V(irtual) P(rivate) N(etworking)
Ιδιωτική Εικονική Διαδικτύωση

Εισηγητής : Αν. Καθηγητής Οικονομίδης Αναστάσιος

ΤΕΧΝΟΛΟΓΙΕΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Φοιτητής : ΓΟΥΤΑΣ ΔΗΜΗΤΡΙΟΣ MIS Β ΕΞΑΜΗΝΟ

ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ 2007 - 2008

ΠΛΑΝΟ ΠΑΡΟΥΣΙΑΣΗΣ

Ορισμοί

Ιδιότητες

Τεχνολογίες/Προαπαιτήσεις Tunneling

Μοντέλα VPN (ανάπτυξη βάση παροχέα)

Τρόποι χρήσης VPN

Αρχιτεκτονικές VPN (σε σχέση με την επιχείρηση)

ΠΛΑΝΟ ΠΑΡΟΥΣΙΑΣΗΣ

(Συνέχεια)

- Τοπολογίες VPN(Σχεδιασμός/Τοπολογία)
- Τεχνολογίες και Πρωτόκολα VPN
- Πρωτόκολα Ασφαλείας
- Κίνδυνοι VPN
- Πλεονεκτήματα VPN

Virtual Private Network (Ορισμός 1)

- Εικονικό ιδιωτικό δίκτυο ονομάζεται η επέκταση ενός ιδιωτικού δικτύου που καλύπτει τις συνδέσεις στα κοινά ή δημόσια δίκτυα όπως το Διαδίκτυο. Ένα VPN επιτρέπει στους χρήστες να ανταλλάξουν στοιχεία μεταξύ υπολογιστών μέσα από ένα κοινό ή δημόσιο δίκτυο με τρόπο που μιμείται τις ιδιότητες μιας PTP σύνδεσης.

Virtual Private Network (Ορισμός 2)

- Ένα VPN είναι μια σύνδεση, που προστατεύεται, μεταξύ δύο οντοτήτων που δεν είναι απαραίτητο να συνδέονται άμεσα.
  - Οντότητα μπορεί να είναι μια καθορισμένη συσκευή υπολογιστή ή ένα δίκτυο (πολλές τέτοιες συσκευές)

Virtual Private Network (Ορισμός 2)

- Προστασία εννούμε :
  - Προστασία των δεδομένων από οτακουστές με την χρήση τεχνικών κρυπτογραφίας όπως RC-4,DES,3DES και AES
  - Προστασία της ακεραιότητας των πακέτων με την χρήση hashing συναρτήσεων όπως MD5,SHA

Virtual Private Network (Ορισμός 2)

- Προστασία από επιθέσεις Man-in-the-Middle με την χρήση μηχανισμών πιστοποίησης της αυθεντικότητας όπως η χρήση κλειδιών ή η χρήση ψηφιακών υπογραφών
- Προστασία από επιθέσεις αντικατάστασης πακέτων με την χρήση σειριακών αριθμών κατά την μετάδοση των προστατευμένων δεδομένων

Virtual Private Network (Ορισμός 2)

- Καθορισμός του μηχανισμού ενθυλάκωσης και προστασίας των δεδομένων και πώς επιτυγχάνεται η προστατευμένη μετάδοση μεταξύ των συσκευών
- Προσδιορισμός των δεδομένων που είναι καίρια και πρέπει να προστατευθούν από κακόβουλες ενέργειες

Virtual Private Network (Ορισμός 3)[1]

- Είναι ένα δίκτυο από εικονικά κυκλώματα μέσω των οποίων διακινούνται ιδιωτικά δεδομένα μέσα από δημόσια ή ιδωτικά δίκτυα όπως το Internet ή δίκτυα τα οποία παρέχουν οι NSP(Network Service Providers)

Virtual Private Networking

- Η πράξη της διαμόρφωσης και της δημιουργίας ενός ιδεατού ιδιωτικού δικτύου είναι γνωστή ως εικονική ιδιωτική δικτύωση.

Κριτήρια Επιλογής VPN9

- Who(Ποιός έχει πρόσβαση)
- Where(Πού έχει πρόσβαση)
- What(Σε τί έχει πρόσβαση)
- What is the cost(Πόσο θα κοστίσει αυτό)

Ελάχιστες Ιδιότητες VPN

- **Πιστοποίηση Χρήστη**

  Θα πρέπει να επιτρέπεται η πρόσβαση μόνο πιστοποιημένων χρηστών.

  Ύπαρξη Μηχανισμών ελέγχου και καταγραφής πρόσβασης
- **Διαχείρηση Διευθύνσεων**

  Θα πρέπει οι διευθύνσεις των χρηστών να κρατούνται μυστικές

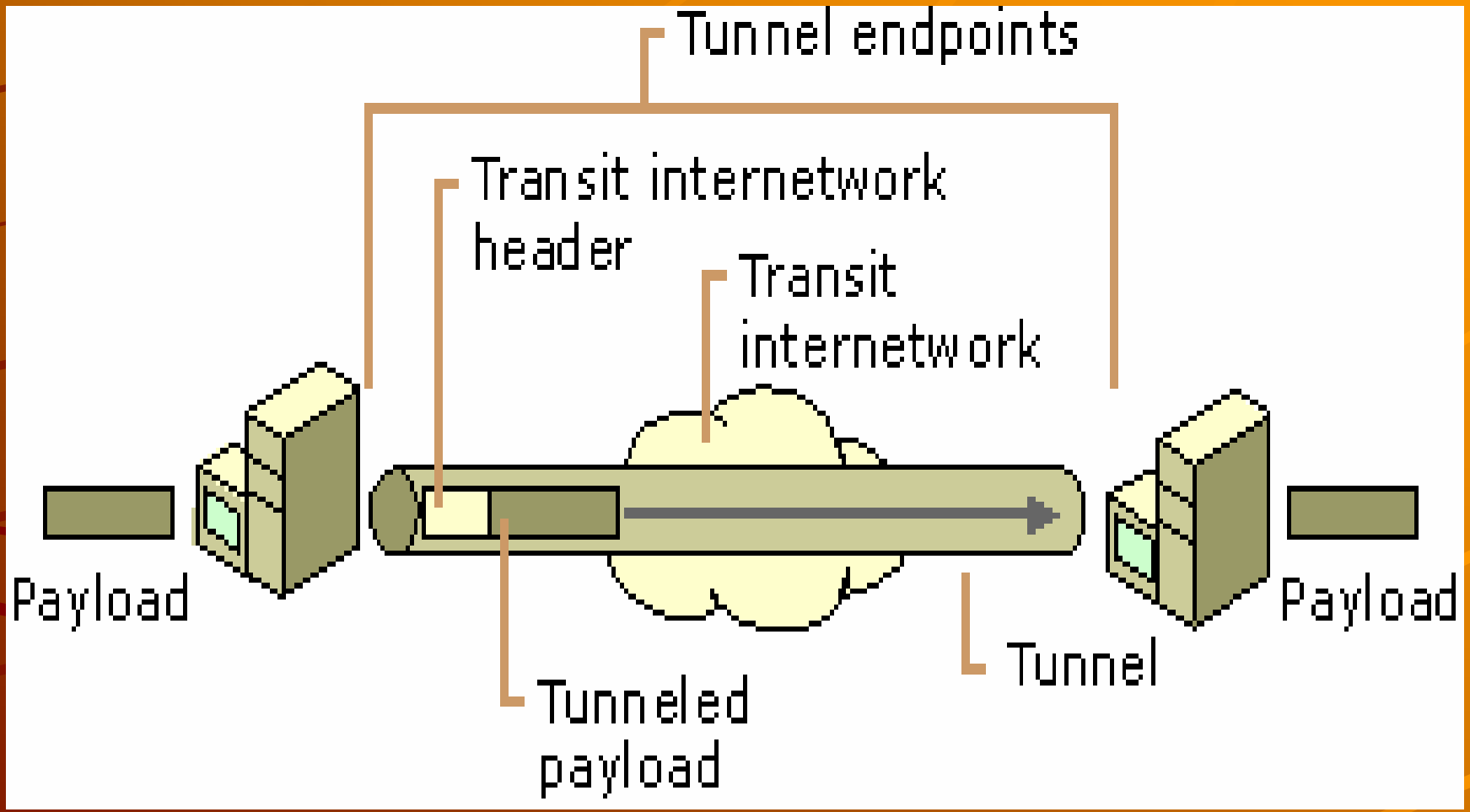
Ελάχιστες Ιδιότητες VPN

- **Κρυπτογραφία Δεδομένων**
  Οι πληροφορίες που διακινούνται μέσα στο δίκτυο θα πρέπει να είναι κρυπτογραφημένες έτσι ώστε να μην είναι δυνατόν η ανάγνωση τους από μη εξουσιοδοτημένους χρήστες
- **Διαχείρηση Κλειδιών**
  Συνεχή ανανέωση κλειδιών κρυπτογράφησης
- **Υποστήριξη Διαφορετικών Πρωτοκόλων**
  Θα πρέπει να είναι η δυνατή η χρήση διαφόρων προτοκόλων π.χ. IP , Internetwork Packet Exchange(IPX), και άλλα.

Tunneling(Σύραγγα)[2]

- Tunneling είναι μια μέθοδος η οποία με την χρήση της υποδομής ενός internetwork μεταφέρει δεδομένα από ένα δίκτυο σε ένα άλλο.
- Τα δεδομένα μπορούν να μεταδοθούν με Frames ή πακέτα κάποιου άλλου πρωτοκόλου.
- Τα frames δεν μεταδίδονται όπως παράγονται από τον αποστολέα αλλά μία επικεφαλίδα(header) προστίθεται σε αυτά η οποία περιέχει πληροφορίες δρομολόγησης.

Tunneling


Tunnel endpoints
Transit internetwork header
Transit internetwork
Payload
Payload
Tunneled payload
Tunnel

Τεχνολογίες Tunneling (Παλιές)

- **SNA tunneling over IP internetworks**

Όταν η κυκλοφορία δικτυακής αρχιτεκτονικής συστημάτων (SNA) στέλνεται πέρα από μια εταιρική IP internetwork, το πλαίσιο SNA είναι τοποθετημένο μέσα σε μια επικεφαλίδα UDP και IP.

Τεχνολογίες Tunneling (Παλιές)

- **IPX tunneling for Novell NetWare over IP internetworks**

  Όταν ένα IPX πακέτο στέλνεται σε έναν Netware server ή IPX router, ο server ή ο router περικλείει το IPX πακέτο μέσα σε μία IP και UDP επικεφαλίδα και μετά το στέλνει στο δίκτυο.

  Ο παραλήπτης IP-to-IPX router αφαιρεί την UDP & IP κεπικεφαλίδα και αποστέλει το πακέτο στον IPX προορισμό.

Τεχνολογίες Tunneling (Νέες)

- **Point-to-Point Tunneling Protocol (PPTP)**

  PPTP επιτρέπει στα δεδομένα που μετακινούνται μέσω IP, IPX ή NETBEUI αφού κρυπτογραφηθούν να ενσωματωθούν μέσα σε μια IP επικεφαλίδα και να αποσταλούν μέσα σε ένα εταιρικό ή δημόσιο δίκτυο.

Τεχνολογίες Tunneling (Νέες)

- **Layer Two Tunneling Protocol (L2TP)**

  L2TP επιτρέπει στα δεδομένα που μετακινούνται μέσο IP, IPX ή NETBEUI αφού κρυπτογραφηθούν να σταλούν σε κάθε μέσω που υποστηρίζει Point-to-Point Datagram παράδοση όπως IP, X.25, Frame Relay, ή ATM

Τεχνολογίες Tunneling (Νέες)

- **IPSec tunnel mode**

Το IPSec αφού κρυπτογραφηθούν τα IP πακέτα και συμπεριληφθούν σε μία IP επικεφαλίδα, να αποσταλούν μέσα σε ένα εταιρικό ή δημόσιο δίκτυο όπως το Internet.

Πρωτόκολα Tunneling2

- Σύμφωνα με το πρότυπο OSI η τεχνολογία Tunneling βασίζεται στα επίπεδα 2 & 3.
- Πρωτόκολα Επιπέδου 2 αναφέρονται στο Επίπεδο Σύνδεσης Δεδομένων (data-link) και για την μεταφορά δεδομένων χρησιμοποιούνται frames.Τα PPTP & L2TP είναι πρωτόκολα αυτού του επιπέδου.

Πρωτόκολα Tunneling

- Πρωτόκολα Επιπέδου 3 αναφέρονται στο Επίπεδο Δικτύου(Network) και χρησιμοποιούν για την μεταφορά πακέτα.Ένα παράδειγμα αυτού του τρόπου είναι το IPSec το οποίο ενσωματώνει IP πακέτα μέσα σε μία IP επικεφαλίδα(Header) πρίν τα στείλει στο IP δίκτυο.
- Για να πραγματοποιηθεί μια τέτοια σύνδεση το tunnel πρωτόκολο που χρησιμοποιούν ο server και ο client πρέπει να είναι τα ίδια.

Βασικές Προαπαιτήσεις Tunneling

- **Πιστοποίηση Χρήστη**

  Το επίπεδο 2 κληρονομεί τις μεθόδους πιστοποίησης του PPP, συμπεριλαμβανομένου της μεθόδου EAP.Πολλά σχήματα tunneling Επιπέδου 3 υποθέτουν ότι τα σημεία προορισμού είναι γνωστά και πιστοποιημένα πρίν πραγματοποιηθεί η σύνδεση.

  Μια παρατυπία σε αυτόν τον κανόνα είναι η IPSec Internet Key Exchange(IKE) διαπραγμάτευση, η οποία παρέχει αμοιβαία επικύρωση των σημείων τέλους.

Βασικές Προαπαιτήσεις Tunneling

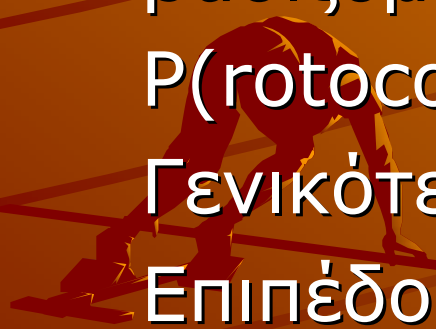
- **Συμβολική υποστήριξη καρτών**

  Χρησιμοποιώντας το E(xtensible) A(uthentication) P(rotocol), το Επιπεδο 2 μπορεί να υποστηρίξει μια ευρεία ποικιλία των μεθόδων επικύρωσης, συμπεριλαμβανομένων των one-time κωδικών πρόσβασης, των κρυπτογραφικών υπολογιστών, και των έξυπνων καρτών.

  Το Επίπεδο 3 μπορεί να χρησιμοποιήσει παρόμοιες μεθόδους π.χ. το IPSec καθορίζει τη δημόσια επικύρωση πιστοποιητικών στη διαπραγμάτευση IKE.

Βασικές Προαπαιτήσεις Tunneling

- **Δυναμική διευθυνσιοδότηση**
  Το Επίπεδο 2 υποστηρίζει δυναμική κατανομή διευθύνσεων χρηστών βασιζόμενο πάνω στο N(etwork) C(ontrol) P(rotocol) μηχανισμό διαπραγμάτευσης. Γενικότερα, τα σχήματα tunneling του Επιπέδου 3 υποθέτουν ότι η διεύθυνση έχει ήδη δωθεί πρίν από την έναρξη του tunneling.



Βασικές Προαπαιτήσεις Tunneling

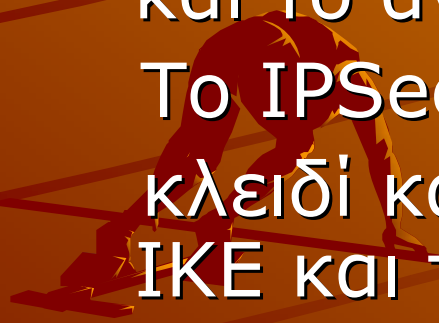
- **Συμπίεση δεδομένων**
  Τα πρωτόκολα Επιπέδου 2 υποστηρίζουν PPP σχήματα συμπίεσης.
- **Κρυπτογραφία δεδομένων**
  Τα πρωτόκολα Επιπέδου 2 υποστηρίζουν PPP μηχανισμούς κρυπτογράφησης.Το PPTP της Microsoft υποστηρίζει χρήση του M(icrosoft) P(oint)-to-P(oint) E(ncryption), βασισμένο πάνω στον αλγόριθμο RSA/RC4. Τα πρωτόκολα Επιπέδου 3 μπορούν να χρησιμοποιήσουν παρόμοιες μεθόδους πχ.IPSec

Βασικές Προαπαιτήσεις Tunneling

- **Διαχείρηση κλειδιού**

  Ένας μηχανισμός Επιπέδου 2 στηρίζεται στο αρχικό κλειδί που παράγεται κατά τη διάρκεια της πιστοποίησης των χρηστών και το ανανεώνει περιοδικά.

  Το IPSec διαπραγματεύεται ρητά ένα κοινό κλειδί κατά τη διάρκεια της ανταλλαγής IKE και το ανανεώνει επίσης περιοδικά.



Βασικές Προαπαιτήσεις Tunneling

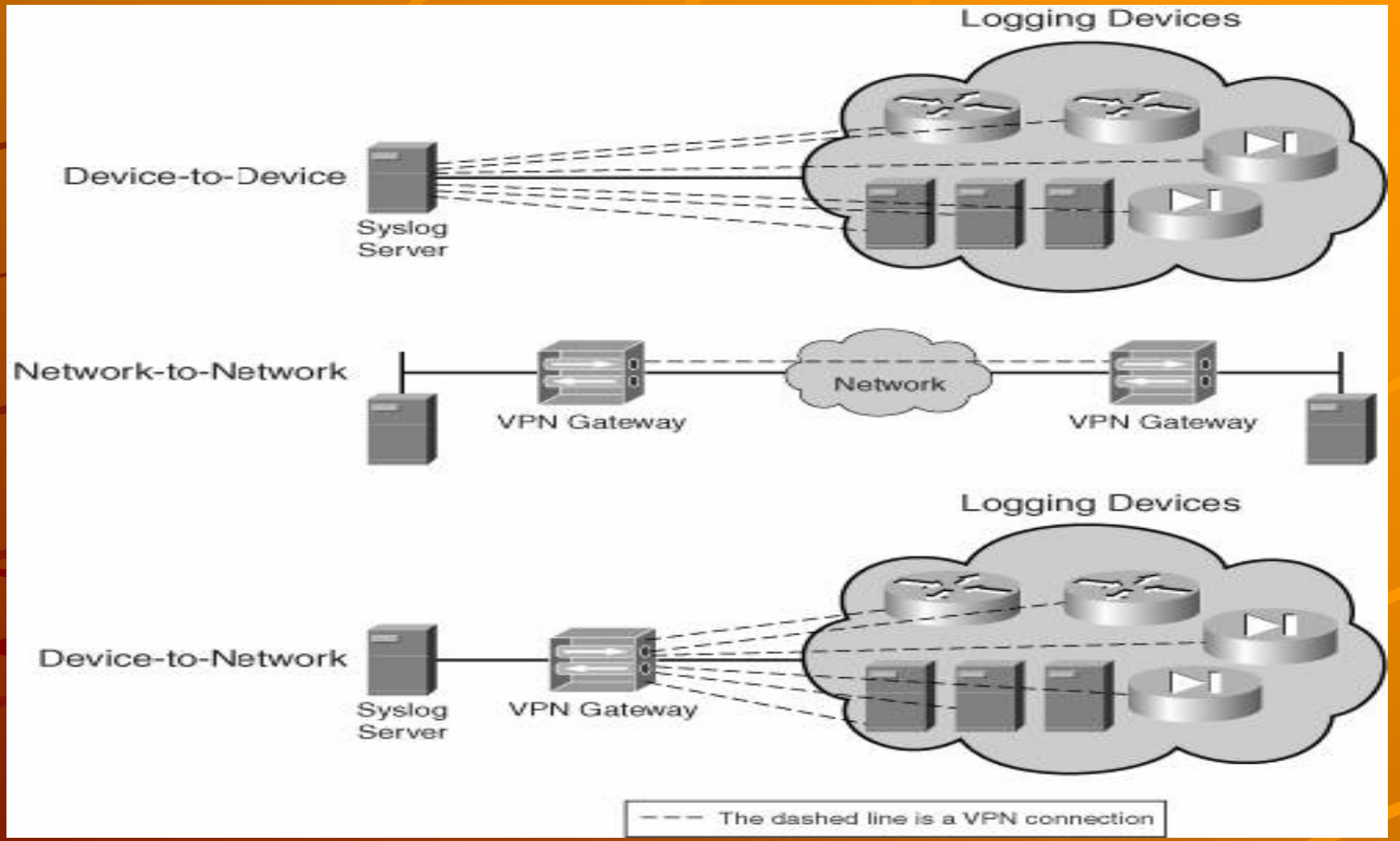
- **Υποστήριξη διαφορετικών πρωτοκόλων**

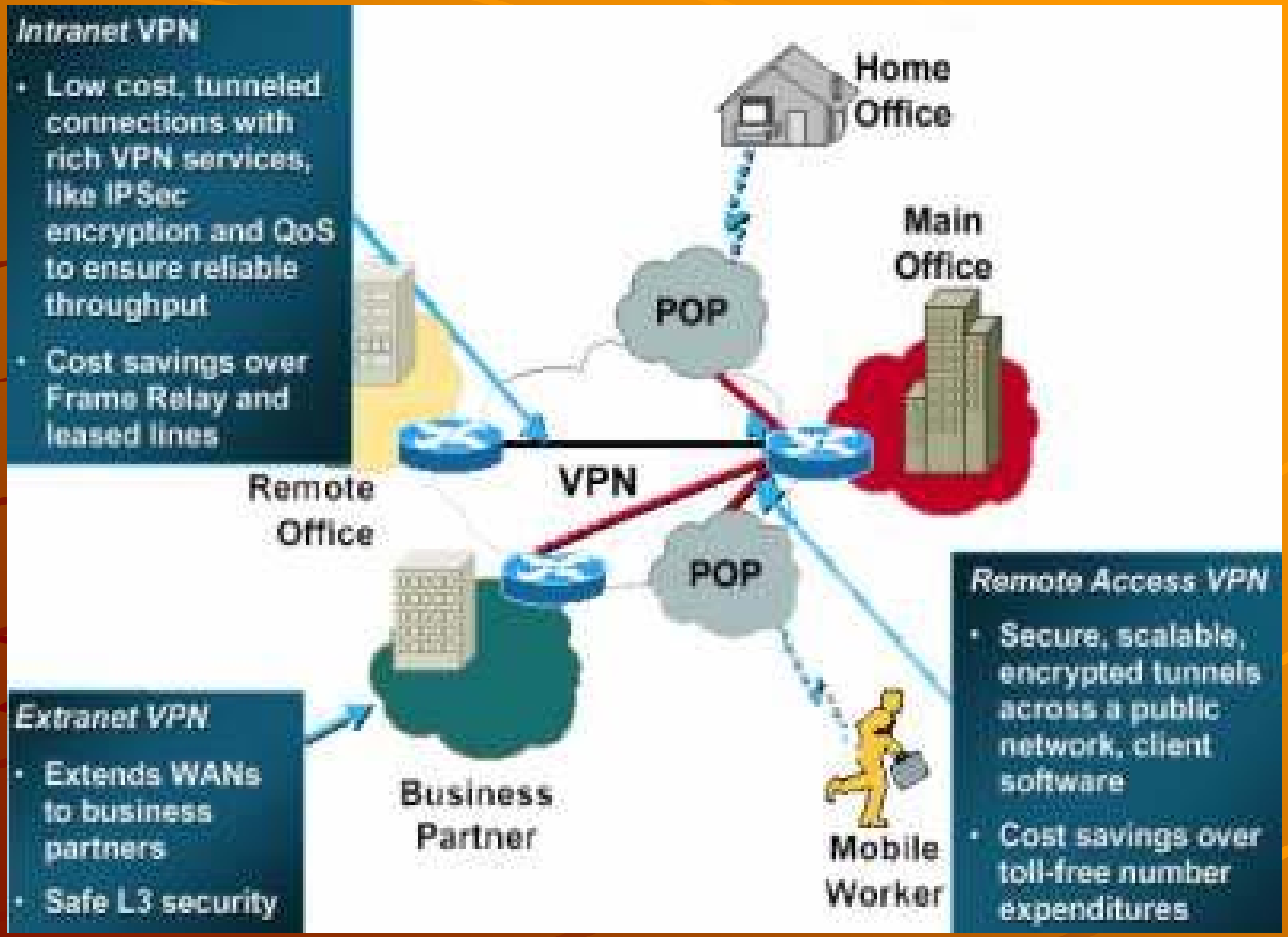
  Το Επίπεδο 2 υποστηρίζει πολλαπλά πρωτόκολα και με αυτόν τον τρόπο κάνει εύκολο στους tunneling χρήστες να έχουν πρόσβαση στα εταιρικά δίκτυα.Σε αντίθεση στο Επίπεδο 3 τα πρωτόκολα όπως το IPSec, υποστηρίζουν δίκτυα αποδέκτες που υποστηρίζουν IP πρωτόκολα.

Βασικοί Τρόποι Σύνδεσης

- Υπάρχουν τρείς βασικοί τρόποι σύνδεσης PTP :
  - Συσκευή-προς-Συσκευή(Device-to-Device)
  - Δίκτυο-προς-Δίκτυο(Network-to-Network)
  - Συσκευή-προς-Δίκτυο(Device-to-Network)

Βασικοί Τρόποι Σύνδεσης




Intranet VPN
• Low cost, tunneled connections with rich VPN services, like IPSec encryption and QoS to ensure reliable throughput
• Cost savings over Frame Relay and leased lines
Home Office
Main Office
POP
VPN
Remote Office
POP
Business Partner
Mobile Worker
Extranet VPN
• Extends WANs to business partners
• Safe L3 security
Remote Access VPN
• Secure, scalable, encrypted tunnels across a public network, client software
• Cost savings over toll-free number expenditures

Μοντέλα VPN (ανάπτυξης βάση παροχέα)[1,5]

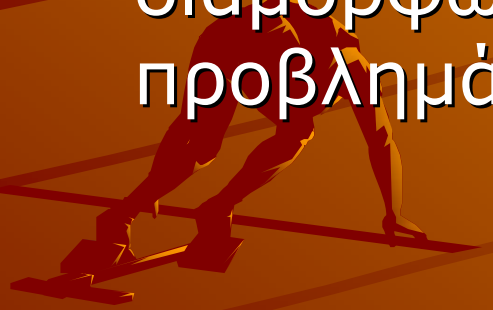
- Τα μοντέλα των VPNs είναι τα εξής :
  - Απλό μοντέλο παροχέα
  - Υβριδικό μοντέλο παροχέα
  - Άκρη-σε-Άκρη μοντέλο

Απλό Μοντέλο

- Σε αυτό το μοντέλο, οι περισσότερες διεργασίες υπάρχουν μέσα στην υποδομή των φορέων παροχής υπηρεσιών και όχι στο δίκτυο της επιχείρησης.
- Η απομακρυσμένη πρόσβαση στο δίκτυο της επιχείρησης γίνεται μέσω αφιερωμένων κυκλωμάτων όπως (T1,T3), συνδέσεις ATM ή αφιερωμένες Frame Relay συνδέσεις

Απλό Μοντέλο

- Σε αυτό το μοντέλο, ο πάροχος έχει τον έλεγχο του δικτύου σε αυξημένο επίπεδο και είναι υπεύθυνος για τον προγραμματισμό της απόδοσης, σχεδίασης, διαμόρφωσης, ελέγχου και επίλυσης προβλημάτων.



Υβριδικό Μοντέλο

- Το υβριδικό μοντέλο περιλαμβάνει τα δίκτυα του παρόχου και της επιχείρησης.Μία VPN σύραγγα αρχίζει από το εσωτερικό του παροχέα και καταλήγει στο δίκτυο της επιχείρησης
- Ο πάροχος είναι υπεύθυνος για την αρχικοποίηση των VPN συράγγων για τους απομακρυσμένους χρήστες μετά την πιστοποίησή τους

Υβριδικό Μοντέλο

- Όταν ο απομακρισμένος χρήστης πάει να μπεί στο δίκτυο της επιχείρησης, μία δεύτερη πιστοποίηση λαμβάνει χώρα πρίν ο χρήστης να πάρει το δικαίωμα πρόσβασης στο ιδιωτικό δίκτυο.Μετά την πιστοποίηση ο χρήστης έχει πρόσβαση στο εσωτερικό δίκτυο της εταιρίας σαν να ήταν μέσα σε αυτο.

Άκρη-σε-Άκρη Μοντέλο

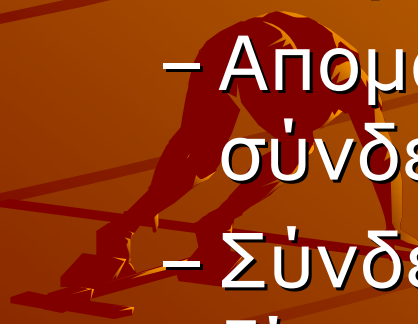
- Σε ένα τέτοιο μοντέλο, ο πάροχος λειτουργεί σαν μεταφορέας των δεδομένων του VPN. Τα τελικά σημεία ή οι σύραγγες μπορούν να είναι ένας υπολογιστής ή μια συσκευή VPN που λειτουργεί σαν proxy για πολλούς υπολογιστές.

Άκρη-σέ-Άκρη Μοντέλο

- Τα τελικά σημεία σύδεσης είναι εκτός του δικτύου του παρόχου υπηρεσιών.
- Αυτό το μοντέλο μπορεί να χρησιμοποιηθεί για απομακρυσμένη πρόσβαση ή για να συνδέσουμε πολλά sites.

ΧΡΗΣΗ VPN[1,4]

- Υπάρχουν πολλοί τρόποι για να χρησιμοποιήσουμε ένα VPN :
  - Σύνδεση περιοχής-με-περιοχή(Site-to-Site)
  - Απομακρισμένης πρόσβασης σύνδεση(Remote access)
  - Σύνδεση της επιχείρησης σε εξωτερικό δίκτυο(Extended Enterprise Extranet Connectivity)

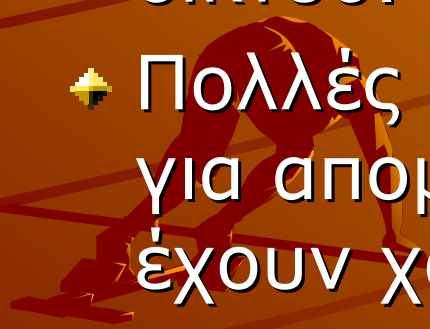


Σύνδεση περιοχής-με-περιοχή

- Αυτού του είδους η σύνδεση βοηθάει διαφορετικά δίκτυα να συνδεθούν με ασφάλεια και με αποτελεσματικότητα σχηματίζοντας ένα μεγάλο δίκτυο.
- Ως συνήθως τέτοιου είδους συνδέσεις χρησιμοποιούνται από επιχειρήσεις που είναι γεωγραφικά απομακρισμένες με σκοπό να δημιουργήσουν ένα κοινό δίκτυο.

Απομακρυσμένης πρόσβασης σύνδεση

- Αυτού του είδους οι συνδέσεις επιτρέπουν εργαζόμενους εκτός εταιρίας να έχουν πρόσβαση στο δίκτυο της εταιρίας, μέσω του Internet, χρησιμοποιόντας ένα ασφαλές δίκτυο.
- Πολλές επιχειρήσεις χρησιμοποιούν VPNs για απομακρυσμένη πρόσβαση με σκοπό να έχουν χαμηλότερο κόστος πρόσβασης για τους εργαζόμενους τους

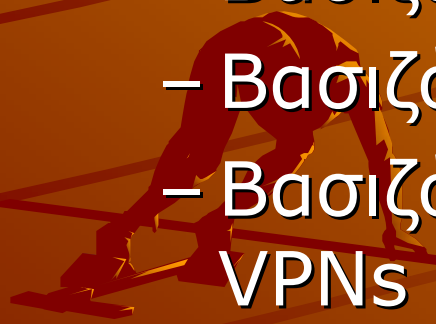


Σύνδεση της επιχείρησης σε εξωτερικό δίκτυο

- Αυτού του είδους οι συνδέσεις παρέχουν συνδέσεις σε δίκτυα εκτός της εταιρίας.
- Παρέχουν ισχυρότερα εργαλεία με σκοπό την διαχείρηση και τον έλεγχο της κίνησης από δίκτυο-σε-δίκτυο
- Το εσωτερικό δίκτυο μπορεί να προστατευθεί από το εξωτερικό μέσω firewalls

Αρχιτεκτονικές VPN (Επιχείρηση)[1,4]

- Οι αρχιτεκτονικές VPN μπορεί να είναι οι ακόλουθες :
  - Βασιζόμενα σε Firewall VPNs
  - Βασιζόμενα σε Router VPNs
  - Βασιζόμενα σε Remote Access VPNs
  - Βασιζόμενα σε Hardware(Black box) VPNs
  - Βσιζόμενα σε Software VPNs



Βασιζόμενα σε Firewall VPNs

- Είναι η πιο κοινή μορφή και ευραίως χρησιμοποιούμενη.
- Οι περισσότερες εταιρίες συνδέονται μέσω firewalls στο Internet, χρειάζονται επιπρόσθετα προγράμματα κρυπτογράφησης και πιστοποίησης

Βασιζόμενα σε Router VPNs

- Υπάρχουν δύο τύποι :
  - Με την εγκατάσταση ενός προγράμματος στον router γίνεται η κρυπτογράφηση των δεδομένων
  - Με την εγκατάσταση μία εξωτερικής κάρτας στον router με σκοπό την μεταφορά της διαδικασίας κρυπτογράφησης από την CPU του router στην κάρτα.

Βασιζόμενα σε Remote Access VPNs

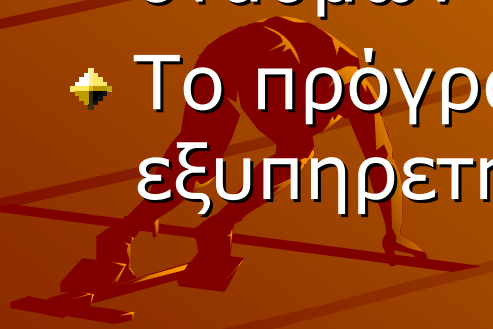
- Με αυτού του τύπου τα VPNs κάποιος από μία απομακρισμένη περιοχή μπορεί να δημιουργήσει ένα κανάλι ή μια σύραγγα μέσω κρυπτογραφίας σε μία συσκευή δικτύου της επιχείρησης.

Βασιζόμενα σε Hardware (Black box) VPNs

- Ο πάροχος προσφέρει ένα black box ή μία συσκευή με πρόγραμμα κρυπτογράφησης, για να δημιουργήσει μία σύραγγα VPN. Αυτή η συσκευή βρίσκεται πίσω από ένα firewall ή στο μέρος που βρίσκεται το firewall με σκοπό να διασφαλίσει την ακεραιότητα των δεδομένων, αλλά το VPN σύστημα μπορεί να είναι ανεξάρτητο από το firewall.

Βασιζόμενα σε Software VPNs

- Σε αυτού του είδους τα VPNs ένα πρόγραμμα χειρίζεται την δημιουργία και διατήρηση της σωλήνωσης και την κρυπτογράφηση των πακέτων μεταξύ των σταθμών εργασίας.
- Το πρόγραμμα αυτό φορτώνεται σε εξυπηρετητή και πελάτη(server-client)

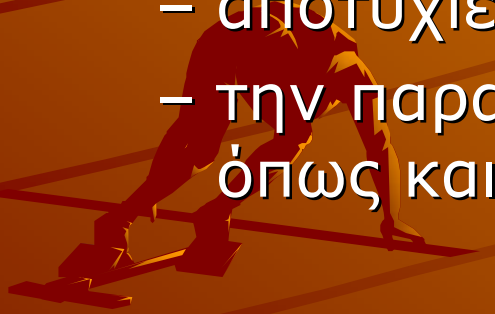


Βασιζόμενα σε Software VPNs

- Κάθε τι που φεύγει από τον client είναι κρυπτογραφημένο ή εμπεριέχεται μέσα σε μια επικεφαλίδα(encapsulation) και μεταβαίνει στον προορισμό της.
- Αυτή η διαδικασία λαμβάνει χώρα κάθε φορά που κάποιος από το εσωτερικό δίκτυο προσπαθεί να μπεί σε κάποιο άλλο που βρίσκεται εκτός και vice-versa

Διαμόρφωση και Σχεδιασμός VPN

- Όταν παραμετροποιούμε ένα VPN , θα πρέπει να καθορίσουμε :
  - το μήκος του κλειδιού που χρησιμοποιεί
  - τους servers που κάνουν την πιστοποίηση
  - αποτυχίες σύνδεσης
  - την παραγωγή πιστοποιητικού και κλειδιού, όπως και μηχανισμούς διανομής.



Τοπολογίες VPN (Σχεδιασμός/Τοπολογία)[1,4]

- Firewall-to-client
- LAN-to-LAN
- Firewall-to-intranet/extranet
- Hardware and software VPN

Firewall-to-client

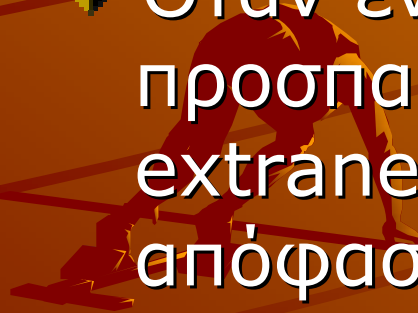
- Είναι η ευραίως χρησιμοποιούμενη τοπολογία σε απομακρισμένους χρήστες που συνδέονται σε ένα εσωτερικό δίκτυο

LAN-to-LAN

- Είναι η δεύτερη πιο διαδεδομένη τοπολογία.Επεκτύνει την firewall-to-client τοπολογία σε διαφορετικά και απομακρισμένα γραφεία, συνεργάτες και προμηθευτές όταν υπάρχει μια VPN συράγγωση μεταξύ δύο sites.

Firewall-to-intranet/extranet

- Στην τοπολογία αυτή το intranet χρησιμοποιείται από τους εργαζόμενους ενώ το extranet χρησιμοποιείται εξωτερικά από τους πελάτες , τους συνεργάτες και από τους προμηθευτές.
- Όταν ένας απομακρισμένος χρήστης προσπαθεί να προσπελάσει servers στο extranet/intranet πρέπει να παρθεί μια απόφαση ποιους μπορεί και πρέπει να προσπελάσει.



Hardware and software VPN

- Είναι μεμονομένες συσκευές οι οποίες έχουν σχεδιαστεί με σκοπό να εφαρμόσουν αλγορίθμους για VPN.
- Μια τέτοια συσκευή βρίσκεται ώς συνήθως πίσω από έναν firewall στο εσωτερικό μας δίκτυο.

Hardware and software VPN

- Τα πακέτα των δεδομένων περνάνε μέσω του firewall και της συσκευής VPN.Κατά το πέρασμα αυτών των πακέτων μέσα από αυτές τις συσκευές, μπορούν να κρυπτογραφηθούν.
- Γενικότερα μέσα από software μοντέλα κρυπτογραφίας όπως το SSL πρωτόκολο δεν απαιτούνται ειδικές συσκευές για την πιστοποίησης και τα πακέτα περνάνε κρυπτογραφημένα.

Τεχνολογίες και Πρωτόκολα VPN[4,6,7,10,11]

PPTP(Point-to-Point or Site-to-Site protocol)

L2TP(Layer 2 Tunneling protocol)

IPSec(Internet Protocol Security)

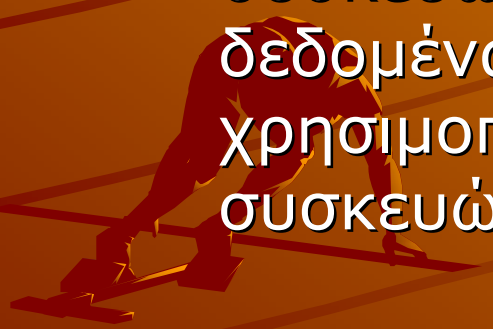
SSL(Secure Socket Layer)

Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs[3,2]

Στα Site-to-Site VPNs η μεταφορά των δεδομένων γίνεται μέσω τεχνικών συράγγωσης μεταξύ συσκευών πελατών(CE devices) ή μεταξύ συσκευών παρόχων(PE devices)(LAN-to-LAN VPNs).

Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs

- **IPSec**
  - Αποτελείται από ένα σύνολο πρωτοκόλων το οποίο είναι σχεδιασμένο να προστατεύει την IP κυκλοφορία μεταξύ ασφαλών πυλών ή συσκευών μέσω των οποίων μεταφέρονται τα δεδομένα. Οι συρραγγώσεις IPSec χρησιμοποιούνται για συνδέσεις μεταξύ CE συσκευών.



Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs

- **GRE**
  - Χρησιμοποιούνται με σκοπό την κατασκευή συρραγγώσεων και για την μεταφορά δεδομένων από διάφορετικά πρωτόκολα μεταξύ συσκευών CE σε ένα VPN. Το GRE έχει μικρή ή καθόλου ενσωματωμένη ασφάλεια, αλλά τέτοιου είδους συρραγγώσεις μπορούν να προστατευθούν με την χρήση του IPSec.

Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs

- **Draft Martini(κάθε μεταφορά πάνω από MPLS(AToM))**
  - Η Draft Martini μεταφορά επιτρέπει την Point2Point μεταφορά μέσω πρωτοκόλων όπως Frame Relay, ATM, Ethernet, Ethernet VLAN(802.1Q), High-Level Data Link Control(HDLC), και PPP κίνηση πάνω από MPLS.

Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs

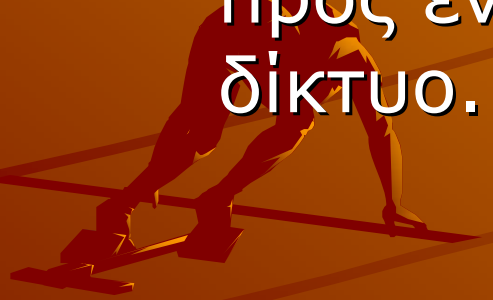
- **L2TPv3**
  - Τα πρωτόκολα L2TPv3 και κάθε μετάδοση μέσω MPLS(AToM) μπορούν να χωριστούν σε τρείς κατηγορίες:
    - Virtual Private Wire Service(VPWS)
      - Αυτού του τύπου το L2VPN παρέχει point-to-point MAN ή WAN μεταφορά πρωτοκόλων επιπέδου 2 και συνδέσεων όπως Ethernet, High-Level Data Link Control(HDLC), PPP, Frame Relay και ATM.

Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs

- Virtual Private LAN Service(VPLS)
  - Αυτό το είδος παρέχει πολυκάναλη συνδεσιμότητα Ethernet
- IP-only Private LAN Service(IPLS)
  - Αυτό είναι ένας καινούργιος τύπος L2VPN και παρέχει πολυκαναλική IP-only συνδεσιμότητα

Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs

- **IEEE 802.1Q tunneling(Q-in-Q)**
  - Η 802.1Q συρράγγωση επιτρέπει σε έναν παροχέα να πραγματοποιήσει μεταφορά δεδομένων μέσω Ethernet πρός ένα πελάτη μέσα σε ένα ιδιωτικό δίκτυο.



Τεχνολογίες και Πρωτόκολα για Site-to-Site VPNs

- **MPLS(Multiprotocol Label Switching) LSPs(Label Switching Routers)**
  - Ένα LSP είναι η διαδρομή μέσω L(abel)S(witch)R(outers) σε ένα MPLS δίκτυο. Τα πακέτα δρομολογούνται βάση των ετικετών που έχει το κάθε πακέτο.

    Το LSP για την μετάδοση χρησιμοποιεί :
    - το TDP(Tag Distribution Protocol)
    - το LDP(Label Distribution Protocol)
    - το RSVP(Resource Reservation Protocol)

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs[11]

- **L2F(Layer 2 Forwarding) protocol**
  - Το L2F πρωτόκολο της CISCO έχει σχεδιασθεί έτσι ώστε να επιτρέπει την PPP συρράγγωση των frames μεταξύ NAS(Network Access Servers) και μίας VPN gateway που βρίσκεται στο πάροχο.

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs

Οι απομακρυσμένοι χρήστες συνδέονται στον NAS και τα PPP frames από τον απομακρυσμένο υπολογιστή μεταφέρονται μέσω συρράγγωσης μέσα από ένα ιδιωτικό δίκτυο σε μια VPN gateway(home).

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs

- **PPTP(Point-to-Point Tunneling Protocol)**
  - Το PPTP είναι ένα πρωτόκολο που έχει κατασκευαστεί από μία κοινοπραξία παρόχων μέσα στους οποίους είναι η Microsoft, 3COM και η Ascend Communications.Ισχύουν τα ίδια και με το L2F.

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs

Αυτό το πρωτόκολο επίσης επιτρέπει να μπορεί να πραγματοποιηθεί συρράγγωση απευθείας του απομακρυσμένου χρήστη με την VPN gateway.Τα πακέτα PPP που περνάνε μέσα από PPTP συρράγγωση ώς συνήθως χρησιμοποιούν Microsoft Point-to-Point Encryption(MPPE).

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs

- **L2TPv2/L2TPv3(Layer 2 Tunneling Protocol versions 2 & 3)**
  - Το L2TP είναι ένα Internet Engineering Task Force(IETF) standard και συνδιάζει τις δυνατότητες των L2F & PPTP. Το L2TP έχει περιορισμένη εσωτερική ασφάλεια και για αυτό οι συρραγγώσεις αυτές χρησιμοποιούν το IPSec.

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs

- **IPSec**
  - Όπως και στα Site-to-Site VPNs, το πρωτόκολο αυτό μπορεί να χρησιμοποιηθεί και στην ασφαλή μεταφορά δεδομένων μέσα από συρργάγγωση μεταξύ ενός απομακρυσμένου χρήστη και ενός VPN gateway.

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs

- **Security Sockets Layer(SSL)**
  - Το SSL είναι ένα πρωτόκολο ασφαλείας το οποίο πρωταρχικά είχε αναπτυχθεί από την Netscape Communications και παρέχει ασφαλή απομακρυσμένη πρόσβαση για απομακρυσμένους χρήστες.

Τεχνολογίες και Πρωτόκολα για Remote Access VPNs

Ένα απο τα πλεονεκτήματα που έχει αυτό το πρωτόκολο είναι οτι για αυτού του τύπου την απομακρυσμένη πρόσβαση δεν χρειάζεται κάποιο ειδικό λογισμικό γιατί οι περισσότεροι web browsers εμπεριέχουν ότι χρειάζεται.(web ή clientless VPNs)

Transport Layer Security(TLS) είναι το standard από την IETF και είναι αντίστοιχο με το SSLv3.

Πρωτόκολα Ασφαλείας[3,6,8,10]

- Το IPSec χρησιμοποιεί δύο πρωτόκολα ασφαλείας :
  - AH(Authentication Header)
  - ESP(Encapsulating Security Payload)

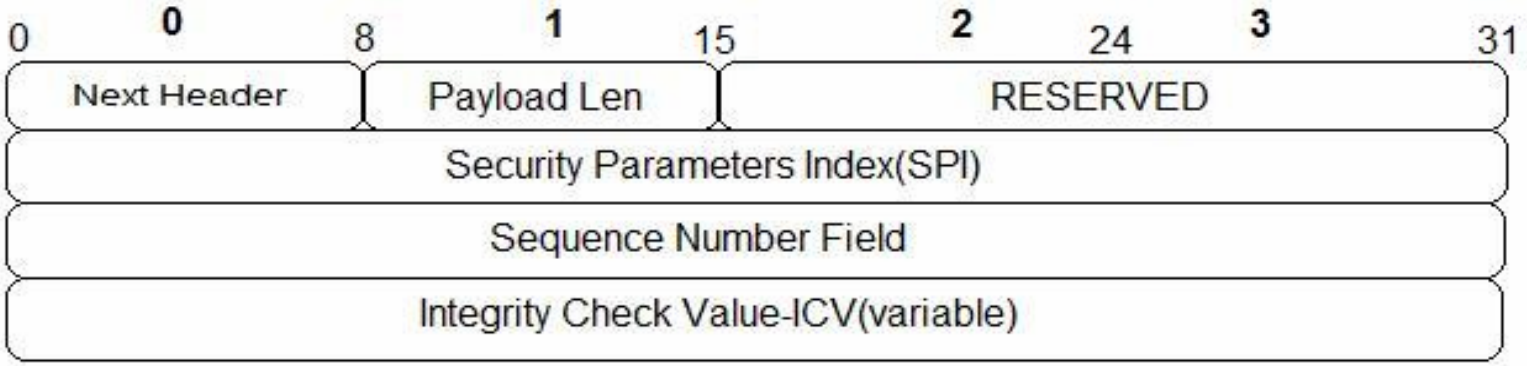
Πρωτόκολα Ασφαλείας

- Authentication Header(AH)

  Είναι μία επικεφαλίδα πακέτου η οποία περέχει τις παρακάτω υπηρεσίες ασφαλείας :
  - Ακεραιότητα σύνδεσης
  - Αυθεντικότητα δεδομένων
  - Επιλεκτική προστασία από επαναλαμβανόμενα πακέτα

  Το AH είναι ένα IP πρωτόκολο με αριθμό 51 βάση IANA

Πρωτόκολα Ασφαλείας
AH HEADER



Next Header : Σε αυτό το πεδίο περιγράφεται ο τύπος της επικεφαλίδας ο οποίος ακολουθεί (π.χ. μια εάν η τιμή είναι 6 αυτό σημαίνει ότι ο επόμενος Header είναι TCP).

Payload Length : Το μήκος του AH σε μορφή λέξεων των 32 bits - 2

Reserved : Είναι δεσμευμένο για μελλοντική χρήση

Security Parameter Index(SPI) : Χρησιμοποιείται από την gateway-αποδέκτη και βοηθάει στην αναγνώριση του τρόπου κωδικοποίησης ασφαλείας του πακέτου

Sequence Number Field : Ένας μοναδικός αριθμός ανά πακέτο που αποτρέπει την επίθεση επανάληψης του πακέτου

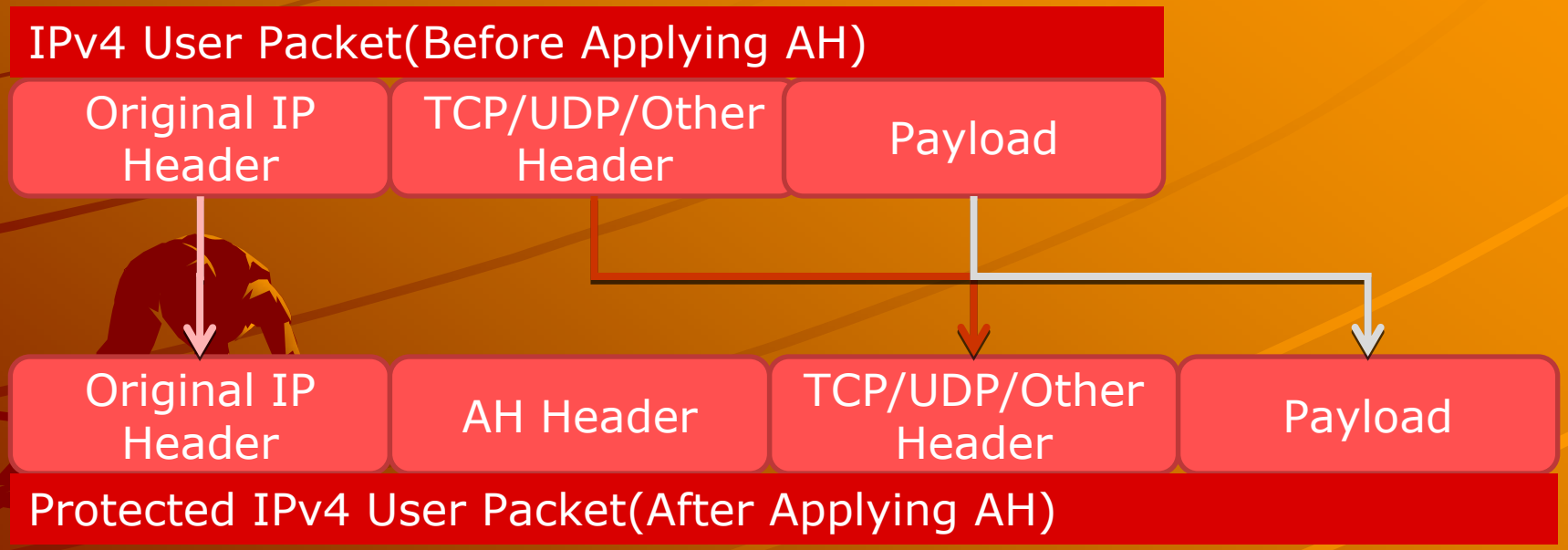
Integrity Check Value-ICV(variable) : Μία κρυπτογραφημένη τιμή(hash) που αντιστοιχεί στο πακέτο και την χρησιμοποιεί η gateway για να πιστοποιήσει την αυθεντικότητα του πακέτου

Τρόποι Λειτουργίας(ΑΗ)

- Υπάρχουν δύο τρόποι λειτουργίας του ΑΗ
  - Mode Μεταφοράς
  - Mode Συρράγγωσης

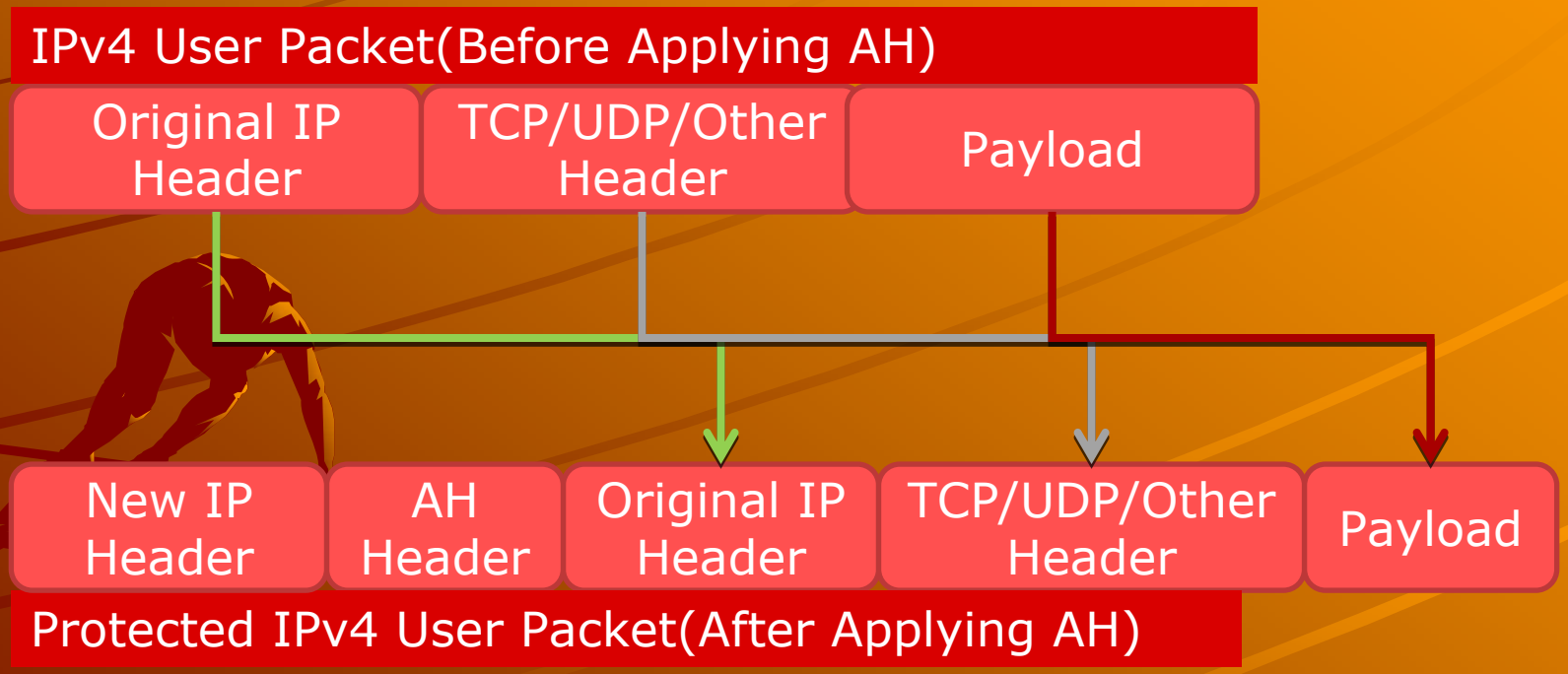
Τρόποι Λειτουργίας(AH)

- Mode Μεταφοράς



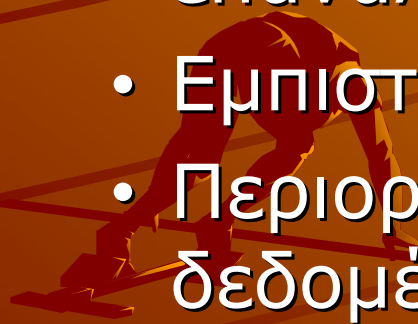
Τρόποι Λειτουργίας(AH)

- Mode Συρράγγωσης



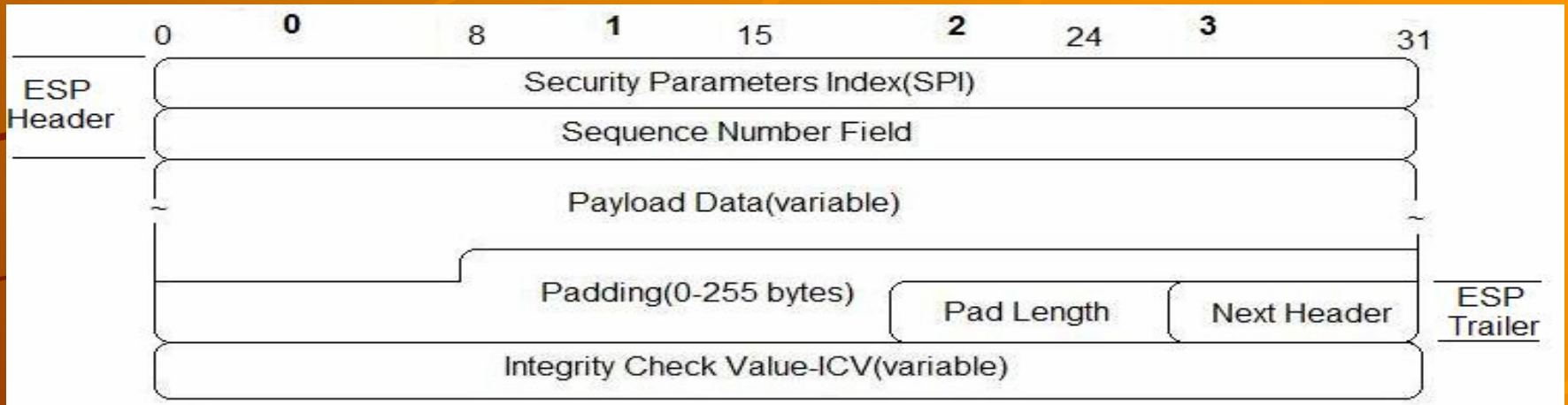
Πρωτόκολο Ασφαλείας ESP (Encapsulating Security Payload)

- Είναι μια επικεφαλίδα πακέτου που παρέχει :
  - Ακεραιότητα σύνδεσης
  - Αυθεντικότητα δεδομένων
  - Επιλεκτική προστασία από επαναλαμβανόμενα πακέτα
  - Εμπιστευτικότητα των δεδομένων
  - Περιορισμένη εμπιστευτικότητα ροής δεδομένων



Το AH είναι ένα IP πρωτόκολο με αριθμό 50 βάση IANA

Πρωτόκολο Ασφαλείας ESP Header



Payload Data : Είναι τα δεδομένα του πακέτου του χρήστη.Αυτό το πεδίο μπορεί να περιέχει έναν Initialization Vector(IV) και Traffic Flow Confidentiality(TFC) μέρος.Μερικοί αλγόριθμοι κρυπτογράφησης χρησιμοποιούν το IV για να κρυπτογραφίσουν το πρώτο block από τα δεδομένα των πακέτων του χρήστη.Το TFC μέρος χρησιμοποιείται για να κρύψει τα χαρακτηριστικά μετάδοσης δεδομένων όπως το μέγεθος του πακέτου του χρήστη

Padding : Χρησιμοποιείται για να διασφαλίσει ότι το πακέτο των δεδομένων του χρήστη είναι πολλαπλάσιο ενός συγγεκριμένου αριθμου bytes(αυτή η πληροφορία μπορεί να είναι χρήσιμη από τον αλγόριθμο κρυπτογράφησης) και επίσης διασφαλίζει την σωστή θέση των Pad Length και Next Header πεδίων των 4 Bytes μέσα στο πακέτο.

Pad Length : Περιλαμβάνει τον αριθμό των bytes στο Padding πεδίο

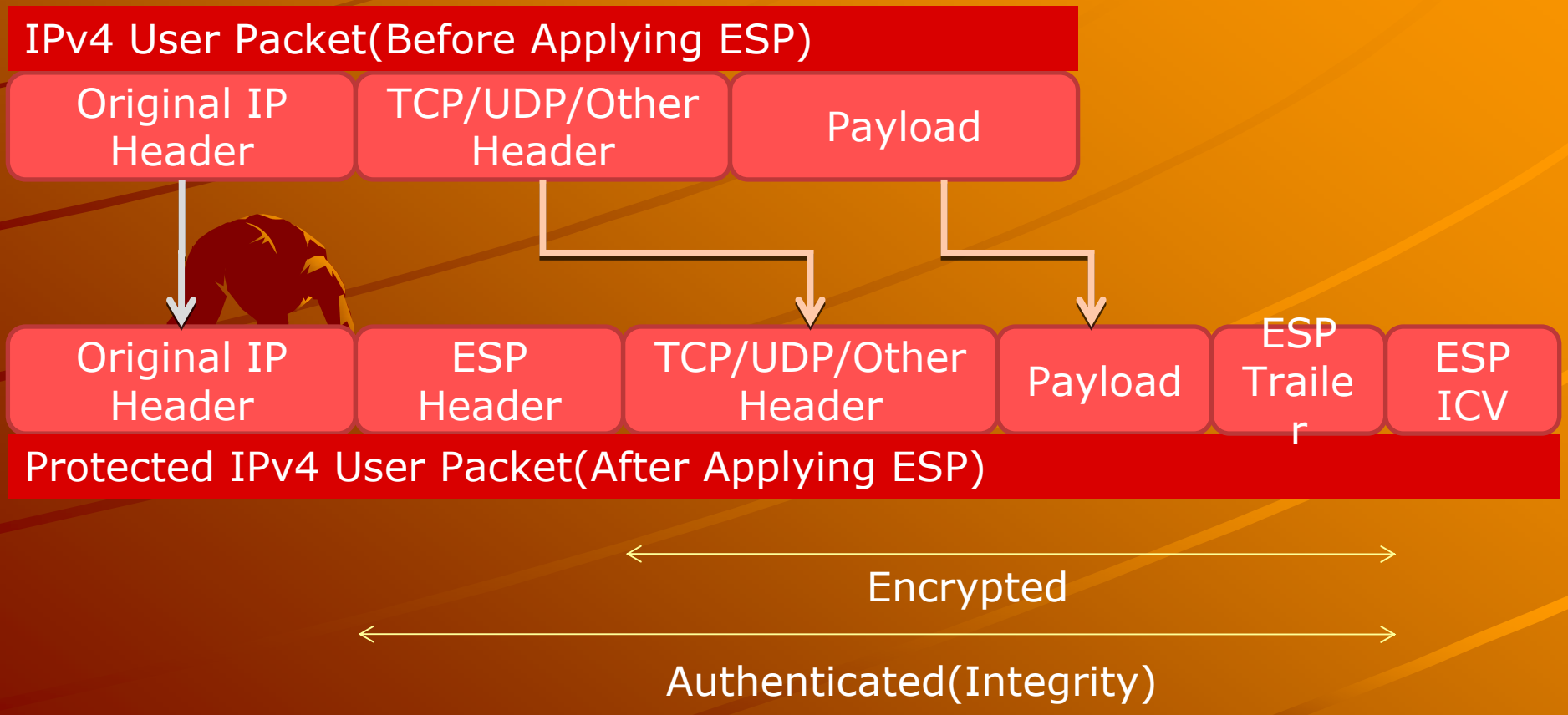
ICV : Είναι ένα μή υποχρεωτικό πεδίο και έχει την ίδια λειτουργία όπως και το ICV στο AH. Το ICV πεδίο είναι παρόν μόνο όταν η διαδικασία Πιστοποίησης είναι ενεργοποιημένη

Τρόποι Λειτουργίας(ESP)

- Υπάρχουν δύο τρόποι λειτουργίας του ESP
  - Mode Μεταφοράς
  - Mode Συρράγγωσης

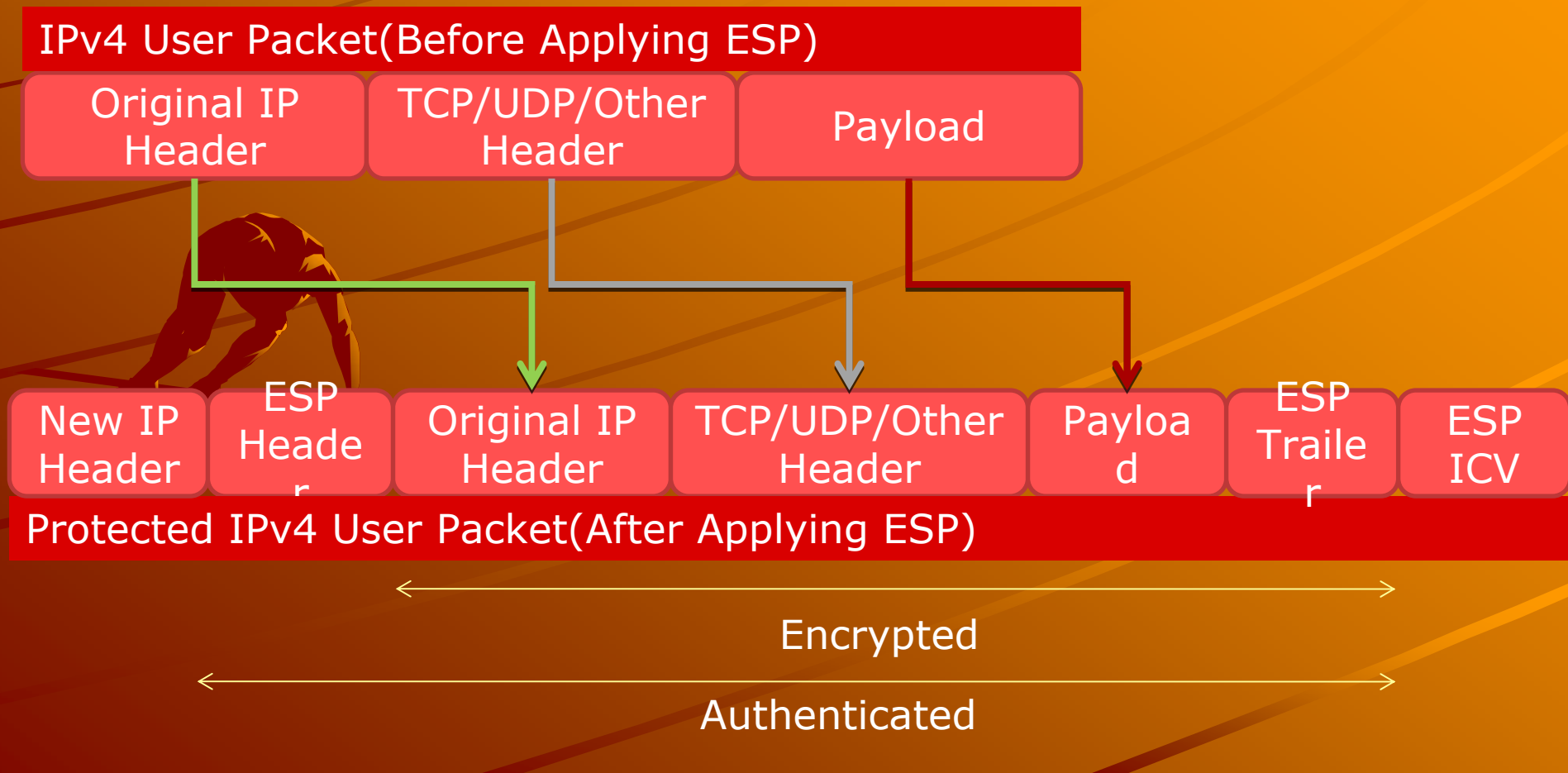
Τρόποι Λειτουργίας(ESP)

- Mode Μεταφοράς



Τρόποι Λειτουργίας(ESP)

- Mode Συρράγγωσης



AH & ESP

Original IP Header	AH Header	ESP Header	TCP/UDP/Other Header	Payload	ESP Trailer

IPv4 User Packet(After Applying AH/ESP)-Transport Mode

Encrypted

Authentication(Except Mutable Fields)

New IP Header	AH Header	ESP Header	Original IP Header	TCP/UDP/Other Header	Payload	ESP Trailer

Protected IPv4 User Packet(After Applying AH/ESP)-Tunnel Mode

Encrypted

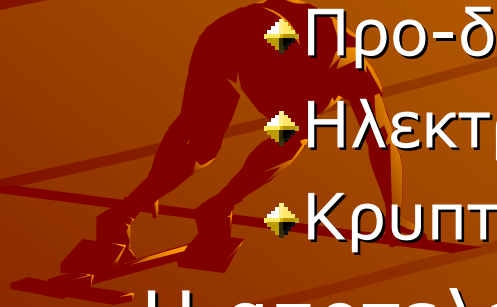
Authentication(Except Mutable Fields)

Internet Key Exchange(IKE)

- Αποτελεί τμήμα του IPSec και έχει σχεδιαστεί με σκοπό να υποστηρίζει αυτοματοποιημένα την διαπραγμάτευση των Security Associations(SA) όπως και της αυτοματοποιημένης δημιουργίας και ανανέωσης κρυπτογραφικών κλειδιών

Internet Key Exchange(IKE)

- **Περιλαμβάνει**
  - Περίπλοκες διαδικασίες κρυπτογράφησης
  - Περίπλοκες διαδικασίες εξακρίβωσης γνησιότητας
    - Προ-διαμοιρασμένο κλειδί
    - Ηλεκτρονικές Υπογραφές
    - Κρυπτογράφηση δημοσίου κλειδιού



Η αποτελεσματικότητα μιας τέτοιας κρυπτογραφικής λύσης εξαρτάται από την ασφαλή μετάδοση του κλειδιού

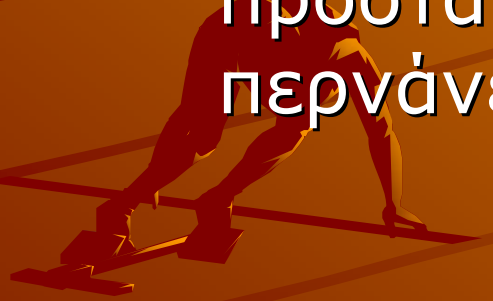
IPSec Βάσεις Δεδομένων

- Το IPSec χρησιμοποιεί τρείς databases με σκοπό να εξασφαλίσει ότι η κυκλοφορία των δεδομένων σε IP επίπεδο λειτουργεί με σωστό τρόπο.

  Οι τρείς αυτές databases είναι :
  - Security Policy Database(SPD)
  - Security Association Database(SAD or SADB)
  - Peer Authorization Database(PAD)

IPSec Βασεις Δεδομένων

- **Security Policy Database(SPD)**
  - Σε αυτήν την βάση δεδομένων καθορίζεται ποιά από τα δεδομένα που κυκλοφορούν θα πρέπει να προστατευθούν από το IPSec και ποιά θα περνάνε εκτός.



IPSec Βασεις Δεδομένων

- **Security Association Database(SAD or SADB)**
  - Το SAD περιλαμβάνει μία εγραφή η οποία περιέχει πληροφορία σχετική με κάθε IPSec SA και παρέχει πληροφορίες στο SPD με στόχο να εξασφαλιστεί η σωστή επεξεργασία των IPSec πακέτων.

IPSec Βάσεις Δεδομένων

- **Peer Authorization Database(PAD)**
  - Η PAD είναι ο σύνδεσμος μεταξύ του πρωτόκολου Internet Key Exchange(IKE) και του SPD.

    Η PAD καθορίζει το εύρος των οντοτήτων (π.χ. IP διευθύνσεις) για τις οποίες η IPSec συσκευή είναι εξουσιοδοτημένη να διαπραγματευθεί τα IPSec SAs μεταξύ των οντοτήτων και επίσης καθορίζει τον τρόπο πιστοποίησης

Κίνδυνοι VPN[1,4,8]

- Επειδή το VPN είναι ένας τρόπος επικοινωνίας για τις επιχειρήσεις οι οποίες χρησιμοποιούν υπηρεσίες τρίτων, οι κύνδυνοι που ελοχεύουν από αυτό μπορούν να κατηγοριοποιηθούν ως εξής:

Κίνδυνοι VPN

- Κίνδυνος Ασφάλειας
- Κίνδυνοι από Τρίτους
- Επιχειρησιακοί Κίνδυνοι
- Κίνδυνος Εφαρμογής
- Λειτουργικοί Κίνδυνοι

Κίνδυνος Ασφάλειας
Νομικοί Κίνδυνοι

- Ανεπαρκής αξιολόγηση της ασφάλειας του συστήματος και των νομικών κινδύνων που προκύπτουν από την χρησιμοποίηση των VPNs
- Ελλειπής χρήση προγράμματων ασφαλείας

Κίνδυνος Ασφάλειας Νομικοί Κίνδυνοι

- Ανεπαρκής προστασία των δεδομένων ενώ βρίσκονται σε σημείο πρίν μπουν στο VPN ή μόλις φτάσουν στο σημείο που αφήνουν το VPN
- Αποτυχία να προστατέψουν τις πληροφορίες όταν είναι μη κρυπτογραφημένες κατά την πορεία τους μέσα σε ένα δίκτυο(εσωτερικά δίκτυα πρίν την συσκευή κρυπτογράφησης ή εξωτερικά μετά την συσκευή αποκρυπτογράφησης)

Κίνδυνος Ασφάλειας Νομικοί Κίνδυνοι

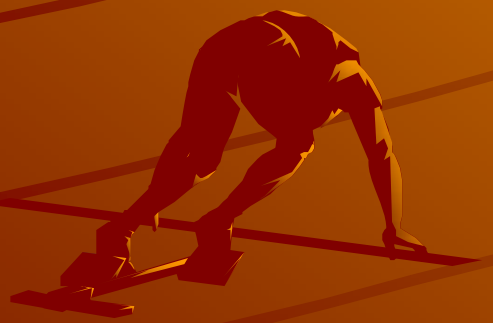
- Αποτυχία της εφαρμογής η οποία θα μπορούσε να οδηγήσει σε ζητήματα εμπιστευτικότητας, ακεραιότητας, μη αναγνώρησης και διαθεσιμότητας

Κίνδυνοι από Τρίτους

- Επιλογή ενός μή κατάλληλου παρόχου
- Ανεπαρκείς ικανότητες διαχείρησης
- Ανεπαρκείς συμφωνίες στο επίπεδο υπηρεσιών(SLA)
- Ανεπαρκής μέτρηση και παρακολούθηση των SLA
- Ελλειπής στρατηγική για την διατήρηση αρχείων ασφαλείας

Κίνδυνοι από Τρίτους

- Κατάχρηση της πρόσβασης στα δεδομένα σε ένα VPN



Επιχειρησιακοί Κίνδυνοι

- Μη συμμόρφωση με την πολιτική της εταιρίας
- Αποτυχία στην προσπάθεια μείωσης του κόστους
- Αποτυχία στο να επιτύχουμε τον επιθυμητό δείκτη ασφαλείας
- Δυσκολία στην χρήση
- Αποτυχία στην κάλυψη των απαιτήσεων των χρηστών

Επιχειρησιακοί Κίνδυνοι

- Αποτυχία της υπηρεσίας σε άλλους τομείς της επιχείρησης

Κίνδυνοι Εφαρμογής

- Η ανεπαρκής προσοχή και η μη κατάλληλη επιλογή σχεδίου
- Λάθος επιλογή του VPN μοντέλου για την επιχείρηση
- Μη κατάλληλη χρήση απο τρίτους
- Ελλειπής προσοχή στην ασφάλεια κατά την διαδικασία του σχεδιασμού

Κίνδυνοι Εφαρμογής

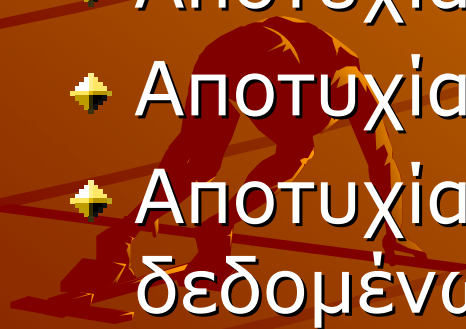
- Μη κατάλληλες διαδικασίες ανάκαμψης
- Αποτυχία στο να σχεδιάσουμε απαιτήσεις για το επίπεδο υπηρεσιών και μετρήσεων
- Αποτυχία στην σχεδίαση αλλαγής στρατηγικής

Κίνδυνοι Εφαρμογής

- Μη αποτελεσματική αλλαγή στο πρόγραμμα ή στην διαχείρηση της εφαρμογής
- Το ίδιο interface διαχειρίζεται την κίνηση στο Internet και VPN

Λειτουργικοί Κίνδυνοι

- Ανεπάρκεια πόρων και μη ικανοποιητική λειτουργία
- Αποτυχία της αξιοπιστίας
- Μείωση της ποιότητας των υπηρεσιών
- Αποτυχία στην διαλειτουργικότητα
- Αποτυχία της διαδικασίας ενθυλάκωσης
- Αποτυχία στην ανάκτηση παλιών δεδομένων



Λειτουργικοί Κίνδυνοι

- Χρήση προσωπικών συσκευών στη εργασία και για την εργασία
- Αποτυχία στην διατήρηση της εμπιστευτικότητας των παραμέτρων λειτουργίας ή των δεδομένων

Πλεονεκτήματα VPN

- Επέκταση δικτύου της επιχείρησης με ευέλικτο τρόπο και σε διαφορετικές περιοχές
- Εξοικονόμηση κεφαλαίου
- Η χρησιμοποίηση του δημόσιου δικτύου σημαίνει πολύ μικρότερα τηλεποικοινωνιακά κόστη, για τους παρόχους(20-80%)

Πλεονεκτήματα VPN

- Ο εξοπλισμός που απαιτείται για την υλοποίηση αυτών συνήθως περιλαμβάνεται στην τιμή διάθεσης τους με την μορφή ενοικίασης.Για την επιχείρηση αυτό σημαίνει οικονομικό όφελος
- Η διαχείρηση, παρακολούθηση και συντήρηση δικτύων πραγματοποιείται από τους παρόχους κεντρικά.
  Άρα η επιβάρυνση της επιχείρησης μειώνεται στο ελάχιστο

Πλεονεκτήματα VPN

- Υψηλή αξιοπιστία με την κατάληλη χρήση εργαλείων και τεχνικών

VPN Protocols – OSI 5

OSI Layers	VPN Protocols
Application	S-Mime, Kerberos, Proxies, SET
Presentation	
Session transport(TCP/UDP)	SOCKS, SSL
Network(IP)	IPSec (AH,ESP) and other tunneling protocols
Data Link	CHAP, PAP, PPTP, L2TP
Physical Layer	

REFERENCES

1. Information System Audit and Control Association, IS Auditing Guideline, Review of Virtual Private Networks, Document #060.020.120, (references:
   - Virtual Private Networking-New issues for Network Security, IT Governance Institute, USA, 2001
   - Control Objectives for Netcentric Technology(ITNCT), IT Governance Institute, USA, 1999)

REFERENCES

2. Γιώργος Διακονικολάου-Αθανασία Αγιακάτσικα-Ηλίας Μπούρας, Επιχειρισιακή Διαδικτύωση, Οκτώβριος 2007
3. Mark Lewis CCIE, Comparing, Designing, and Deploying VPNs,CISCO Press,April 2006
4. International Engineering Consortium (IEC)

   http://www.iec.org/online/tutorials/vpn/topic01.html

REFERENCES

5. Christina Ledesma(CISA, CISM) and John G. Ott(CISA, CPA), Information Systems Audit and Control Association, Virtual private Network(VPN) : Audit Approach Based on Standard SDLC Concepts
6. Vijay Bollapragada-Mohamed Khalid-Scott Wainner, IPSec VPN Design, Cisco Press, April 2005

REFERENCES

7. Wei Luo, - CCIE No. 13.291, Carlos Pignataro, - CCIE No. 4619,Dmitry Bokotey, - CCIE No.4460, Anthony Chan,- CCIE No.10.266, Layer 2 VPN Architectures, Cisco Press, March 2005
8. Mark Lewis, Troubleshooting Virtual Private Networks, Cisco Press, May 2004
9. Joseph Steinberg and Timothy Speed, SSL VPN, Understanding, evaluating and planning secure, web-based remote access, February 2005

REFERENCES

10.Sherali Zeadally(Network Systems Laboratory, Departement of Computer Science and Information Technology, University of the District of Columbia, Washington DC, USA)

Nikolas Sklavos(University of Patras, Greece)

Moganakrishnan Rathakrishnan(Dow Jones and Company, South Brunswick, NJ, USA)

REFERENCES

Scott Fowler(Adaptive Communications Networks, Research Group, Aston University, Birmingham, UK),

End-to-End Security Across Wired-Wireless Networks for Mobile Users,

Information Systems Security, Volume 16,September/October 2007

REFERENCES

11. Deloitte & Touche, e-COMMERSE SECURITY, Securing The Network Perimeter, Technical Reference Series