ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Ευφυή Δίκτυα (Ι)

Εικονικά Ιδιωτικά Δίκτυα - Virtual Private Networks (VPN)

Πρωτόκολλα Tunneling, GRE & IPsec

Ανωνυμία, Πρωτόκολλα Tor (The Onion Router), Dark Web

Β. Μάγκλαρης

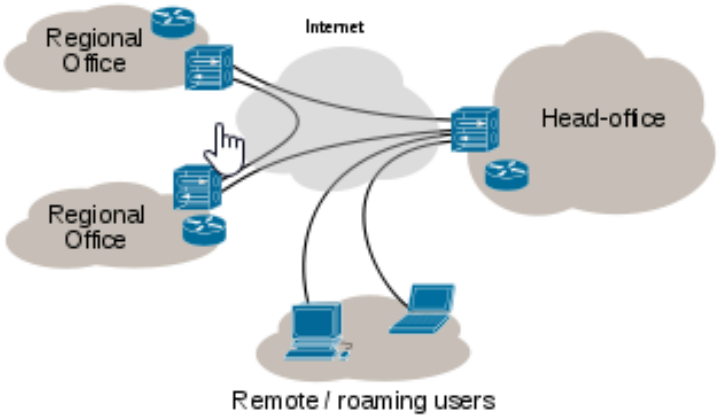
maglaris@netmode.ntua.gr

www.netmode.ntua.gr

3/12/2018

ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ

Virtual Private Networks - VPNs

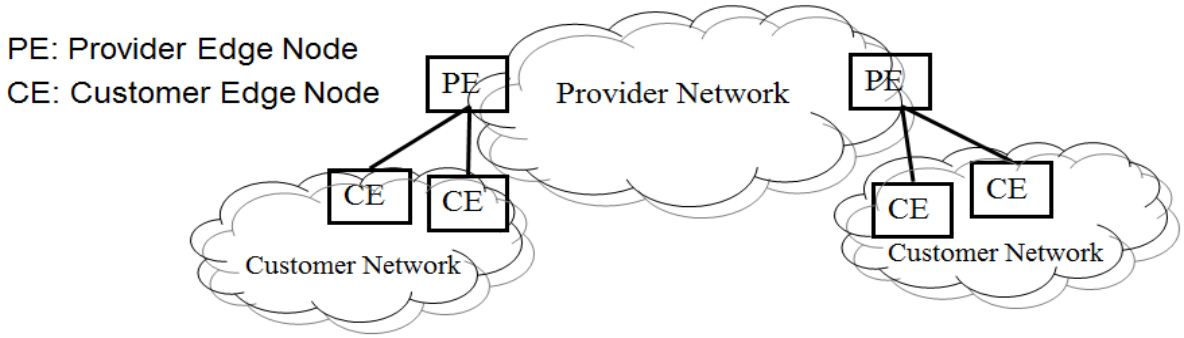


https://en.wikipedia.org/wiki/Virtual_private_network

Με τα **VPNs** χρήστες κοινών κατανεμημένων πόρων δημιουργούν **ιδιωτικές** υποδομές **Overlay Networks** ή εταιρικά δίκτυα **Intranet/Extranet** πάνω από **δημόσια** δίκτυα όπως το **Internet** ή δίκτυο μακράς αποστάσεως (Wide Area Network – WAN) ενός ISP αρχιτεκτονικής **IP/MPLS** ή **Enterprise Local Area Networks - LANs** & **Data Centers** με πολλαπλές αυτόνομες κοινότητες χρηστών, διασφαλίζοντας:

- Απομόνωση από άλλες κοινότητες π.χ. μέσω ενθυλάκωσης πακέτων του VPN (μαζί με τους ιδιωτικούς headers) σε πακέτα συμβατά με πρωτόκολλα Δημοσίου Δικτύου (**tunneling**)
- Διαχείριση δικτυακών πόρων & υπηρεσιών ανά VPN:
  - Επέκταση πεδίου διευθύνσεων **VLAN tags** ή **IP** σε απομακρυσμένες νησίδες ενός VPN
  - Δρομολόγηση με περιορισμούς ασφαλείας και διαμοιρασμού φορτίου – **traffic engineering**
  - Ασφαλής μετάδοση και σηματοδοσία όπως σε αυστηρά ελεγχόμενο τοπικό δίκτυο (LAN)

ΕΙΔΗ VPNs & Tunneling Protocols

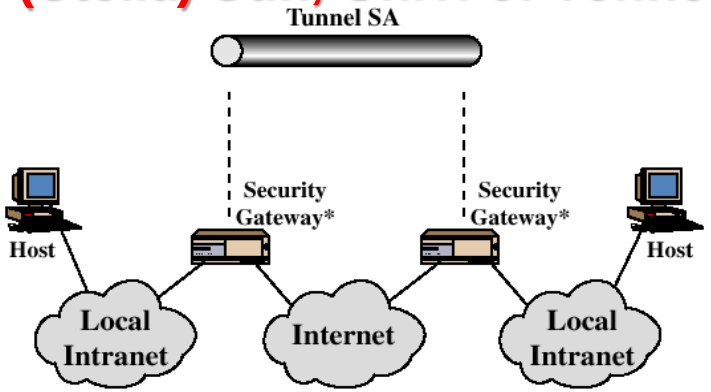


- Layer 2 VPN (**L2VPN**): Επέκταση L2/VLAN over Provider WAN π.χ.
  - Point-to-point **L2TP** (Layer 2 Tunneling Protocol) πάνω από IP/MPLS Provider Network
  - Point-to-point Επεκτάσεις **PW** (Pseudo-Wire) πάνω από IP/MPLS Provider Network
  - Multipoint **VPLS** (Virtual Private LAN Service) πάνω από MPLS Provider Network
  - Επέκταση **Mac-in-Mac** (IEEE 802.1ah) πάνω από L2 Provider Bridge Network
  - Επέκταση από VLAN (VLAN ID: 12 bits) σε **VXLAN** – Virtual Extensible LAN για Layer 2 διασύνδεση σε Data Centers πάνω από IP/UDP tunnels μεταξύ VXLAN Tunnel Endpoint - **VTEPs** (VXLAN ID: 24 bits/VTEP)
- Layer 3 VPN (**L3VPN**): Επέκταση IP Intranet σε Extranet μέσω Provider WAN π.χ.
  - IP ή MPLS tunnels μεταξύ εικονικών δρομολογητών (Virtual Routing & Forwarding, **VRF**) ορισμένων στους PE Nodes (Routers) ανά VPN
  - Διαδικασία Ασφαλούς Επικοινωνίας **IPsec Tunnels** μεταξύ PE's BGP/IP Provider Network(s)
  - Generic Routing Encapsulation **GRE Tunnels** μεταξύ PE's BGP/IP Provider Network(s)
  - Διαδικασία Ασφαλούς Επικοινωνίας **OpenVPN Tunnels** μεταξύ τερματικών συσκευών χρηστών client - server, hosted σε διαφορετικά διαχειριστικά περιβάλλοντα μέσω SSL/TLS (προτιμάται η χρήση πρωτοκόλλων UDP και η προ-εγκατάσταση certificates στον client)

IPsec

ECE 454/CS 594, Jinyuan (Stella) Sun, Univ. of Tennessee, Fall 2011

IPsec: Ανεξάρτητο Εφαρμογών
ενώ
TLS: για Web
SSH: για Remote Login



Transport Mode

Ασφάλεια Περιεχομένου σε υποσύνολα της σύνδεσης e2e (*encryption του payload*)

IP header (real dest)	IPsec header	TCP/UDP header + data

Tunnel Mode

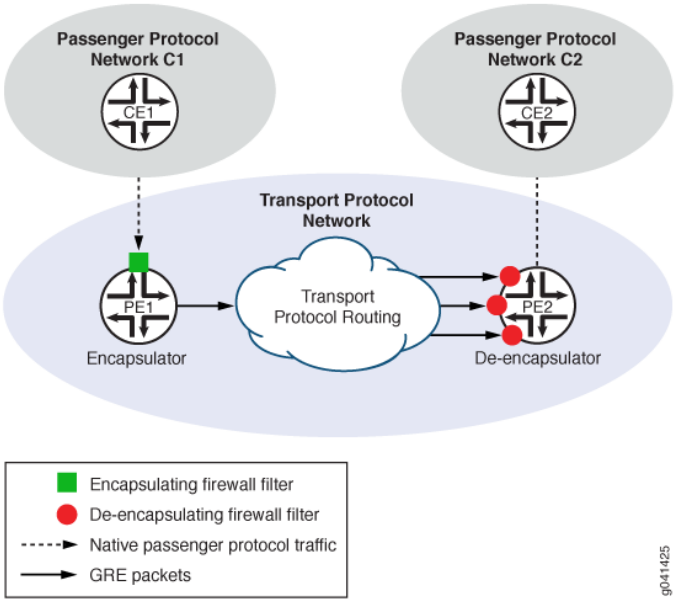
Ασφάλεια Πακέτου σε tunnel μεταξύ Security Gateways (*encryption αρχικού πακέτου*)

IP header (gateway)	IPsec header	IP header (real dest)	TCP/UDP header + data

- **SA**: Security Associations (one way)
  - SPI: Security Parameter Index (Cryptographic algorithms, keys, lifetimes, sequence numbers, mode - transport or tunnel)
  - Εναλλακτικές SA, αποθηκευμένες σε IPsec nodes, ενεργοποιούνται με επιλογή του πακέτου
- **AH**: Authentication Header
  - Επιβεβαίωση ταυτότητας αποστολέα (Sender Authentication) & μη παραποίησης μηνύματος (Message Integrity)
- **ESP**: Encapsulating Security Payload
  - Εμπιστευτικότητα (Confidentiality)
- **IKE**: Internet Key Exchange
  - Handshaking protocol για συμφωνία SA

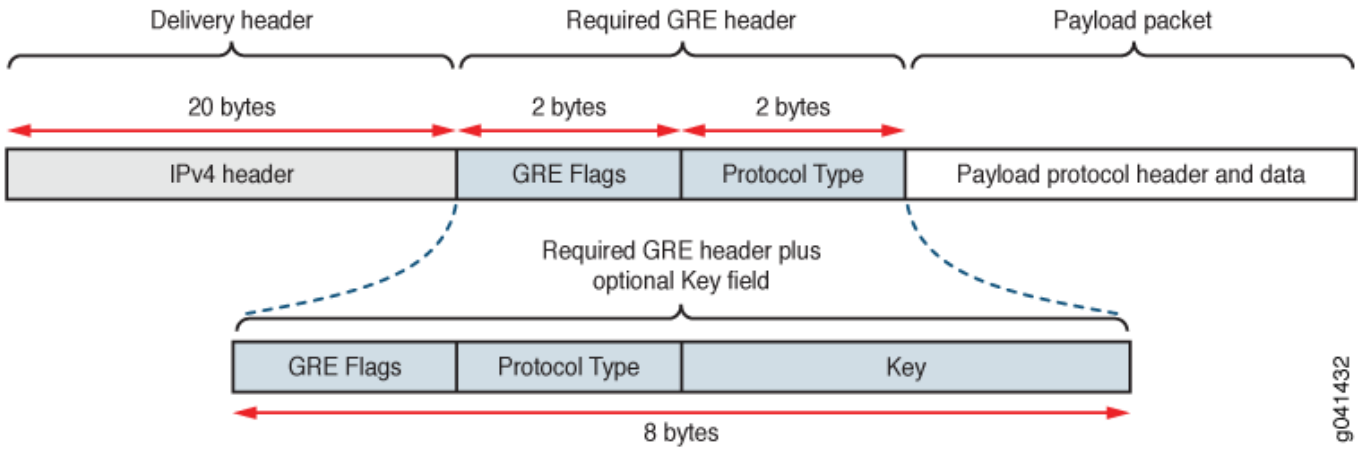
Generic Routing Encapsulation (GRE)

http://www.juniper.net/documentation/en_US/junos13.2/topics/concept/firewall-filter-tunneling-ipv4-gre-components.html



ΔΙΑΔΙΑΚΑΣΙΑ ΕΝΘΥΛΑΚΩΣΗΣ - GRE Tunneling

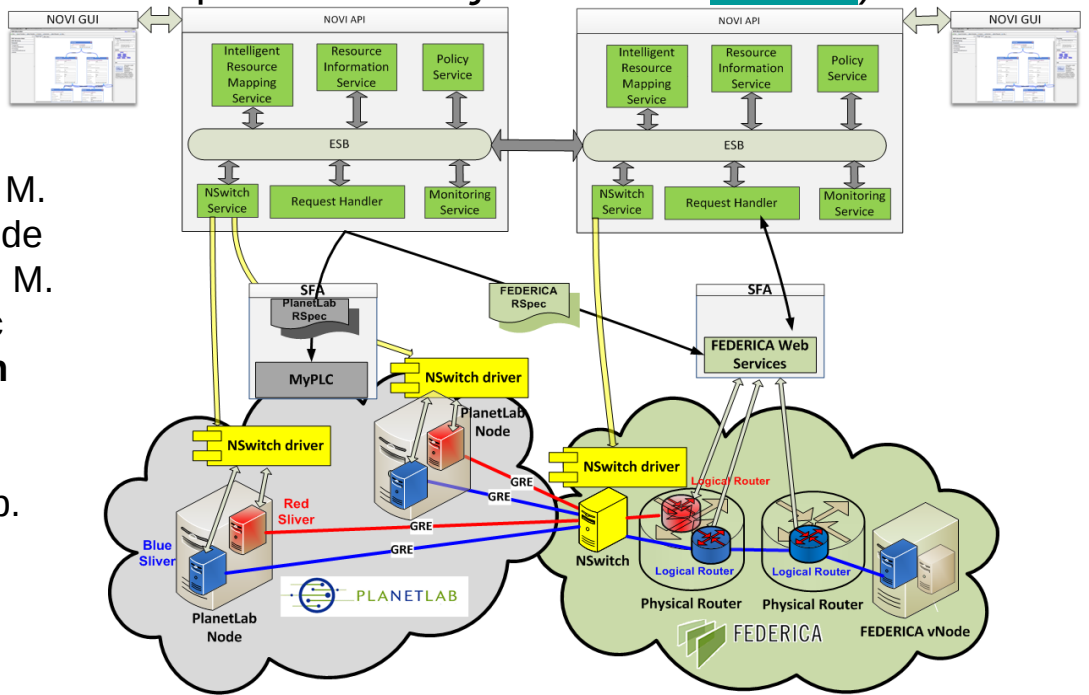
- Το payload packet πρέπει να μεταφερθεί από Customer (εφαρμογή) **C1** σε απομακρυσμένο Customer **C2** όπως σε απευθείας μονοκατευθυντική σύνδεση μεταξύ τοπικών κόμβων ζεύξης **CE1** (Customer Edge 1) και **CE2** (Customer Edge 2)
- Το Encapsulation filter στον διαδικτυακό κόμβο εισόδου **PE1** (Provider Edge 1) εισάγει GRE header με μοναδικό κλειδί για πακέτα **C1 → C2** (δεν ισχύει για C2 → C1)
- Το αποτέλεσμα ενθυλακώνεται με IPv4 header και προωθείται σαν IP datagram από τον Encapsulator **PE1** στον De-encapsulator **PE2** μέσω TCP/IP WAN (Internet)
- Το De-encapsulation filter στον διαδικτυακό κόμβο εξόδου **PE2** (Provider Edge 2) ανακτά το payload packet και το προωθεί στον **C2**



VPNs ΣΕ ΟΜΟΣΠΟΝΔΙΑ ΔΙΑΧΕΙΡΙΣΤΙΚΩΝ ΠΕΡΙΟΧΩΝ

Κοινοτικό Έργο NOVI (Networking innovations Over Virtualized Infrastructures)

- Συνύπαρξη σε διασυνδεόμενα δίκτυα πολλαπλών VPNs μέσω απομονωμένων εικονικών υποδομών με ασφαλή πρόσβαση τελικών χρηστών
- Οι εξουσιοδοτημένοι χρήστες δημιουργούν εικονικές φέτες - **slices** από «αφιερωμένα» στοιχεία - **slivers**: Virtual Machines (VMs), Virtual (Logical) Routers, Ethernet switches…
- Μη κρυπτογραφημένες συνδέσεις WAN: **GRE over IP tunnels** στο Internet & **layer 2 VLANs**
- Πειραματική υλοποίηση: Δημιουργία & λειτουργία απομονωμένων virtual slices με VM's στις εικονικές πειραματικές υποδομές ***PlanetLab*** (πάνω από το Internet) και ***FEDERICA*** (με Ethernet/VLANs των Ευρωπαϊκών ΑΕΙ & Ερευνητικών Κέντρων, των Εθνικών Ερευνητικών - Ακαδημαϊκών Δικτύων **NRENs** και του Πανευρωπαϊκού τους Διαδικτύου **GÉANT**)



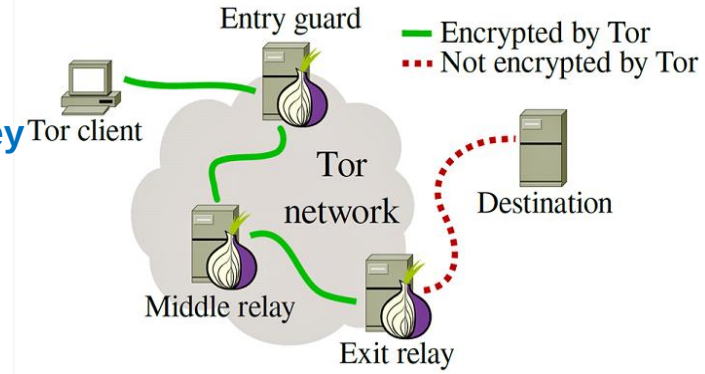
Κύρια Αναφορά:

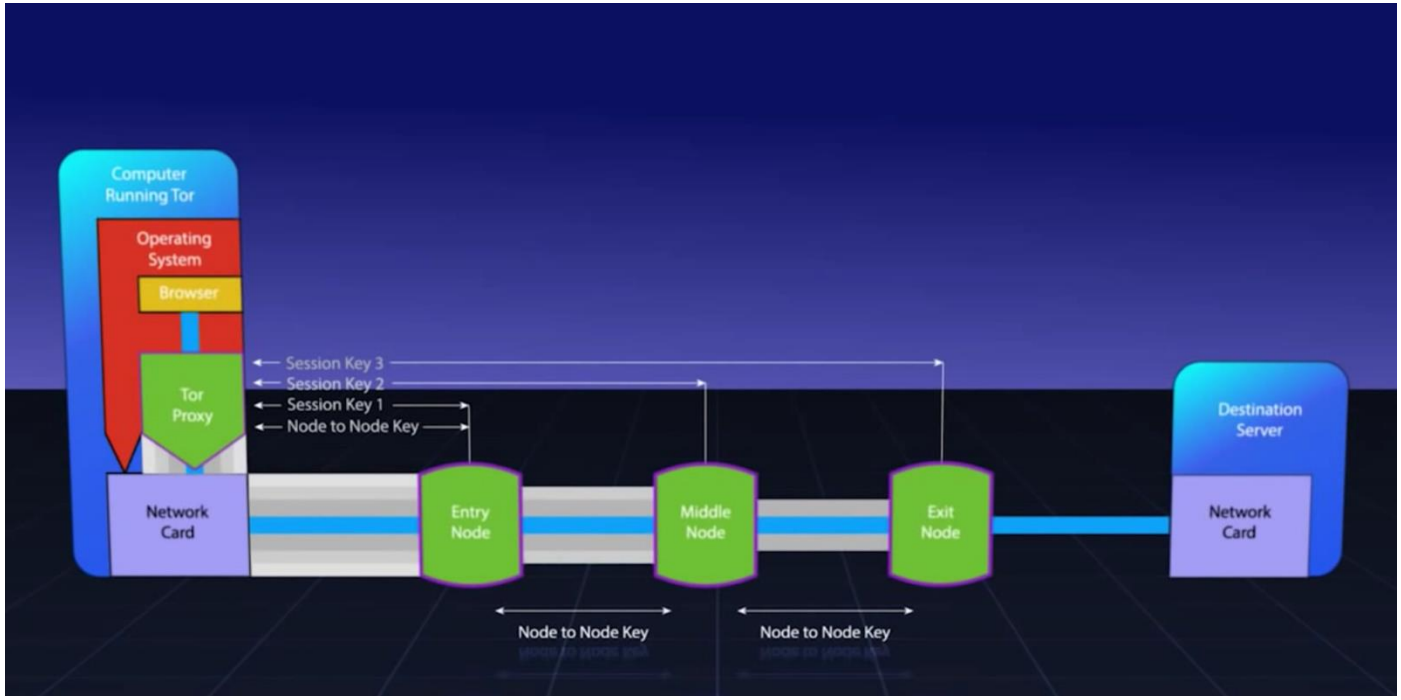
V. Maglaris, C. Papagianni, G. Androulidakis, M. Grammatikou, P. Grosso, J. van der Ham, C. de Laat, B. Pietrzak, B. Belter, J. Steger, S. Laki, M. Campanella & S. Sallent, **"Toward a Holistic Federated Future Internet Experimentation Environment: The Experience of NOVI Research & Experimentation"**, *IEEE Communications Magazine*, Vol. 53, No. 7, pp. 136-147, July 2015

Anonymity Network - The Onion Router (Tor)

http://fossbytes.com/everything-tor-tor-tor-works/

- **Tor Project**: Δεκαετία 1990 με κρατική χρηματοδότηση από ΗΠΑ!
- Απαιτείται ειδικός browser στον client
- Βασίζεται σε υπερκείμενο (overlay) δίκτυο από **Tor relays** συνδεμένα σε public Internet routers
- Ο browser του χρήστη ανοίγει **Encrypted TLS** session από τον **Tor client** στον **Entry Node** δημιουργώντας **Session Key 1**
- Το session επεκτείνεται σε **Middle Node** μέσω **Node-to-Node Key** και δημιουργείται **Session Key 2**
- Ο **Exit Node** ανοίγει session με τον Server και μεσολαβεί για **Session Key 3** με τον **Entry Node** χωρίς να γνωρίζει το IP του χρήστη (anonymity)
- Η ανταλλαγή data μεταξύ user browser και server περνά από διαδοχικά στρώματα κρυπτογράφησης (εξ' ου και onion router)





Tor Encrypted Overlay: The Dark Web

https://www.quora.com/What-is-the-deep-web-and-how-do-you-access-it

- **Deep Web**: Sites μη ανοικτής πρόσβασης (not indexed by search engines, π.χ. Google)
- **Dark Web**: Υποσύνολο του Deep Web με προστασία ανωνυμίας sites & users π.χ. μέσω Tor