

# Security to schools

## 2nd School Networking Workshop





# Agenda

- ▶ Brief introduction
- ▶ Internet access and services
- ▶ cert.pt
- ▶ Conclusions



# Brief introduction

3

- ▶ FCCN runs and operates Portuguese NREN, TLD .pt and Portuguese IX
- ▶ Ministry of Education and FCCN firmed a contract for 2<sup>o</sup> and 3<sup>o</sup> levels elementary and secondary schools (1200)
- ▶ Ministry of Science and Technology firmed a contract for 1<sup>o</sup> level elementary schools (7400)

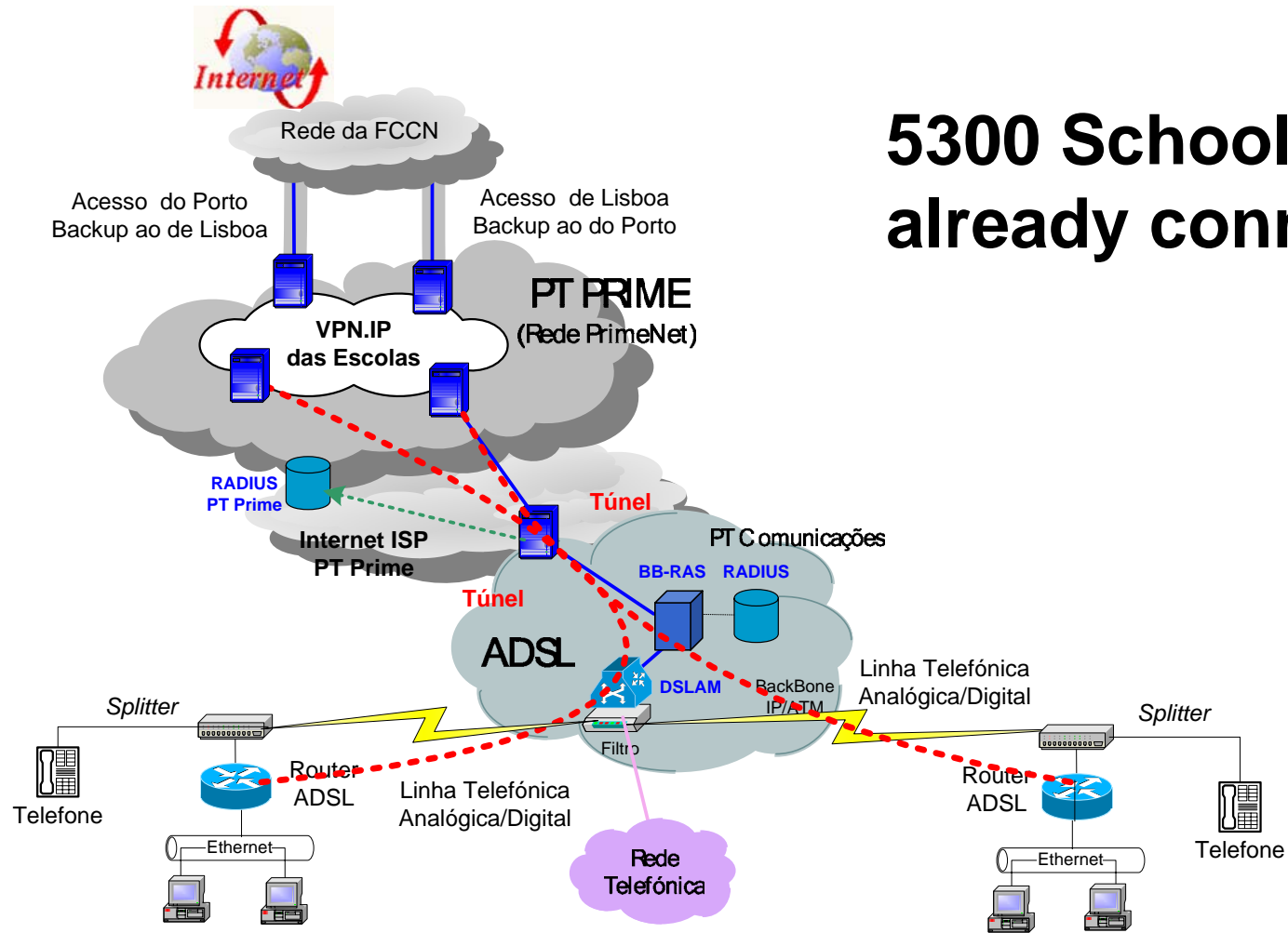
# Brief introduction

4

- ▶ Internet access
  - All schools connected via ISDN (1997-2001)
  - Broadband deployment (2004-2005)
- ▶ Router management
- ▶ Internet services
  - PoP (15) located services (1997)
  - Centralized platform (2000)
  - 2nd generation centralized platform (2006)
- ▶ User support (1st and 2nd lines)
- ▶ Security services

# Internet broadband access

5



**5300 Schools  
already connected**

# Internet services

6

- ▶ Centralized cluster (linux based)
  - Two layer infrastructure (front-end, backend)
  - Perimeter security using IPTables and SNORT
- ▶ Messaging services
  - Building-block including SMTPAUTH (DQD), POP3, anti-virus (clamAV), anti-spam (assassin) and SPF
  - Webmail
  - Listserv
- ▶ Web-hosting
- ▶ Self-service Web
  - Content filtering, Web proxying, password management, ...
  - Access router configuration (LAN settings, PAT, firewalling, IDS, ...)

- ▶ Offering technical support to computer users in resolving security incidents, advising on best-practices, analysing artefacts, and coordinating actions with the parties involved.
- ▶ Gather and disseminate a set of information about vulnerabilities and recommendations, pertaining to potential security risks and ongoing malicious activities

- ▶ Gather from accredited sources information related to security vulnerabilities, and act on the community with the goal of minimizing impact at the National level
- ▶ Promote the creation of new CERT/CSIRTs in Portugal, and raise awareness of security issues on computer users.



# cert.pt - constituency

9

- ▶ cert.pt constituency is the Portuguese National Educational and Research Network's user community
- ▶ RFC2350
- ▶ RIPE IRT object
- ▶ TI accredited team



# cert.pt - authority

10

- ▶ Comes out from the network AUP
- ▶ Minor severity procedure
  - Contact school
  - 24h later verify activity
  - Cut access if no procedure as been taken
- ▶ Major severity procedure
  - First cut then ask questions

# Incident handling

11

- ▶ There were no reports coming from schools
- ▶ 65% of all reports did comprise schools
- ▶ Incident classification
  - Probes 54%
  - SPAM 36%
  - Malware 7%
  - Copyright violation 3%
- ▶ No intrusion attempts nor root compromise nor DoS attacks



# Conclusions

- ▶ Illicit activity
  - First experiences
  - BotNETs
  - Peer-to-peer copyright violation
- ▶ Lack of experience and security awareness
  - System administrators
  - Teachers
  - Students



# Conclusions

13

- ▶ Foster security awareness
  - Students curricula
  - Training
  - Information for schools within cert.pt
- ▶ Build trust network with system administrators
  - “premium” services (ICT labs)
  - Lightweight security bulletins
- ▶ Cooperation
  - Exchange of information
  - Exchange of content for dissemination



**Thats all folks!**