



# SYN flood use-case

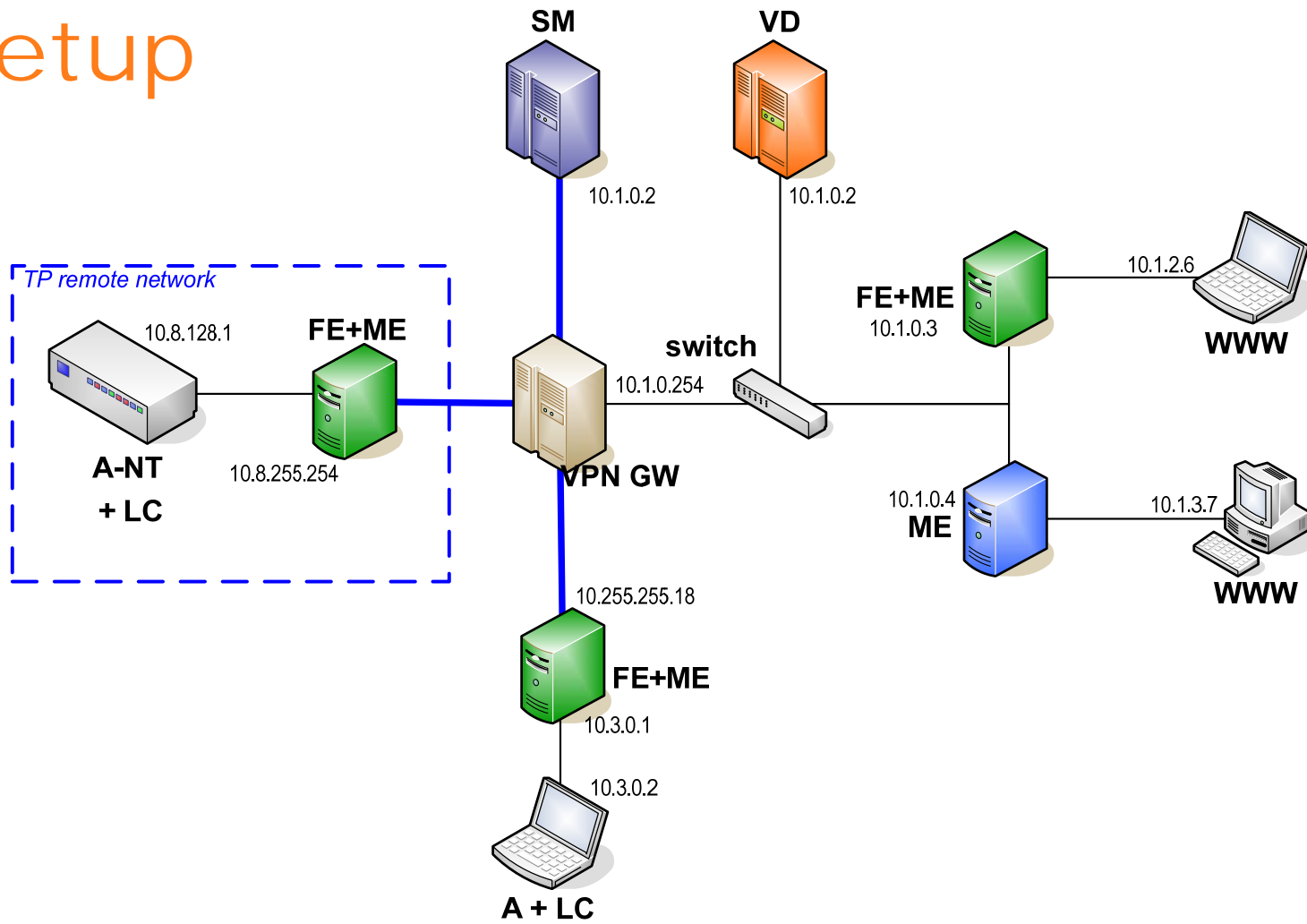
Yannick Carlinet (FT)

# Motivations



- ➔ SYN flood attacks are very common
  - ▶ Inferring Internet Denial-of-Service Activity (2006)
  - ▶ In 3 years: 68,700 attacks, 34,700 distinct targets
- ➔ Attack tools widely available
  - ▶ Trinoo, Tribe Flood Network, TFN2K, Stracheldraht
  - ▶ Ability to manage the agent network
  - ▶ Sophisticated (decoy packets sent to non-target networks, encryption, no communications from agents to master)
- ➔ Can target many services (web, e-mail, authentication,...)

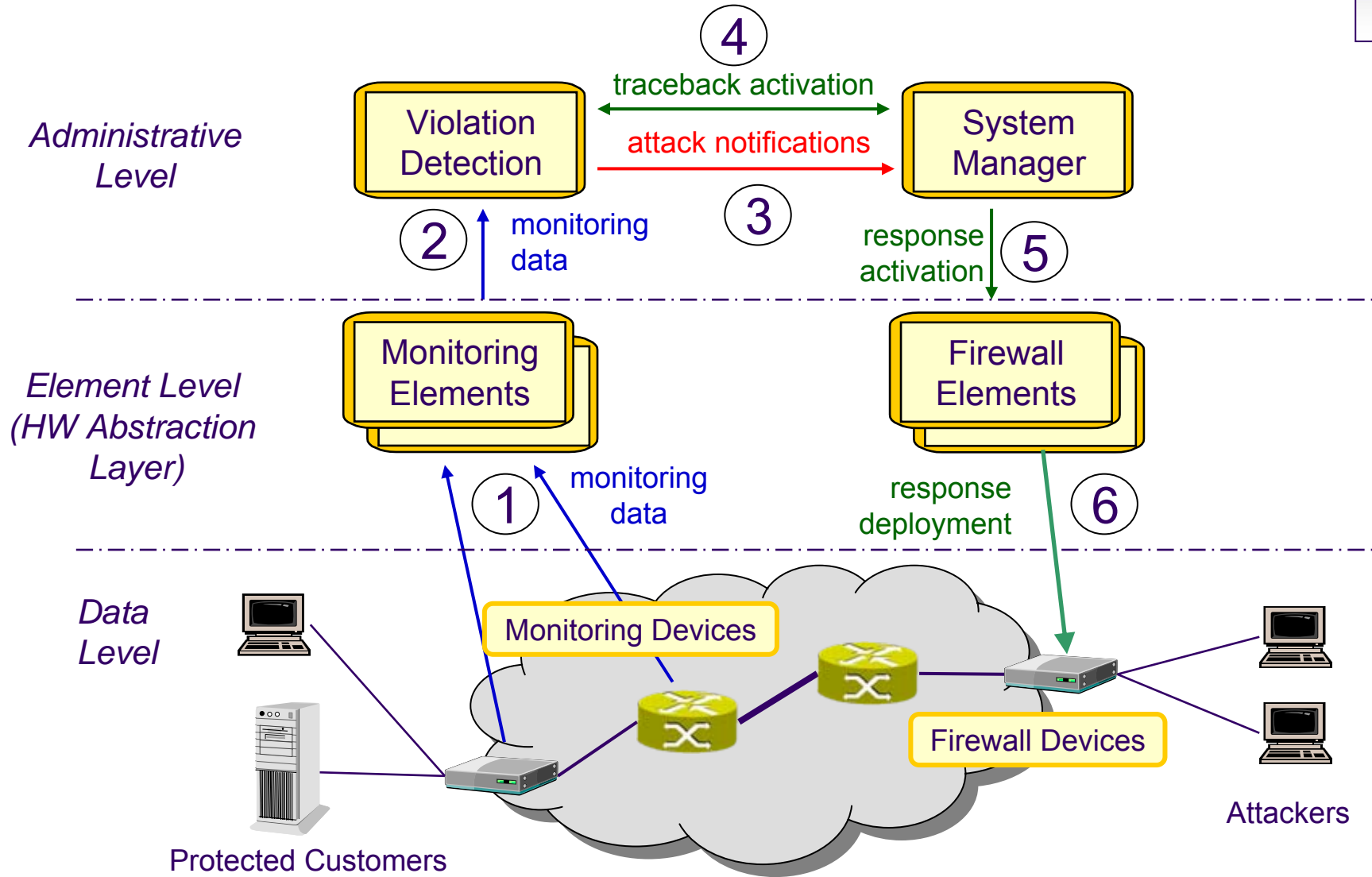
# Setup



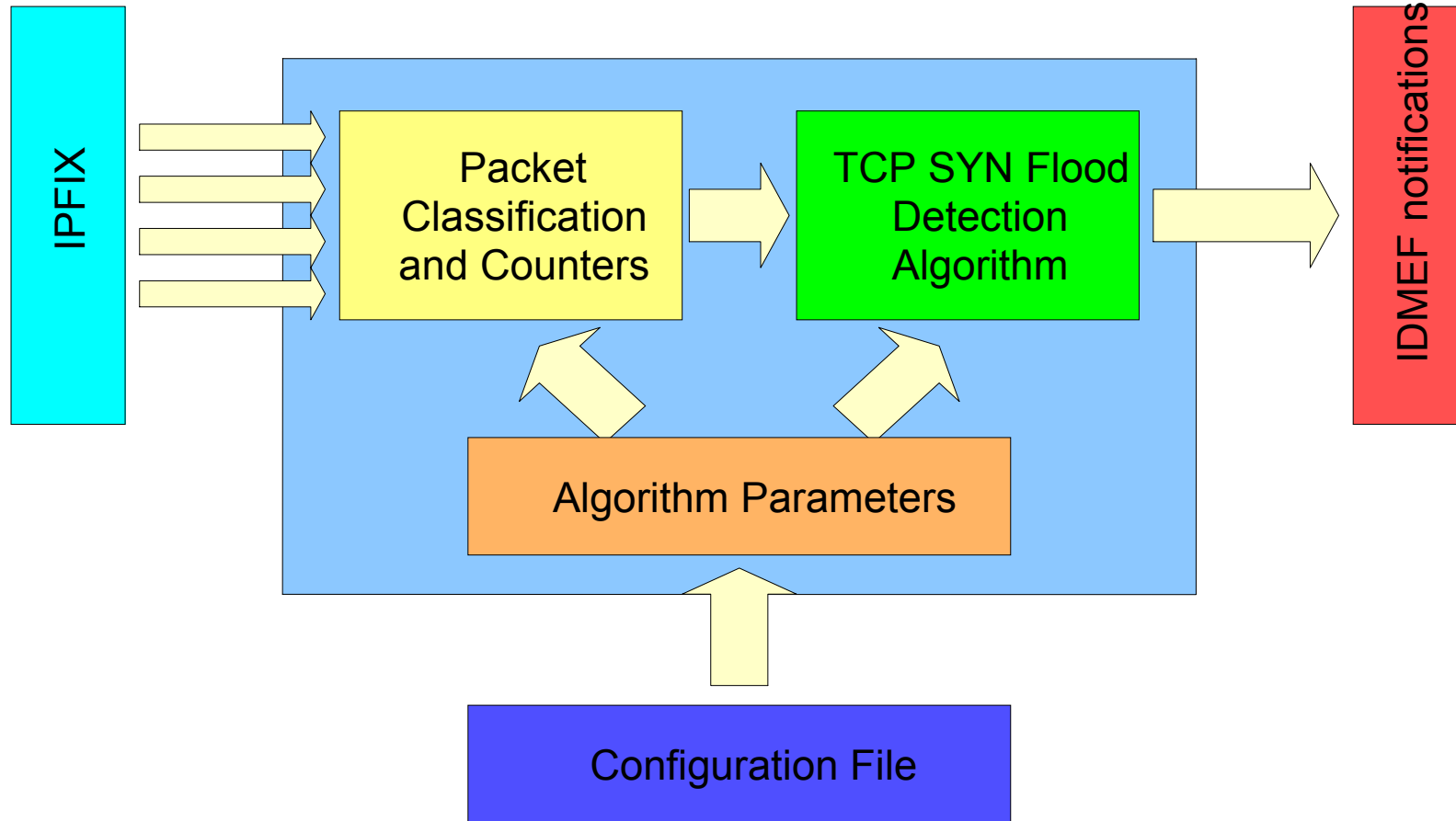
- ➔ A-NT: Agilent NetTester
- ➔ LC: Legitimate Client
- ➔ FE: Firewall Element
- ➔ ME: Monitoring Element

- ➔ SM: System Manager
- ➔ VD: Violation Detection
- ➔ WWW: victim web server
- ➔ VPN GW: VPN Gateway

# Demo overview

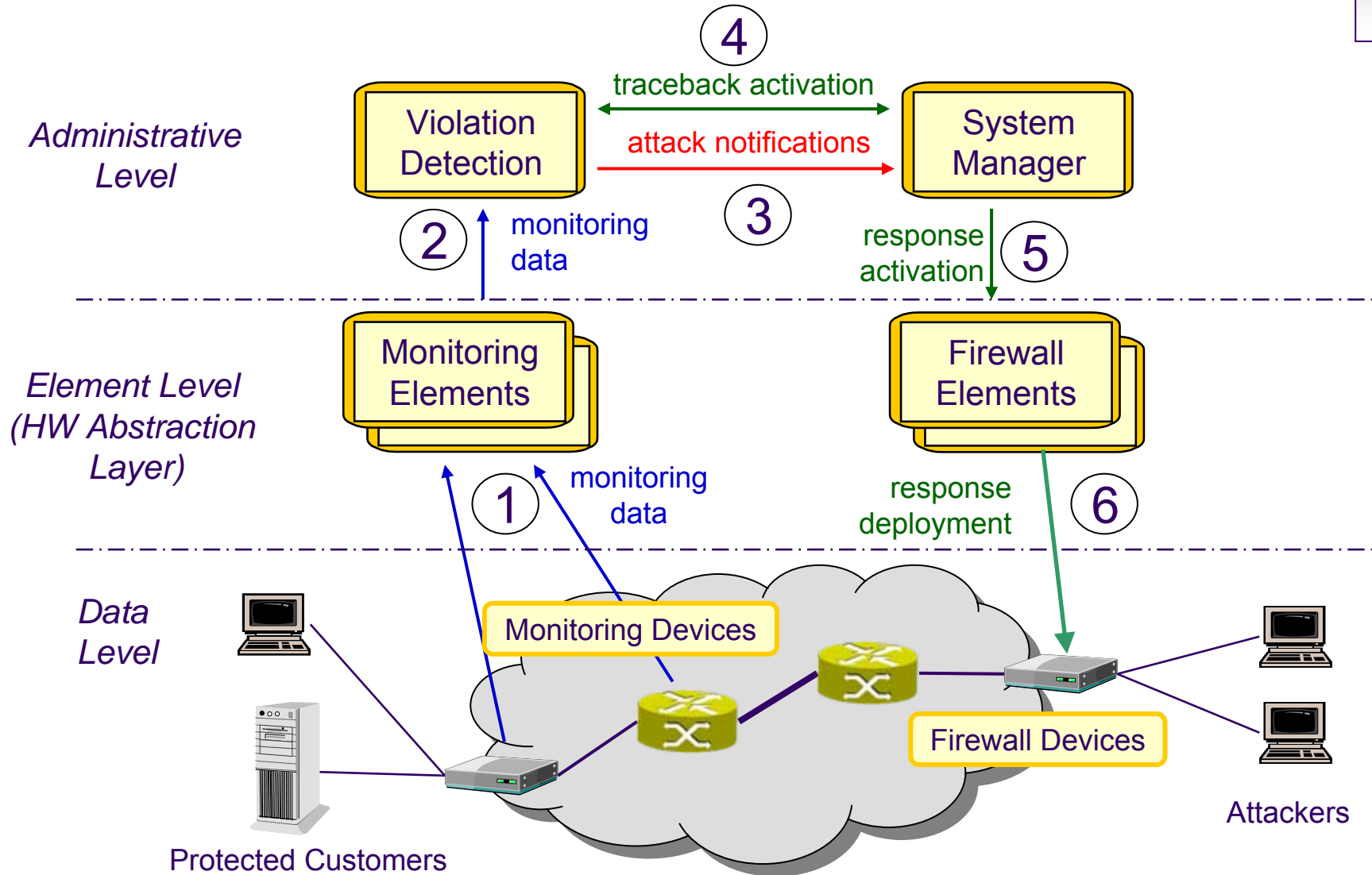


# Detection

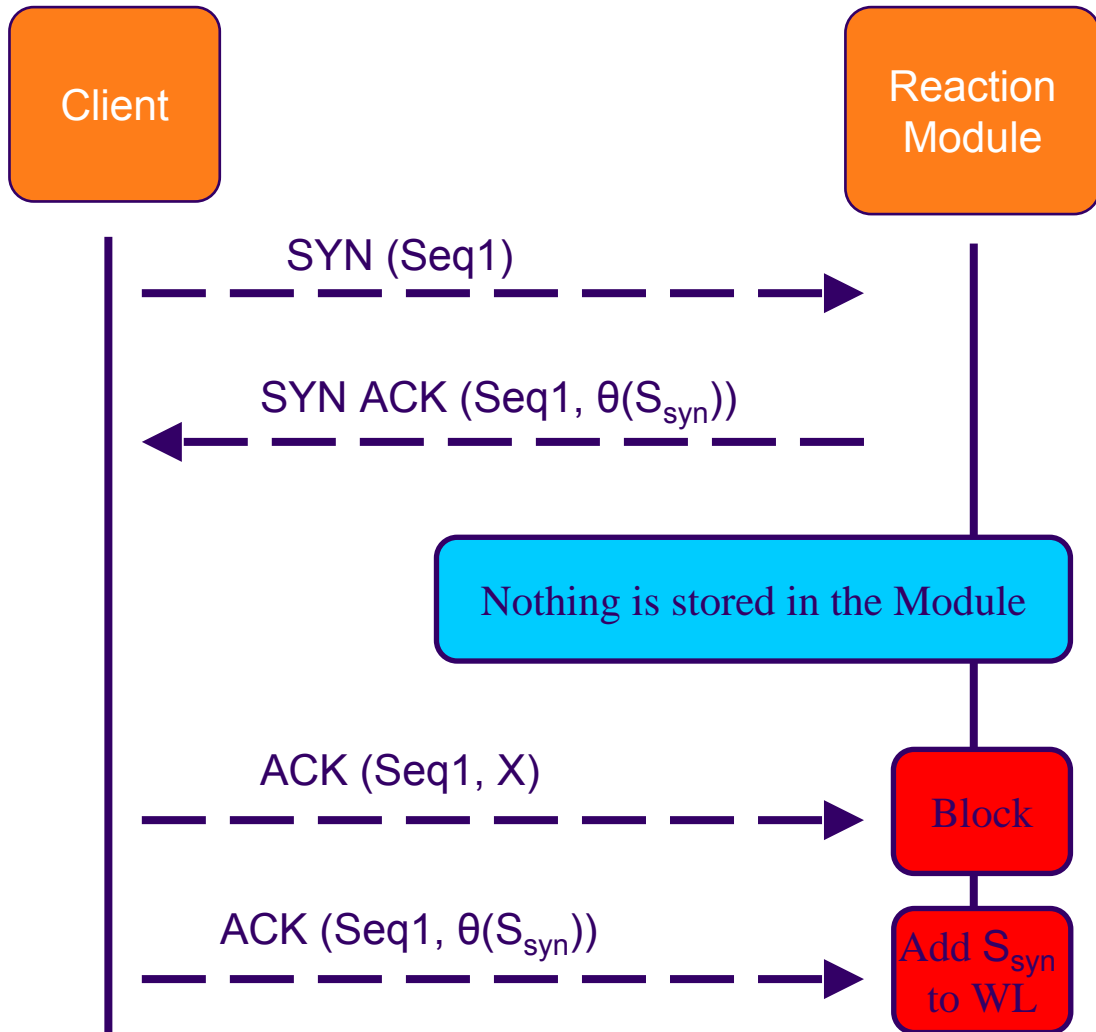


- ➔ Uses cumulative sum algorithm (CUSUM)
- ➔ Counts TCP SYN and SYN/ACK packets
- ➔ Attack is detected when a given threshold is exceeded

# Demo overview



# Reaction



**Seq1**: sequence number chosen by the client

**$\theta$** : encryption function

**$S_{syn}$** : source address of the TCP SYN message

# Demo overview

