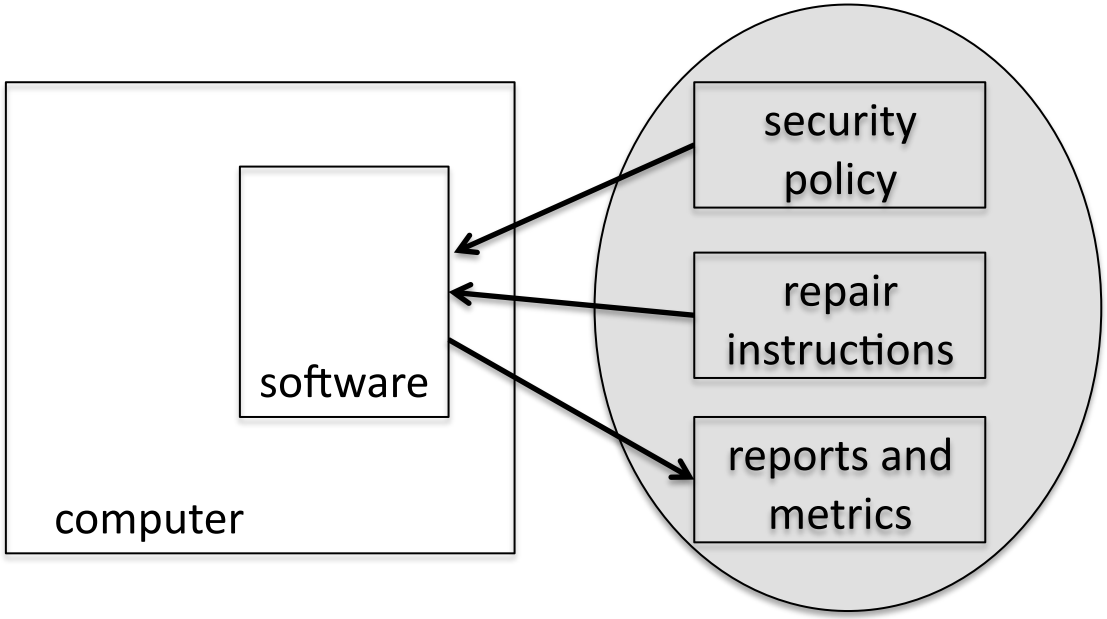
Looking at SCAP from an IETF Network Management Perspective

Architectural Considerations

Jürgen Schönwälder

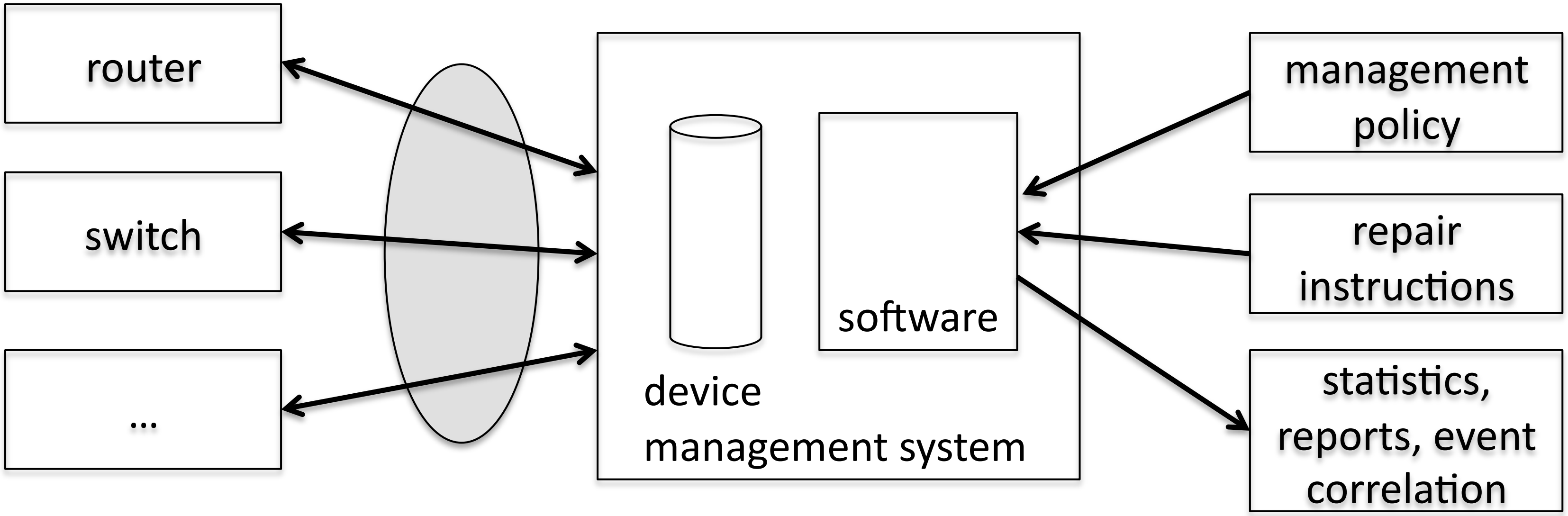
Jacobs University

SCAP (my interpretation of it)



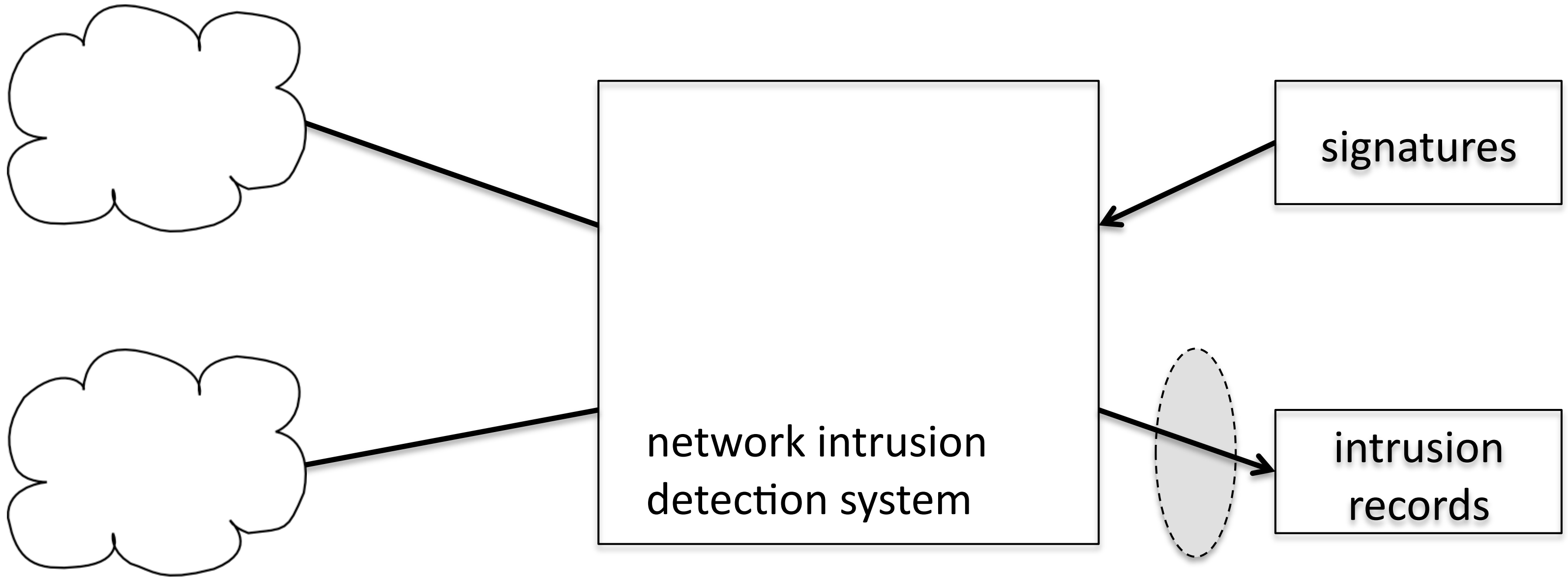
- Typical system administrator viewpoint
- Software on the box to do security auditing

Network Device Management



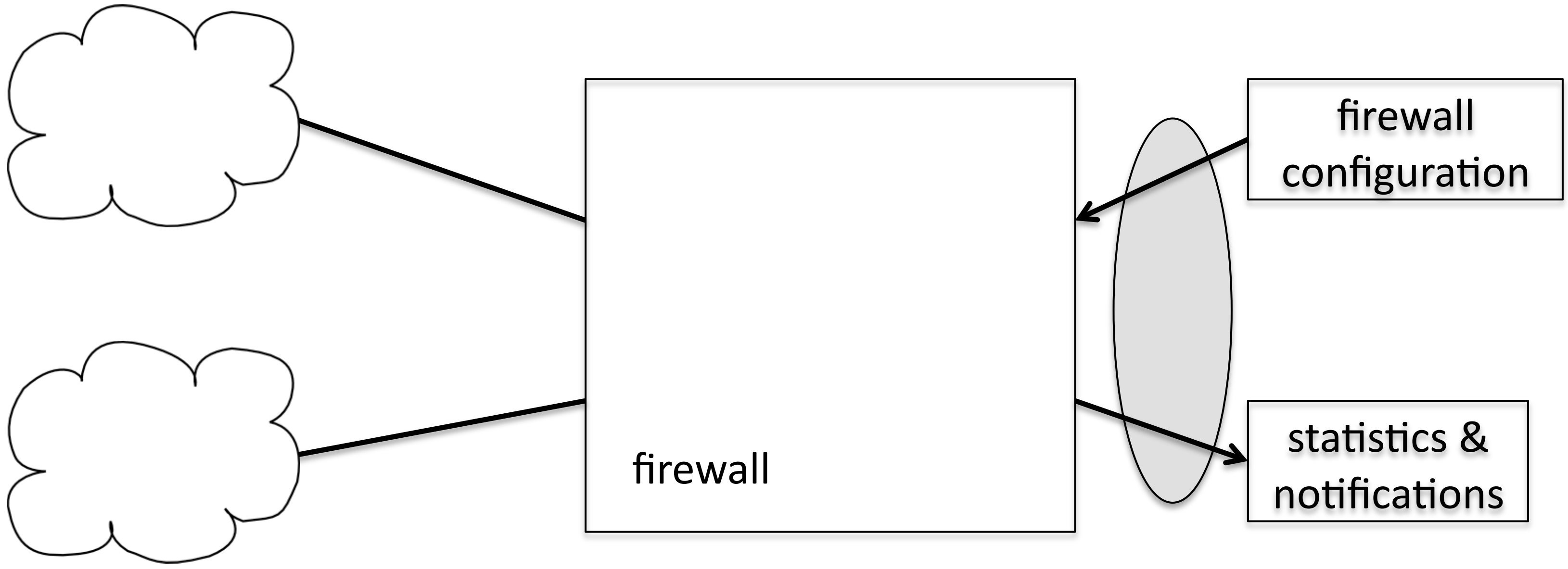
- Typical network management viewpoint
- Software outside the boxes does the management
- Protocols to access device configuration, status information, statistics, and event notifications (NETCONF [RFC4741], SNMP [RFC3410], IFPFIX [RFC5101], SYSLOG [RFC5424], …)

Network Intrusion Detection Systems



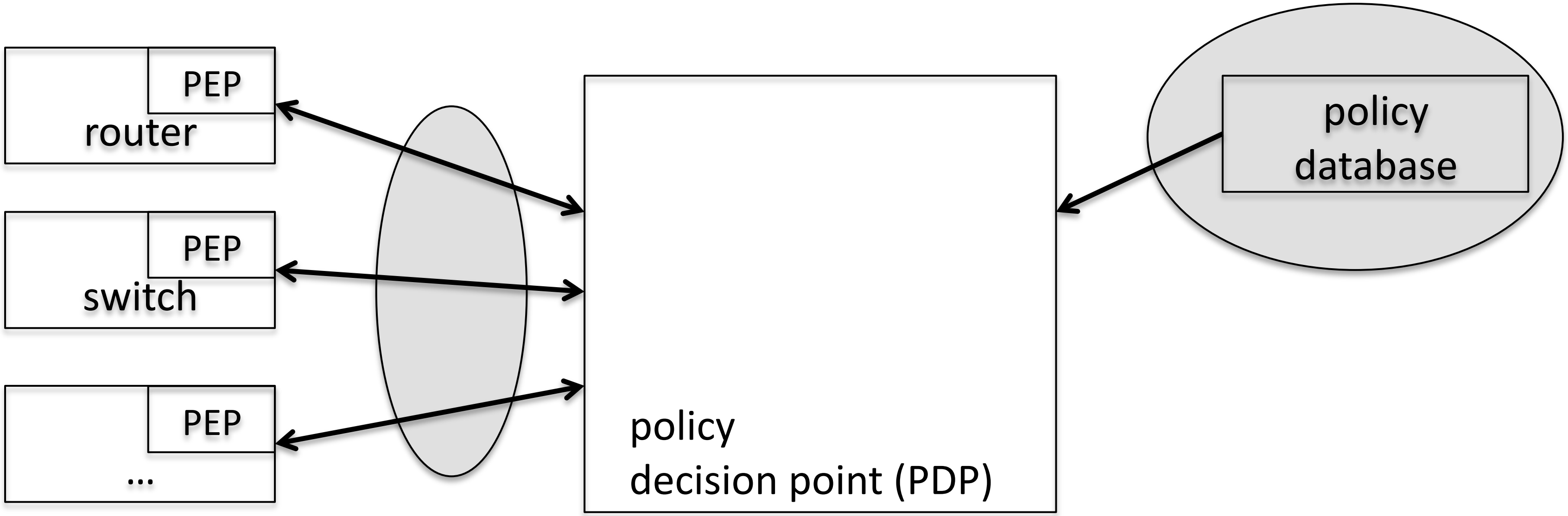
- Intrusion Detection Message Exchange Format (IDMEF) [RFC4765] and Intrusion Detection Exchange Protocol (IDXP) [RFC4767]
- Experimental RFCs (WG concluded before publication)

Middleboxes aka Firewalls



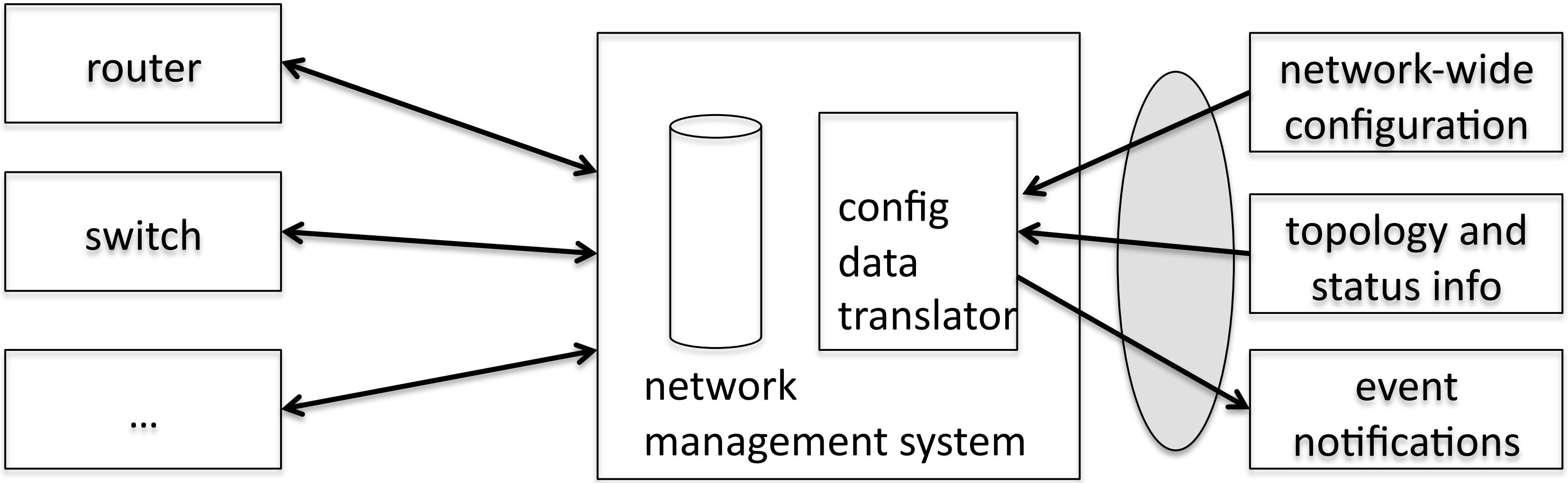
- MIDCOM-MIB module for SNMP [RFC5190]
- Middlebox Communication Protocol [RFC5189]
- Deployment of the two mechanisms?

Policy-based Management



- COPS [RFC2748] and COPS-PR [RFC3084] were designed to outsource policy decisions from a PEP to a PDP or to provision policy decisions from a PDP to a PEP
- Policy Core Information Model [RFC3060, RFC3460] (work done in some collaboration with the DMTF, part of CIM today)

Network-wide Configuration



- Use NETCONF/YANG as a tool to develop standard interfaces for network-wide configuration
- Some implementers are developing products in this space
- Can be seen as a (late) implementation of RFC3139

Some Questions…

- What is the focus of SCAP? A single device or a a collection of devices or the network as a whole?
- What can the IETF learn from previous related efforts? What has been successful and why? What failed and why?
- To what extend is SCAP different from just more configuration and reporting?
- Does SCAP integrate into the idea of network-wide configuration?