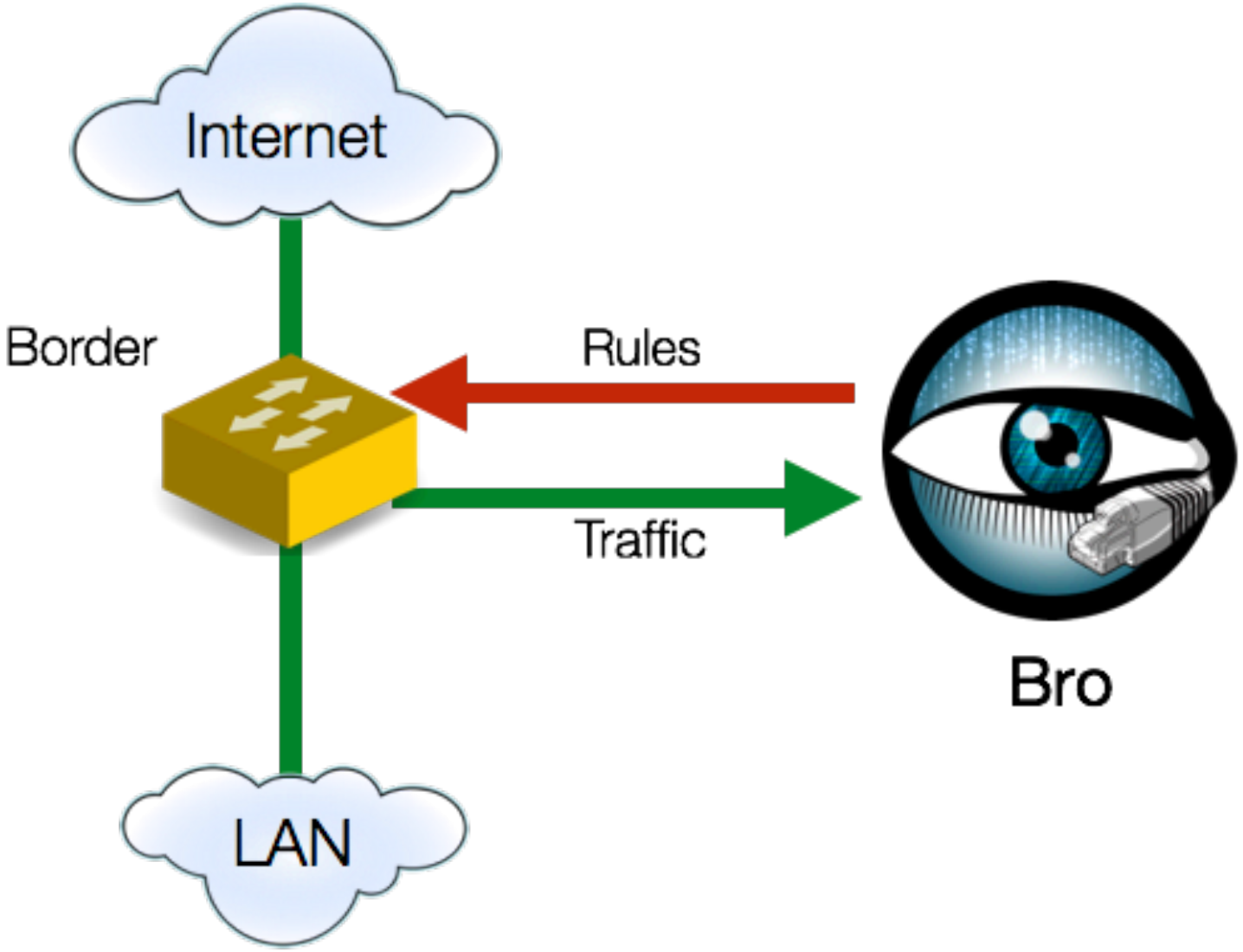
# Effective and Economical Protection for High-Performance Research and Education Networks

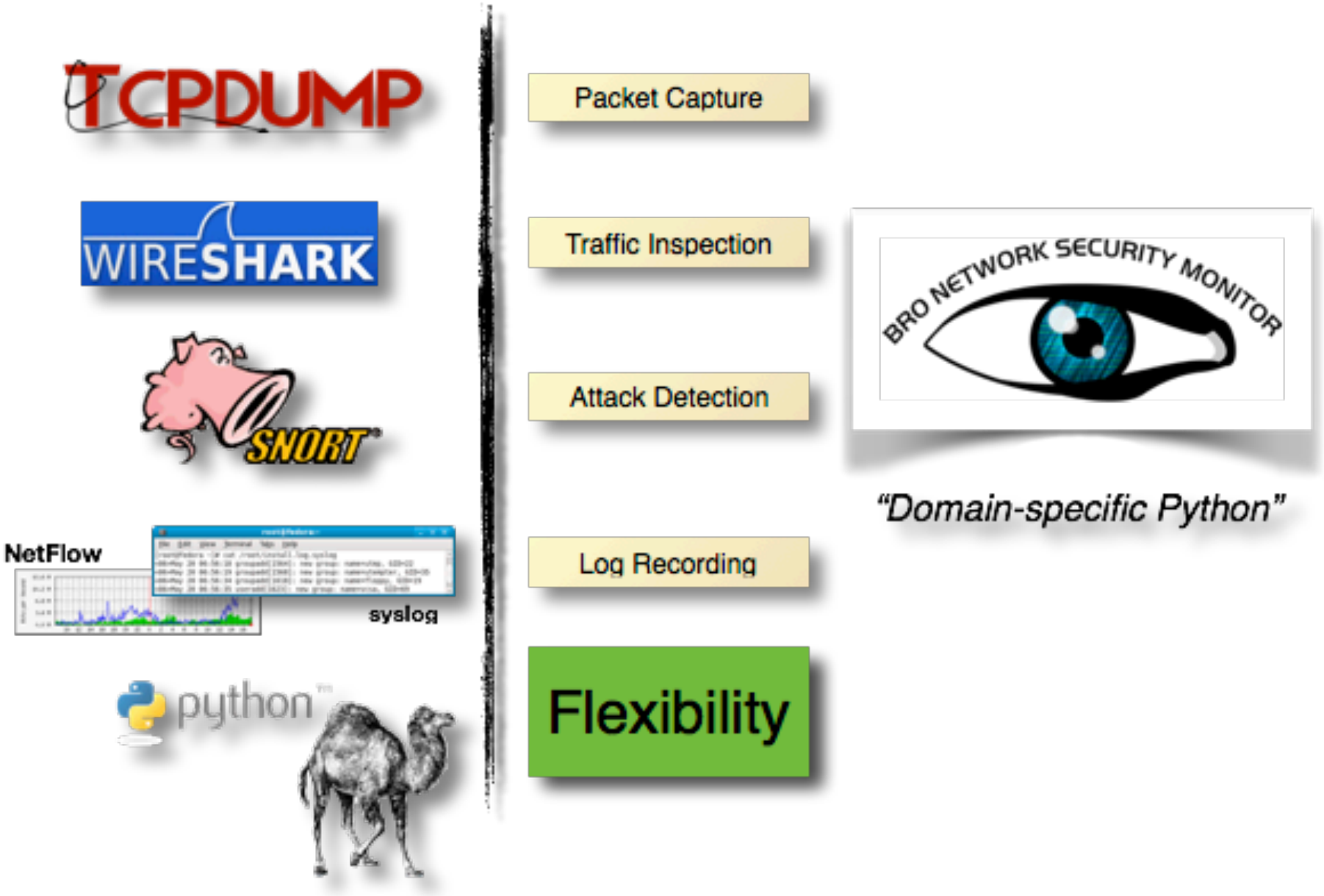
Johanna Amann

johanna@icir.org

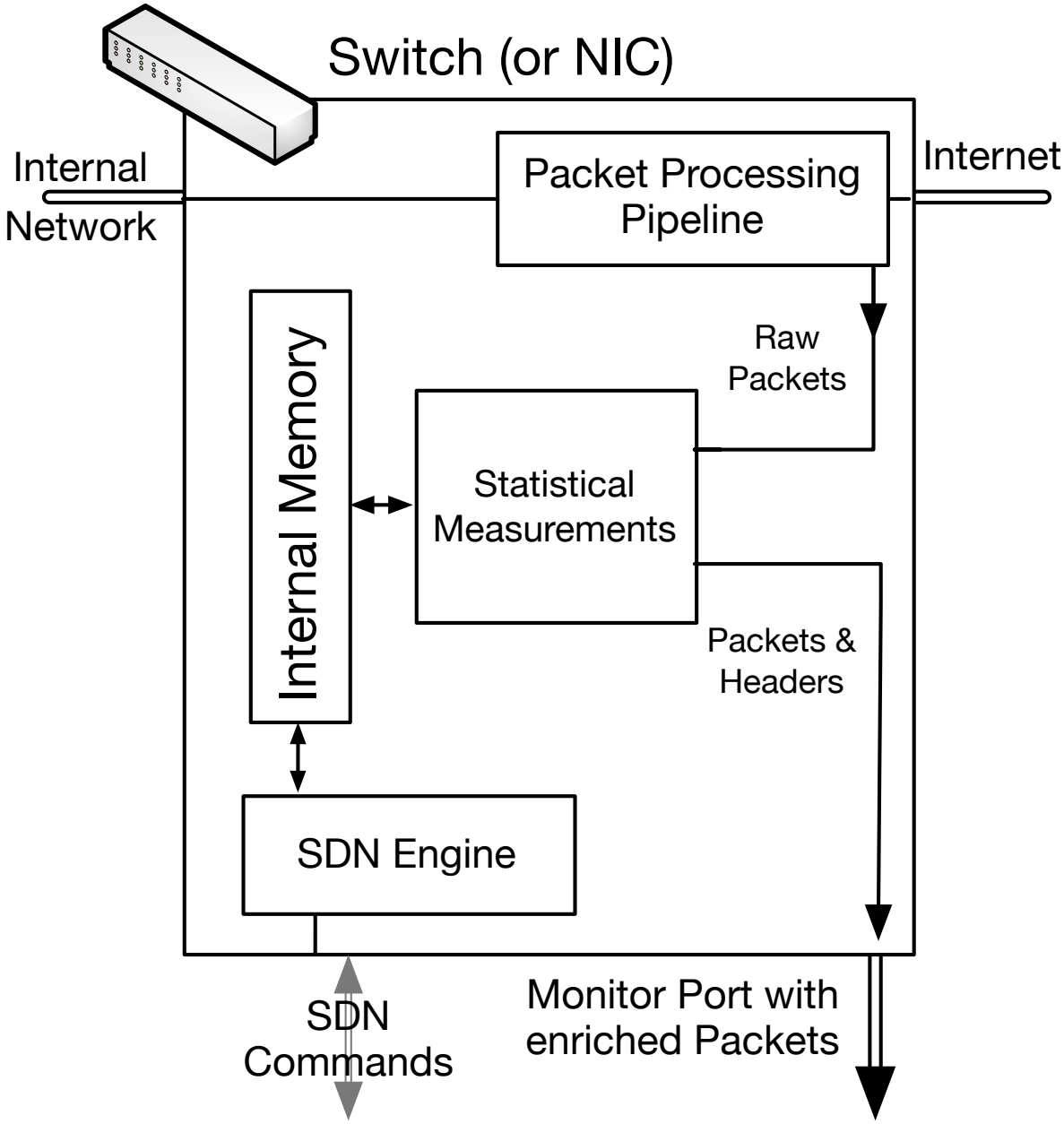
# Typical Network Monitoring Setup



# What is Bro?


TCPDUMP
WIRESHARK
SNORT
NetFlow
syslog
python
Packet Capture
Traffic Inspection
Attack Detection
Log Recording
Flexibility
BRO NETWORK SECURITY MONITOR
"Domain-specific Python"

# Hard/Software Co-Design for Network Monitoring



# Domain-Specific Security Monitoring

- Domain-specific protocols
- User authentication
- Network activity profiling
- Security policy enforcement
- DOS Protection