ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - NETWORK MANAGEMENT

Διαχείριση Ασφαλείας - Security Management (II)

Συστήματα Ηλεκτρονικού Ταχυδρομείου - eMail Protocols & Architectures
Προστασία μέσω Firewalls
Intrusion Detection Systems (IDS)
Παρακολούθηση Δικτυακής Κίνησης - Network Monitoring

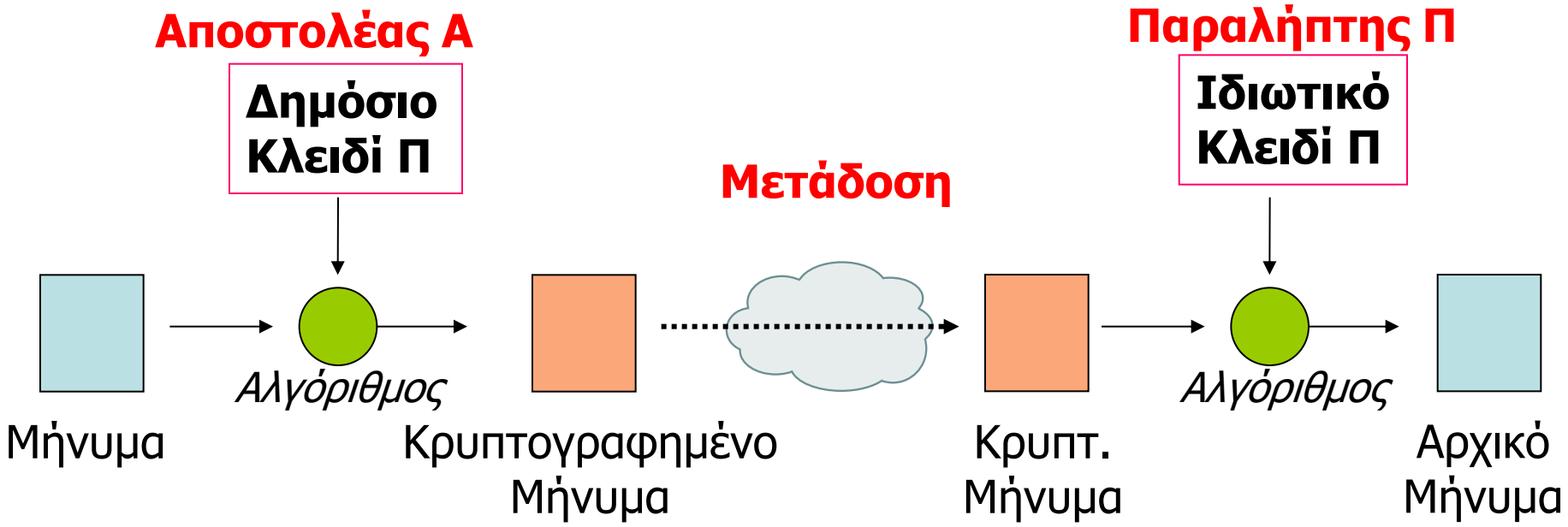
Β. Μάγκλαρης
maglaris@netmode.ntua.gr
www.netmode.ntua.gr

13/12/2021

ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

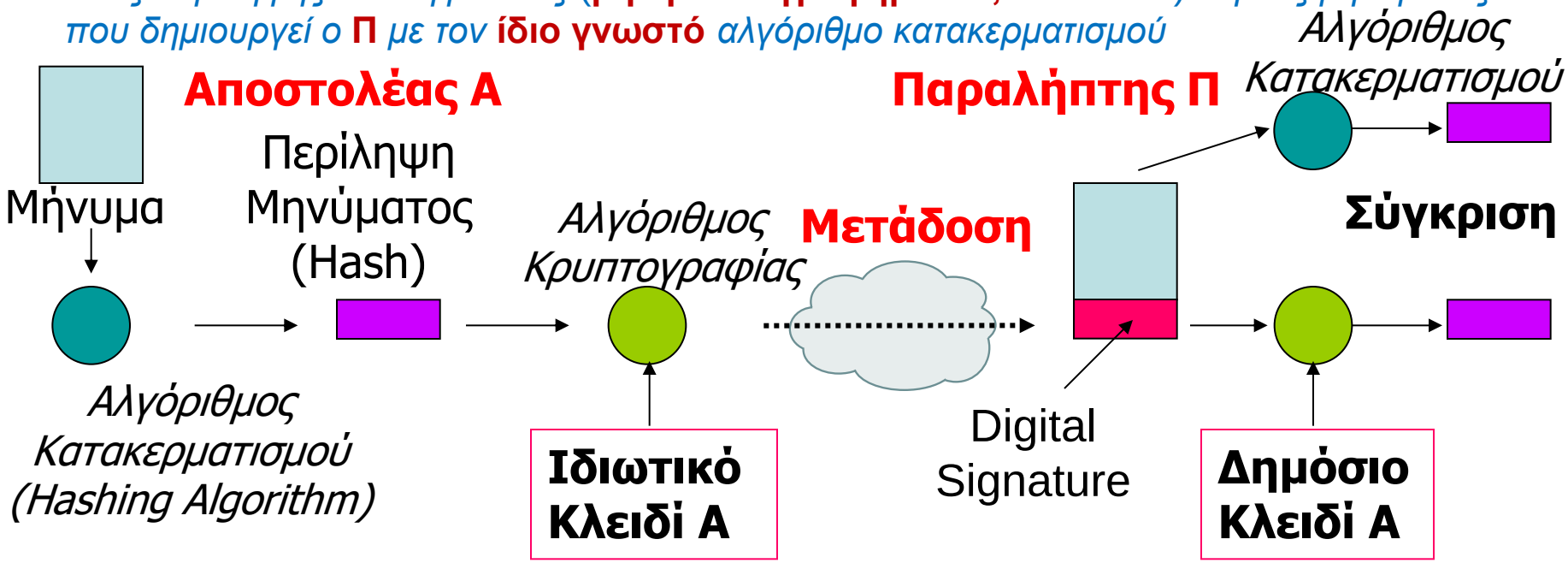
Pubic Key Encryption: Confidentiality (*Επανάληψη*)

- Ο Αποστολέας **Α** γνωρίζει το **Δημόσιο Κλειδί** του Παραλήπτη **Π** (π.χ. με Ψηφιακό Πιστοποιητικό από Certification Authority **CA**, self-signed ή υπογραμμένο από 3ης έμπιστη οντότητα – Third Trusted Party **TTP**, στα πλαίσια Υποδομής Δημοσίου Κλειδιού - **Public Key Infrastructure PKI**)
  - *Κρυπτογράφηση στον* **Α**: *Με το* **Δημόσιο Κλειδί** *του* **Π**
  - *Αποκρυπτογράφηση στον* **Π**: *Με το* **Ιδιωτικό Κλειδί** *του* Π



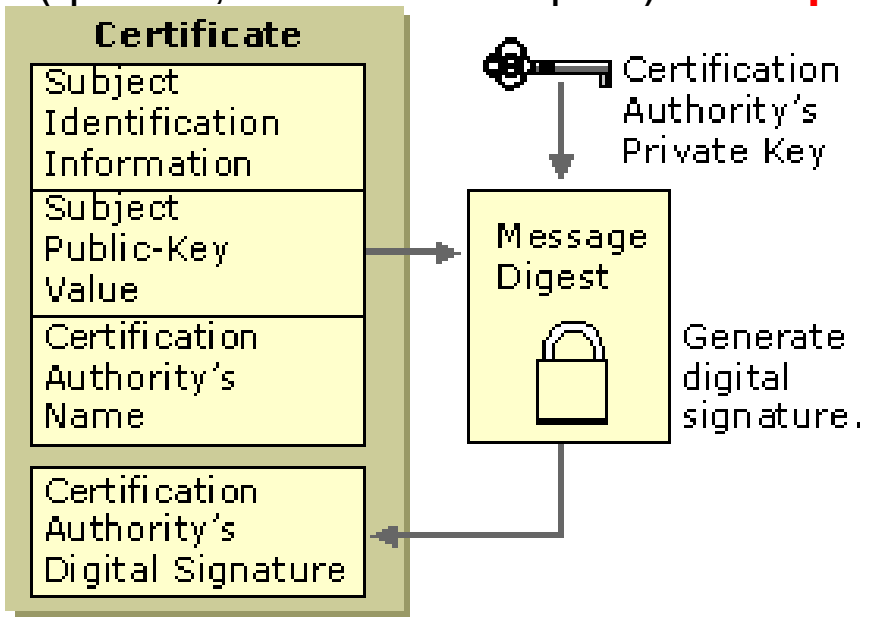
ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ:
Sender Authentication / Non Repudiation – Message Integrity (*Επανάληψη*)

- Οι Αποστολέας **Α** και Παραλήπτης **Π** κατέχουν ζεύγη Δημοσίου & Ιδιωτικού Κλειδιού και έχουν αμοιβαία γνώση των **Δημοσίων Κλειδιών** & αλγορίθμων κρυπτογράφησης - κατακερματισμού
- Ο Αποστολέας **Α** προσθέτει Ψηφιακή Υπογραφή (**Digital Signature**) στο μήνυμα με κρυπτογράφηση με το Ιδιωτικό του κλειδί περίληψης (**hash**) του μηνύματος που προκύπτει με αλγόριθμο κατακερματισμού (**hashing algorithm**)
- Ο Παραλήπτης **Π** επιβεβαιώνει (**authenticate**) την ταυτότητα του **Α**, χωρίς δυνατότητά του **Α** άρνησης της αποστολής (**non-repudiation**) & επιβεβαιώνει την μη αλλοίωση του μηνύματος (**message integrity**) με βάση την σύγκριση:
  - *Ψηφιακής Υπογραφής, αποκρυπτογραφημένης στον* **Π** *με το* **γνωστό** *Δημόσιο Κλειδί του* **Α**
  - *Νέας περίληψης του ληφθέντος* (**μη κρυπτογραφημένου, clear text**) *κυρίως μηνύματος που δημιουργεί ο* **Π** *με τον* **ίδιο γνωστό** *αλγόριθμο κατακερματισμού*



ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ X.509 (*Επανάληψη*)

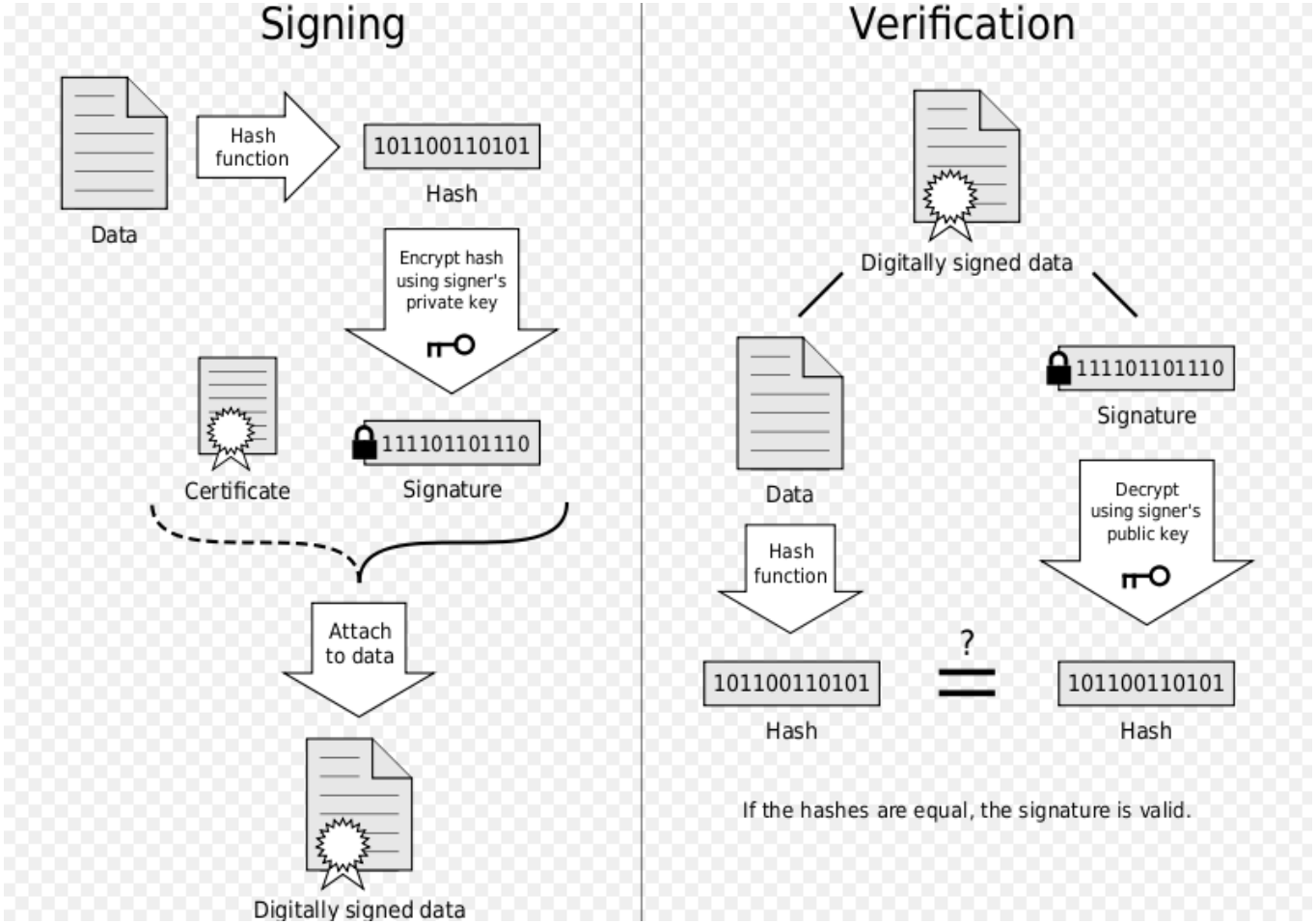
- Αν συνοδεύουν υπογραμμένο μήνυμα, βεβαιώνουν τη γνησιότητα του **Δημοσίου Κλειδιού** του αποστολέα (subject) κατά μια Τρίτη Έμπιστη Οντότητα **TTP - Third Trusted Party**: Την Αρχή Πιστοποίησης, **Certification Authority – CA**
- **Μη Κρυπτογραφημένα Πεδία Ψηφιακού Πιστοποιητικού**: Πληροφορίες για τον αποστολέα (subject) μηνύματος (**ID**, **Public Key**,…) και της **CA**
- **Κρυπτογραφημένο Πεδίο**: Ψηφιακή Υπογραφή Πιστοποιητικού από **CA**
- Η **CA** υπογράφει με το **Ιδιωτικό Κλειδί** της. Το **Δημόσιο Κλειδί** της πρέπει να είναι γνωστό στους παραλήπτες (π.χ. ενσωματωμένο στον Web Browser) ή αποδεκτό λόγω σχέσης εμπιστοσύνης (π.χ. σε περιπτώσεις **Self-Signed CA**)
- Αν χρειάζεται και έλεγχος του **Δημοσίου Κλειδιού** της **CA**, μπορεί να αποστέλλεται και 2ο (ή και 3ο, 4ο …πιστοποιητικό) από **ιεραρχικά δομημένες CA**



https://technet.microsoft.com/en-us/library/cc962029.aspx

ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ (*Επανάληψη*)

http://en.wikipedia.org/wiki/Digital_signature



ΜΕΙΚΤΟ ΣΥΣΤΗΜΑ ΑΣΦΑΛΟΥΣ ΠΡΟΣΒΑΣΗΣ
Access Control, Mixed Schema (*Επανάληψη*)
SSL/TLS: Secure Sockets Layer/Transport Layer Security

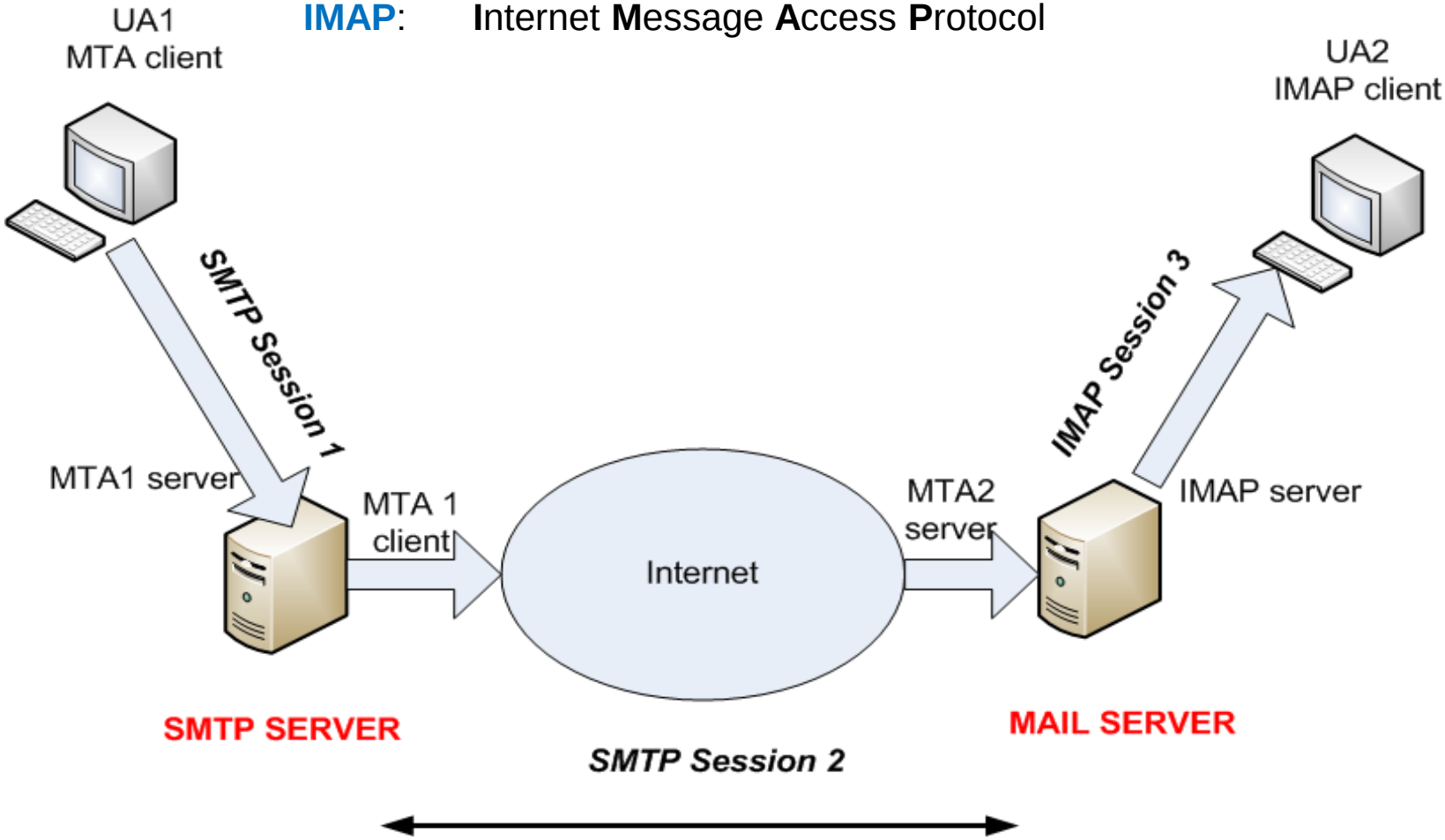
- **1η Φάση: Handshaking**
  - Ο χρήστης (User) **U** λαμβάνει γνώση του **Δημοσίου Κλειδιού** του εξυπηρετητή (Server) **S** με Ψηφιακό Πιστοποιητικό από Certification Authority **CA** self-signed ή υπογραμμένο από 3ης έμπιστη οντότητα – Third Trusted Party **TTP**, στα πλαίσια αρχιτεκτονικής **Public Key Infrastructure PKI**
  - Ο **U** δημιουργεί Κοινό **Συμμετρικό Κλειδί** με τυχαίο αλγόριθμο και το κοινοποιεί στον **S** κρυπτογραφημένο με το **Δημόσιο Κλειδί** του **S**
- **2η Φάση: Κρυπτογραφημένος Διάλογος με Κοινό Συμμετρικό Κλειδί**
  - Γρήγορη συμμετρική κρυπτογραφία σε **Secure Channel** μεταξύ **S – U** (το Συμμετρικό Κλειδί ισχύει μόνο για το συγκεκριμένο session)
- **ΠΑΡΑΤΗΡΗΣΗ:**
  - Ο **U** δεν απαιτείται να έχει Πιστοποιητικό με **Δημόσιο Κλειδί** (ψηφιακή υπογραφή), μόνο ο **S** έχει Πιστοποίηση μέσω TTP ή self-signed (**Server Based Authentication**)
  - Για Ταυτοποίηση – Εξουσιοδότηση του **U** από τον **S** (**Client & Server Based Authentication**) απαιτείται μετάδοση από το secure channel της **Digital Identity** του Client (συνήθως **User_Name/Password** ή **Client Certificates** αν υπάρχουν, εναλλακτικά **PIN** για ταυτοποίηση με e-mail ή SMS σε κινητό του **U**) → έλεγχος στον **S** σε Βάση Δεδομένων Χρηστών (με πρωτόκολλο **LDAP - TCP** για εφαρμογές Web, Mail… ή με πρωτόκολλο **RADIUS - UDP** αν μεσολαβεί **Remote Access Server** π.χ. για πρόσβαση σε υπηρεσία DSL, WiFi roaming…)

ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΧΡΗΣΤΗ (*Επανάληψη*)
User Access Control,
Authentication & Authorization Infrastructure (AAI)
Single Sign-On (SSO), Identity Providers (IdP)

- Ταυτοποίηση (**Authentication**) & Εξουσιοδότηση (**Authorization**) χρήστη με:
  - Username, Password
  - LDAP Server (Lightweight Directory Access Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)
  - Active Directory (MS Windows)
- Οι Υποδομές Ταυτοποίησης & Εξουσιοδότησης (**AAI**) επιτρέπουν πρόσβαση **Single Sign-On (SSO)** σε χρήστες διαδικτυακών πόρων κατανεμημένων σε παρόχους με αμοιβαία εμπιστοσύνη:
  - Ταυτοποίηση (Authentication) μια φορά
  - Εξουσιοδότηση (Authorization) ξεχωριστά με κάθε πάροχο
- Μεσολάβηση Παρόχου Ταυτότητας (**Identity Provider - IdP**) π.χ. **Facebook, Twitter, Google User Accounts** για
  - Εξουσιοδότηση Single Sign-On σε υπηρεσίες με σχετικό security token συνδρομητή από IdP σε **Service Providers** που το εμπιστεύονται (π.χ. **OAuth** – Open standard for Authorization**,** **SAML** - Security Assertion Markup Language)
  - Επιβεβαίωση Ισχυρισμών Ταυτότητας (**Identity Assertion**) από **WAYF** (Where Are You From) servers μέσω πρωτοκόλλου **SAML** ή από **LDAP** servers με πιστοποιητικά **X509**
- Συνέργεια **IdP** σε ομόσπονδα σχήματα **AAI** (π.χ. US Internet2 **Shibboleth**, GÉANT **eduGAIN**)

ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ (1/3)

UA: **U**ser **A**gent
MTA: **M**essage **T**ransfer **A**gent
SMTP: **S**imple **M**ail **T**ransfer **P**rotocol
IMAP: **I**nternet **M**essage **A**ccess **P**rotocol



ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ (2/3)

UA: **U**ser **A**gent
MTA: **M**essage **T**ransfer **A**gent
SMTP: **S**imple **M**ail **T**ransfer **P**rotocol
IMAP: **I**nternet **M**essage **A**ccess **P**rotocol

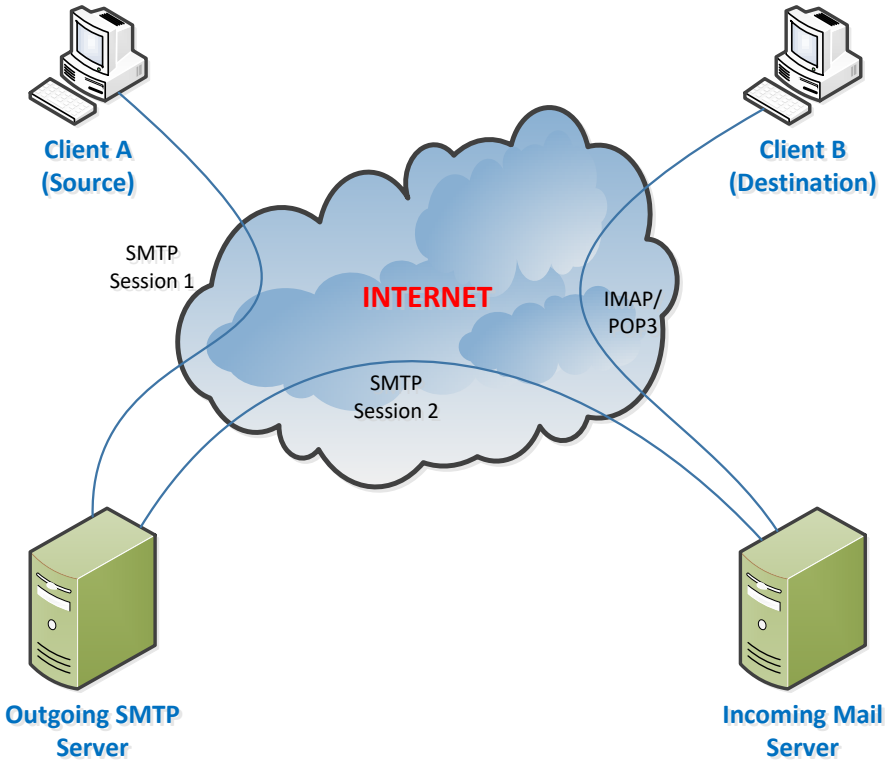
- **UA 1 → MTA 1 (Session 1)**
  - User Agent → Message Transfer Agent
  - SMTP (TCP Session 1)
  - Δυνατότητα SSL/TLS security
- **MTA 1 → MTA 2 (Session 2)**
  - SMTP (TCP Session 2)
  - Δυνατότητα κρυπτογράφησης (αν υποστηρίζεται από το Mail S/W – π.χ. sendmail)
- **MTA 2 (Mail Server) → UA 2 (Session 3)**
  - Πρωτόκολλα POP/IMAP (TCP Session 3)
  - Δυνατότητα SSL/TLS

ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ (3/3)

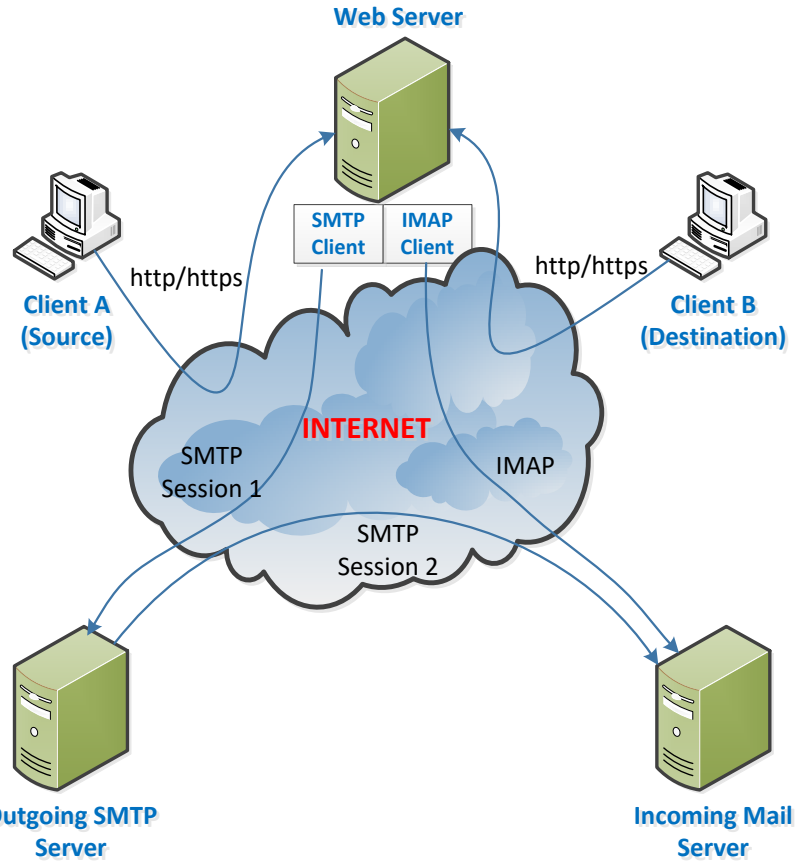
Σχήμα με IMAP/POP3 Clients (Outlook, Thunderbird, Fedora…)

IMAP: Κρατάει αντίγραφα emails και συντηρεί mail folders των users στον server

POP3: Δεν κρατάει αντίγραφα emails στον server αφού διώξει τα emails στον client (πρόβλημα για χρήστες που λαμβάνουν email σε πολλαπλούς clients)



Παράδειγμα Web Mail



ΣΥΣΤΗΜΑΤΑ ΔΙΚΤΥΑΚΗΣ ΠΡΟΣΤΑΣΙΑΣ (1/3)
Firewalls

- Τι είναι ένα **Firewall**:
  Ένα σύστημα ή συνδυασμός συστημάτων που ελέγχουν την πρόσβαση και παρέχουν έναν βαθμό ασφάλειας μεταξύ δικτύων, ***Marcus J. Ranum***, δημιουργός του πρώτου firewall

- Λειτουργία
  - Δρομολογητής που ελέγχει την κίνηση (Screening router / Bastion Host). Μπορεί να συνδυαστεί με την ύπαρξη ιδιωτικών εσωτερικών διευθύνσεων και μετάφραση στο σύνορο (**NAT** - Network Address Translation).
  - Ο πιο απλός Firewall είναι ο δρομολογητής (router) με σωστά στημένες Access Lists (**ACLs**)

- Για να χρησιμοποιήσουμε Firewall χρειάζεται να σχεδιαστεί κατάλληλα το δίκτυο, σύμφωνα με τις πολιτικές ασφαλείας

ΣΥΣΤΗΜΑΤΑ ΔΙΚΤΥΑΚΗΣ ΠΡΟΣΤΑΣΙΑΣ (2/3)
Firewalls

- Βασικοί κανόνες

  <RuleGroup>

  <Action> Deny ή Allow

  <Protocol> IP, TCP, UDP, ICMP, κ.λπ.

  <SrcPort> <DstPort>

  <SrcIP> <SrcMask> Πηγή - Ξεχωριστές διευθύνσεις IP ή ομαδοποιήσεις τους

  <DstIP> <DstMask> Προορισμός

- Παράδειγμα από δρομολογητή Cisco:

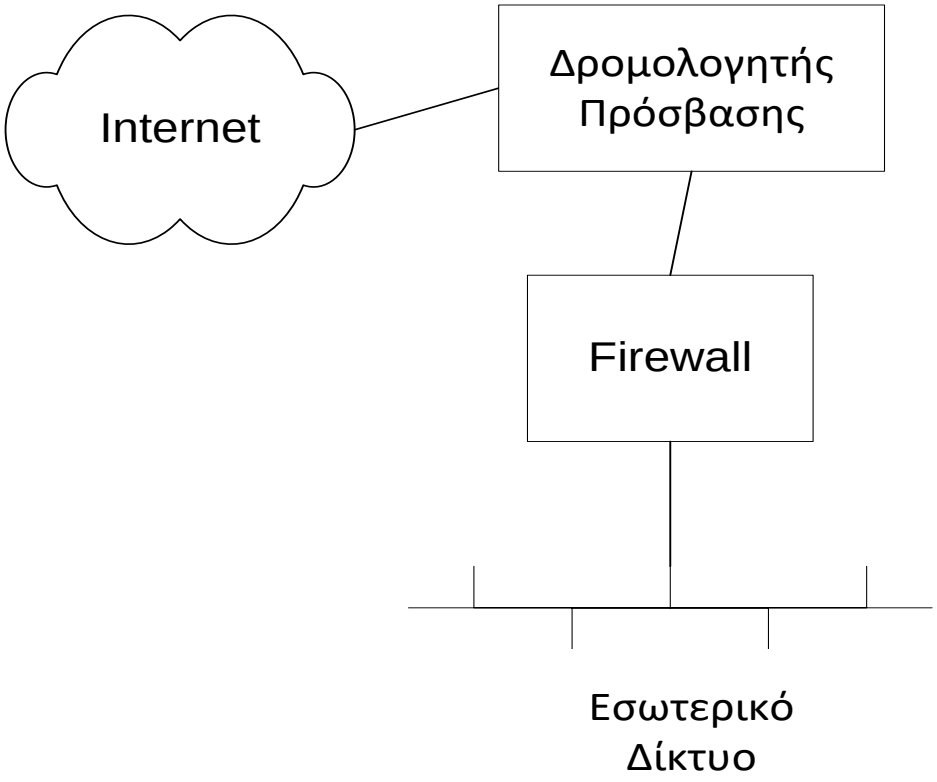
```
access-list 100 permit tcp any host 171.16.23.1 eq 80
```

- Οι σύγχρονες Firewall έχουν πολλά επιπλέον χρήσιμα χαρακτηριστικά:
  - Γραφικό περιβάλλον
  - Ορισμό ομάδων κανόνων
  - Ορισμό περιοχών προστασίας και ομάδων χρηστών
  - Διαδικασία ενημέρωσης κανόνων μέσω εξυπηρετητών και σύμφωνα με τις εταιρικές πολιτικές ασφαλείας κ.λπ.

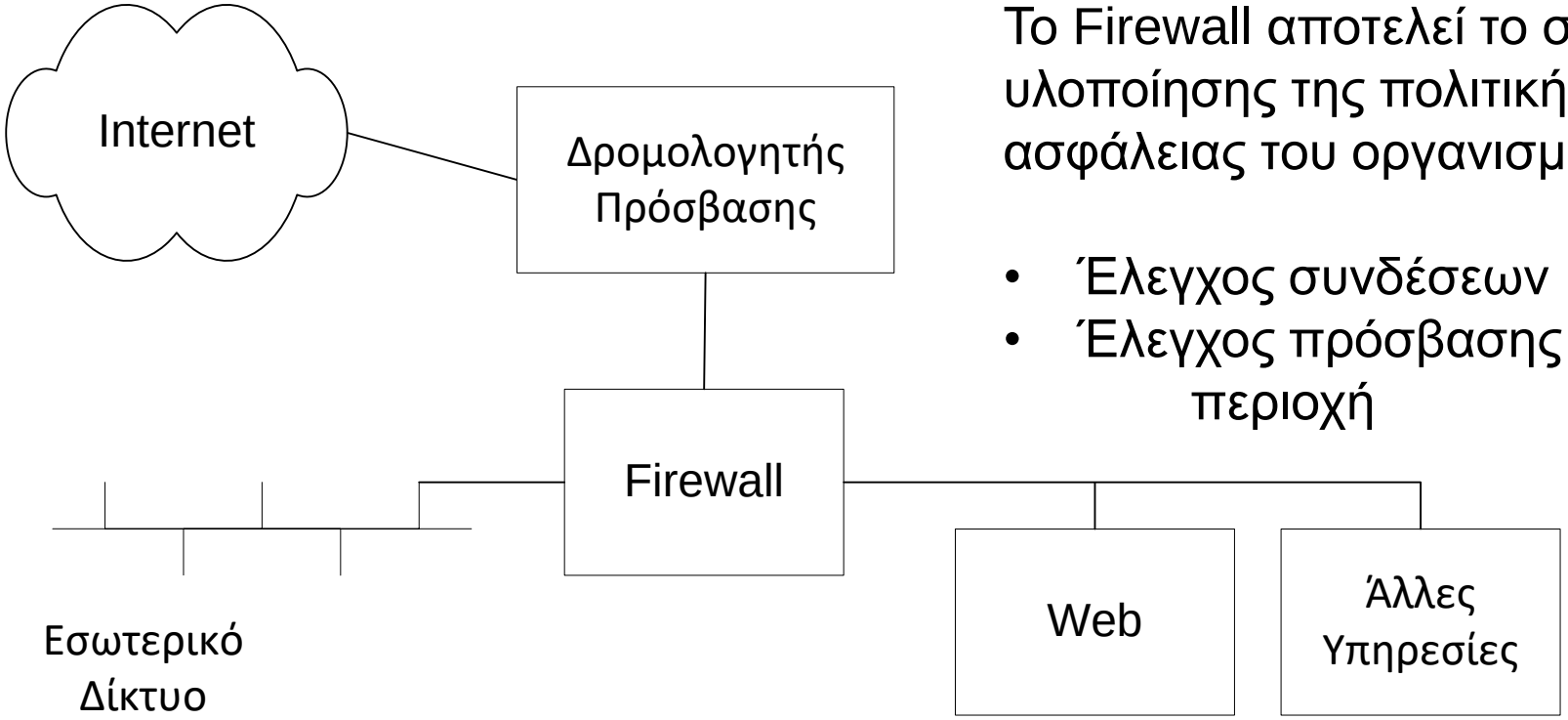
ΣΥΣΤΗΜΑΤΑ ΔΙΚΤΥΑΚΗΣ ΠΡΟΣΤΑΣΙΑΣ (3/3)
Firewalls

- Πολιτικές πρόσβασης
  - Απαγόρευση όλων των συνδέσεων πλην εξαιρέσεων ("Deny unless allowed") – χρησιμοποιείται για ισχυρή προστασία, συνήθως στην εισερχόμενη κίνηση ενός δικτύου
  - Διέλευση όλων πλην εξαιρέσεων ("Allow unless denied") – δίνει μεγαλύτερη ελευθερία
  - Επιπλέον δυνατότητες:
    - Διέλευση κίνησης που έχει ήδη ολοκληρώσει το TCP Three Way Handshake (Established)
    - Απαγόρευση πακέτων που δεν έχουν τις προβλεπόμενες διευθύνσεις προέλευσης (προστασία από το spoofing)

ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ - Firewalls (1/3)



ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ - Firewalls (2/3)



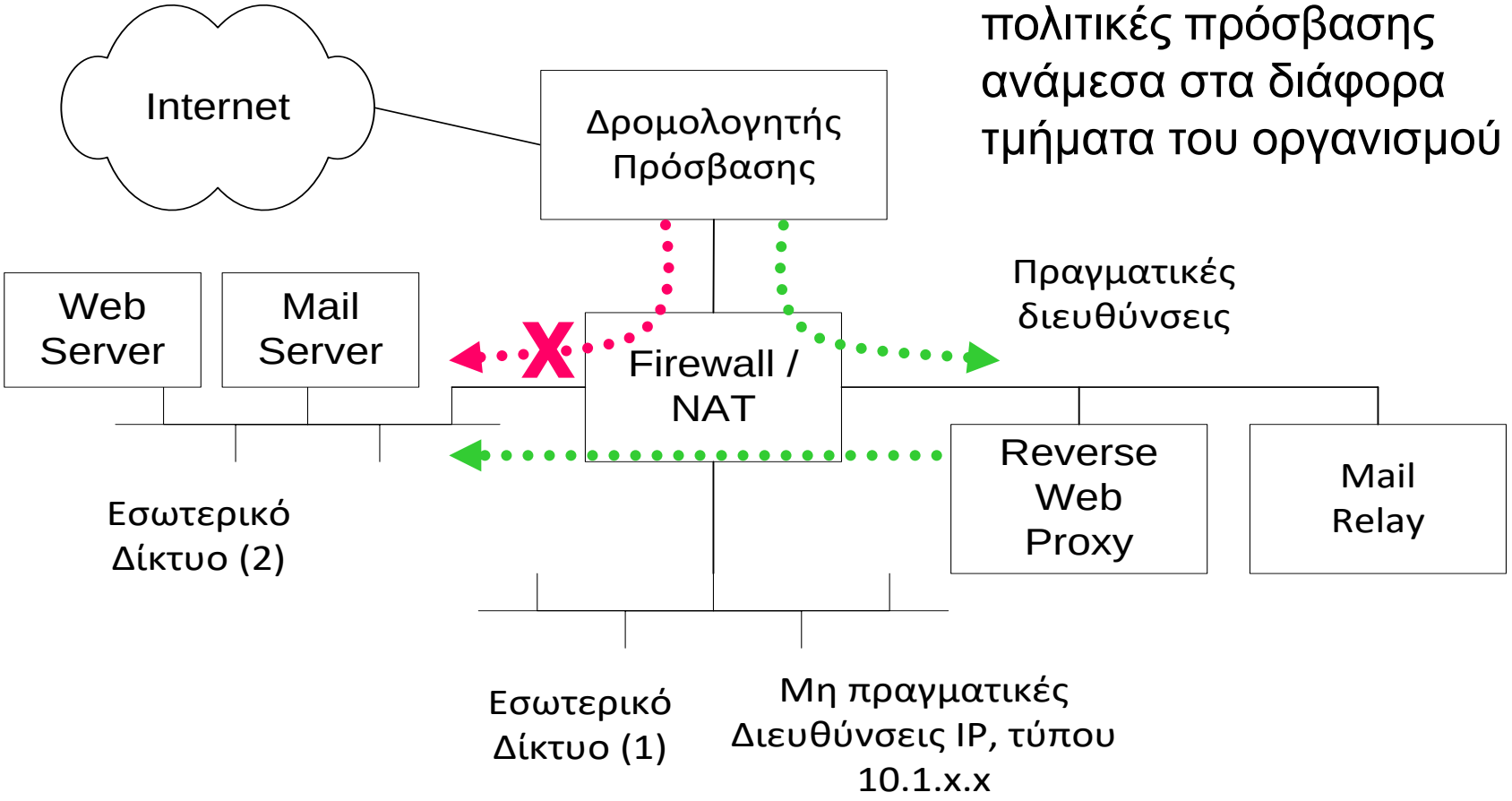
Το Firewall αποτελεί το σημείο υλοποίησης της πολιτικής ασφάλειας του οργανισμού:

- Έλεγχος συνδέσεων
- Έλεγχος πρόσβασης ανά περιοχή

"Αποστρατικοποιημένη Ζώνη"
Demilitarized Zone - DMZ
Παρέχει αυξημένη πρόσβαση σε κάποια συστήματα του δικτύου χωρίς να θέτει σε κίνδυνο το υπόλοιπο

ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ - Firewalls (3/3)

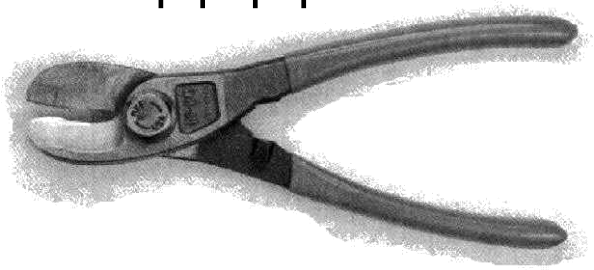
Το Firewall υλοποιεί πολιτικές πρόσβασης ανάμεσα στα διάφορα τμήματα του οργανισμού



ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (1/4)
Intrusion Detection Systems – IDS

- Τα υπολογιστικά συστήματα, ασχέτως κατασκευαστή και λειτουργίας, είναι ευάλωτα σε πολλαπλές απειλές, η δε πλήρης εξασφάλιση τους είναι τεχνικά δύσκολη και οικονομικά ασύμφορη.

- Η απόλυτη (;;;) ασφάλεια:



- Ένα IDS παρακολουθεί το περιβάλλον στο οποίο είναι εγκατεστημένο
  - Υπολογιστικό σύστημα (**Host based IDS**)
  - Δίκτυο (**Network Based IDS**)

- Μεθοδολογίες ανίχνευσης
  - Σύγκριση των στοιχείων που συλλέγονται με συγκεκριμένες "υπογραφές" (signatures) γνωστών περιστατικών ασφαλείας (**Misuse Detection**)
  - Στατιστική ανάλυση κάποιων παραμέτρων ώστε να αναγνωριστεί η απόκλιση από τις συνηθισμένες τιμές τους (**Anomaly Detection**)

ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (2/4)
Το IDS Snort

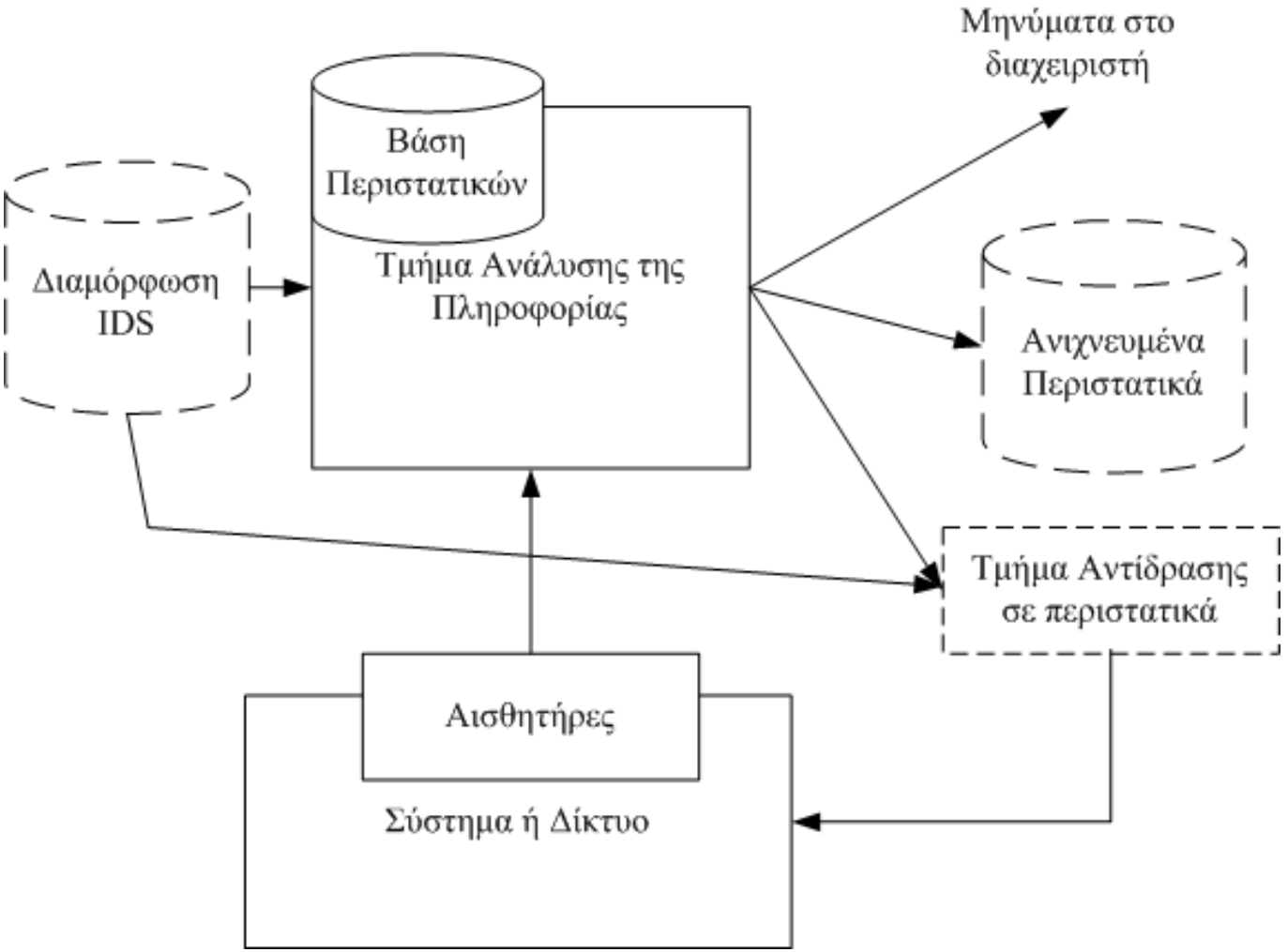
- **Snort**: Σύστημα **NIDS** (Network Intrusion Detection System) & **NIPS** (Network Intrusion Prevention System) που παρακολουθεί την κίνηση στο δίκτυο αναζητώντας υπογραφές γνωστών επιθέσεων στα πακέτα που παρακολουθεί.
  - Εγκατάσταση σε σημείο απ' όπου διέρχεται η κίνηση του δικτύου
  - Οι υπογραφές περιγράφονται με κανόνες που εισάγονται στο σύστημα
- Σύστημα ανοιχτού κώδικα (Open Source Project)
- Υποστήριξη επεκτάσεων (plugins) για πρόσθετη λειτουργικότητα

Παράδειγμα κανόνα **alert** σε προσπάθεια παράνομης εκτέλεσης εντολών με **cmd.exe** στον εξυπηρετητή WEB-IIS:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-IIS cmd.exe access"; flow:to_server,established;
uricontent:"cmd.exe"; classtype:web-application-attack;)
```

ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (3/4)

Βασική Αρχιτεκτονική IDS



ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (4/4)

Παράμετροι Αποτίμησης Ποιότητας IDS

ΟΡΙΣΜΟΙ

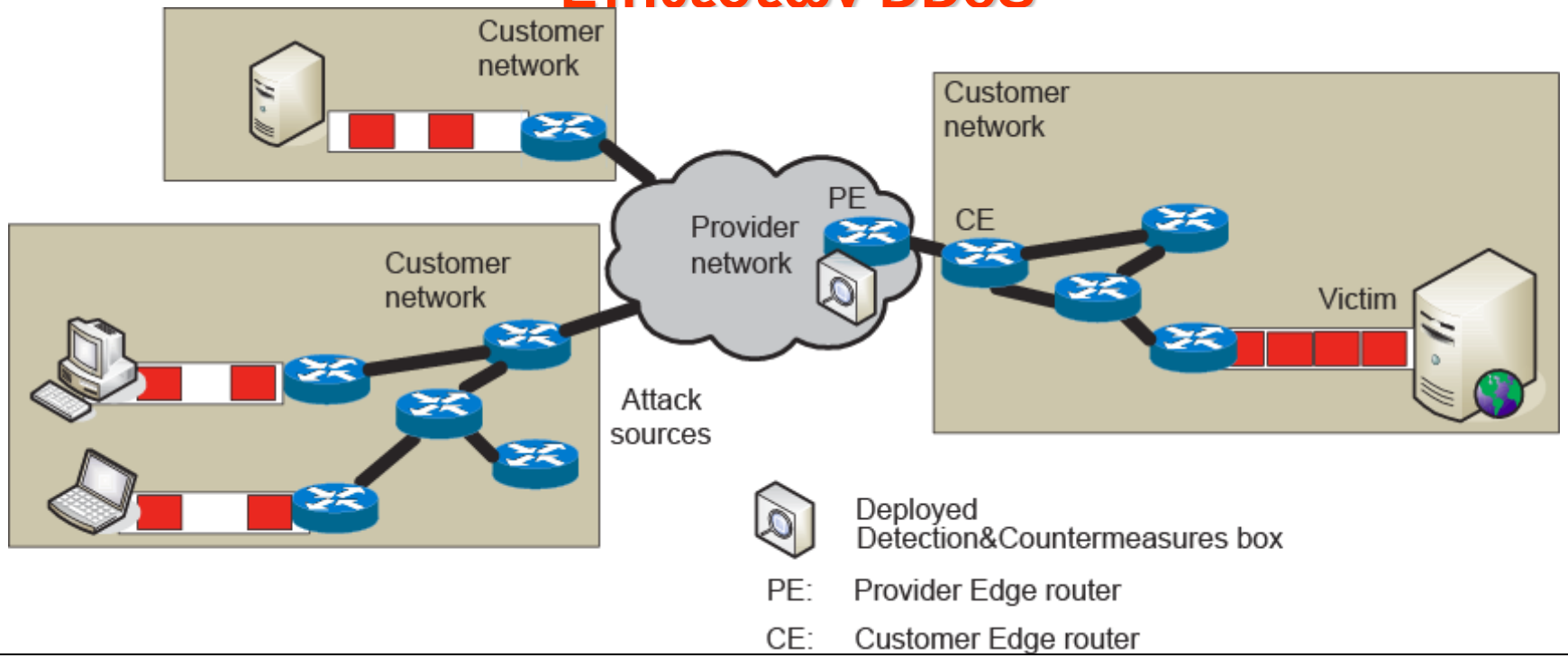
- **P-Positives: Επιθέσεις**
- **N-Negatives: Κανονική λειτουργία**
- **TP- True Positives: Ορθώς διαγνωσμένες επιθέσεις**
- **TN-True Negatives: Ορθώς μη διαγνωσμένες επιθέσεις**
- **FP-False Positives: Λανθασμένες διαγνώσεις επιθέσεων (*false alarms*)**
- **FN-False Negatives: Επιθέσεις που δεν διαγνώστηκαν**

ΠΑΡΑΜΕΤΡΟΙ ΑΠΟΤΙΜΗΣΗΣ IDS

- **Ευαισθησία: TP/P** (συχνότητα ορθών διαγνώσεων επιθέσεων)
- **Ακρίβεια: TN/N** (συχνότητα ορθώς μη διαγνωσμένων επιθέσεων)
- **Απόδοση:** Ταχύτητα συλλογής στοιχείων και επεξεργασίας αναφορών. Ειδικά σε περιπτώσεις όπου υπάρχει μεγάλη ροή πληροφορίας (π.χ. συστήματα NIDS που παρακολουθούν δικτυακές συνδέσεις υψηλής ταχύτητας)
- **Αντοχή σε επιθέσεις** προς το ίδιο το σύστημα IDS
- **Ταχύτητα κατάληξης σε συμπεράσματα,** ενεργοποίηση αντίμετρων πολιτικών μετριασμού (mitigation policy) σε επιθέσεις (π.χ. firewall rules, incident reporting σε ομάδες CSIRT - Computer Security Incident Response Teams)

ΕΙΔΙΚΑ ΘΕΜΑΤΑ:

Ανίχνευση (Identification) & Αντιμετώπιση (Mitigation) Επιθέσεων DDoS



ΤΑΞΙΝΟΜΗΣΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ (Feature Classification) ΕΠΙΘΕΣΕΩΝ

- Εκτίμηση Στατιστικών ιδιοτήτων δικτυακής κίνησης (**traffic datasets** από μηχανισμούς **network traffic monitoring**)
- Ανάγκη αποθήκευσης και ευρείας διαθεσιμότητας **traffic datasets** (ομαλής κίνησης - **benign traces** & περιστατικών επιθέσεων - **attack traces**), ζητήματα privacy/confidentiality, πολιτικές scrabbing (in-house ή outsourced σε παρόχους)
- Μέθοδοι ανίχνευσης ανωμαλιών (outliers): Από radar detectors (1950) σε σύγχρονους αλγορίθμους **Machine Learning**

ΕΙΔΙΚΑ ΘΕΜΑΤΑ:

Παρακολούθηση (Monitoring) Δικτυακής Κίνησης

➢ **Εναλλακτικοί τρόποι Monitoring**

– **SNMP *MIB*** Counters → ***MRTG*** Graphs μέσω αποθήκευσης σε ***RRD*** (round-robin databases)

– **NetFlow**: Καταγραφή μετρητών ροών (packet flows) σε ***Layer 3 Routers*** (π.χ. αριθμός πακέτων ή bytes ανά ροή) από ***packet headers***. Οι ροές ορίζονται για εύλογο χρονικό διάστημα βάσει 5 παραμέτρων:

- 1: Πρωτόκολλο
- 2-3: Διευθύνσεις IP
- 4-5: TCP/UDP ports
- Καταχώρηση σε μετρητές αυξανόμενους ανά πακέτο ή ***δειγματοληπτικά*** (1/100, 1/1000) για ζεύξεις υψηλών ταχυτήτων. Ανά διαστήματα οι μετρητές προωθούνται σε εξωτερικούς servers (***Collectors***) για αποθήκευση και στατιστική επεξεργασία

– **sFlow**: ***Δειγματοληψία*** (sampling) καταγραφής πακέτων (των αρχικών bytes τους, ***headers+***) σε ***Layer 2 Switches*** με ***sFlow agents*** και επεξεργασία μέσω ***sFlow Collectors***

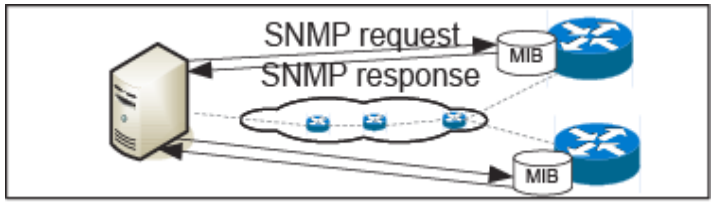
– **OpenFlow (OF)**: OF Table Counters → Controllers

– **Packet Capturing:** Αντιγραφή κίνησης ζεύξεων μεταξύ routers/switches (***Port Mirroring, Passive split***), δυνατότητα πλήρους καταγραφής πακέτων ***headers*** + ***payload, Deep Packet Inspection (DPI)***

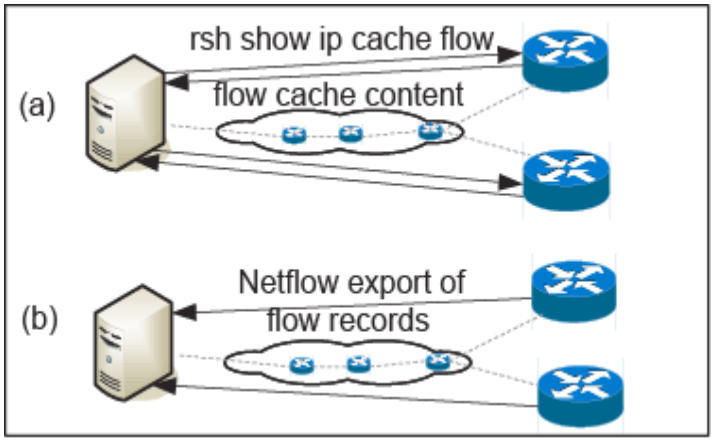
– **Inband Network Telemetry (INT): Μετρήσεις στο *Data Plane* χωρίς μεσολάβηση *Control Plane*, *DPI*, *P4*…**

➢ **Διάφοροι περιορισμοί**: Δυσκολία χρήσης, χρονική ακρίβεια, ακρίβεια μέτρησης, απαιτούμενοι πόροι (υπολογιστική ισχύς, μνήμη, ταχύτητα καταγραφής)

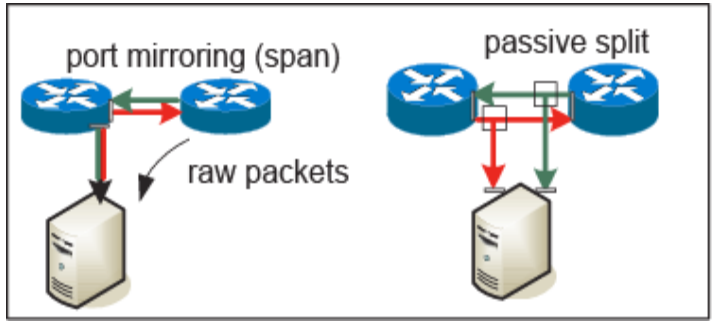
Μέσω SNMP MIB Counters



Μέσω NetFlow



Μέσω Packet Capturing



ΕΙΔΙΚΑ ΘΕΜΑΤΑ:

Ανίχνευση Επίθεσης TCP SYN

Τα μετρικά bps, pps δεν είναι πάντα αποτελεσματικά χαρακτηριστικά (features)

Για ανίχνευση TCP SYN Attack, το πλήθος flows από SYN flags δεν αποκαλύπτει ύποπτες ασυμμετρίες στο TCP (περίπου συμμετρικό σε κανονικές συνθήκες λειτουργίας)

Καλό μετρικό είναι SFR (Syn Fin Ratio) (μέτρηση με **packet capture**):

$$\frac{\text{εξερχομενα } SYN \text{ } packets/sec}{\text{εισερχομενα } FIN \text{ } packets/sec}$$