Lehrstuhl für Rechnernetze und Internet
Wilhelm-Schickard-Institut für Informatik, Universität Tübingen
Prof. Dr. Georg Carle

Netzbasierte Angriffs- und Anomalieerkennung mit TOPAS

Lothar Braun, Gerhard Münz

12.07.2006

Eberhard Karls
Universität
Tübingen

Überblick

- Motivation
- IPFIX / PSAMP
- Eigenschaften
- Architektur und Funktion
- Durchsatzmessung
- Anwendung
- Zusammenfassung und Ausblick

Motivation

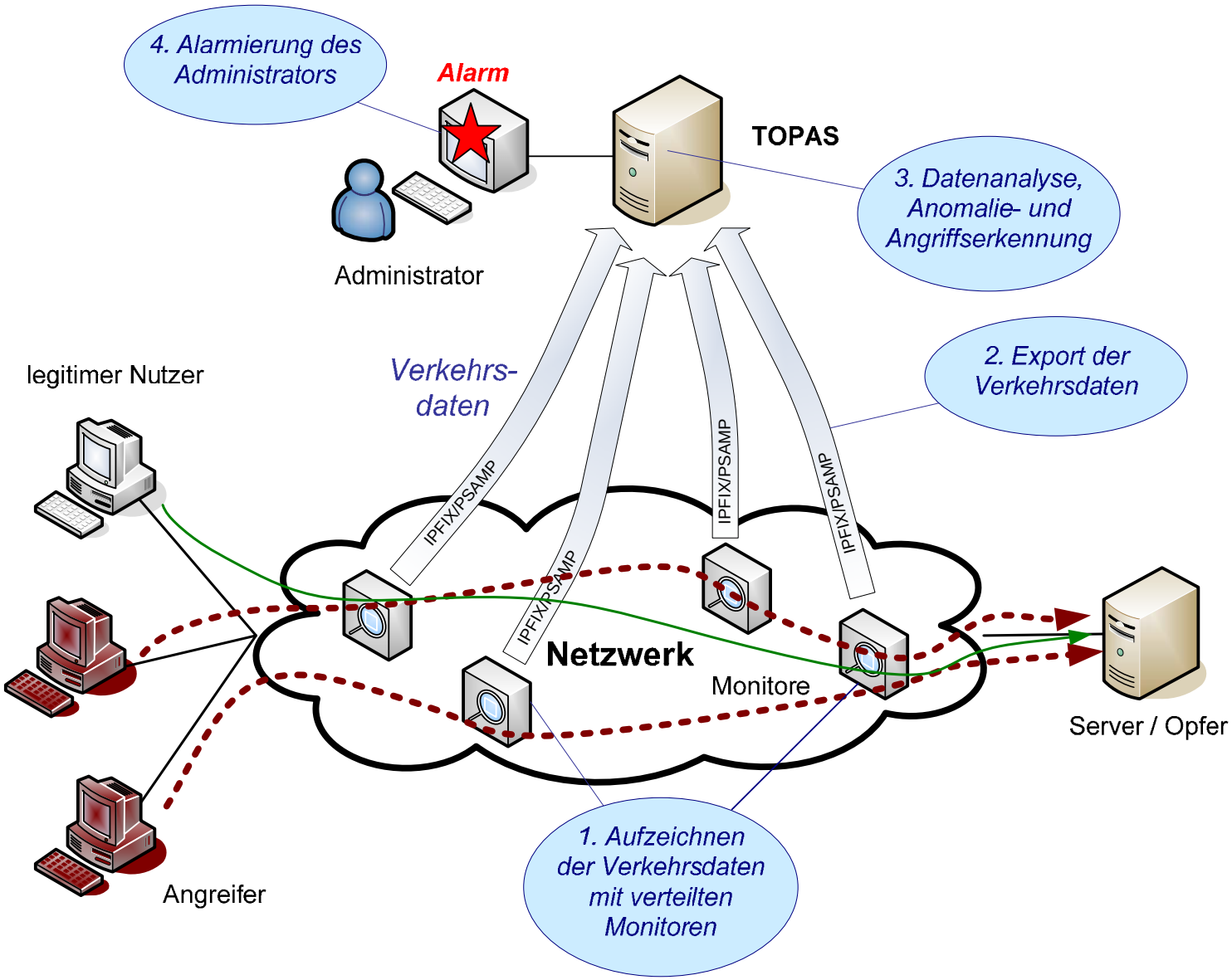
- Netzbetreiber erheben Verkehrsdaten für verschiedene Anwendungen:
  - Netzüberwachung
  - Verkehrsuntersuchung
  - Accounting und Charging

- Bisherige Ansätze verfolgen meist Offline-Datenanalyse
  - Daten werden in großer Datenbank gespeichert
  - Verzögerte Auswertung anhand der gespeicherten Daten

- Idee: Verkehrsdaten zur Anomalie- und Angriffserkennung verwenden
  - Schnelle Alarmierung des Netzbetreibers
  - Schnelle Reaktion auf Ereignisse, wie z.B. DoS-Angriffe

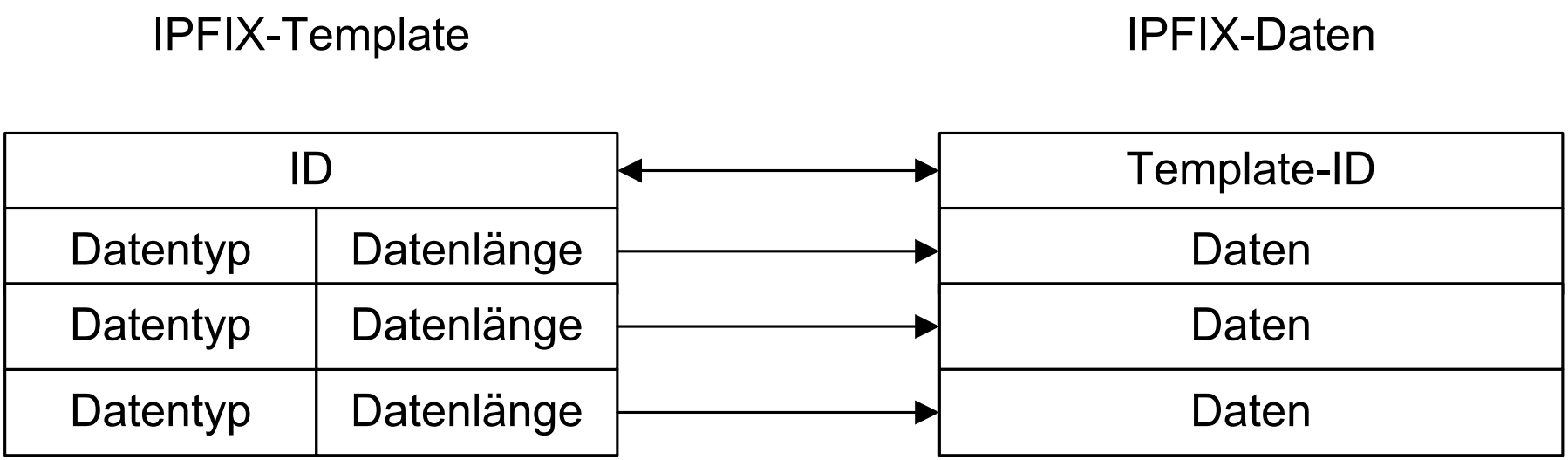
➔ System zur Echtzeitdatenverarbeitung der Verkehrsdaten erforderlich

TOPAS = Traffic flOw and Packet Analysis System



IPFIX / PSAMP

- IETF-Standards
- Kompatibilität zu bereits eingesetzten Netzwerkmonitoren
  - Einfache Integration in bestehende Netze
- PSAMP (Packet Sampling)
  - Ermöglicht Übertragung von Paketdaten
- IPFIX (IP Flow Information Exchange, Nachfolger von NetFlow)
  - Flow-Daten (Flow = Pakete mit gemeinsamen Eigenschaften)
  - Bsp: IP-5-Tupel (Transportprotokoll, Quelladresse und –port, Zieladresse und –port)

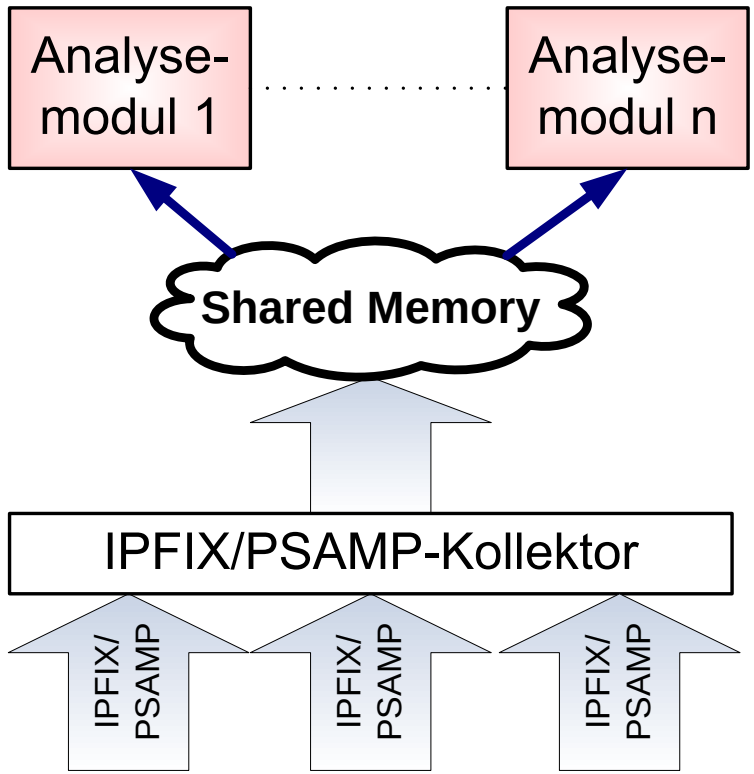


Eigenschaften von TOPAS

- Empfang von Flow-Daten (IPFIX) und Paketdaten (PSAMP) mit einem gemeinsamen Kollektor
- Echtzeitverarbeitung der Daten in parallel arbeitenden Analysemodulen
- Gleichzeitige Anwendung verschiedener Analysemethoden
  - Statistische Anomalieerkennung
  - Signaturbasierte Angriffserkennung
- Dynamisches Starten, Beenden und Rekonfigurieren von Modulen
  - Adaptive Datenanalyse: verschiedene Algorithmen zu unterschiedlichen Zeitpunkten ausführen
  - Reaktion auf Änderungen im Netzwerkverkehr
  - Auslösen einer genaueren Untersuchung bestimmter Flows oder Pakete
- Einsatz in Hochgeschwindigkeitsnetzen (Gigabit-Ethernet)
  - Angepasst für Parallelisierung auf Multiprozessorsystemen
- Anforderungen
  - Standard-Linux-PC

Interne Architektur

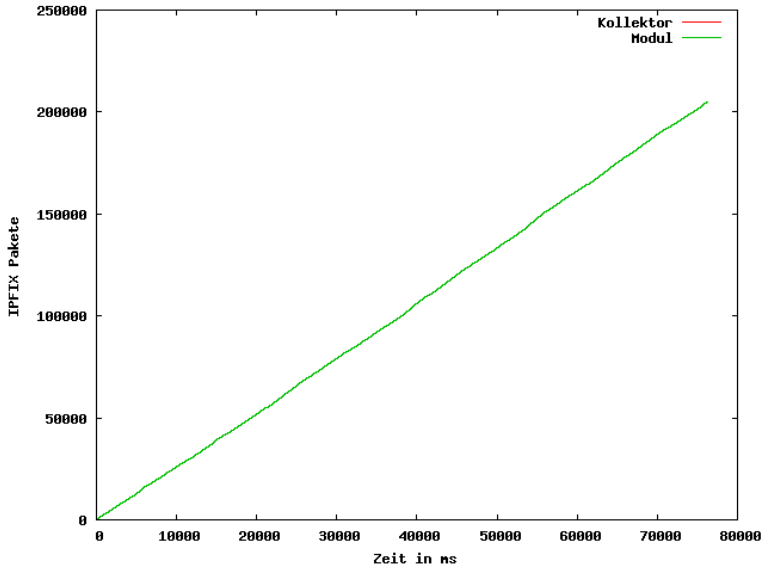
- Kollektor und Module laufen in eigenständigen Prozessen:
  - getrennte Adressräume
  - problemloses Starten und Beenden von Modulen zur Laufzeit
  - große Stabilität: Fehler/Absturz eines Modules beeinträchtigt nicht das Gesamtsystem

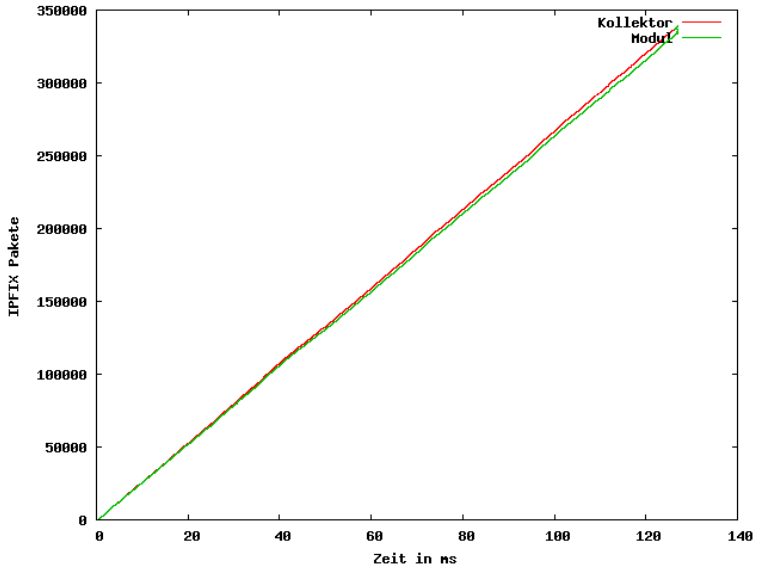


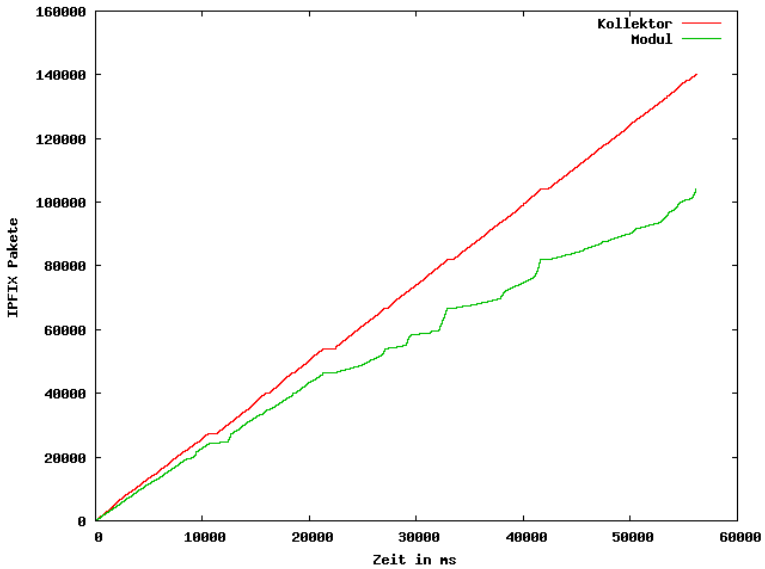
- Interprozesskommunikation:
  - Weiterleiten der Verkehrsdaten über RAM-Disk
  - Modulüberwachung und Signalisierung über Shared Memory und Semaphore

- Zentrale Modulverwaltung
  - Starten und Beenden von Modulen
  - Erkennen von Fehlfunktionen der Modulen (Absturz oder Inaktivität)
  - Automatischer Neustart abgestürzte Module (optional)

Erste Messungen







- Arbeitsbereiche
  - Optimal – Verarbeitung der Pakete in konstanter Zeit
  - Grenzbereich – Verarbeitung in akzeptablem Zeitintervall, aber mit der Zeit steigend
  - Überlast – Inakzeptable Verarbeitungszeit, Beendigung oder Absturz von Modulen wegen Speichermangel

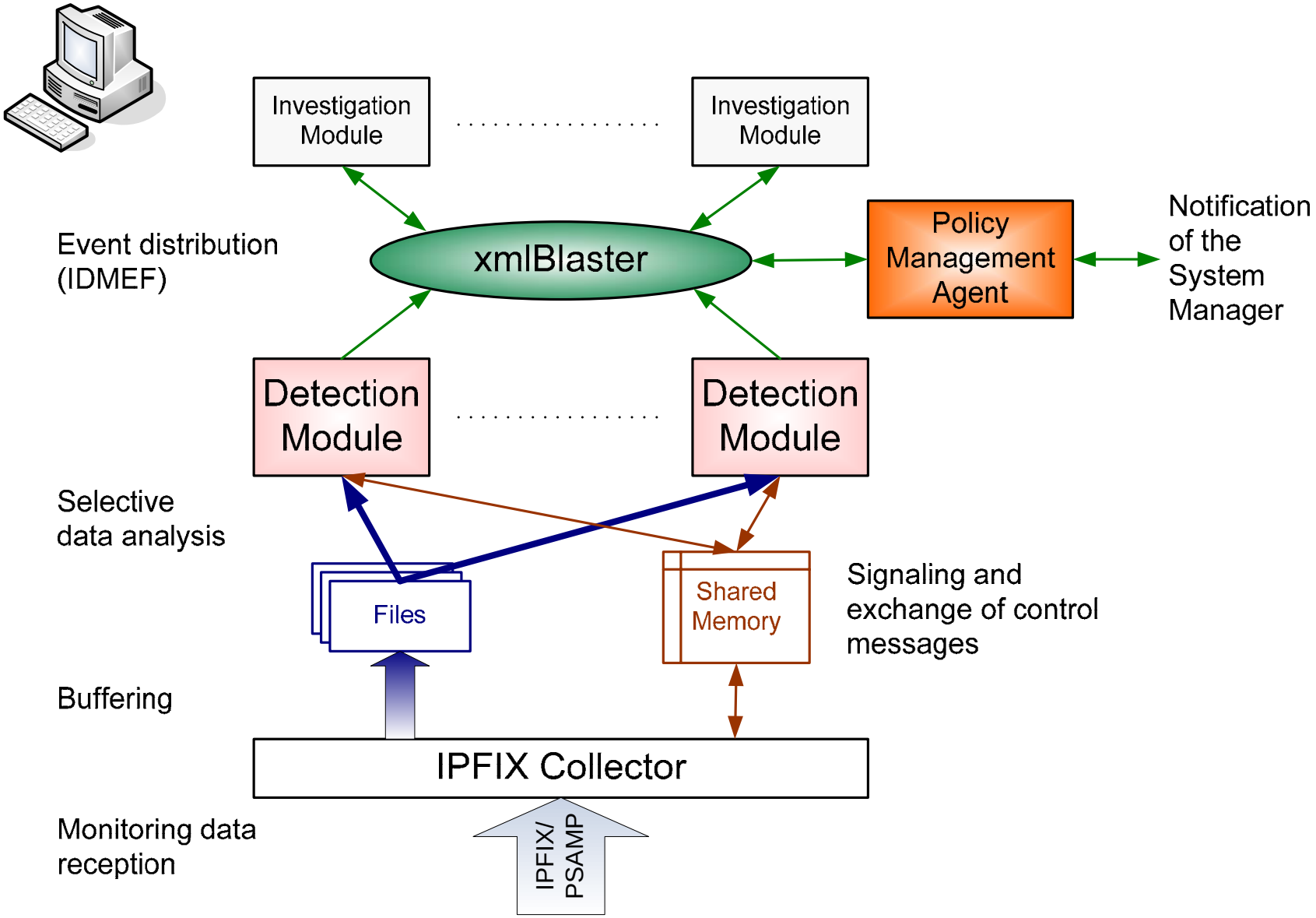
Anwendung

Es existieren schon einige Module für TOPAS:

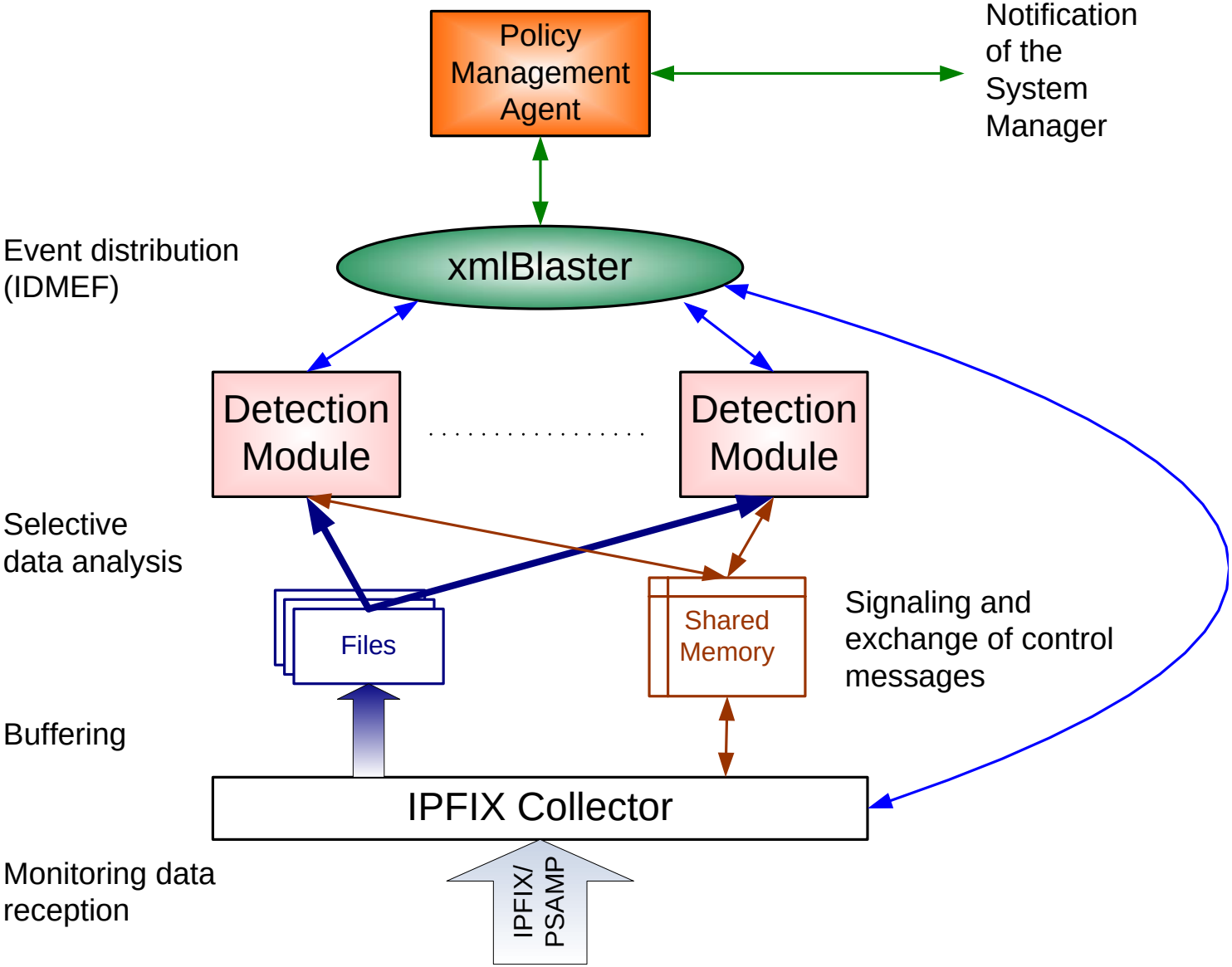
- Snortmodule:
  - Signaturbasierte Angriffserkennung mit Snort
- stat-modules
  - Statistische Anomalieerkennung
- Webserver Overloading Detection Module
  - Erkennung von Angriffen auf Webserver
- SYN-Flood Detection Module (Syndog)
  - Erkennung von SYN-Flood Angriffen
- Traceback
  - Erkennung von Angriffen mit gespooften IP-Adressen

- TOPAS wird im EU-Projekt *Diadem Firewall* eingesetzt

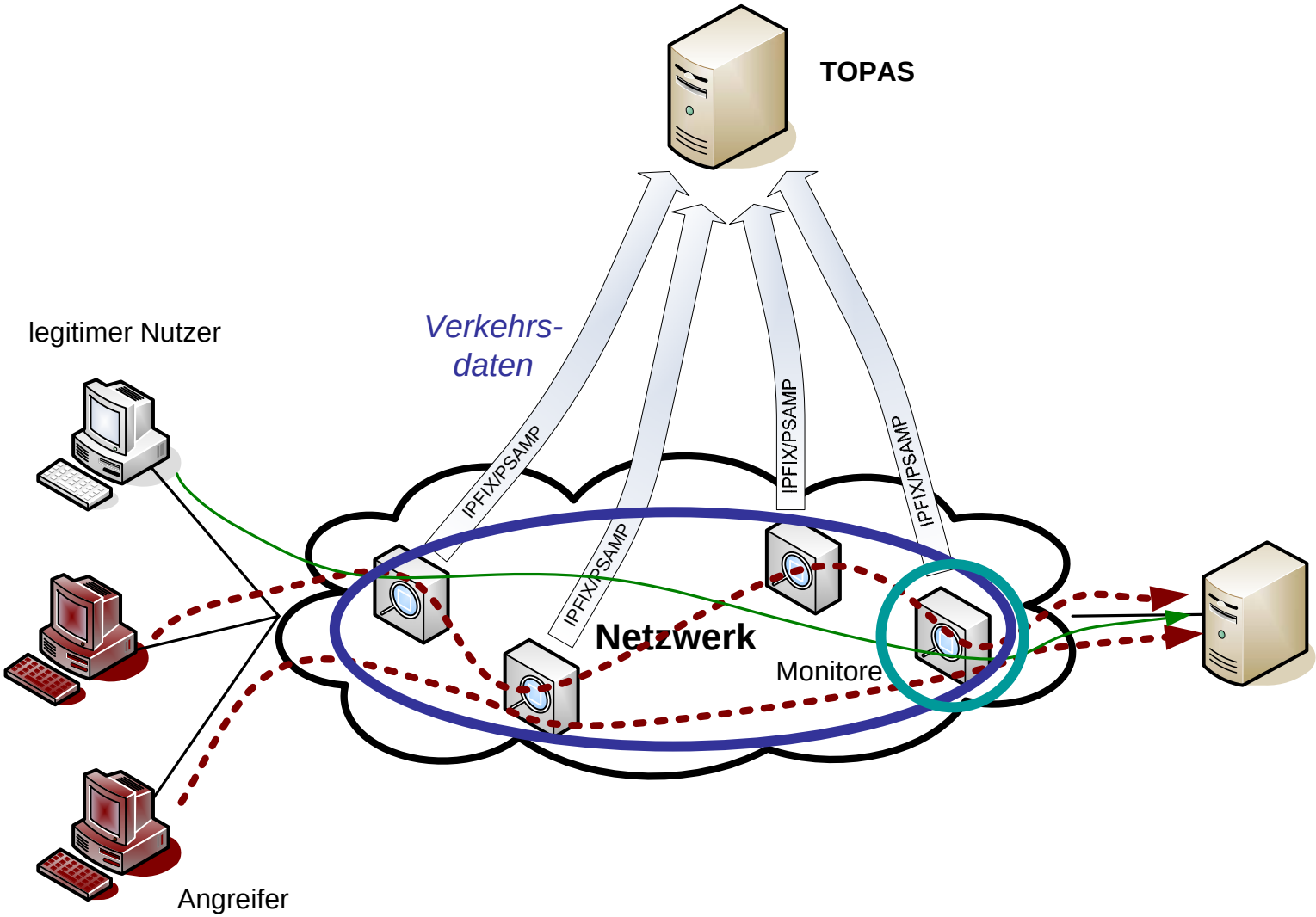
Verwendung in *Diadem Firewall*



Rekonfiguration und Nachstarten



Rekonfiguration



Zusammenfassung und Ausblick

- TOPAS:
  - Leistungsfähiges System zum Empfang und Verarbeiten von Flow- und Paketdaten (IPFIX/PSAMP)
  - Durchsatzkapazität: > 5800 IPFIX-Pakete/Records pro Sekunde (ermittelt mit Dummy-Modul)
  - Echtzeiterkennung von Angriffen und Anomalien
  - Dynamische Rekonfiguration
  - Erfolgreicher Einsatz in *Diadem Firewall*
  - Baldige Veröffentlichung unter Open-Source-Lizenz

- Grundlage für vielfältige zukünftige Arbeiten:
  - Implementierung verschiedener Erkennungsalgorithmen
  - Erweiterung zu einem autonom arbeitenden NIDS
  - Einsatz für andere Anwendung
    - Echtzeit-Accounting
    - QoS-Messungen

Vielen Dank für die Aufmerksamkeit

Fragen?