



# Security @ the EBU

Laurent Patrigot

# Agenda

- Presentation of the EBU network
- EBU security architecture
- Perimeter & inner protections

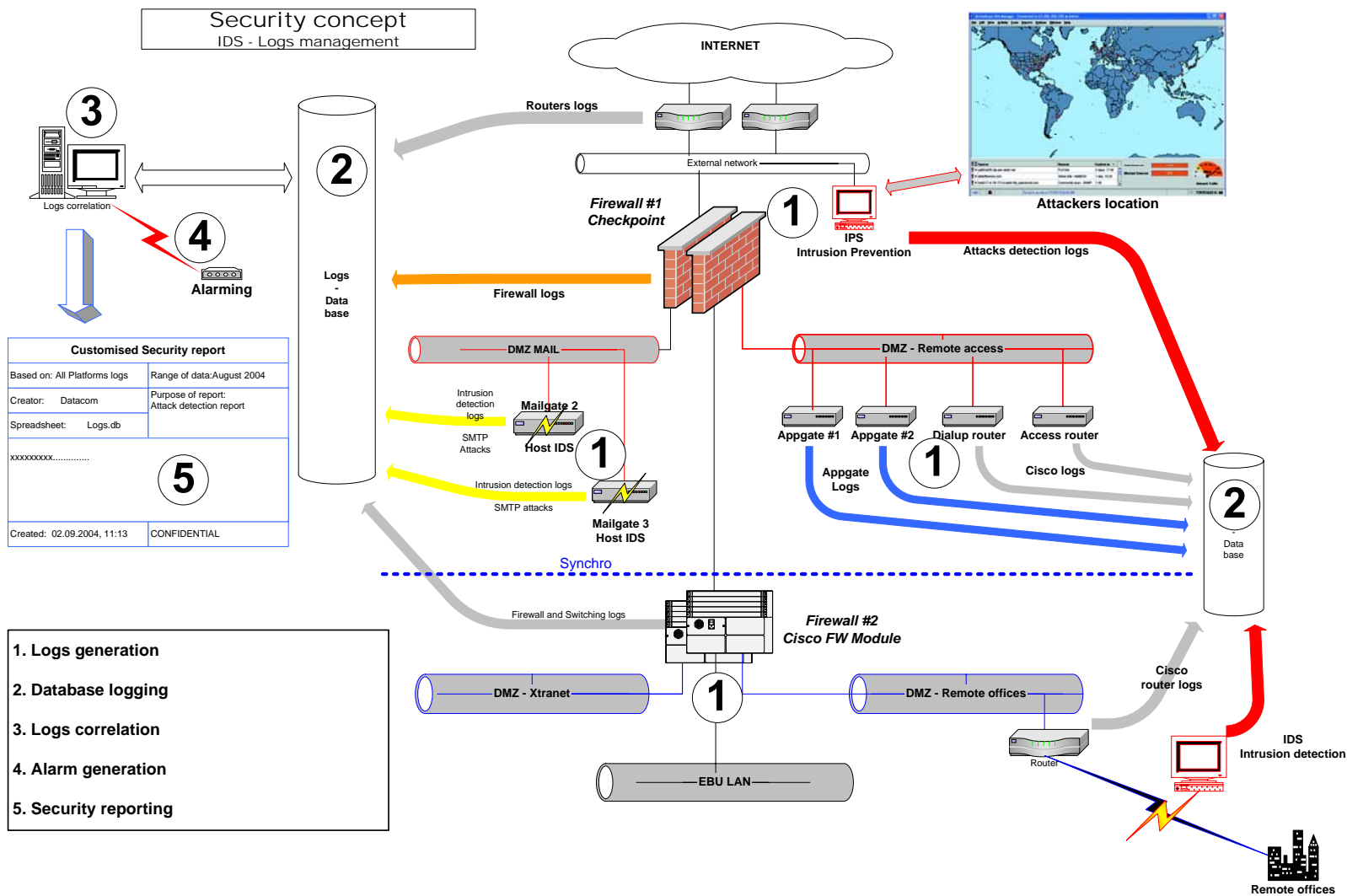
# The EBU network

- Full restructuration in 2004
- Cabling : Cat 6
- Network :
  - Full IP based
  - Layer 3 network
  - 10 Gbs backbone
- Security :
  - Global protection
  - Transparency (as possible)
  - Performance

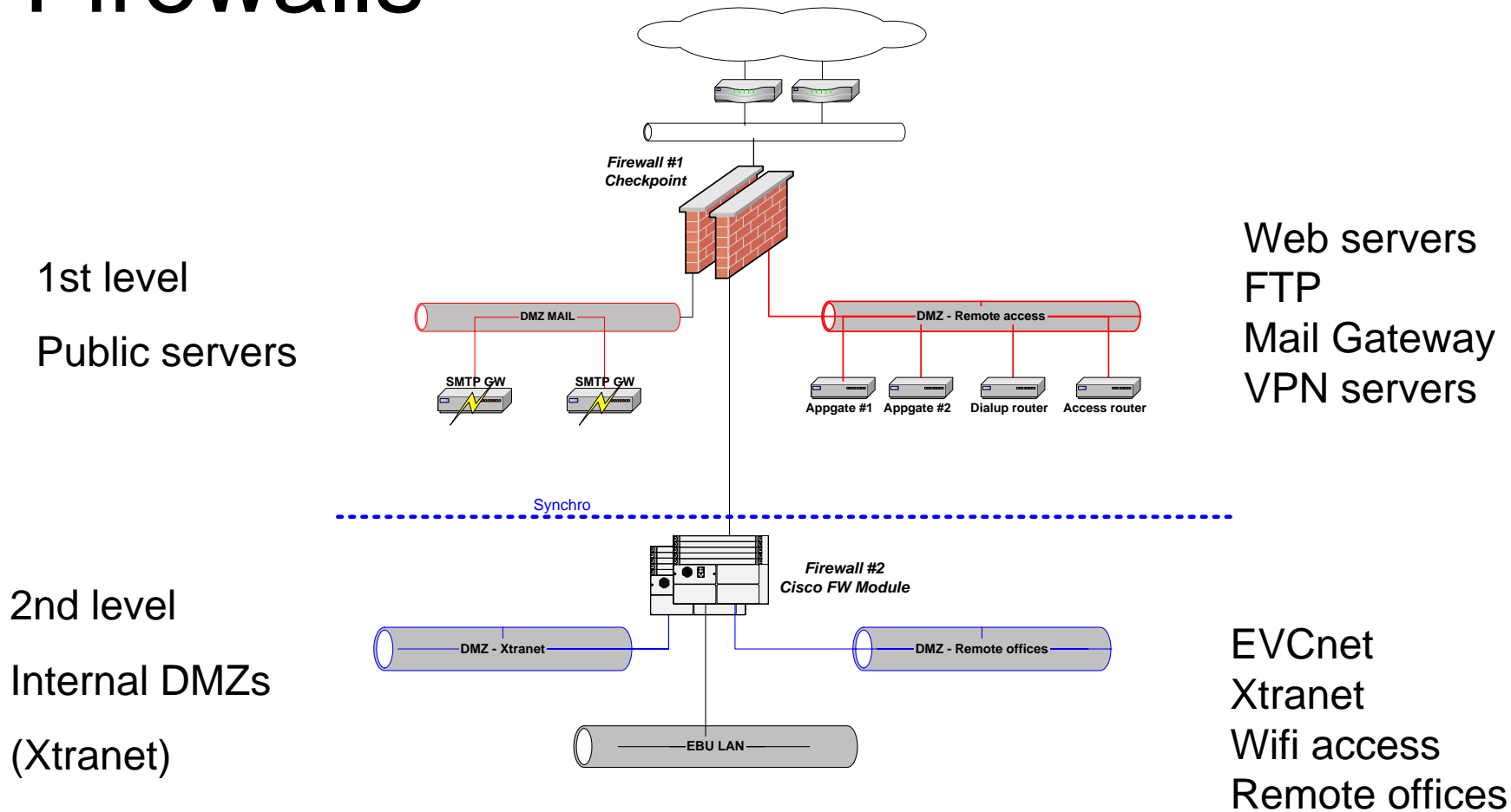
# Security requirements

- Protection of public servers (www...)
- Protection of internal servers
- Protection from internal attacks or viruses
- DMZ specificities (EVCnet, Xtranet...)
- Performance
- Evolutivity

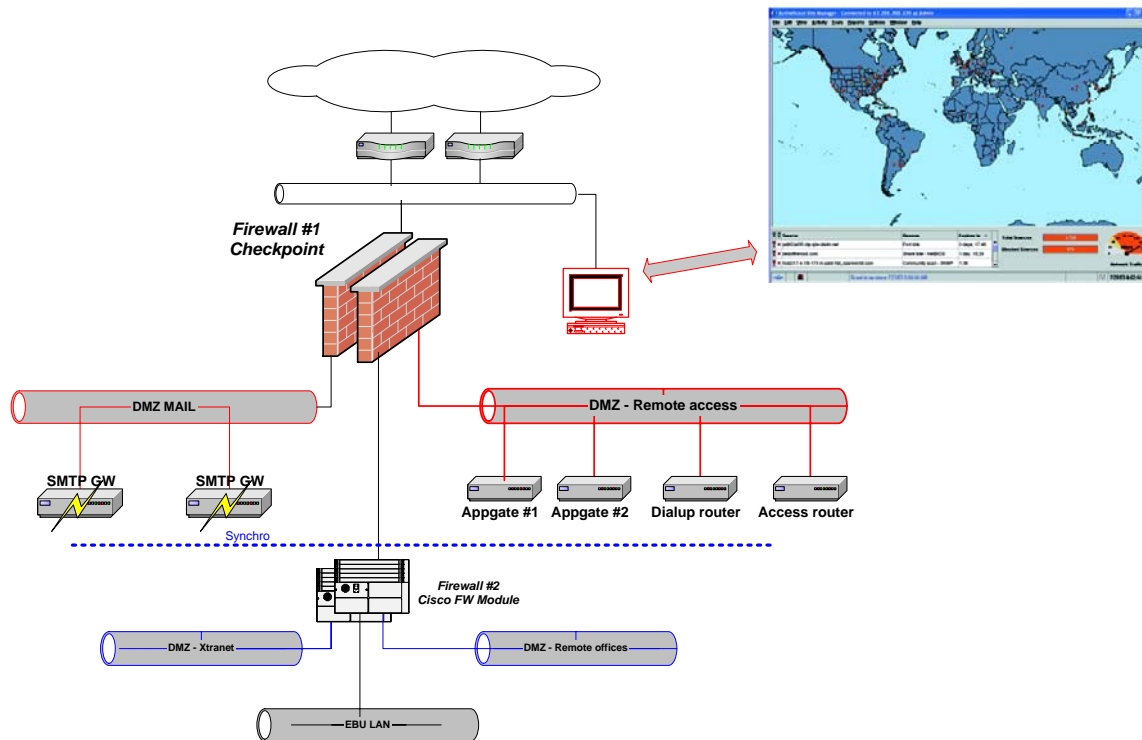
# EBU Global Architecture



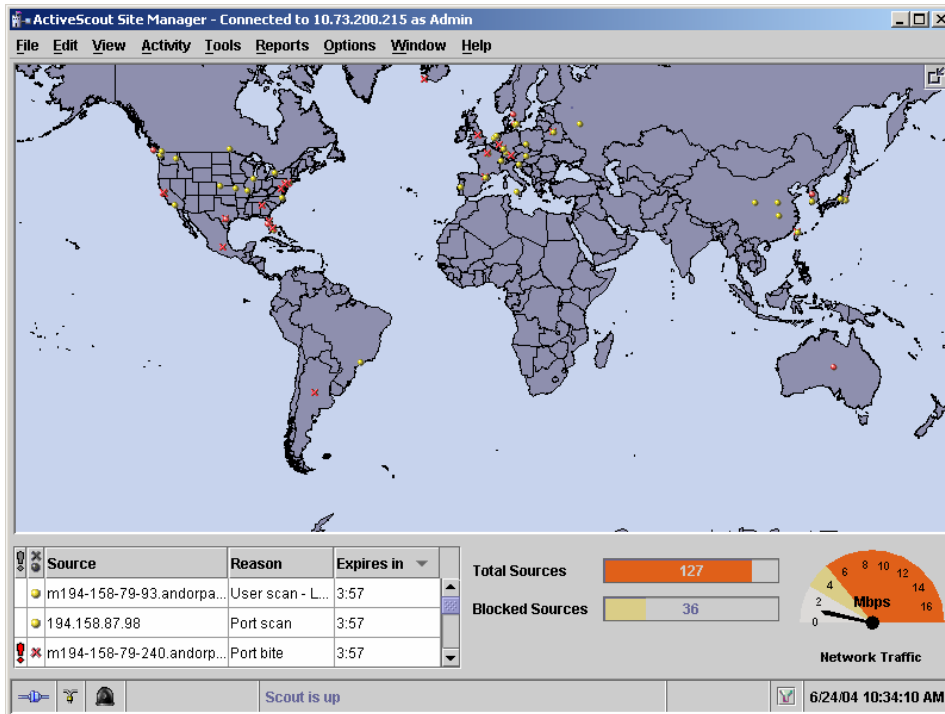
# Firewalls



# IPS Protection



# IPS : Intrusion Prevention System



Front End sensor

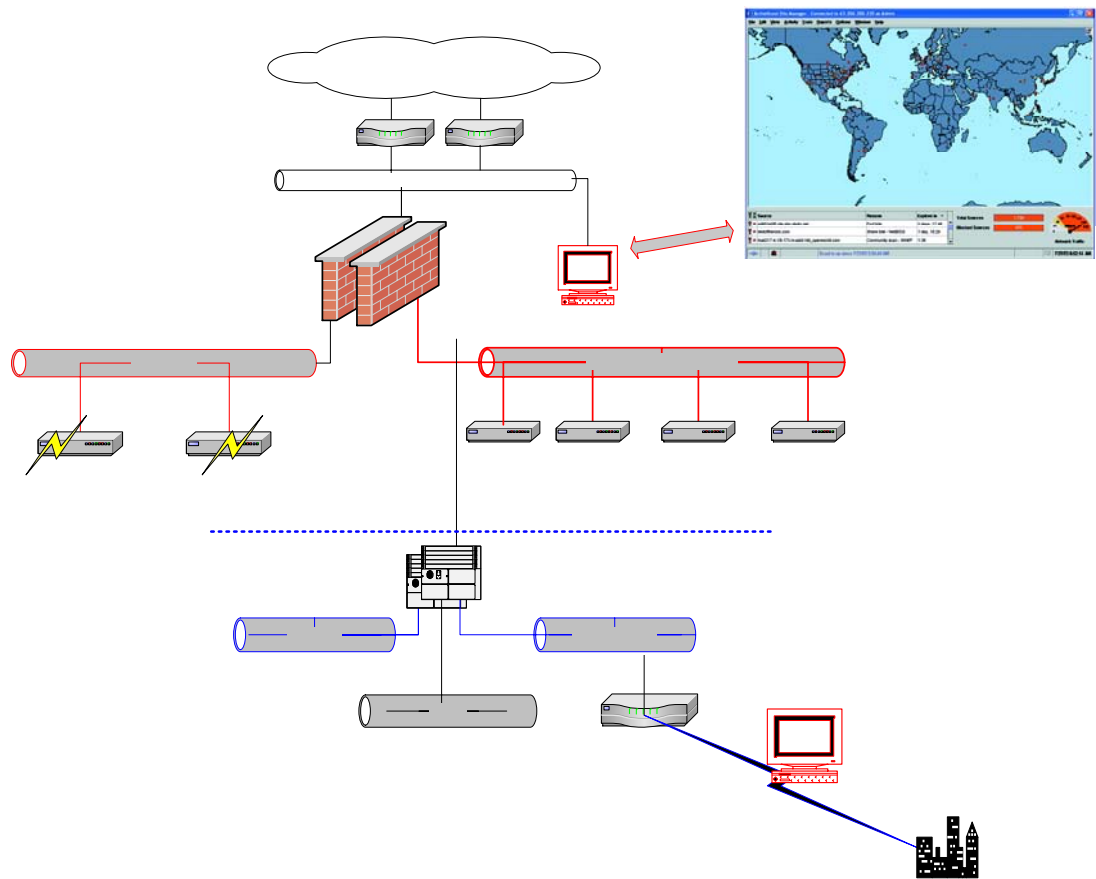
ProActive detection

Based on behaviour not on signatures

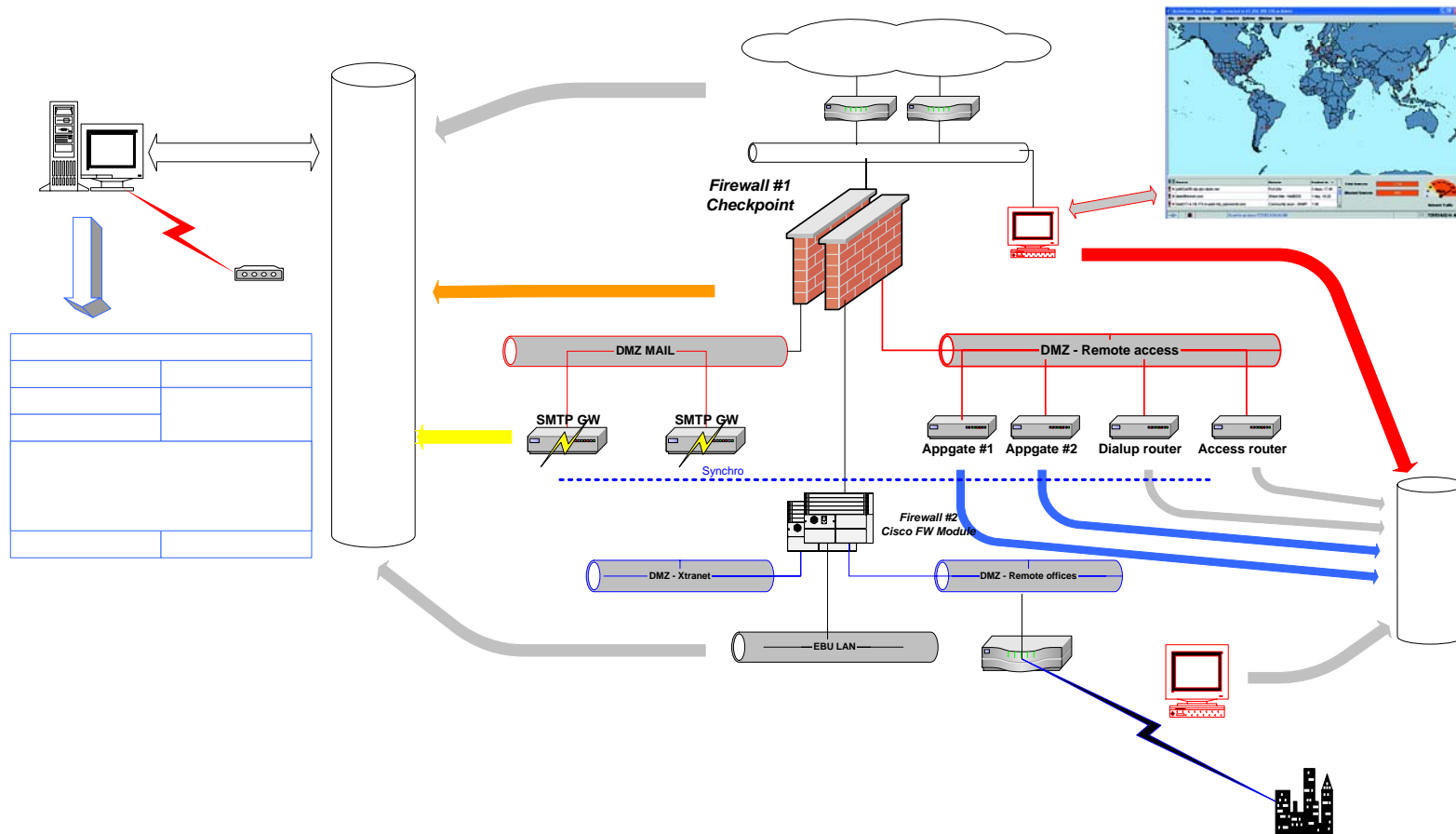
Block IPs before the firewall



# IDS (Intrusion Detection System)



# Logs correlation



# Inner protection

- Antivirus
  - SMTP Gateway (Antispam)
  - Exchange servers
  - Workstation
  - Laptop
- Laptop
  - Personal firewall (centralized management)
- Web contents filtering
  - Virus
  - Mobile codes
- Wifi
  - 802.1x (certificates)
  - NAC (Network access Control)

# Thanks for your attention

## **Questions ?**