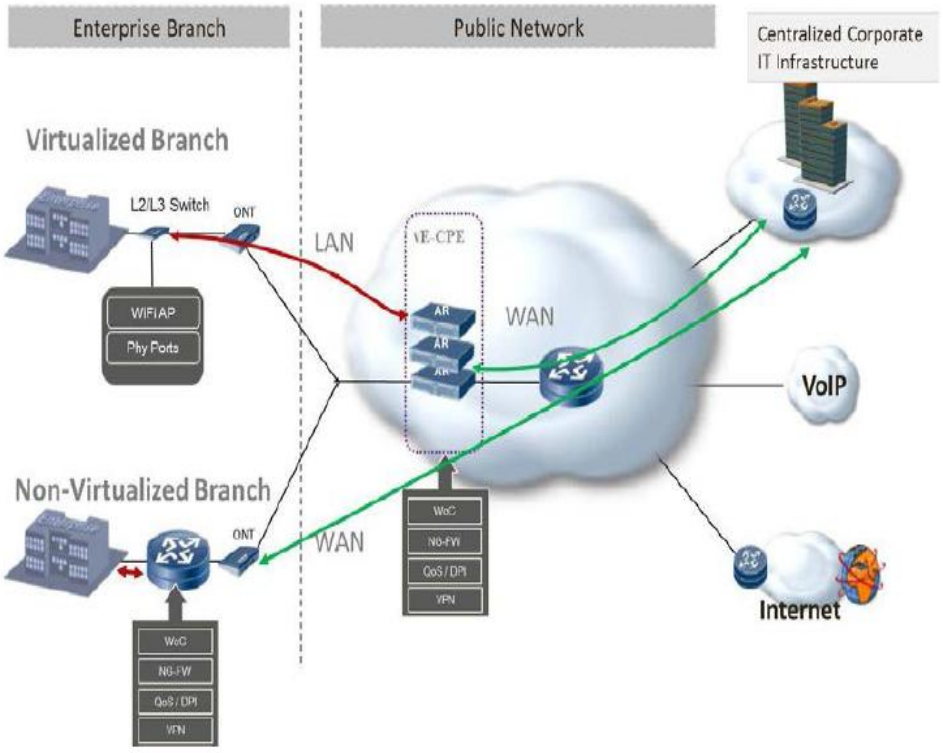
✓ **Μερική εικονικοποίηση:**

Ένα συνδυασμένο μοντέλο εικονικοποίησης αποτελείται από την παροχή εικονικών δικτυακών υπηρεσιών, ενώ διατηρεί τις PE λειτουργίες που προσανατολίζονται στον πυρήνα. Αυτό το σενάριο αποδόμησης του PE μπορεί να περιορίζεται σε υλοποιήσεις μονού προμηθευτή, καθώς η διασυνεργασία θα απαιτούσε τυποποίηση της διεπαφής μεταξύ του PE και των ιδιωτικών εικονικών δικτυακών υπηρεσιών που προβλέπονται από τον πάροχο (κάτι το οποίο ενδέχεται να μην είναι εντός του πλαισίου του NFV). (Σχήμα 10)



Σχήμα 10: Εικονικοποίηση υπηρεσιών, με παράλληλη διατήρηση των λειτουργιών που προσανατολίζονται προς το δίκτυο κορμού στο πραγματικό PE

✓**Σενάρια ανάμεικτης εικονικοποίησης:**



Σχήμα 11: Συνύπαρξη του παραδοσιακού εταιρικού εξοπλισμού και του vE-CPE που φιλοξενείται από τον πάροχο

Υπάρχουν 2 διακλαδώσεις σε αυτά τα σενάρια (όπως βλέπουμε στο παραπάνω σχήμα 11).

Στη πάνω διακλάδωση, το vE-CPE υλοποιείται στο NFV δίκτυο του παρόχου. Το υποδίκτυο τοπικής κίνησης επεκτείνεται στο δίκτυο του παρόχου και τερματίζει στο vE-CPE.

Στη κάτω διακλάδωση, παρουσιάζεται μια παραδοσιακή λύση, η οποία παρέχεται από τις μη-εικονικοποιημένες συσκευές. Σε αυτή τη περίπτωση, η τοπική επιχείρηση μένει εντός της διακλάδωσης.

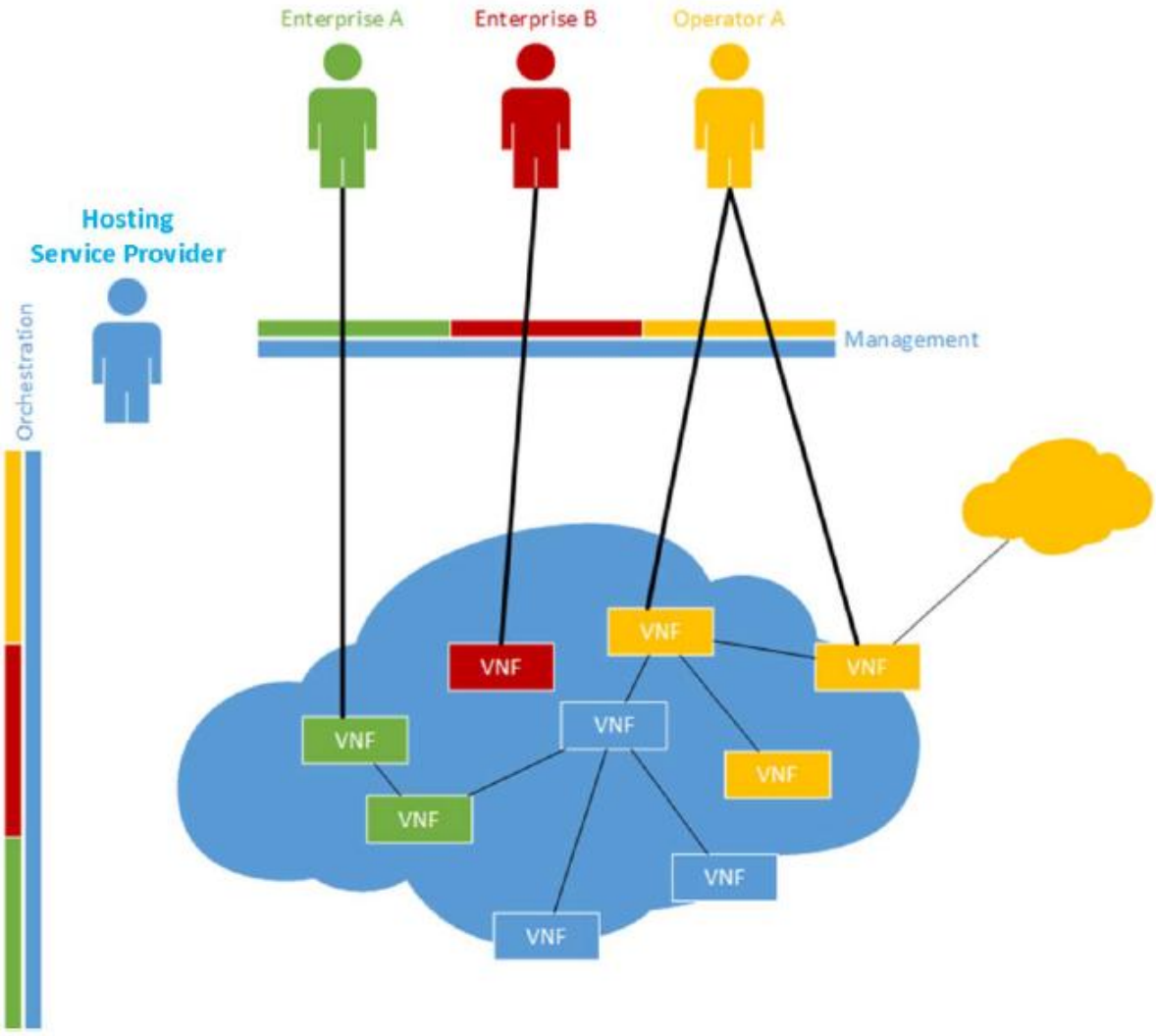
Ασύρματη συνδεσιμότητα διατηρείται μεταξύ εικονικοποιημένων και μη-εικονικοποιημένων διακλαδώσεων, αναπτύσσοντας ένα παραδοσιακό (legacy) WAN.

1.3.2.4 Προβλήματα/θέματα που προκύπτουν

Προκύπτουν όμως μια σειρά από προβλήματα, Προκειμένου να περιοριστεί το κόστος κλιμάκωσης, ένας μεγάλος αριθμός εικονικοποιημένων συσκευών θα χρειάζεται να ενσωματωθούν σε περιορισμένο αριθμό από CPUs. Με την αναμενόμενη αύξηση των απαιτήσεων σε επιχειρηματικό εύρος ζώνης, το απαιτούμενο εύρος ζώνης ανά CPU δύναται να ξεπεράσει τις σημερινές δυνατότητες μιας CPU
Για να πετύχουν την ζητούμενη απόδοση, οι εικονικές PE λειτουργίες, θα πρέπει **να είναι σε θέση να ενσωματωθούν σε μια εικονική μηχανή. Επιπλέον, να**

διαμοιραστούν σε ένα κύριο σετ εικονικών δικτυακών λειτουργιών και εικονικών δικτυακών λειτουργιών γενικότερα.
Το vPE πρέπει να είναι σε θέση να κλιμακώνεται δυναμικά, προκειμένου να υποστηρίξει έναν μεγαλύτερο πίνακα προώθησης και έναν μεγαλύτερο αριθμό ροών. Για να επιτευχθεί αυτή η κλιμάκωση για το vPE μπορεί να γίνει για παράδειγμα **με αλλαγή των πόρων υποδομής που δεσμεύονται σε μια vPE σταθερά, π.χ. αύξηση μνήμης, το οποίο συνεπάγεται αύξηση συνολικού κόστους για μνήμες σε μια επιχείρηση. Άλλη λύση είναι, η δημιουργία επιπλέον σταθερών από το vPE, που σημαίνει περισσότερος χώρος για να αποθηκευτούν, το οποίο πάλι αυξάνει το κόστος των πόρων που χρειάζονται για τη λειτουργία του.**

1.3.3 Πλατφόρμα Εικονικού Δικτύου Ως Υπηρεσία (VNPaaS)



Σχήμα 12 Παράδειγμα επιχείρησης εξωτερικού συνεργάτη που μοιράζεται την υποδομή ενός παρόχου υπηρεσίας

1.3.3.1 Στόχος εικονικοποίησης

Όλες οι δικτυακές λειτουργίες να μπορούν να διαμοιράζονται με τρίτους. Η υπόθεση εδώ είναι ότι η χρήση εικονικών δικτυακών λειτουργίων, συνεπάγεται ένα συγκεκριμένο επίπεδο διαχωρισμού φόρτου εργασίας

1.3.3.2 Συνύπαρξη των εικονικοποιημένων και των μη-εικονικοποιημένων λειτουργιών

Οι πάροχοι σήμερα πρέπει να μοιράζονται πόρους υποδομών, όταν παρέχουν υπηρεσίες σε πολλαπλούς χρήστες. Οι λειτουργίες που διαμοιράζονται εντός αυτού του πλαισίου μπορεί να παραμείνουν μη-εικονικοποιημένες. Η επικοινωνία με τις εικονικές δικτυακές λειτουργίες θα βασίζεται σε τυποποιημένες διεπαφές.

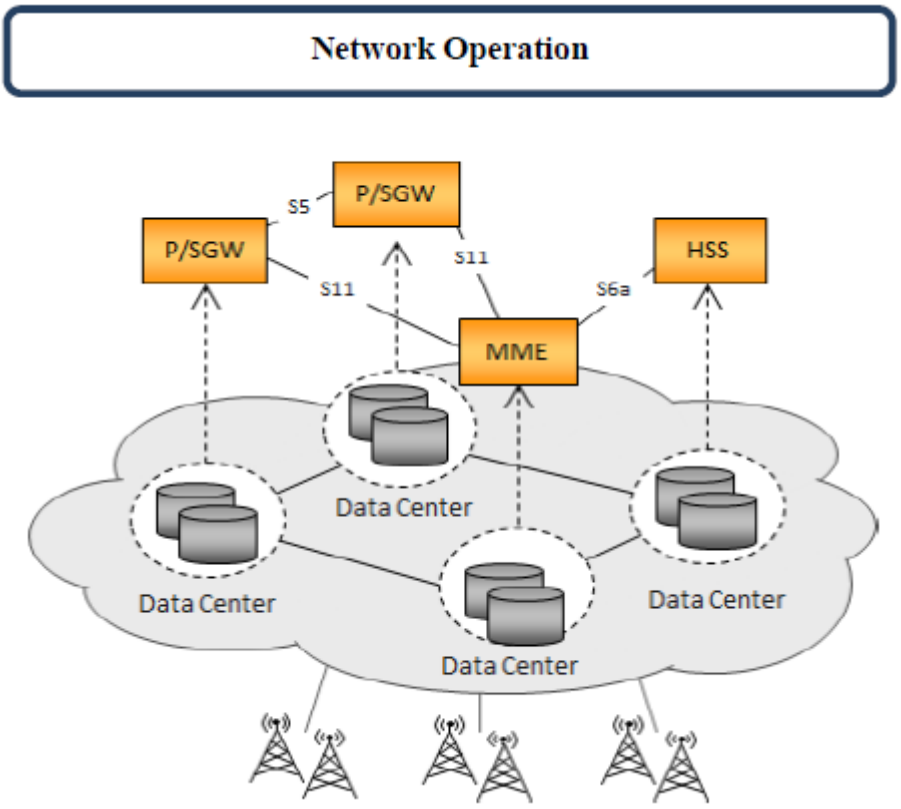
1.3.3.3 Προβλήματα/θέματα

Προκειμένου να γίνει διαμοιρασμός πόρων υποδομής με τρίτους, πρέπει να τηρούνται ορισμένες προυποθέσεις. Πρώτο και κύριο, ο έλεγχος πρόσβασης σε όλες τις κλήσεις API πρέπει να βασίζεται σε εξουσιοδοτημένη ταυτότητα χρήστη. Εξίσου σημαντικό είναι, οι πόροι υποδομής να μπορούν να παρέχουν μηχανισμούς για τον διαχωρισμό φόρτου εργασίας από διαφορετικούς παρόχους. Τέλος, οι πόροι υποδομών και οι δικτυακές λειτουργίες χρειάζεται να παρέχουν μια διεπαφή για να παρακολουθεί, εγγυάται και να περιορίζει ττη χρήση αυτού του πόρου από τον κάθε πάροχο

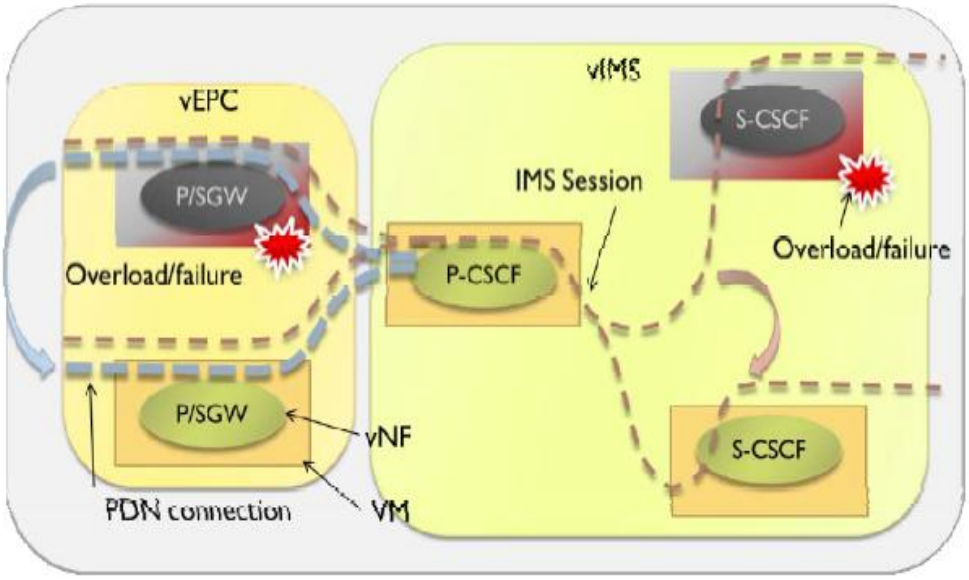
1.3.4 Εικονικοποίηση του Mobile Core Network και της υπηρεσίας IMS

1.3.4.1 Πλεονεκτήματα εικονικοποίησης του Mobile Core Network και του IMS

Αρχικά, παρουσιάζεται μειωμένο TCO (Total cost of ownership, συνολικό κόστος ιδιοκτησίας). Επιπρόσθετα, παρατηρείται βελτιωμένη αποτελεσματικότητα στη χρήση του δικτύου, μεγαλύτερη διαθεσιμότητα υπηρεσιών, ελαστικότητα και επαναδιαμόρφωση τοπολογίας



Σχήμα 13: Εικονικοποίηση του EPC



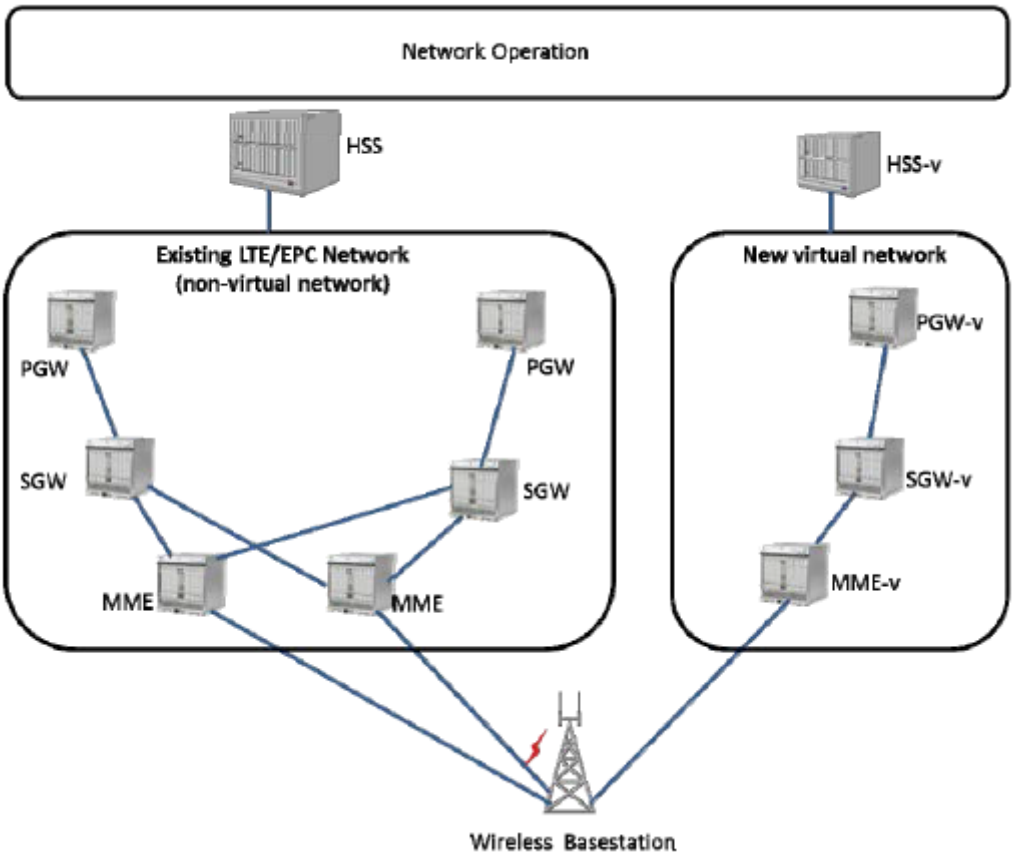
Σχήμα 14: Επανατοποθέτηση EPC λόγω σφάλματος υπερφόρτωσης δεδομένων

1.3.4.2 Στόχοι εικονικοποίησης

Οι δικτυακές λειτουργίες που ακολουθούν πρέπει να εικονικοποιηθούν. Πρώτα από όλα οι επιπρόσθετες λειτουργίες δικτυακές λειτουργίες EPC. Παραδείγματα τέτοιων λειτουργιών είναι το MME (Mobility Management Entity) και τα Source/Packet-Gateways που περιγράφονται σε επόμενη ενότητα εκτενέστερα, καθώς και την PCRF (Policy And Charging Rules Function, Λειτουργία Πολιτικής και Κανόνων Χρέωσης), η οποία αποτελεί ένα εργαλείο πολιτικής, το οποίο παίζει καθοριστικό ρόλο στα δίκτυα νέας γενιάς, Εν αντιθέσει με προηγούμενες εφαρμογές πολιτικής, οι οποίες απλά προστέθηκαν σε ένα ήδη υπάρχον δίκτυο για να ενισχύσουν μια πολιτική, το PCRF είναι ένα τμήμα λογισμικού που λειτουργεί στο πυρήνα του δικτύου και έχει πρόσβαση σε βάσεις δεδομένων χρηστών και άλλες εξειδικευμένες λειτουργίες, όπως ένα σύστημα χρέωσης με ένα κεντρικοποιημένο τρόπο. Και επειδή λειτουργεί σε πραγματικό χρόνο, το PCRF έχει μια αυξημένη στρατηγική σημασία και έναν ευρύτερο ρόλο δυνατότητων, σε σχέση με τις παραδοσιακές εφαρμογές πολιτικής. Κάτι που από το 2006 οδήγησε σε πολλαπλασιασμό των PCRF προιόντων

Ακόμη, οι 3G/EPC δικτυακές λειτουργίες διασυνεργασίας όπως για παράδειγμα είναι το SGSN (Serving GPRS support node), υπεύθυνο για την παράδοση πακέτων δεδομένων από και προς τους κινητούς σταθμούς εντός της γεωγραφικής περιοχής υπηρεσιών. Οι ρόλοι του περιλαμβάνουν δρομολόγηση και μεταφορά πακέτου, διαχείριση φορητότητας, διαχείριση λογικής συνδεσης, και λειτουργίες χρέωσης και αυθεντικοποίησης. Άλλο παράδειγμα είναι το GGSN (Gateway GPRS support node), που είναι το κύριο κομμάτι του GPRS δικτύου. Είναι υπεύθυνο για την διασυνεργασία μεταξύ, του GPRS δικτύου και εξωτερικά δίκτυα μεταγωγής πακέτου όπως το διαδίκτυο και τα X.25 δίκτυα. Τέλος, όλες οι IMS δικτυακές λειτουργίες όπως οι P/S/I-CSCF, MGCF και AS.

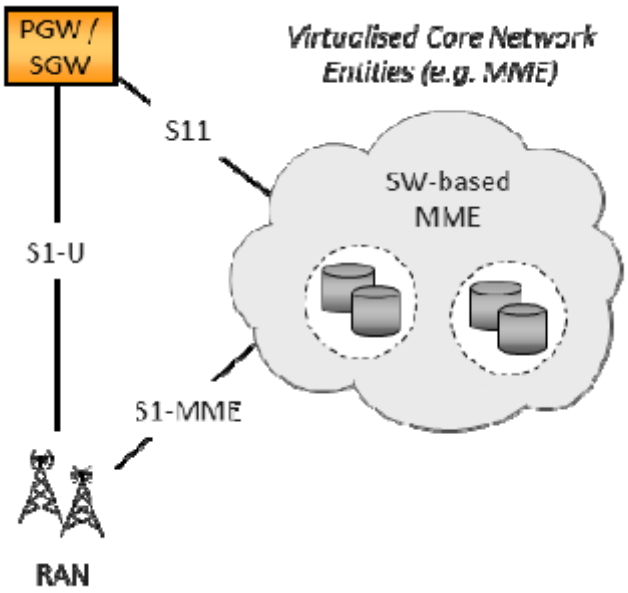
1.3.4.3 Συνύπαρξη των εικονικοποιημένων και των μη-εικονικοποιημένων λειτουργιών



Σχήμα 15: Παράδειγμα συνύπαρξης των εικονικοποιημένων και των μη-εικονικοποιημένων δικτύων κορμού κινητού παρόχου

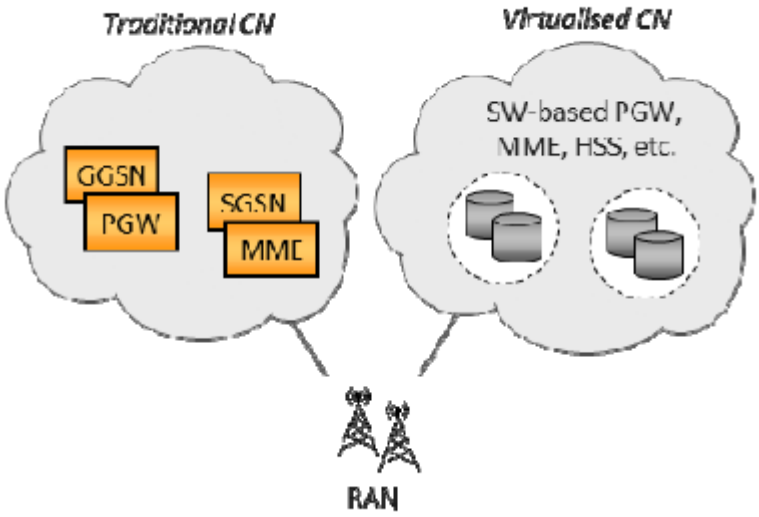
Δύο πιθανά σενάρια:

- **Εικονικοποίηση κάποιων μερών του δικτύου κορμού κινητού παρόχου.** Σε αυτή τη περίπτωση μόνο κάποιες δικτυακές λειτουργίες γίνονται εικονικοποιημένες. Ενδέχεται να υπάρχουν EPC λειτουργίες ελέγχου, HSS ή κόμβοι εξυπηρέτησης



Σχήμα 16: Μερική εικονικοποιήση του δικτύου κορμού κινητού παρόχου

- **Συνύπαρξη του εικονικοποιημένου and του μη-εικονικοποιημένου *κορμού κινητού παρόχου*.** Σε αυτή τη περίπτωση, ο πάροχος αναπτύσσει έναν εντελώς εικονικοποιημένο κορμό δικτύου, ενώ διατηρεί τον μη-εικονικοποιημένο κορμό. Ο εικονικοποιημένος κορμός μπορεί να χρησιμοποιηθεί για συγκεκριμένες υπηρεσίες ή/και συσκευές (παράδειγμα machine-to-machine) ή για όταν η κίνηση ξεπερνάει τη χωρητικότητα του μη-εικονικοποιημένου δικτύου.



Σχήμα 17: Εικονικοποίηση του δικτύου κορμού κινητού παρόχου συγκεκριμένη ως προς τις υπηρεσίες

Για τα προηγούμενα σενάρια, οι πολιτικές σχεδίασης χρειάζεται να ξεκαθαριστούν:

1. **Δίκτυο Ασύρματης Πρόσβασης (Radio Access Network (RAN)):** Όπου συγκλίνουν το εικονικοποιημένο δίκτυο κορμού κινητού παρόχου και το μη-εικονικοποιημένο δίκτυο κορμού κινητού παρόχου.
2. **Συστήματα Διαχείρισης Δικτύων (Network Operation Systems):** Πως το NOS για μη-εικονικοποιημένο δίκτυο επικοινωνεί με τη συγκεκριμένη λειτουργία του

εικονικού δικτύου κορμού κινητού παρόχου και εάν χρειάζονται νέα συστήματα υποστήριξης λειτουργίας δικτύου ή αν πρέπει να ενισχυθούν τα υπάρχοντα.

3. **Επιστροφή στο μη-εικονικοποιημένο δίκτυο:** Μηχανισμός ανάκαμψης από σφάλμα μέσω της επιστροφής σε μη-εικονικοποιημένο δίκτυο όταν αυτό απαιτείται.

1.3.4.4 Προβλήματα/θέματα που ανακύπτουν

Υπάρχουν κάποιες προκλήσεις υψηλού επιπέδου που πρέπει να ληφθούν σοβαρά υπόψιν για να μπορέσει να δοθεί μια πλήρης λύση σε αυτή τη περίπτωση χρήσης.

1) Κλιμάκωση πόρων και αποκλιμάκωση τους εντός του MCN και της υπηρεσίας IMS
2) Ενημέρωση Υπηρεσίας που σημαίνει δέσμευση πόρων στις δικτυακές λειτουργίες.
3) Διαφάνεια της εικονικοποίησης ως προς τις υπηρεσίες, έτσι ώστε οι υπηρεσίες να μπορούν να διακρίνουν αν η εκάστοτε λειτουργία είναι εικονικοποιημένη ή όχι
4) Διαφάνεια της εικονικοποίησης ως προς τον έλεγχο και τη διαχείριση δικτύου, έτσι ώστε να γνωρίζει τόσο ο έλεγχος δικτύου όσο και το πεδίο διαχείρισης αν η εκάστοτε λειτουργία είναι εικονικοποιημένη ή όχι.
5) Συντήρηση καταστάσεων τόσο του δικτύου όσο και των λειτουργιών του δικτύου μέσω συστήματος διαχείρισης κατά την επανατοποθέτηση, κλιμάκωση πόρων και αντιγραφή της κάθε λειτουργίας.
6) Παρακολούθηση/εντοπισμός σφαλμάτων/διάγνωση/ανάκαμψη. Πρέπει να υπάρχει ένας κατάλληλος μηχανισμός για να υποστηρίξει διάγνωση για όλα τα μέρη και τις καταστάσεις τους μετά την εικονικοποίηση πχ. VNF σταθερές, υλικό, hypervisor
7) Διαθεσιμότητα υπηρεσιών, εξασφαλίζοντας τον ίδιο βαθμό διαθεσιμότητας σε ένα από-άκρο-σε-άκρο εικονικοποιημένο Mobile Core Network όσο και σε ένα μη-εικονικοποιημενο με μειωμένο κόστος
8) Μηχανισμοί για τον έλεγχο του διαχωρισμού της κίνησης. Αναγνώριση/διαχωρισμός των υπηρεσιών Διαχείρισης Κίνησης και Διαχείρισης Δεδομένων τόσο για εικονικοποιημένα όσο και για μη-εικονικοποιημένα δίκτυα
9) Ελαχιστοποίηση αντικτύπου σε σχετικές δικτυακές λειτουργίες που είναι μη-εικονικοποιημένες και υποστήριξη δικτυακών λειτουργικών συστημάτων

1.3.5 Άλλες Περιπτώσεις Χρήσης

Με βάση τις προδιαγραφές του ETSI, περιγράφονται επισήμως και τις ακόλουθες περιπτώσεις χρήσης τα οποία αναφέρουμε επιγραμματικά, καθώς δεν καλύπτουν το γνωστικό πεδίο στο οποίο θα εστιάσουμε.

1.3.5.1 VNF Γράφοι Προώθησης

Ένας VNF Γράφος Προώθησης είναι το αντίστοιχο του να συνδέει κάποιος φυσικές συσκευές με καλώδια όπως αυτά περιγράφονται στην επίσημη έκθεση του NFV. Με δύο λόγια, παρέχει τη λογική σύνδεση μεταξύ εικονικών συσκευών.

1.3.5.2 Εικονικοποίηση του Σταθμού Βάσης

Η εικονικοποίηση του σταθμού βάσης, μπορεί να πετύχει διαμοιρασμό πόρων μεταξύ πολλαπλών λογικών RAN κόμβων από διαφορετικά συστήματα,δεσμεύοντας δυναμικά το πόρο αλλά και ελαττώνοντας την κατανάλωση ρεύματος.

1.3.5.3 Εικονικοποίηση Οικείου Περιβάλλοντος

Η NFV τεχνολογία διευκολύνει την εικονικοποίηση υπηρεσιών και την μετάβαση της λειτουργικότητας από τις οικιακές συσκευές στο NFV YN. Σε αυτή τη περίπτωση, ακολουθούμε την VNF πρόταση του NFV και διατηρούμε ένα εικονικοποιημένο αντίγραφο της αρχικής συσκευής. Έτσι, διατηρούνται όσο το δυνατόν περισσότερο οι αρχικές διεπαφές.

1.3.5.4 Εικονικοποίηση Δικτύων Μεταφοράς Περιεχομένων

Η ενσωμάτωση κόμβων των Δικτύων Μεταφοράς Περιεχομένων (CDNs) σε δίκτυα παρόχων, μπορεί να είναι ένας τρόπος και οικονομικά συμφέρων και αποτελεσματικός, προκειμένου να δοθεί μια απάντηση στη πρόκληση της Μεταφοράς Κίνησης Βίντεο (VTD). Παράγοντας τις ροές περιεχομένου από κόμβους υπολογιστικούς/αποθήκευσης πιο κοντά στον τελικό πελάτη, εξοικονομούνται σύνδεσμοι ανωτέρου δικτύου και ο εξοπλισμός. Επίσης επιτρέπει στις ροές να μεταφέρονται με μεγαλύτερο εύρος ζώνης και σε πιο αξιόπιστη ποιότητα.

1.3.5.5 Εικονικοποίηση Δικτύου Σταθερής Πρόσβασης

Η εικονικοποίηση των λειτουργιών του δικτύου πρόσβασης, θα εφαρμοστεί αρχικά σε DSL κόμβους υβριδίου ίνας, όπως ο FTTcab και ο FTTdp. Αυτοι οι κόμβοι, θα βρίσκονται βαθιά μέσα στο δίκτυο πρόσβασης, εντός ήδη υπαρχόντων καμπινών (FTTcab) ή στη περίπτωση του FTTdp, τοποθετημένο υπόγεια ή σε πόλους ή σε κτήρια πολλαπλής κατοχής. Εφαρμόζοντας τις NFV αρχές, η πολυπλοκότητα του υλικού στον κινητό κόμβο,μπορεί να ελαττωθεί εξοικονομώντας ενέργεια και ενισχυμένο βθαμό προφύλαξης καθώς οι υπηρεσίες εξελίσσονται

1.4 EPC

Το EPC (Evolved Packet Core) αποτελεί κομμάτι της εξέλιξης της αρχιτεκτονικής του συστήματος (System Architecture Evolution, γνωστό ως εκ τούτου και με το όνομα SAE Core). Σκοπός του EPC είναι η εξυπηρέτηση ως το ισοδύναμο των GPRS Networks μέσω των επιμέρους κομματιών (components) του (Mobility Management Entity, Serving Gateway, PDN Gateway ή PGW).

1.4.1 Mobility Management Entity (MME)

Το MME είναι ο κύριος κόμβος ελέγχου για το δίκτυο πρόσβασης LTE. Είναι υπεύθυνο για το idle mode UE (User Equipment) paging and tagging procedure (διαδικασία σελιδοποίησης και ταμπελοποίησης σε ανενεργή κατάσταση εξοπλισμού χρήστη) συμπεριλαμβανομένων και των αναμεταδόσεων. Εμπλέκεται στην διεργασία ενεργοποίησης/απενεργοποίησης ορίων και είναι επίσης υπεύθυνο για την επιλογή του S-GW για ένα UE κατά την αρχική προσάρτηση και κατά τη στιγμή της παράδοσης εσωτερικά του LTE, κάτι που περιλαμβάνει επανατοποθέτηση κόμβου του πυρήνα του δικτύου. Είναι υπεύθυνο για την αυθεντικοποίηση του χρήστη (επικοινωνώντας με το HSS).

Η σηματοδότηση Στρώματος-Άνευ-Πρόσβασης (Non Access Stratum, NAS) τερματίζει στο MME και είναι επίσης υπεύθυνο για την γένεση και δέσμευση των προσωρινών ταυτοτήτων σε UEs. Τσεκάρει την εξουσιοδότηση του UE για εγκατάσταση στο ασύρματο δίκτυο δημόσιας έκτασης (Public Land Mobile Network, PLMN) του παρόχου υπηρεσιών και ενισχύει τους περιορισμούς περιαγωγής. Το MME είναι το σημείο τερματισμού στο δίκτυο για προστασία κρυπτογράφησης/ακεραιότητας για τη NAS

σηματοδότηση και χειρίζεται τη διαχείριση κλειδιών ασφαλείας. Νόμιμη υποκλοπή του σηματοδότηση επίσης υποστηρίζεται από το MME. Το MME επίσης παρέχει τη λειτουργία πεδίου ελέγχου (control plane) για φορητότητα ανάμεσα στα δίκτυα πρόσβασης LTE και 2G/3G με την διεπαφή S3 να τερματίσει στο MME από το SGSN. Το MME επίσης τερματίζει την διεπαφή S6a προς το home HSS για UEs περιαγωγής.

1.4.2 Πύλη Εξυπηρέτησης - Serving Gateway (S-GW)

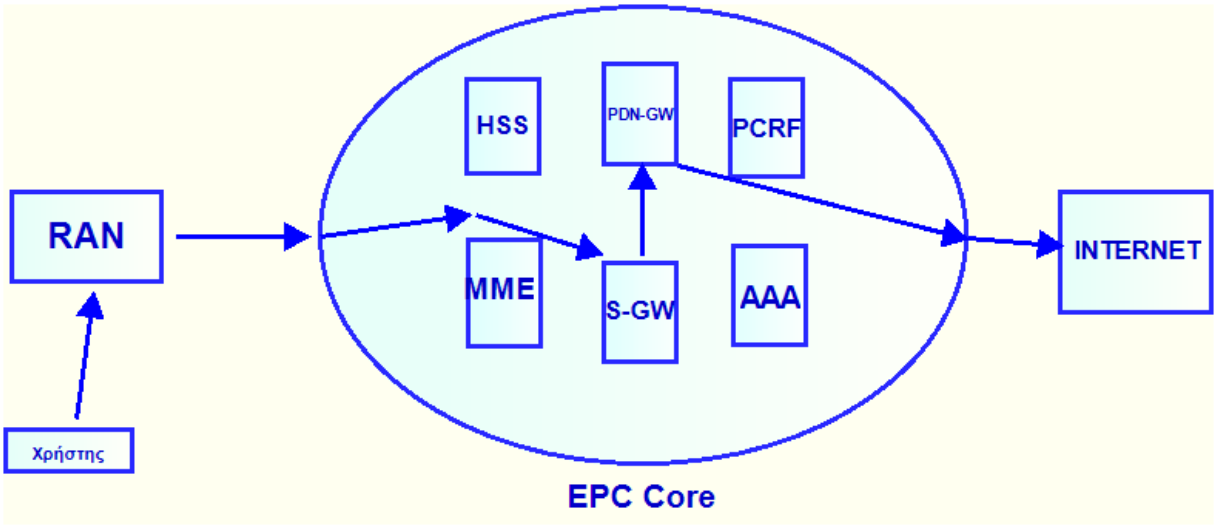
Το S-GW δρομολογεί και προωθεί πακέτα δεδομένων χρηστών, ενώ λειτουργεί επίσης σαν άγκυρα φορητότητας για το πεδίο χρήστη (user plane) κατά τη διάρκεια των παραδόσεων εσωτερικά του eNodeB και ως η άγκυρα για φορητότητα μεταξύ LTE και άλλων 3GPP τεχνολογιών (τερματίζει τη διεπαφή S4 και την μετεγκατάσταση κίνησης μεταξύ των 2G/3G συστημάτων και του P-GW). Για UEs ανενεργού κατάστασης, το S-GW τερματίζει το κατερχόμενο μονοπάτι δεδομένων (downlink datapath) και εκκινεί προσπάθεια εντοπισμού όταν τα downlink δεδομένα φτάνουν για το UE. Διαχειρίζεται και αποθηκεύει UE περιεχόμενα, όπως για παράδειγμα παραμέτρους της IP υπηρεσίας κομιστή, πληροφορίες εσωτερικής δρομολόγησης δικτύου, αντιγράφει επίσης τη κίνηση του χρήστη σε περίπτωση νόμιμης υποκλοπής.

1.4.3 Πύλη Δικτύωσης Πακέτων Δεδομένων - Packet Data Networking Gateway (PDN Gateway ή P-GW)

Το PDN Gateway, παρέχει συνδεσιμότητα μεταξύ του UE και των εξωτερικών δικτύων πακέτων δεδομένων, στο σημείο εξόδου και εισόδου της κίνησης για το UE. Το UE μπορεί να έχει ταυτόχρονη συνδεσιμότητα με πάνω από ένα PGW για να έχει πρόσβαση σε πολλαπλά PDNs. Το P-GW εκτελεί ενίσχυση πολιτικής, φιλτράρισμα πακέτων για κάθε χρήστη, υποστήριξη χρέωσης νόμιμη υποκλοπή και διαλογή πακέτων. Άλλος ένας σημαντικός ρόλος του PGW είναι να λειτουργεί ως η άγκυρα μεταξύ 3GPP και μη-3GPP τεχνολογίες όπως το WiMAX και 3GPP2 (CDMA 1X και EvDO).

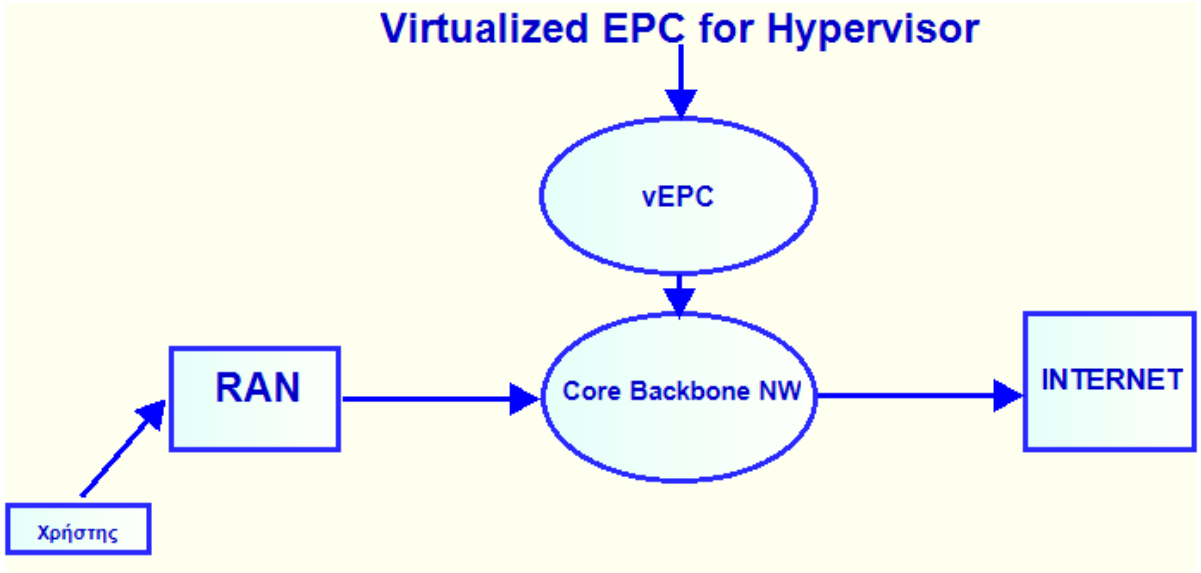
1.5 Αρχιτεκτονικός Σχεδιασμός

Στο παρόν κεφάλαιο, θα σχεδιάσουμε μια αρχιτεκτονική σε επίπεδο υπηρεσίας YN. Σκοπός της σχεδίασης αυτής, είναι να δώσουμε μια πλήρη περιγραφή της πορείας δεδομένων από-άκρο-σε-άκρο (end-to-end). Μια περιγραφή η οποία περιλαμβάνει τα πρωτόκολλα τα οποία πρέπει να τηρηθούν καθώς και τους μηχανισμούς κρυπτογραφίας μέσω των οποίων, μπορούμε να εγγυηθούμε την ασφαλή μετάβαση των δεδομένων από το σημείο A στο σημείο B, ελαχιστοποιώντας δυνατότητα παρέμβασης από κακόβουλους τρίτους, με σκοπό την υποκλοπή δεδομένων



Σχήμα 18: Η πρώτη εικόνα του EPC (Evolved Packet Core)

Σε αυτή την πρώτη εικόνα βλέπουμε την διαδρομή των δεδομένων από χρήστες του δικτύου, σε μεταδότες τύπου RAN, οι οποίοι το μεταδίδουν με τη σειρά τους στο πυρήνα του EPC, και από εκεί, στο διαδίκτυο.



Σχήμα 19: Η πλήρης εικόνα του Πεδίου Ελέγχου (Control Plane): (Χρήστης – RAN – vEPC – INTERNET) και του Πεδίου Χρήστη (User Plane): (Χρήστης – RAN – Core Backbone NW – INTERNET)

Θα εστιάσουμε περισσότερο στο πεδίο χρήστη, για να εντοπίσουμε τα πρωτόκολλα που ακολουθούνται, τους κανόνες ασφαλείας που διέπουν τη λειτουργία του αλλά και τους κανόνες κρυπτογραφίας που εφαρμόζονται. Όπως αναφέραμε και προηγουμένως, θα δείξουμε το «ταξίδι» ενός πακέτου δεδομένων από τον χρήστη ενός δικτύου πρόσβασης (AN) μέσω του YN στις ακόλουθες περιπτώσεις: σε κάποιον πάροχο, στο ίδιο το AN και σε κάποιον διεθνή κόμβο.
Πριν από αυτό, όμως, θα δούμε κάποιους βασικούς κανόνες για το πως δύνανται να λάβει χώρα μια τέτοια ενέργεια. Ποιά πρωτόκολλα χρησιμοποιούνται εντός του YN, το

ρόλο που παίζουν τα μοντέλα κρυπτογραφίας-ως-υπηρεσία (Cryptography as a Service) και ασφάλειας-ως-υπηρεσία (Security as a Service) στο κρίσιμο ζήτημα της ασφάλειας μεταφοράς δεδομένων.

1.5.1 ΠΡΩΤΟΚΟΛΛΑ ΕΝΤΟΣ ΥΝ

Προκειμένου να προχωρήσουμε στην περιγραφή του εκάστοτε πρωτοκόλλου, θα δούμε πρωτίστως από ποια επιμέρους τμήματα (components) αποτελείται το ΥΝ και με ποια πρωτόκολλα επικοινωνούν αυτά μεταξύ τους:

- MME
- S/P-GW
- HSS
- PCRF

Εμάς, σύμφωνα και με το αρχικό Σχήμα 1.1, μας απασχολεί η επικοινωνία των Service Gateway και Packet (Data Network) Gateway. Τα components αυτά, επικοινωνούν μέσω του GTPv1 πρωτοκόλλου.

1.5.2 Κρυπτογραφία ως Υπηρεσία (Cryptography as a Service, CaaS)

Το μοντέλο Cryptography as a Service (CaaS) επιτρέπει σε ενέργειες να γίνονται χωρίς την έκθεση των κρυπτογραφικών κλειδιων. Κρυπτογραφικές ενέργειες όπως κρυπτογράφηση και αποκρυπτογράφηση, πραγματοποιούνται από τον CaaS πάροχο εκ μέρους μιας συσκευής μέσω APIs διαδικτυακών υπηρεσιών. Τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται για να λάβουν χώρα αυτές οι ενέργειες, αποθηκεύονται εντός του CaaS παρόχου, έτσι ώστε οι συσκευές να μην κατέχουν τα κλειδιά ανα πάσα στιγμή.

1.5.3 Ασφάλεια ως Υπηρεσία (Security as a Service)

Το **Security as a service (SECaaS)** μοντέλο αποτελεί ένα επιχειρηματικό μοντέλο στο οποίο ένας μεγάλος πάροχος υπηρεσιών ενσωματώνει τις υπηρεσίες ασφαλείας τους σε μια εταιρική υποδομή σε μια βάση εγγραφής, με μεγαλύτερη αποτελεσματικότητα ως προς το κόστος σε σχέση με ότι μπορούν να προσφέρουν πολλοί μεμονωμένοι ή εταιρείες, όταν μιλάμε για τελικό κόστος ιδιοκτησίας.
Σε αυτό το σενάριο, η ασφάλεια μεταφέρεται σαν μια υπηρεσία από το ΥΝ, χωρίς να απαιτεί εγκατεστημένο υλικό, αποφεύγοντας έτσι, σημαντικές δαπάνες κεφαλαίου. Αυτές οι υπηρεσίες ασφαλείας συχνά περιλαμβάνουν **αυθεντικοποίηση, anti-virus, anti-malware/spyware, έλεγχο εισβολής, και διαχείριση συμβάντων ασφαλείας, μεταξύ άλλων.**
Το Security as a Service, παρέχει μια σειρά από προνόμια:

- Συνεχείς ενημερώσεις σε ορισμό ιών τα οποία δεν εξαρτώνται από την ανεκτικότητα του χρήστη.
- Μεγαλύτερη εξειδίκευση ασφαλείας η οποία είναι τυπικά διαθέσιμη εντός μιας οργάνωσης.
- Ταχύτερη τροφοδοσία του χρήστη.

- Εξωτερική ανάθεση των διοικητικών εργασιών, όπως διαχείριση καταγραφής, για εξοικονόμιση χρόνου και χρήματος και να επιτρέψει σε μια οργάνωση να αφιερώσει παραπάνω χρόνο στους κύριους ανταγωνιστές της.
- Μια δικτυακή διεπαφή, η οποία επιτρέπει οικιακή διοίκηση κάποιων εργασιών, καθώς και μια οπτική του περιβάλλοντος ασφαλείας, και των δραστηριοτήτων που λαμβάνουν χώρα εκεί.

Ένα παράδειγμα υλοποίησης του Security-as-a-Service, **αποτελεί η πρόταση της Alert Logic**, που χωρίζεται σε 3 βασικά κομμάτια:

I) Διαχειριστής απειλών (Threat Manager) Activewatch

Ο διαχειριστής απειλών της ActiveWatch παρακολουθεί 24 ώρες το 24ωρο την κίνηση εντός του δικτύου, και μέσω ενός έξυπνου συσχετισμού πολλών παραγόντων, είναι σε θέση να αναγνωρίσει γρήγορα περιστατικά ασφαλείας που απαιτούν προσοχή.
Χαρακτηριστικά του αποτελούν τα ακόλουθα:

- **Είναι σχεδιασμένο για ανάπτυξη σε κάθε περιβάλλον.** Και σε δημόσιο και σε ιδιωτικό ΥΝ, είναι ελαστικό ως προς τη κλιμάκωση του. Παρέχει μια φιλοξενούμενη υποδομή που έχει εποπτεία του ΥΝ, καθώς και χρέωση ανάλογα με τη χρήση προκειμένου να ανταποκριθεί στις ανάγκες του μοντέλου χρήσης του ΥΝ.
- **Κανόνες και υπογραφές απειλών.** 52000 υπογραφές απειλών σε μια βάση δεδομένων που ανανεώνεται κάθε εβδομάδα. Σύνολο κανόνων που καθορίζεται από ποικίλες πηγές (ερευνητική ομάδα της AL, επερχόμενες απειλές, συνεργασίες με τρίτους ανοιχτού λογισμικού). Ανανέωση υπογραφών στο εξειδικευμένο σύστημα της AL, σε πραγματικό χρόνο. Προσαρμοσμένη δημιουργία και επεξεργασία κανόνων.
- **Εκτίμηση ευπάθειας και εντοπισμός εισβολής.** Απεριόριστα και εσωτερικά σκαναρίσματα. Ευρεία ορατότητα σκαναρίσματος και εντοπισμού. Υποδομή δικτύου και διακομιστή. Εφαρμογές σημαντικές για τις επιχειρήσεις. Δικτυακές τεχνολογίες (IPv6, Ajax, SQL Injection κλπ). Κίνηση εισβολών βασισμένη σε SSL.
- **Ανάλυση και εκθέσεις.** Δυνατότητα προσαρμοσμένων εκθέσεων. Σύστημα Καταμέτρησης Κοινής Ευπάθειας για εκτίμηση ρίσκου. Εκθέσεις έτοιμες για λογιστικό έλεγχο. Λεπτομερείς έκθεσεις για ευπάθεια και εξυπηρέτηση που παρέχουν λεπτομερείες περιγράφες και λίστες των εξυπηρετητών που επηρεάζονται, των επιπέδων ρίσκου και των προτάσεων εξυγίανσης. Μονή κονσόλα βασισμένη στο δίκτυο για όλο το περιβάλλον. Διαχείριση χρήστη. Ανάλυση drill-down και dashboards. Προγραμματισμός, δημιουργία και αξιολόγηση εκθέσεων. Προγραμματισμός σκαναρίσματος και αξιολόγηση αποτελεσμάτων.
- **Ολοκληρωμένα διαχειριζόμενες υπηρεσίες ασφαλείας.** Πιστοποιημένοι από το GIAC ερευνητές και αναλυτές ασφαλείας. 24ωρο Κέντρο Επιχειρήσεων Ασφαλείας τελευταίας τεχνολογίας. Εκπαιδευμένοι ειδικοί σε λύσεις της Alert Logic. Δυνατότητες παρακολούθησης, ανάλυσης και καθοδήγησης από ειδικούς. Προσαρμοσμένες διαδικασίες ειδοποίησης και κλιμάκωσης. Ημερήσια αξιολόγηση από έμπειρο αναλυτή και διαθέσιμη εβδομαδιαία έκθεση. Διαθέσιμη αξιολόγηση των NetFlow δεδομένων για ενισχυμένο κακόβουλο λογισμικό και APT.
- **Υποστήριξη Συμβατότητας.** Προμηθευτής Σκαναρίσματος εγκεκριμένο από το PCI. Ελεγμένος προμηθευτής επιπέδου 2 PCI. Υποστήριξη για πολλαπλές εντολές συμμόρφωσης. PCI DSS, HIPAA, SOX, GLBA, CoBIT κλπ. 6μηνη αποθήκευση όλων των ακατέργαστων IDS δεδομένων συμβάντων. Κέντρα

δεδομένων με πιστοποίηση SSAE 16 τύπου II. Απεριόριστος αποθηκευτικός χώρος και αρχείο ανάλυσης και περιπτώσεων περιστατικών

- **Απόδοση του Security-as-a-Service.** Άμεση ανάπτυξη και κλιμάκωση ανάλογα με τις ανάγκες που υπάρχουν. Χρέωση-κατά-την-έξοδο, ελάχιστες δαπάνες κεφαλαίου. Πάντα χρησιμοποιείται το νεότερο λογισμικό και η χαρακτηριστική βάση δεδομένων. Δεν υπάρχουν κρυμμένα κόστη – η εγγραφή περιλαμβάνει: ανανεώσεις λογισμικού και υλικού. Δομημένο για πολυχρηστική εξυπηρέτηση. Εύκολα αναπτύσσεται σε δημόσιο ΥΝ, ιδιωτικό ΥΝ, διαχειριζόμενη εξυπηρέτηση, επιχείρηση κέντρου δεδομένων ή υβριδικά περιβάλλοντα

II) Αναπτυσσόμενος εντοπισμός απειλών (Advancing Threat Detection) Activeintelligence

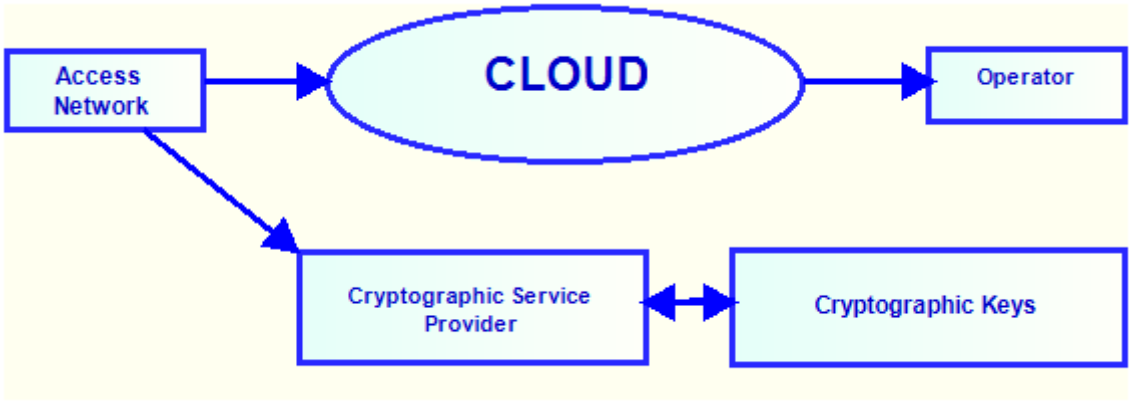
Η δημιουργία και συντήρηση ενημερωμένου περιεχομένου, είναι ένα κρίσιμο κομμάτι μιας ισχυρής στρατηγικής. Η εφαρμογή ActiveIntelligence Alert Logic ανταποκρίνεται σε αυτή την απαίτηση και παίζει έναν σημαντικό ρόλο στην ικανότητα του Alert Logic Cloud Defender να παρέχει συνεχή προστασία για τα ευαίσθητα δεδομένα της οργάνωσης. Η εφαρμογή αυτή αποτελείται από ερευνητές ασφαλείας και αναλυτές ευφυίας απειλών, οι οποίοι συνεργάζονται για να δημιουργήσουν και διαχειριστούν περιεχόμενο ασφαλείας. Αυτό το περιεχόμενο επιτρέπει στην πρόταση της Alert Logic να αναγνωρίσει περιστατικά που απαιτούν αξιολόγηση από την Alert Logic ActiveWatch ομάδα, ενώ διαγράφουν άσχετα περιστατικά ασφαλείας. Αντίθετα με άλλες προτάσεις ασφαλείας που απαιτούν οργανισμούς να βρουν, δημιουργήσουν και να διαχειριστούν εν τέλει το ίδιο τους το περιεχόμενο ασφαλείας, η Alert Logic επενδύει σημαντικά στην έρευνα αυτή, που καθιστά τον Alert Logic Cloud Defender πραγματικά μοναδικό.
Ενώ δεν είναι επιφορτισμένοι με τον έλεγχο της υποδομής του πελάτη μέρα-με-τη-μέρα, οι ευθύνες που έχουν οι ερευνητές του περιεχομένου ασφαλείας είναι εξίσου σημαντικές. Οι ερευνητές περιεχομένου ασφαλείας τυπικά χωρίζουν το χρόνο τους σε διαχείριση του υπάρχοντος περιεχομένου απειλής και συστημάτων ευφυίας, ανάπτυξη κανόνων τείχους προστασίας δικτυακών εφαρμογών, παραγωγή αναλυτών διαχείρισης εισόδου, συνεργασία με τη τροφοδοσία δεδομένων από τρίτους, δημιουργία λογικής συσχέτισης και υλοποίηση στατιστικής ανάλυσης. Οι ερευνητές έχουν έναν απλό σκοπό – να δημιουργήσουν κατανοητό περιεχόμενο ασφαλείας με τη ευρύτερη δυνατή κάλυψη απειλών.

III) Διαχειριστής εισόδου (Log Manager)

- **Χαρακτηριστικά και δυνατότητες της τεχνολογίας.** Ευκολία στη χρήση των δικτυακών διεπαφών με ευκολονόητη διεπαφή αναζήτησης. Πάνω από 4000 αναλυτές διαθέσιμοι σε κάθε νέο τύπο εισόδου που προστίθεται συχνά. Αποθηκευτικός χώρος υ.ν. με δημιουργία αντιγράφου εκτός του χώρου για ανάκτηση σε περίπτωση καταστροφής.
- **Συσχέτιση συμβάντων και ειδοποίηση.** Ανεπτυγμένες δυνατότητες συσχέτισης. Σχεδιασμένο για να εντοπίζει ύποπτη δραστηριότητα. Αυτόματα σήματα συναγερμού στέλνονται όταν κάποιος κανόνας παραβιάζεται. Οι κανόνες που εξαρτώνται από το PCI συμμορφώνται με τις απαιτήσεις του 10.6

Ακολουθούν τα σενάρια-διαφορετικές αρχιτεκτονικές, που περιγράψαμε στην αρχή. Ας σημειωθεί ότι θα αναφερόμαστε στα σημεία τερματισμού ως εξής: Ε1 (Δίκτυο Πρόσβασης) Ε2 (ΥΝ) Ε3 (Πάροχος, ΔΠ ή διεθνείς κόμβους). Υπάρχουν τα ακόλουθα σενάρια που θα μελετήσουμε λοιπόν:

1.5.4 Σενάριο 1ο: ΔΙΚΤΥΟ ΠΡΟΣΒΑΣΗΣ – Υ.Ν. – ΠΑΡΟΧΟΣ



Σχήμα 20 Σχήμα διασύνδεσης Δικτύου πρόσβασης – Υ.Ν. – Παρόχου

Σε αυτό το σχήμα, παρατηρούμε το μονοπάτι το οποίο ακολουθεί ένα πακέτο δεδομένων από το δίκτυο πρόσβασης για να φτάσει στο υ.ν. και από εκεί σε κάποιον πάροχο. Αυτά που λαμβάνουν χώρα είναι τα κάτωθι:

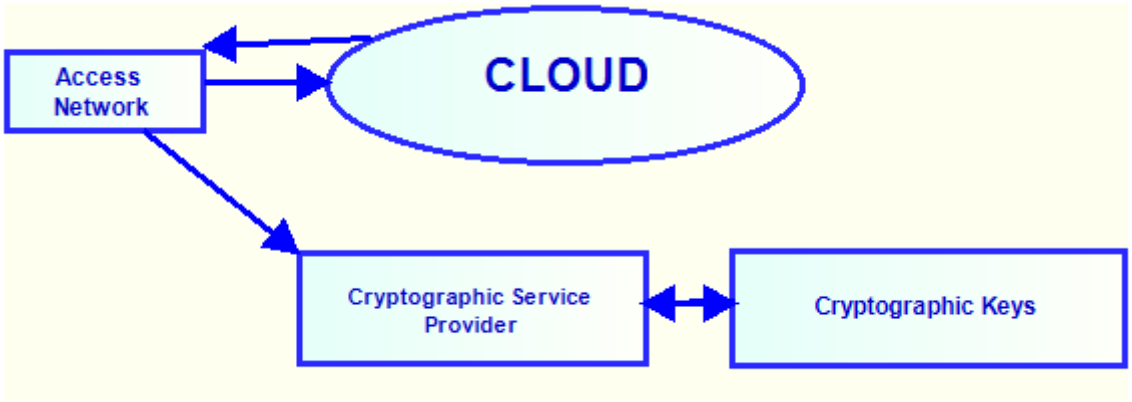
- **Επικοινωνία δικτύου πρόσβασης και παρόχου με δίκτυο παρόχου κρυπτογραφικής υπηρεσίας και κρυπτογραφικών κλειδιών** που φροντίζει κανένας από τα 2 σημεία τερματισμού (E1, E3) να μην έχει τα κλειδιά, βάσει του Cryptography as a Service μοντέλου.
- **Επικοινωνία δικτύου πρόσβασης με ΥΝ** για την μετάβαση του πακέτου από το ΔΠ στο ΥΝ.

Η μετάβαση του πακέτου δεδομένων (και του κάθε μηνύματος) από το σημείο πρόσβασης (ΣΠ) ενός δικτύου πρόσβασης προς οποιονδήποτε γίνεται μέσω πρωτοκόλλου 802.11 (παράλληλα έχουμε αναμετάδοση προς την αντίθετη κατεύθυνση, γιατί στο δίκτυο πρόσβασης χρησιμοποιείται το πρωτόκολλο 802.3, άρα πρέπει να γίνει προσαρμογή).

Το ΥΝ για να λάβει το πακέτο δεδομένων, αξιοποιεί το δίπολο MME – HSS, το οποίο αποφασίζει την αυθεντικοποίηση του χρήστη που στέλνει το πακέτο αυτό. Μόλις η διαδικασία αυτή ολοκληρωθεί επιτυχώς, το πακέτο βρίσκεται εντός του ΥΝ.

- **Μετακίνηση εντός του ΥΝ** – Πραγματοποιείται μέσω του GTPv1 πρωτοκόλλου ανάμεσα στα S-GW και P-GW τμήματα του ΥΝ. Κύριος ρόλος του S-GW (Serving Gateway), είναι η δρομολόγηση και προώθηση πακέτων δεδομένων χρηστών όπως ειπώθηκε και προηγουμένως. Όταν ο χρήστης επιθυμήσει να προωθηθεί το πακέτο του σε εξωτερικό δίκτυο, εκεί χρησιμοποιείται το P-GW (Packet Gateway). Το P-GW, φροντίζει για την επιλογή, μη-υποκλοπή και σωστή προώθηση του πακέτου αυτού
- **Επικοινωνία ΥΝ με πάροχο** – Η μετάβαση του πακέτου δεδομένων από το ΥΝ στον πάροχο γίνεται μέσω του πρωτοκόλλου 802.11.

1.5.5 Σενάριο 2ο: ΔΙΚΤΥΟ ΠΡΟΣΒΑΣΗΣ – Υ.Ν. – ΔΙΚΤΥΟ ΠΡΟΣΒΑΣΗΣ



Σχήμα 21 Σχήμα διασύνδεσης Δικτύου πρόσβασης – Υ.Ν. – Δικτύου Πρόσβασης

Σε αυτό το σχήμα, παρατηρούμε το μονοπάτι το οποίο ακολουθεί ένα πακέτο δεδομένων από το δίκτυο πρόσβασης για να φτάσει στο ΥΝ και από εκεί πίσω στο δίκτυο πρόσβασης. Αυτά που λαμβάνουν χώρα είναι τα κάτωθι:

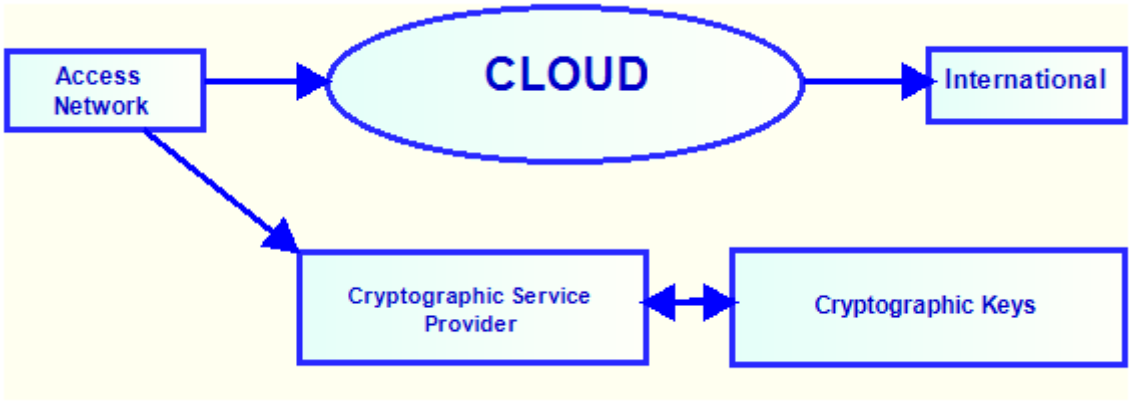
- **Επικοινωνία δικτύου πρόσβασης και παρόχου με δίκτυο παρόχου κρυπτογραφικής υπηρεσίας και κρυπτογραφικών κλειδιών** που φροντίζει κανένας από τα 2 σημεία τερματισμού (Ε1, Ε3) να μην έχει τα κλειδιά, βάσει του Cryptography as a Service μοντέλου.
- **Επικοινωνία δικτύου πρόσβασης με ΥΝ** για την μετάβαση του πακέτου από το ΔΠ στο ΥΝ.

Η μετάβαση του πακέτου δεδομένων (και του κάθε μηνύματος) από το σημείο πρόσβασης (ΣΠ) ενός ΔΠ προς οποιονδήποτε γίνεται μέσω πρωτοκόλλου 802.11 (παράλληλα έχουμε αναμετάδοση προς την αντίθετη κατεύθυνση, γιατί στο Access Network χρησιμοποιείται το πρωτόκολλο 802.3, άρα πρέπει να γίνει προσαρμογή).

Το ΥΝ για να λάβει το πακέτο δεδομένων, αξιοποιεί το δίπολο MME – HSS, το οποίο αποφασίζει την αυθεντικοποίηση του χρήστη που στέλνει το πακέτο αυτό. Μόλις η διαδικασία αυτή ολοκληρωθεί επιτυχώς, το πακέτο βρίσκεται εντός του ΥΝ.

- **Μετακίνηση εντός του ΥΝ** – Πραγματοποιείται μέσω του GTPv1 πρωτοκόλλου ανάμεσα στα S-GW και P-GW τμήματα του ΥΝ. Κύριος ρόλος του S-GW (Serving Gateway), είναι η δρομολόγηση και προώθηση πακέτων δεδομένων χρηστών όπως αναφέρθηκε και προηγουμένως. Όταν ο χρήστης επιθυμήσει να προωθηθεί το πακέτο του σε εξωτερικό δίκτυο, εκεί χρησιμοποιείται το P-GW (Packet Gateway). Το P-GW, φροντίζει για την επιλογή, μη-υποκλοπή και σωστή προώθηση του πακέτου αυτού.
- **Επικοινωνία ΥΝ με δίκτυο πρόσβασης** Η μετάβαση του πακέτου δεδομένων (και του κάθε μηνύματος) από το ΥΝ προς το σημείο πρόσβασης (ΣΠ) ενός δικτύου πρόσβασης γίνεται μέσω πρωτοκόλλου 802.11 (παράλληλα έχουμε αναμετάδοση προς την αντίθετη κατεύθυνση, γιατί στο δίκτυο πρόσβασης χρησιμοποιείται το πρωτόκολλο 802.3, άρα πρέπει να γίνει προσαρμογή).

1.5.6 Σενάριο 3ο: ΔΙΚΤΥΟ ΠΡΟΣΒΑΣΗΣ – Υ.Ν. – ΔΙΕΘΝΗΣ ΚΟΜΒΟΣ



Σχήμα 22 Σχήμα διασύνδεσης Δικτύου Πρόσβασης – Υ.Ν. – Διεθνής κόμβος

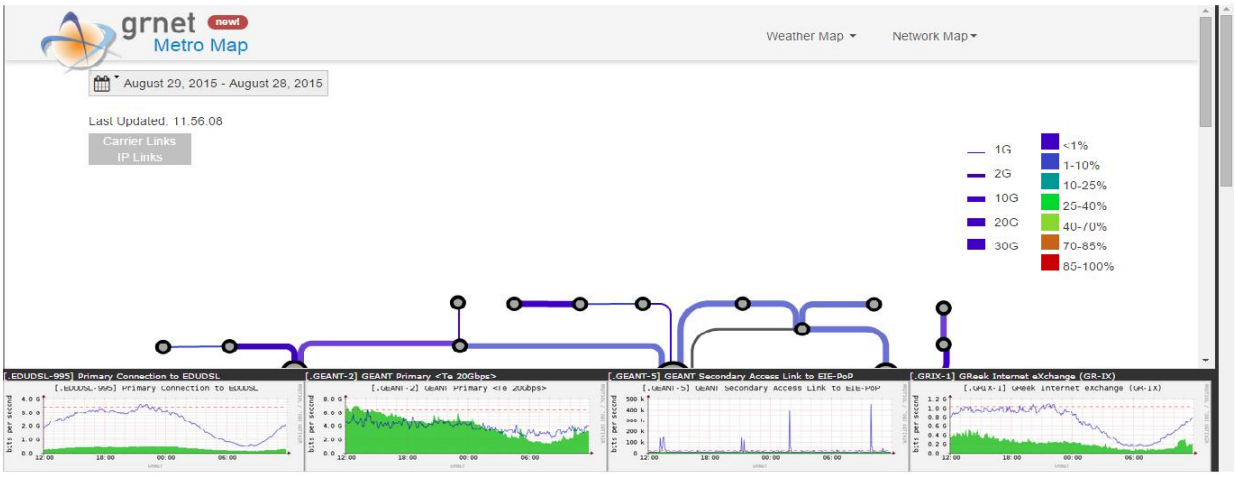
Σε αυτό το σχήμα, παρατηρούμε το μονοπάτι το οποίο ακολουθεί ένα πακέτο δεδομένων από το δίκτυο πρόσβασης για να φτάσει στο ΥΝ, και από εκεί σε κάποιον διεθνή κόμβο. Αυτά που λαμβάνουν χώρα είναι τα κάτωθι:

- **Επικοινωνία δικτύου πρόσβασης και διεθνούς κόμβου με δίκτυο παρόχου κρυπτογραφικής υπηρεσίας και κρυπτογραφικών κλειδιών** που φροντίζει κανένας από τα 2 σημεία τερματισμού να μην έχει τα κλειδιά, βάσει του Cryptography as a Service μοντέλου.
- **Επικοινωνία δικτύου πρόσβασης με ΥΝ.** για την μετάβαση του πακέτου από το δίκτυο πρόσβασης στο ΥΝ..

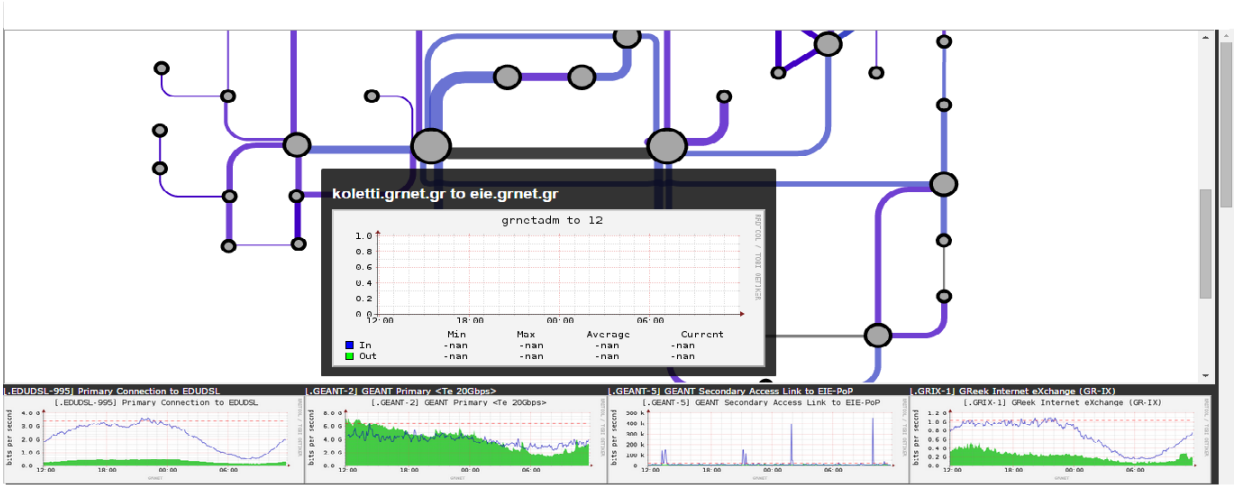
Η μετάβαση του πακέτου δεδομένων (και του κάθε μηνύματος) από το σημείο πρόσβασης ενός δικτύου πρόσβασης προς οποιονδήποτε γίνεται μέσω πρωτοκόλλου 802.11 (παράλληλα έχουμε αναμετάδοση προς την αντίθετη κατεύθυνση, γιατί στο δίκτυο πρόσβασης χρησιμοποιείται το πρωτόκολλο 802.3, άρα πρέπει να γίνει προσαρμογή).

Το ΥΝ για να λάβει το πακέτο δεδομένων, αξιοποιεί το δίπολο MME – HSS, το οποίο αποφασίζει την αυθεντικοποίηση του χρήστη που στέλνει το πακέτο αυτό. Μόλις η διαδικασία αυτή ολοκληρωθεί επιτυχώς, το πακέτο βρίσκεται εντός του ΥΝ.

- **Μετακίνηση εντός του ΥΝ** – Πραγματοποιείται μέσω του GTPv1 πρωτοκόλλου ανάμεσα στα S-GW και P-GW τμημάτων του ΥΝ. Κύριος ρόλος του S-GW (Serving Gateway), είναι η δρομολόγηση και προώθηση πακέτων δεδομένων χρηστών όπως ειπώθηκε και προηγουμένως. Όταν ο χρήστης επιθυμήσει να προωθηθεί το πακέτο του σε εξωτερικό δίκτυο, εκεί χρησιμοποιείται το P-GW (Packet Gateway). Το P-GW, φροντίζει για την επιλογή, μη-υποκλοπή και σωστή προώθηση του πακέτου αυτού.
- **Επικοινωνία ΥΝ με διεθνή κόμβο** – Η μετάβαση του πακέτου δεδομένων (και του κάθε μηνύματος) από το ΥΝ σε οποιονδήποτε διεθνή κόμβο γίνεται μέσω πρωτοκόλλου 802.11. Παρακάτω χρησιμοποιούμε για παράδειγμα, screenshots από το Dashboard που παρέχει το grnet, το οποίο Dashboard, μας δίνει πληροφορίες για την κίνηση πακέτων μεταξύ κόμβων των Πανεπιστημίων σε όλη την Ελλάδα. Στις εικόνες αυτές βλέπουμε το εύρος ζώνης σε Gbit (Σχήμα 2.7) και εστιάζουμε στο κομμάτι επικοινωνίας του server kolleti.grnet.gr και eie.grnet.gr, ως χαρακτηριστικό παράδειγμα επικοινωνίας με international κόμβο. Ένας ακόμη λόγος που το χρησιμοποιούμε είναι για να δείξουμε ότι για να πραγματοποιηθεί με τις μικρότερες δυνατές καθυστερήσεις η κίνηση από και πρός το ΥΝ προς και από έναν international κόμβο απαιτείται bandwidth της τάξεως των 30 Gbit.



Σχήμα 23 Εύρος ζώνης (Bandwidth) σε G



Σχήμα 24 Παράδειγμα σύνδεσης με international κόμβο

2. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ασφάλεια των υπηρεσιών του ΥΝ, είναι ένα ζήτημα που ανέκαθεν απασχολούσε, και θα συνεχίσει να απασχολεί, όσο το κομμάτι αυτό της επιστήμης των Τηλεπικοινωνιών προοδεύει και εξελίσσεται. Οι απειλές για το υλικό των χρηστών του ΥΝ, διαρκώς εξελίσσονται, σχεδόν παράλληλα με την εξέλιξη των τεχνολογιών του ΥΝ. Από την υποκλοπή δεδομένων από κακόβουλους χρήστες μέχρι την αλλοίωση των δεδομένων αυτών από ιούς, οι κίνδυνοι παραμένουν και πρέπει να αντιμετωπίζονται με τη δέουσα σοβαρότητα.

Ως εκ τούτου, καταλήγουμε αρχικά στην χρήση των κρυπτογραφικών κλειδιών (εκτός του ΥΝ όπως είδαμε αναλυτικά προηγουμένως) για να προφυλάξουμε τα δεδομένα του χρήστη κατά τη μετάβαση του κάθε πακέτου από το σημείο πρόσβασης του δικτύου προσβασης προς το ΥΝ, ενισχύοντας έτσι την ασφάλεια τους έναντι του εκάστοτε κακόβουλου τρίτου, που θα επιχειρήσει να τα υποκλέψει. Το δεύτερο εργαλείο που χρησιμοποιείται, είναι τα πρωτόκολλα για την κίνηση εντός του ΥΝ. Μέσω των πρωτοκόλλων αυτών, τα δεδομένα κινούνται με ασφάλεια εντός του ΥΝ, χωρίς φθορές και με απόλυτο έλεγχο του τι πράξη λαμβάνει χώρα επάνω τους.

Αυτό που τελικά διαπιστώνουμε είναι, πως με κατάλληλη χρήση των μεθόδων/μηχανισμών κρυπτογραφίας που υπάρχουν διαθέσιμοι σε συνδυασμό με τις ήδη γνωστές αρχές περί λειτουργίας του ΥΝ και του NFV, μπορεί κάποιος να εγγυηθεί έναν σίγουρο περιορισμό των επιθέσεων σε προσωπικά δεδομένα από κακόβουλους, ελαττώνοντας σημαντικά το κόστος για την εγκαθίδρυση των μηχανισμών αυτών.

ΑΝΑΦΟΡΕΣ

[1] http://www.sdncentral.com/whats-network-functions-virtualization-nfv/

[2] http://www.f5.com/pdf/white-papers/service-provider-nfv-white-paper.pdf

[3] http://www.etsi.org/technologies-clusters/technologies/nfv

[4] http://en.wikipedia.org/wiki/Network_Functions_Virtualization

[5] http://en.wikipedia.org/wiki/Cloud_computing_security

[6] http://en.wikipedia.org/wiki/Cloud_communications

[7] http://www.alcatel-lucent.com/solutions/cloud

[8] https://en.wikipedia.org/wiki/Policy_and_charging_rules_function

[9] https://mon.grnet.gr/rg/dashboard/NOC Dashboard/

[10] https://en.wikipedia.org/wiki/Policy_and_charging_rules_function

[11] https://en.wikipedia.org/wiki/Capital_expenditure

[12] https://en.wikipedia.org/wiki/Operating_expense

[13] https://www.alertlogic.com/assets/threat-manager/AL_threat-manager_overview.pdf

[14] https://www.alertlogic.com/assets/activeintelligence/ActiveIntelligence-Overview.pdf

[15] https://www.alertlogic.com/assets/log-manager/AL_log-manager_overview.pdf

[16] ETSI Group Specifications NFV 001V.1.1.1 (2013-10)