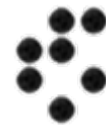




DIADEM Firewall Project



Jozef Stefan Institute



Groupe des Ecoles des
Télécommunications

Imperial College
London



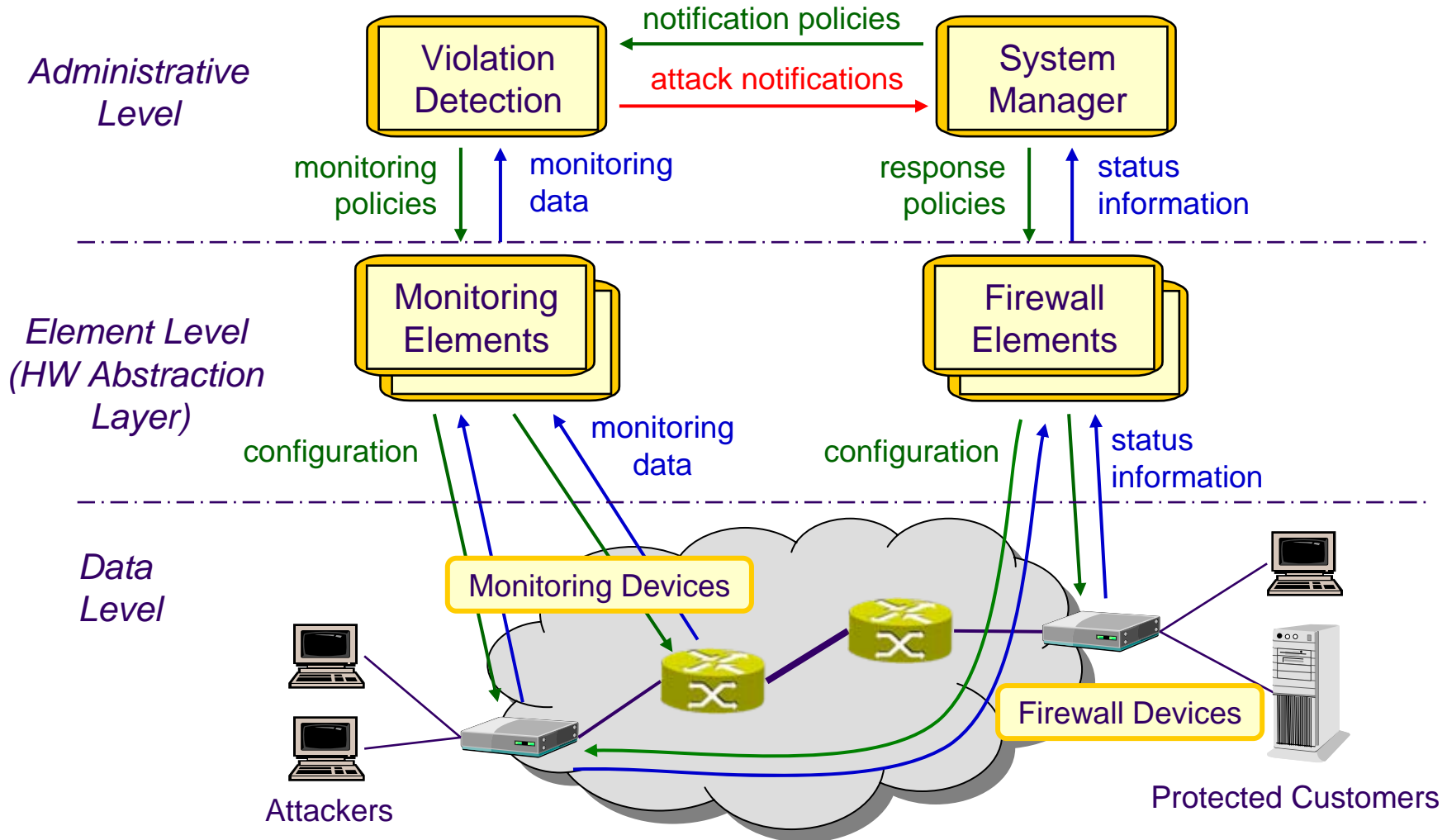
Universität Tübingen

Objectives

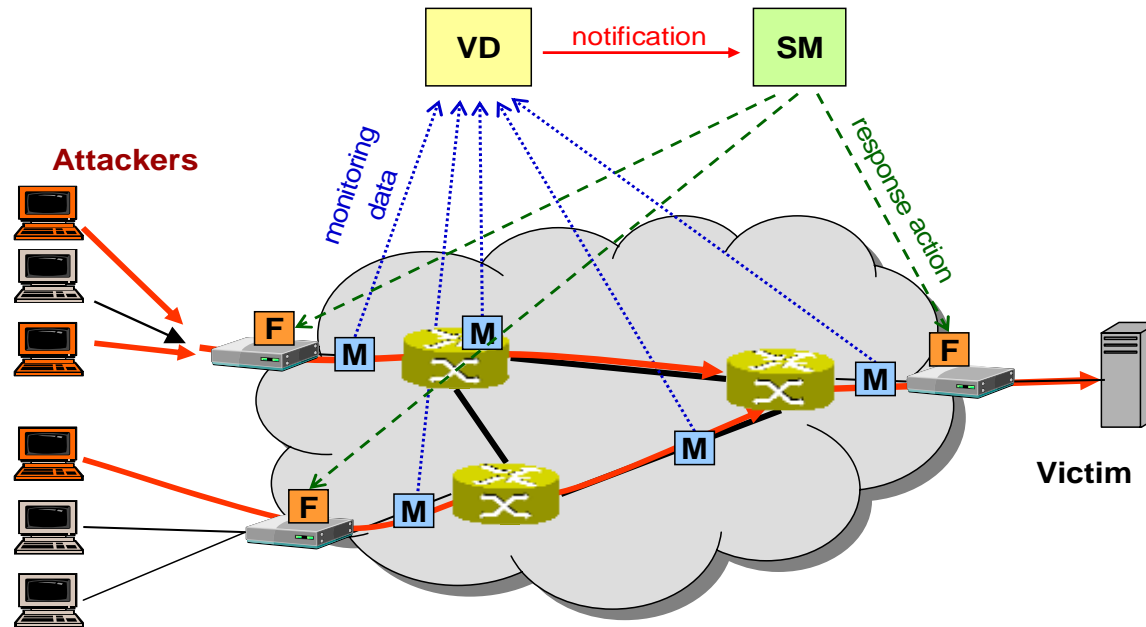


- Develop innovative network components for network operators to **protect** broadband services in an **effective** and **cost-efficient** way
 - **Distributed firewalls managed by the network operator**
- Protection
 - ▶ algorithms for attack detection
 - ▶ distributed adaptive responses
- Effective
 - ▶ flexible – device independent abstractions
 - ▶ high-speed FPGA based packet processing hardware
 - ▶ distributed monitoring of application traffic
- Cost-efficient
 - ▶ Automated policy-based techniques for
 - Adaptive monitoring and violation detection
 - Configuration of network elements
 - Responding to attacks

Diadem Architecture



Example of Deployment



VD : Violation Detection

SM : System Manager

M : Monitoring Element

F : Firewall Element

Monitoring and Violation Detection



- Primary Goal: Attack Detection and Characterization
- Monitoring Elements
 - ▶ Abstraction of hardware specifics via open interfaces
 - ▶ Using existing/upcoming standard monitoring technologies where possible in order to ensure easy deployment in existing network environments – IPFIX, IDMEF
- Design and development of a Violation Detection framework
 - ▶ Meeting given requirements such as modularity, extensibility, scalability
 - ▶ Multiple policy based VD components
 - ▶ Interaction with System Manager
- Attack detection algorithms
 - ▶ Focus on two use-cases: web server overloading and TCP SYN flood
 - ▶ Simulation and implementation of non-intrusive Traceback

Firewall Elements



- ➔ Abstraction of specific hardware elements via open interfaces
- ➔ Maps interface into hardware specific commands for configuring rules
- ➔ Implemented support for:
 - ▶ Linux
 - ▶ Cisco
 - ▶ FPGA based high speed classifiers (up to 1Gbit links)

Policy Based Management



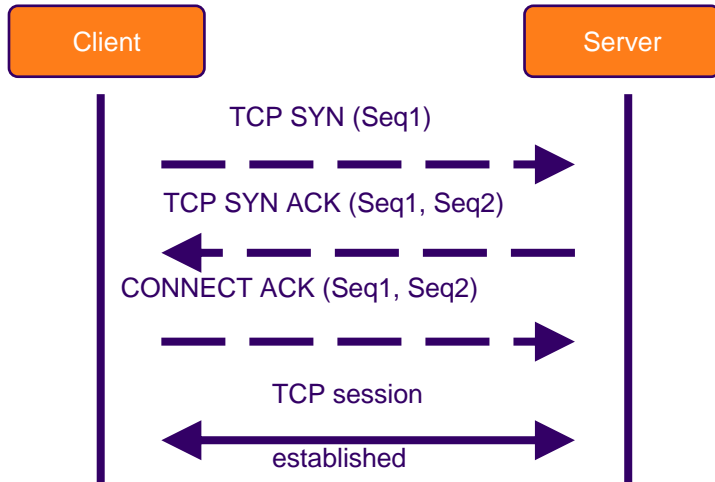
→ Response Policies

- ▶ Specify action(s) to be taken to stop or mitigate an attack, using parameters from the event notification
 - Perform an action on Firewall Element or Violation Detection
 - Generate and send a new event
 - Traceback
 - Enable/Disable new set of policies for specific monitoring

→ Policy Management Agents (PMAs)

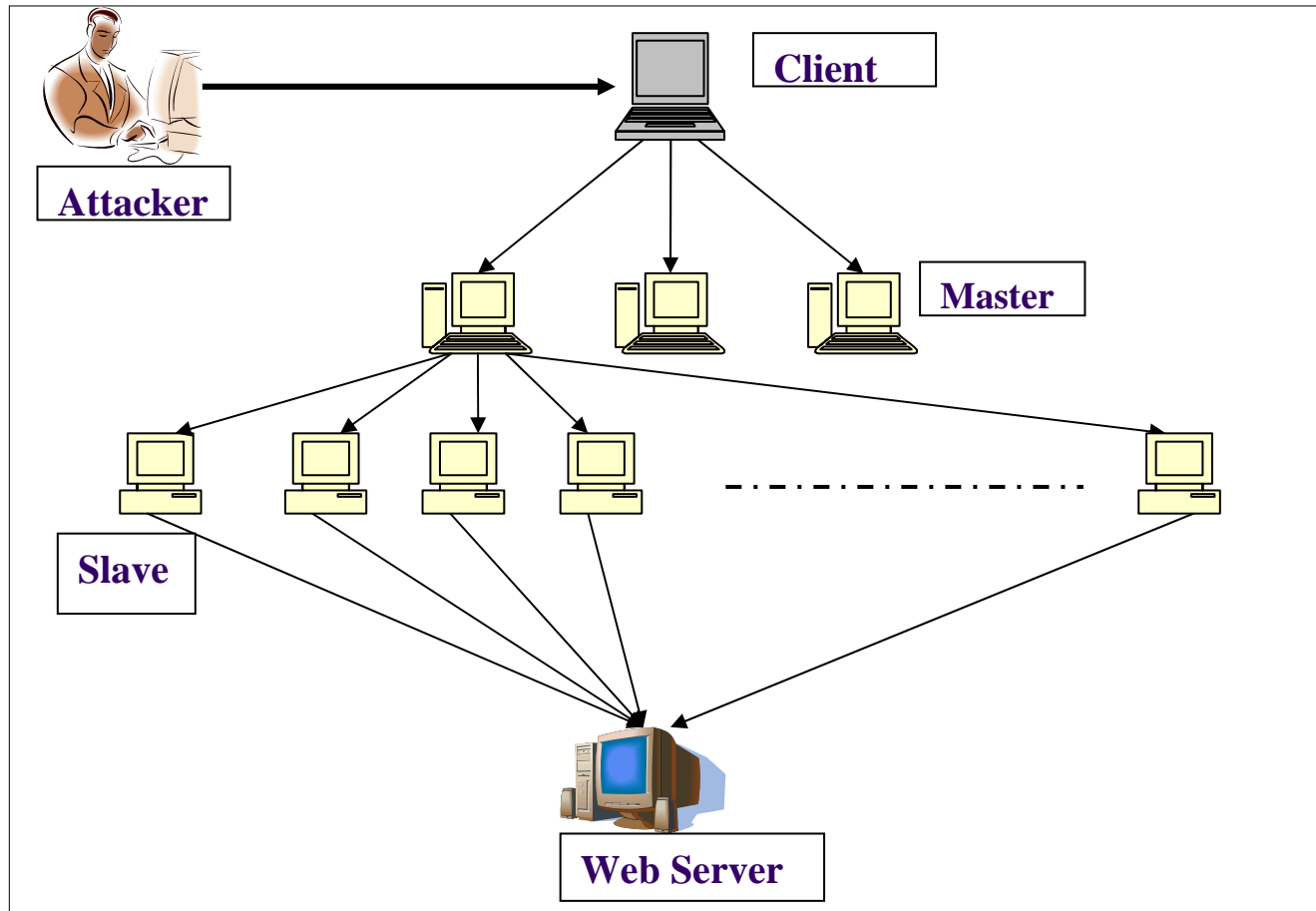
- ▶ Provide automated policy enforcement
- ▶ Load and enable policies in the PMA
- ▶ Subscribe to relevant events needed to trigger policies

Typical Attacks – Syn Flood



- A TCP connection is established in 3 steps:
- Upon reception of a SYN message the server keeps the context of the connection in memory, in a queue called backlog
- The DDoS attacks consists in flooding the server with SYN
- When the backlog is full, the server denies all subsequent connection attempts
- A lot of sophisticated attack tools available: Tribe Flood Network (TFN), TFN2K, Stacheldraht

Typical Attacks – Web Server DDOS



Demos



➔ Next Door