Network Security

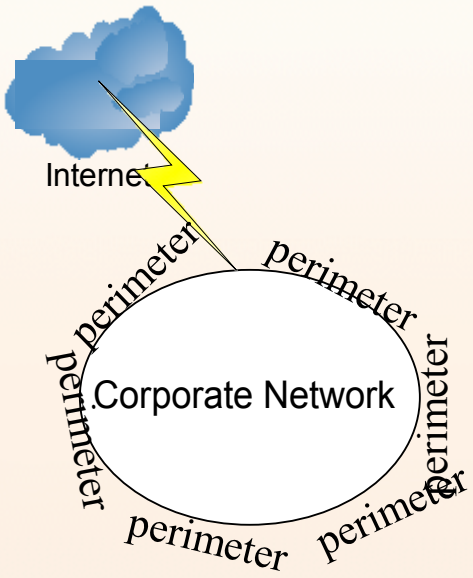
What is (not) Network Security

John Iliadis
Network Security Administrator
TEIRESIAS S.A.

Network Perimeter

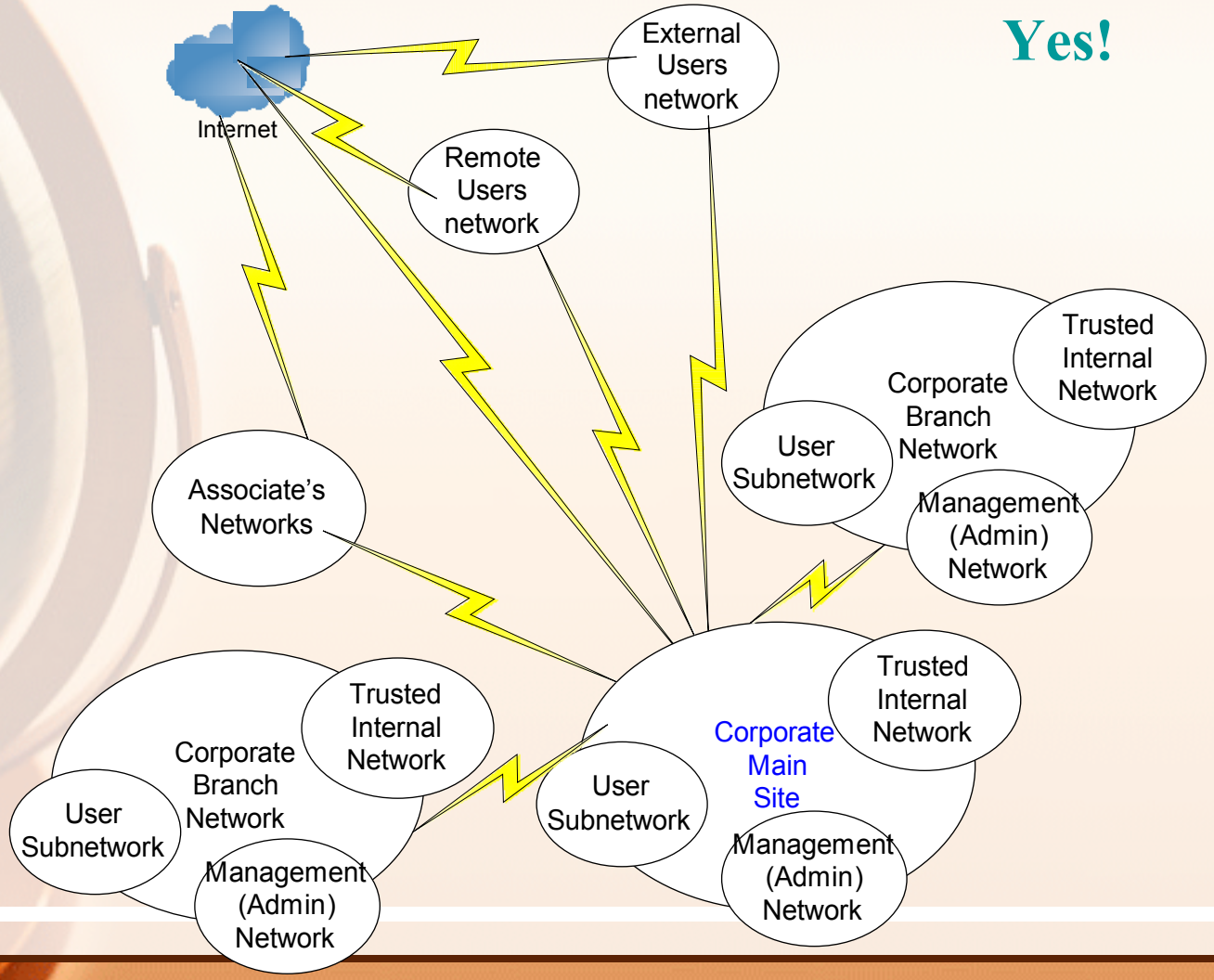
- *It is vital to guard our network perimeter, meaning…*
  - Access Control (in/out the perimeter borders)
  - Confidentiality and integrity protection of information crossing network perimeters
  - etc…
- Where is the network perimeter?

What is (not) a network and its perimeter



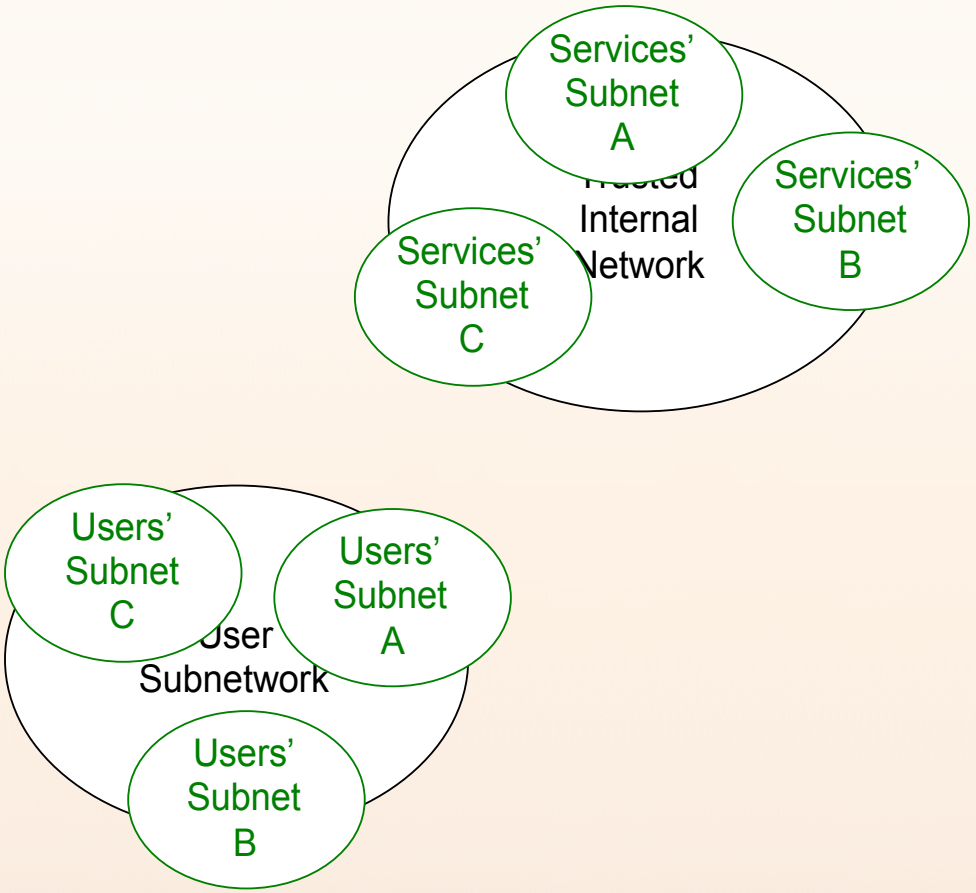
No!

What is a network and its perimeter (1)



Yes!

What is a network and its perimeter (2)



Some threats

- **Lack of availability**
- **Breach of confidentiality**
- **Unauthorised access**

Lack/degradation of availability – 10 Countermeasures

- Good network planning
- Good network planning
- Good network planning
- Good network planning
- Good network planning

- Quality of Service
- Quality of Service
- Quality of Service
- Quality of Service
- Quality of Service

Good network planning (1)

- Identify and document your network's perimeter
- Subnet wisely
  - Meaningful subnets
  - Route summarisations
  - Documentation
  - Availability of address space per subnet
- Evaluate criticality of lines, based on business needs
  - Specific services' unavailability
  - User dissatisfaction
  - Loss of income
  - *Network security* (e.g. unavailability of security updates)

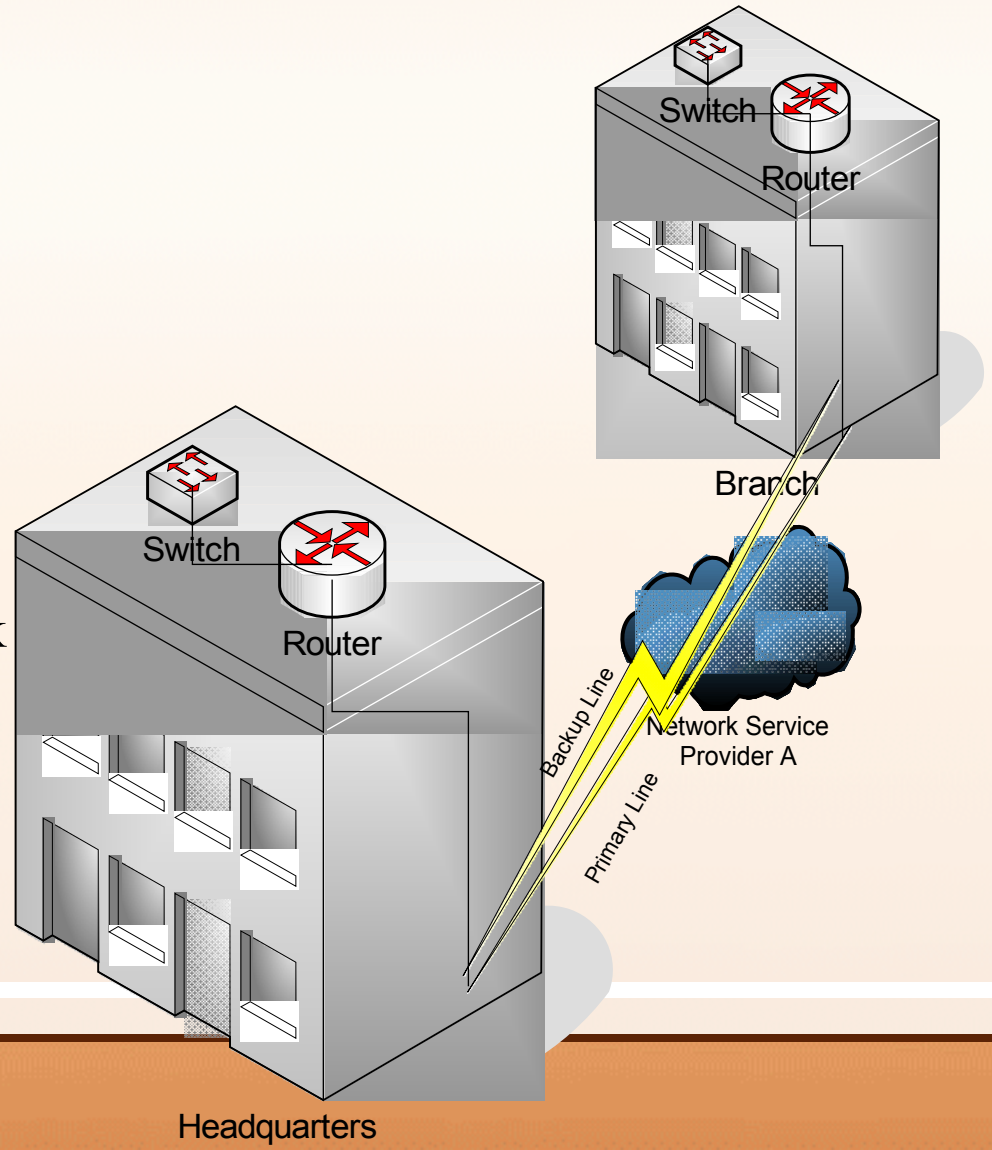
Good network planning (2)

- Redundant links
  - Auto/Manual
  - Bandwidth of redundant link depending on SLAs, estimated primary line downtime, cost
  - Avoid Single Points of Failure (both primary and redundant link(s) going down)

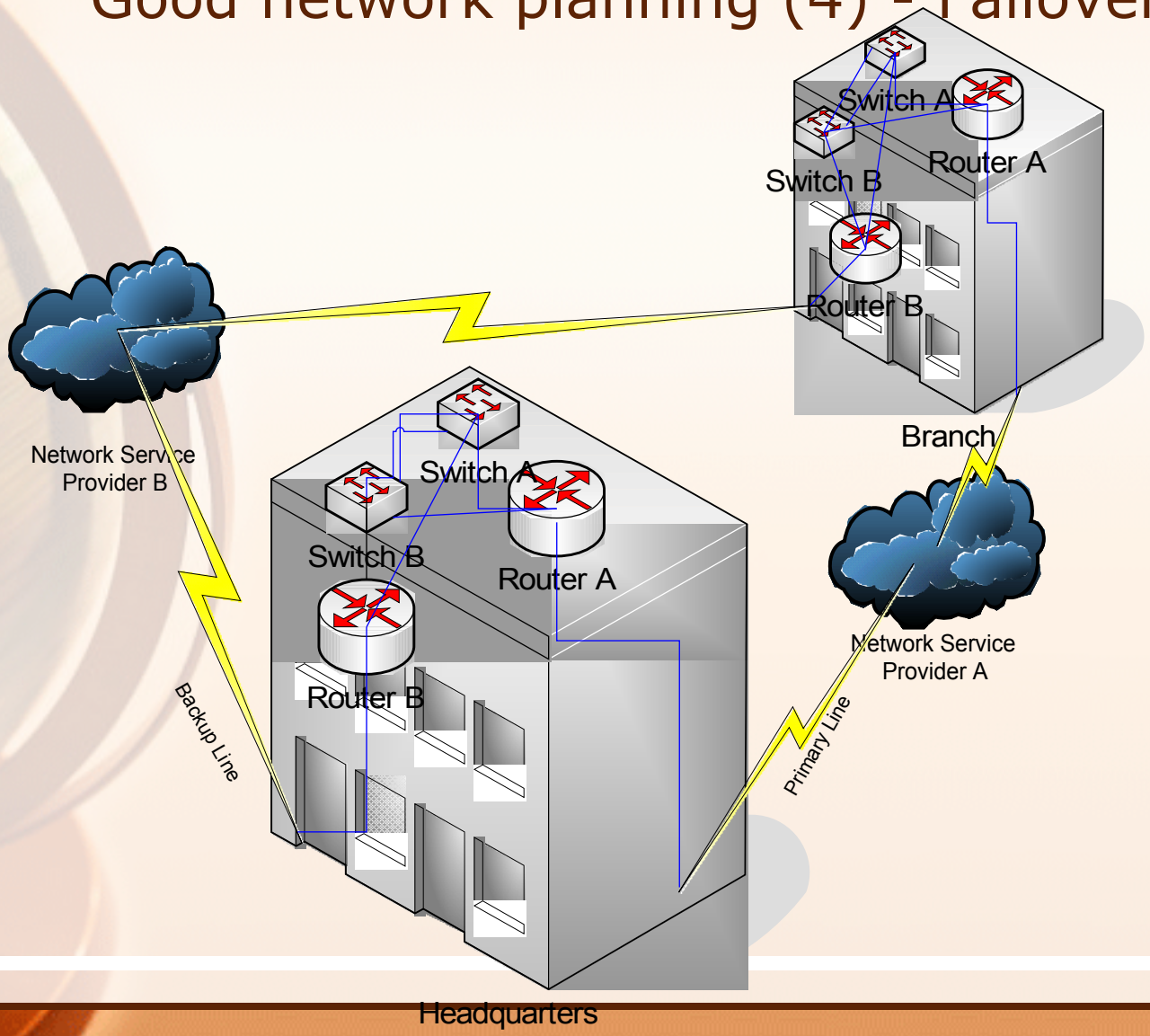
Good network planning (3) - Failover

Single Points of Failure:

3. Switches
4. Routers
5. Internal building cabling
6. External building cabling (e.g. construction work around the building)
7. Network Service Provider's network



Good network planning (4) - Failover



Quality of Service (1)

All services are born equal.
Some are more equal than others

- The need for QoS
  - Expected user experience (SLA or not)
  - Business traffic versus leisure traffic
  - Just won't work without it (e.g. VoIP, some network management traffic)
  - Protect against malicious attempts (DoS, DDoS)

Quality of Service (2)

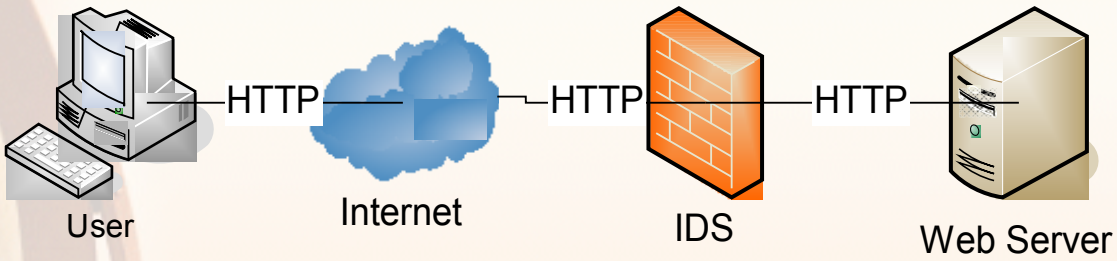
- QoS – How To
  - Limit bandwidth
  - Limit packet rate
  - Guarantee bandwidth
  - Guarantee packet rate
  - Burst rates
  - Absolute values, fractions of total capacity, fractions of remaining capacity
  - Best Effort: children of a lesser God
  - Limitations imposed upon notification from IDS/IPS (fight DoS, DDoS)
  - more…

Breach of confidentiality (privacy?) - Countermeasures

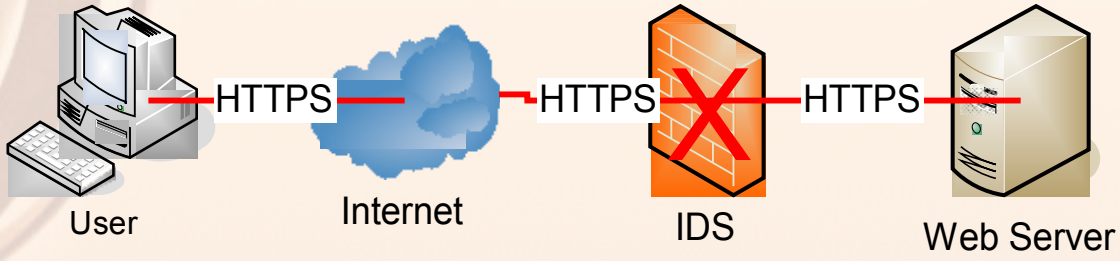
- Encryption
  - SSL
  - IPsec
  - SSH tunnels
  - WEP?
  - Others…

SSL – wrong implementations

Before

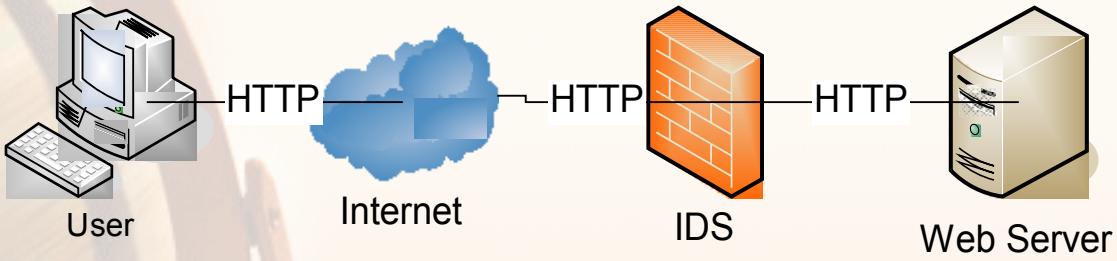


After

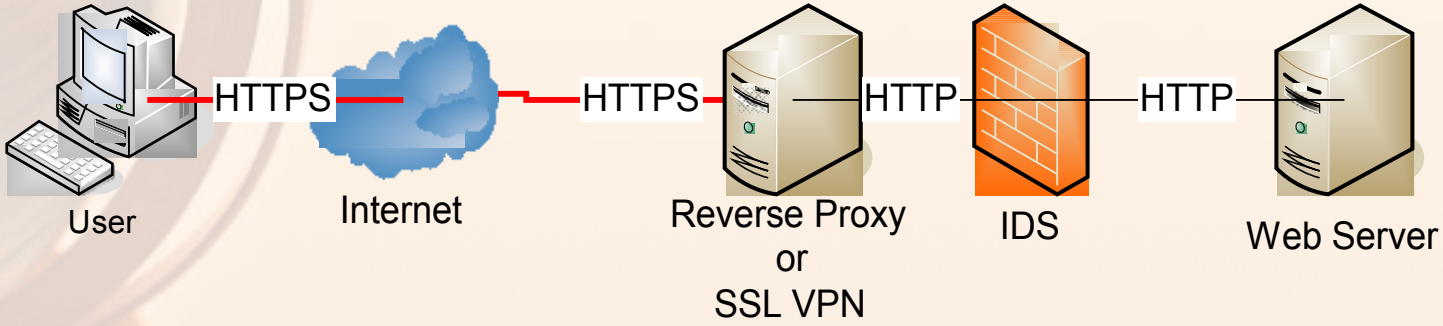


SSL – the proper way*

Before



After



reduced privacy…

IPsec – what is it not about

- Not about “securing communications”
- Not about “protecting confidentiality”
- Not about “preventing unauthorised access”

…then what?

IPsec – what is it about

- It is about cryptography, and cryptography is about shifting the domain of a problem, i.e.
  - Problem: "Protect confidentiality of communication"
  - Solution: "Shift the problem's domain from *confidentiality protection* to *key management*"

Key Management – Symmetric Crypto

- Problem's domain remains *confidentiality protection*, but

2. Data to be protected (keys) are less

4. Frequency of data to be protected (keys) is lower

6. Data to be protected (keys) can be communicated out of band (more) easily

Key Management – Asymmetric Crypto

- Problem's domain changes to key material's integrity protection
- Key material can (more) easily be communicated out of band
- Existing structures (e.g. PKI hierarchies, PGP web of trust, etc) to facilitate integrity protection, once the infrastructures have been jumpstarted

WEP: Wireless Encryption Protocol (aka Where Everything is Permitted)

-"Good morning sir, we have a nice ADSL offering for you today. It is cheap and we can install it right away"

-"No, thanks. A company near my house is running WEP encryption for its 802.11 wireless network and they have a 20Mbps leased line to the Internet"

note1: if it's broken, it's broken

note2: for wireless networks, VPN over your WEP/WPA

Unauthorised Access - Countermeasures

- Before the fact
  - Strong authentication (e.g. two factor)
  - Isolation of services
  - Separation of duties
  - Eliminate covert channels
- After the fact
  - Audit
  - Audit more…
  - Audit: the proper way to do it, if it were not for privacy

Strong Authentication

- What you know
  - Password
  - Passphrase
- What you have
  - Certificate on computer
  - Certificate on token (smart card, USB device)
  - Pseudorandom Number Generator device (time sync issues)

Isolation of Services

- IPsec: Separate keying material per user groups and services they are authorised to access
- Subnets and packet filtering (firewalling)
- VLANs
- Few (one?) service per host
- Shutting down not required services on hosts

note: contrary to popular belief, virtual machines may not be the way to go

Separation of duties

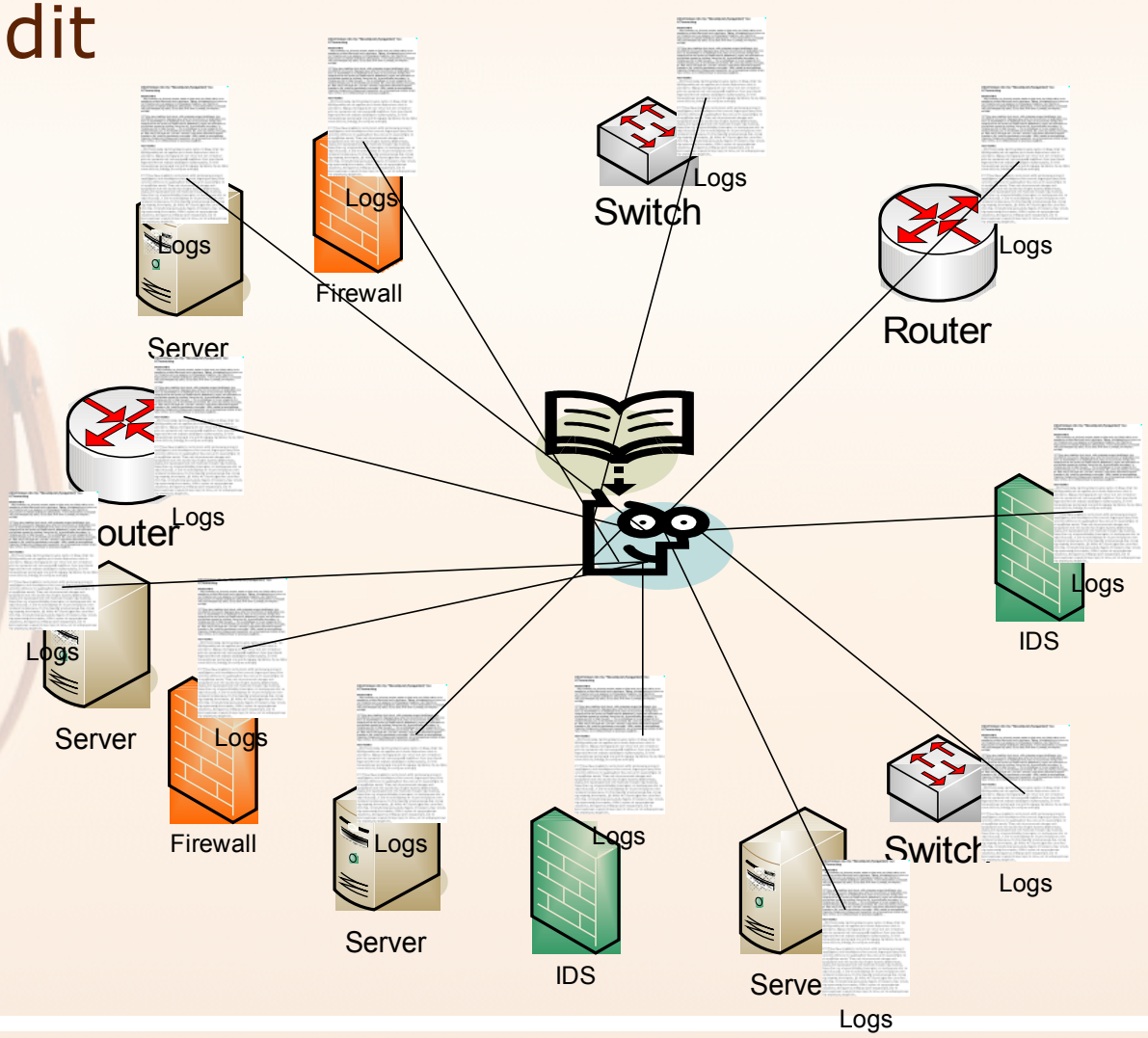
- System Administrators
- Network Administrators
- System Security Administrators
- Network Security Administrators
- Auditors
- Risk Analysts
- Security Officers

Eliminate covert channels

- Well known ones
  - Port knocking
  - Tunneling (e.g. running another IP layer over an Application layer)
  - Steganographic
- Hard to detect
- Solutions:
  - Port knocking: allow only specific ports, limit packet rate
  - Tunneling: inspect application layer contents for syntax/format violations
  - Steganography: steganalysis, steganographic sanitisation

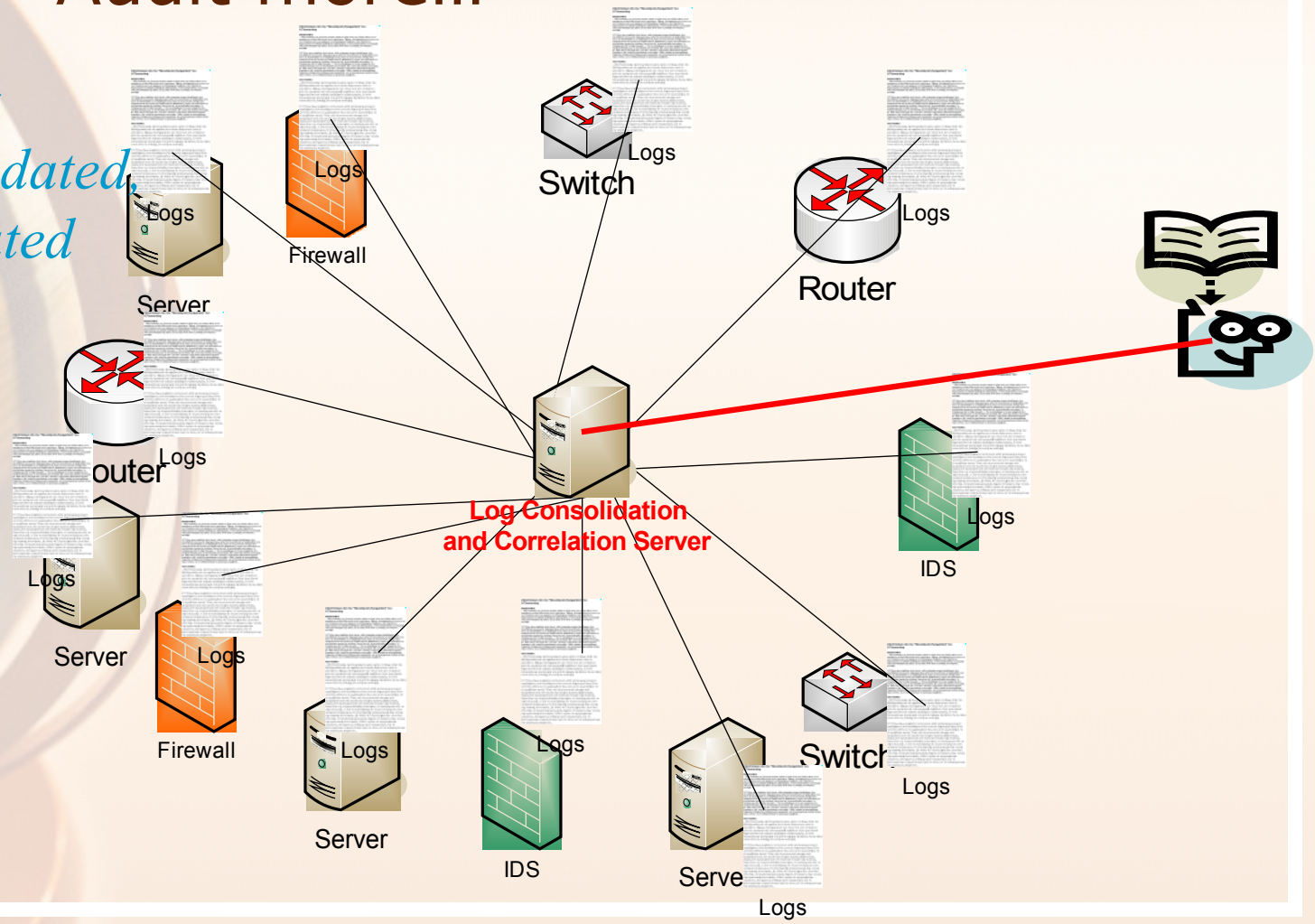
Audit

Inspecting log files



Audit more…

Inspect consolidated, correlated logs and alerts



Audit properly (privacy issues…)

Inspect consolidated, correlated logs, alerts and captured traffic possibly related to the alerts