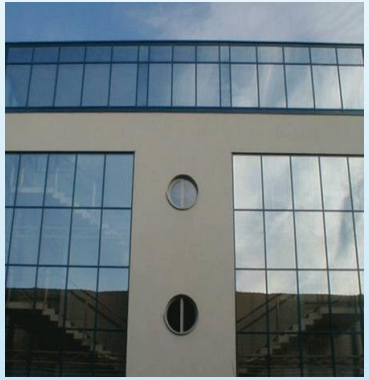
Cybersecurity (und IoT) in Schulen?

Cybersecurity (und IoT) in Schulen?

Sag zum Schulnetz leise servus!



Prof. DI Christian Schöndorfer
Academy Lead Austria
christian@schoendorfer.cc

Der Fortschritt geschieht heute so schnell, dass, während jemand eine Sache für gänzlich undurchführbar erklärt, er von einem anderen unterbrochen wird, der sie schon realisiert hat.“

Albert Einstein († 18. April 1955)

DIGITALISIERUNG

2010

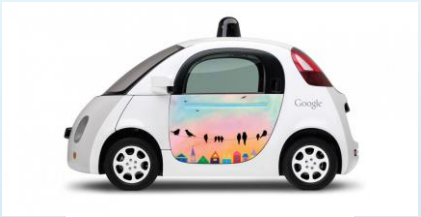
12.5 bn

2015

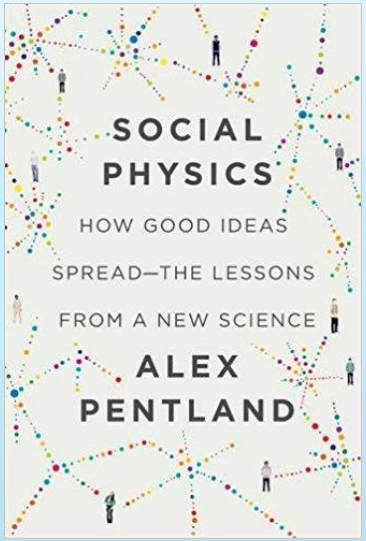
25 bn

2020

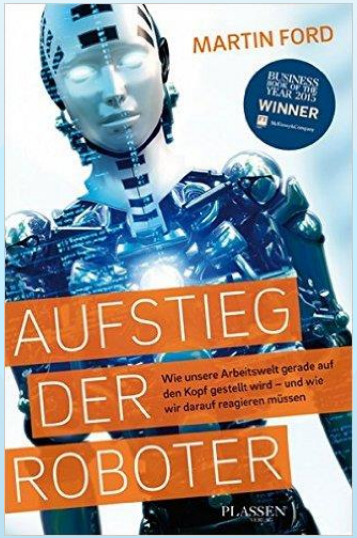
50 bn



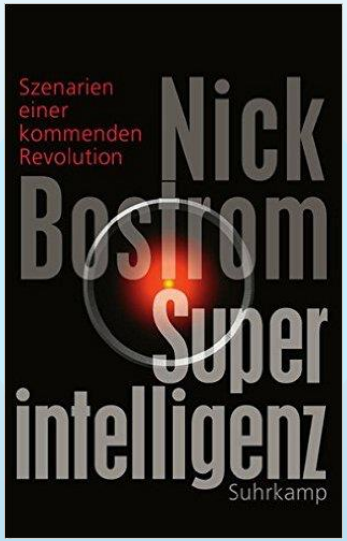
TRENDS



BigData



Automation



Artificial Intelligence

TECHNOLOGIE

STOP: Wir sprechen doch über Schule?

BlockChaining

Software Defined Network
Compute / Storage

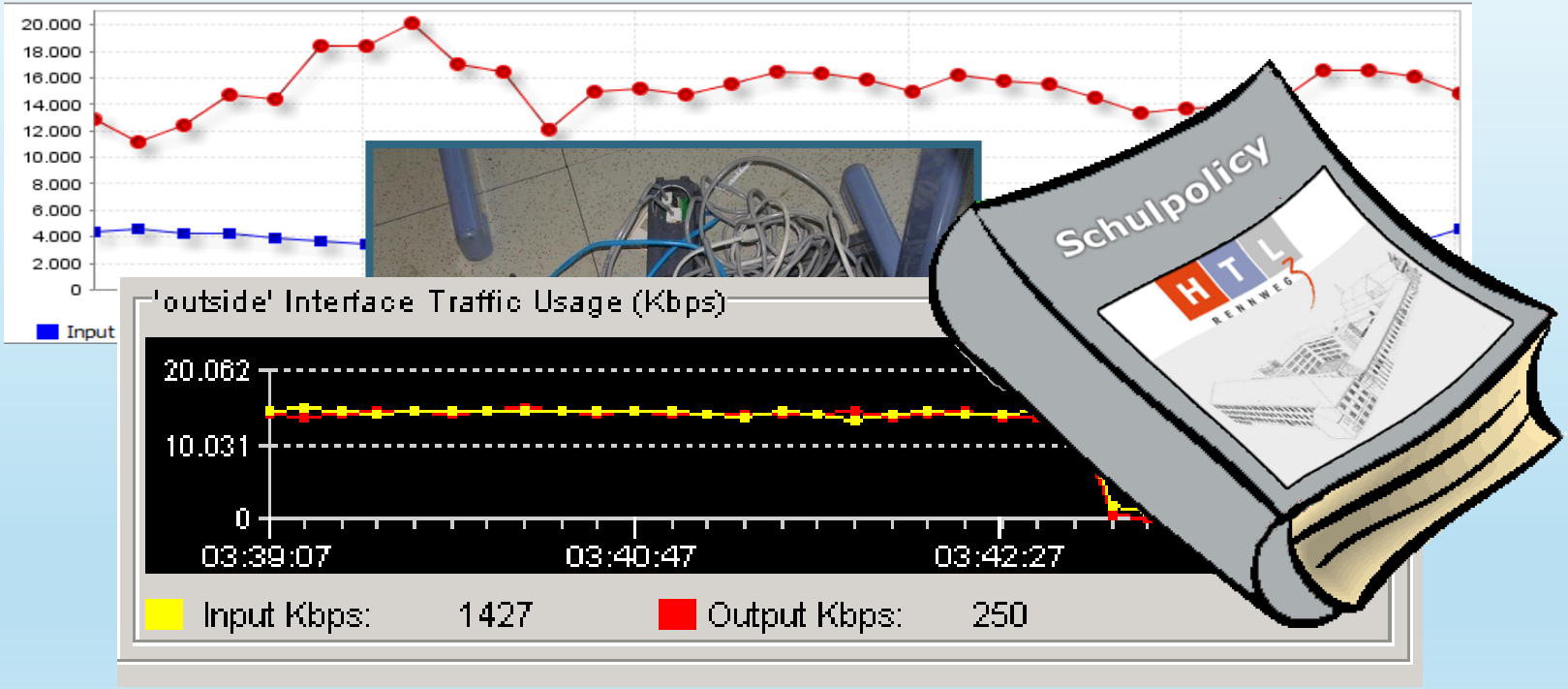
Fog Computing

Ein konsistentes System?

Von der Vision zur Projektidee

- Fakten:
  - 80 k SchülerInnen als „Zielgruppe“ im Fokus
  - Davon ca. 70% mit (zumindest teilweisem {>50%}) Internetzugang
  - ca 35 Wochenstunden „Zeit“ vor Ort
  - An unserem Schulstandort
    - 1200 SchülerInnen (entspricht Median)
    - Etwa 3.800 Mobile Geräte pro Sekunde im WLAN
    - 2 GB Internetanbindung zum Desktop
    - Internetauslastung…

Bekannte Faktoren?



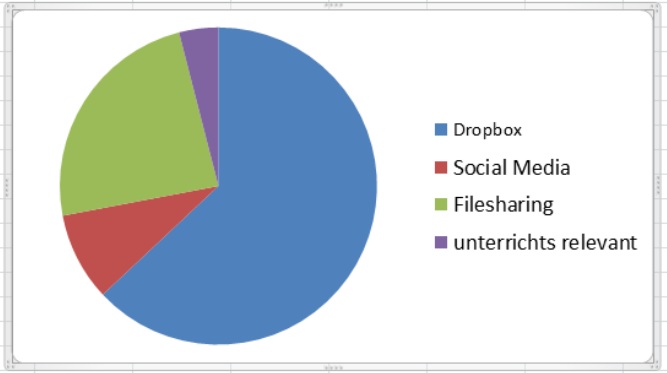
Von der Vision zur Projektidee

- Problemfelder
  - Datenschutz
  - Privatspähre versus Bildungsauftrag
  - Strafrechtsrelevante Delikte!
  - Wie soll ein Internetzugang „gestaltet“ werden?
    - Das Prinzip des Verbietens - und die Sache mit dem Aufwand!
    - Keine zentralen Vorgaben / Richtlinien?
    - Fachwissen?
    - Motivation der MitarbeiterInnen / SchülerInnen?

Von der Vision zur Projektidee

- Conclusio:
  - Wir benötigen Fakten und Zahlen!
  - Woher sollen die Daten kommen?
  - Ach ja: und der **Datenschutz**!
  - Mitarbeit von SchülerInnen!
  - Erster Ansatz: Syslog

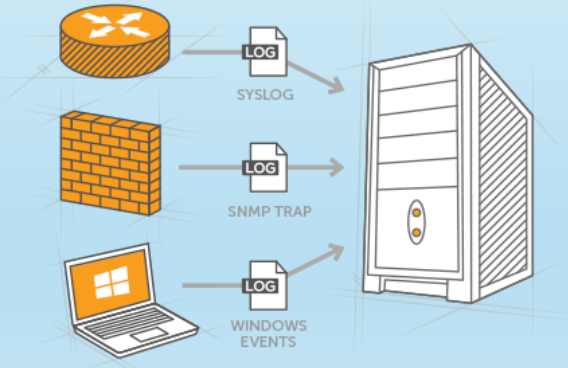
IP's	Counter
31.13.81.23	15516
66.220.152.19	6913
213.199.179.14	6298
213.199.179.15	6156
8.8.8.8	4996
173.194.70.120	4859
31.13.81.7	4751
31.13.86.16	4640
173.194.70.132	4491
173.194.70.139	4251
173.194.70.113	4157
173.194.70.138	4051
31.13.72.39	3980
173.194.70.100	3961
173.194.70.101	3884
173.194.65.95	3828



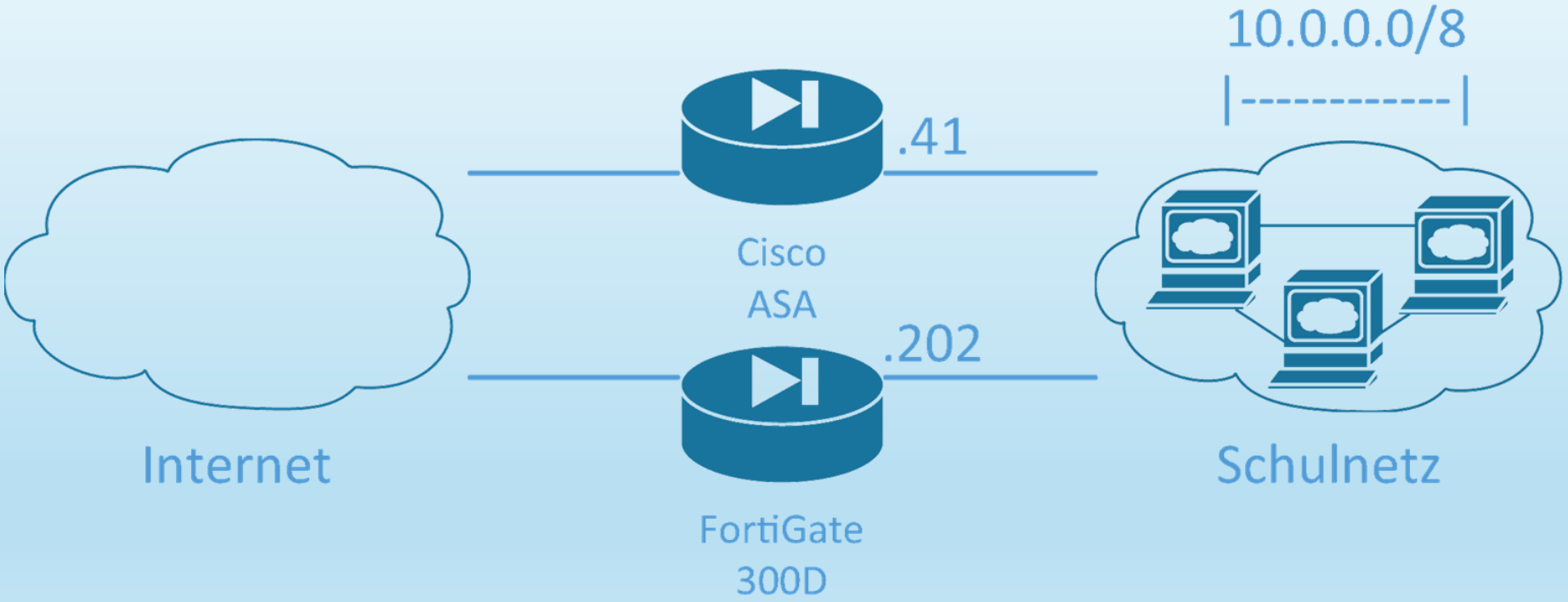
Die Projektidee :: Schritt 1

- Zentrale Auswertung von Syslogging
  - Dazu einmal Syslog „aktivieren“
  - Aber welcher Level / Intensität?
  - Auf welchen Geräten sollen Syslog betrieben werden?

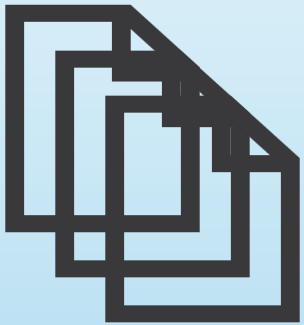
  - Ergebnis: Daten, Daten, Daten,…
  - Welche Hardware schafft das?
  - Datenschutz – Auftrag zur Datenverwaltung!?

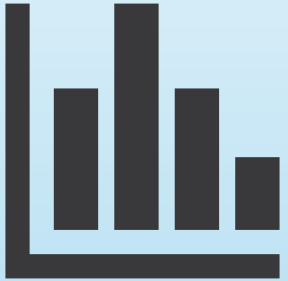


Erster Ansatz



Von Logfiles zur Auswertung





Von Logfiles zur Auswertung

- Welche Geräte „verursachen“ Traffic:
  - Cisco ASA
    - Serverlandschaft
    - Logumfang: 1.111.317 Zeilen; 659.163.564 Bytes (Stand: 09.01.2017)
  - FortiGate 300D
    - WLAN, Serverraum 078, verkabelte Klassen
    - Logumfang: 3.313.207 Zeilen; 1.926.514.346 Bytes (Stand: 09.01.2017)
  - 3 x Catalyst 4600
    - Schulnetz-Core
    - Logumfang: 37.317.209 Zeilen; 17.246.324.322 Bytes (Stnad: 10.01.2017)

Von Logfiles zur Auswertung

1

Beispiel-Logentry: *date=2017-01-13 time=10:43:14 srcip=10.14.81.11 srcport=53404 dstip=65.52.108.136 dstport=443 …*

2

date	time	srcip	srcport	dstip	dstport
13.01.2017	10:43.14	10.14.81.11	53404	65.52.108.136	443

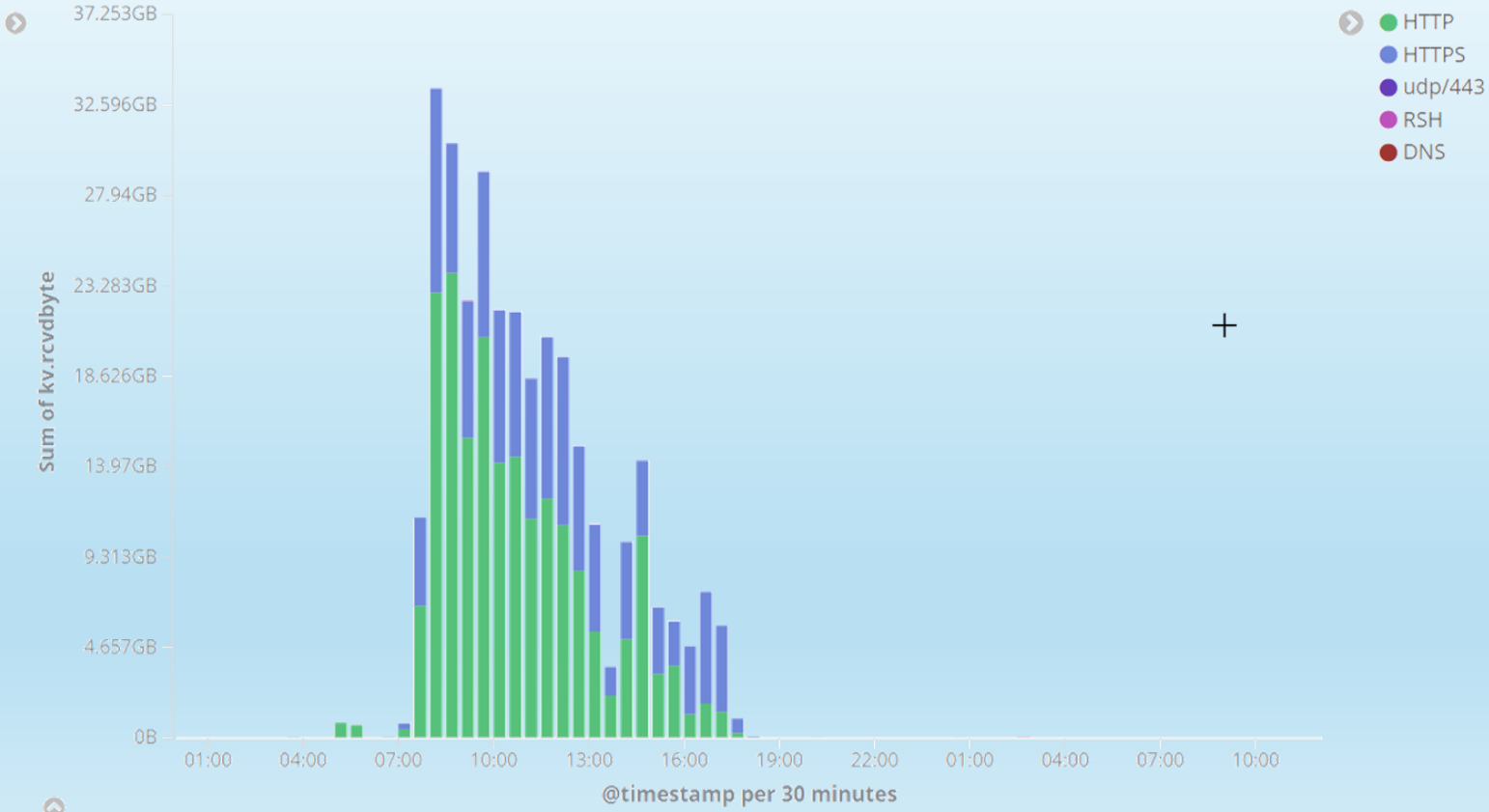
3

date	time	srcip	srcport	dstip	dstport
13.01.2017	10:43.14	WLAN Schulnetz	53404	United States	HTTPS

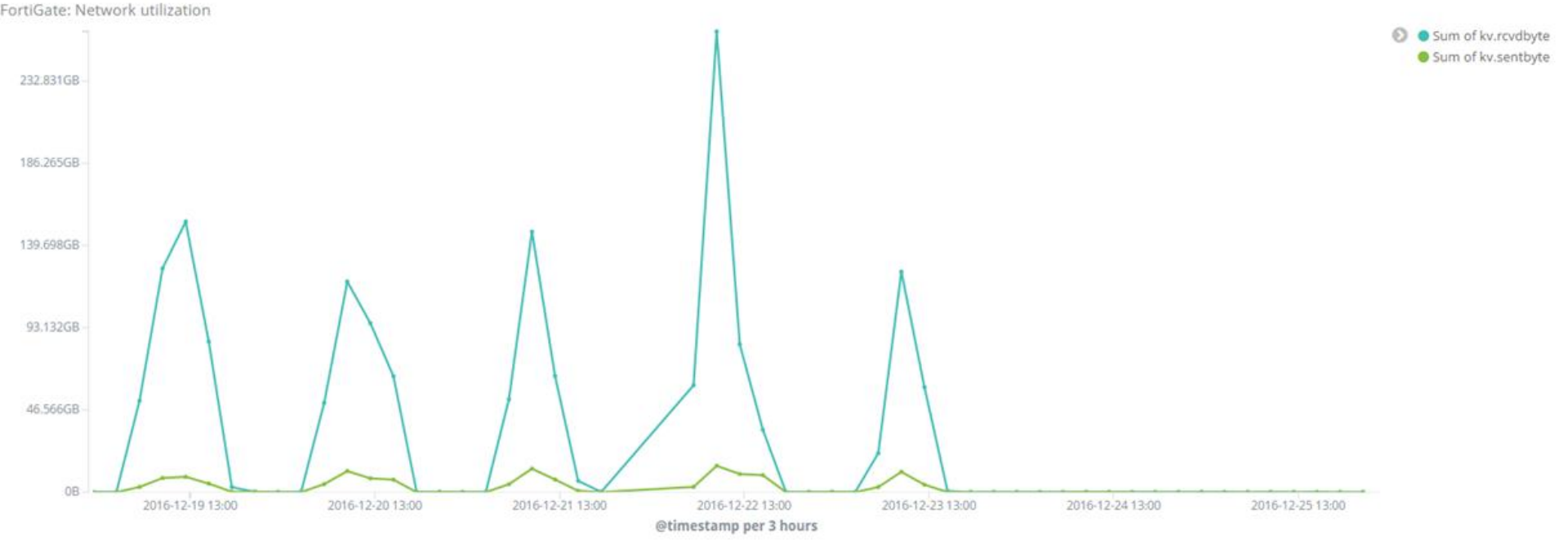
4

An die Datenbank senden

Ein erstes Ergebnis?



Ein erstes Ergebnis



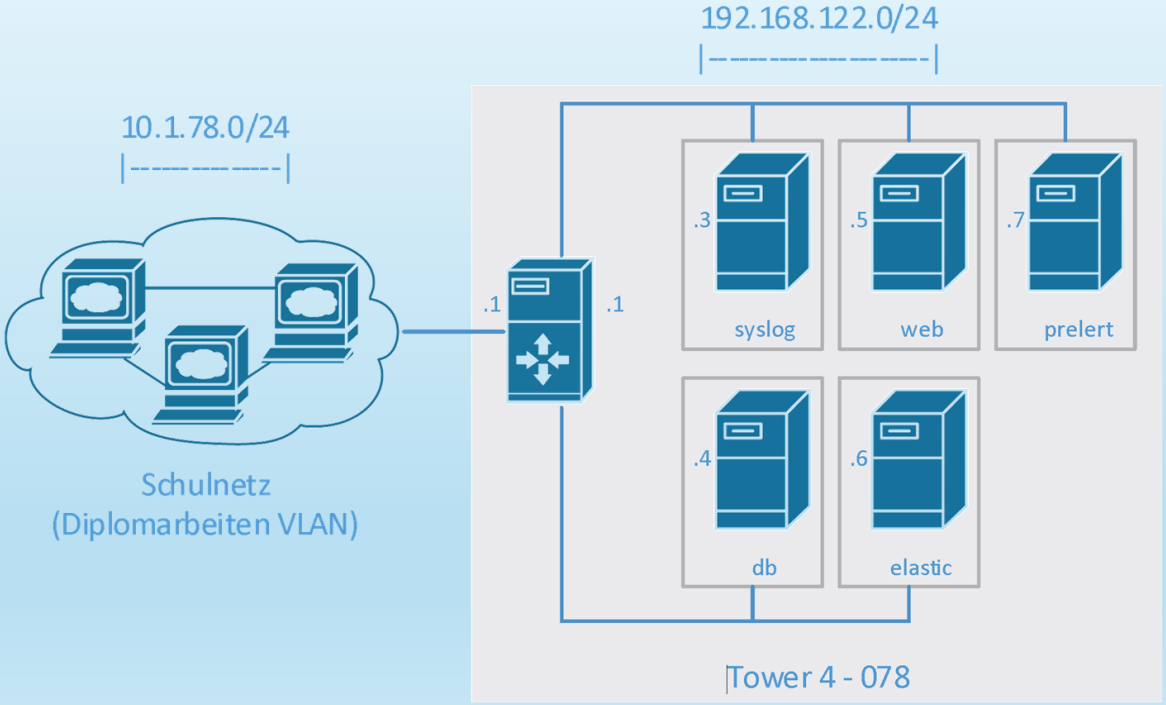
Ein erstes Ergebnis

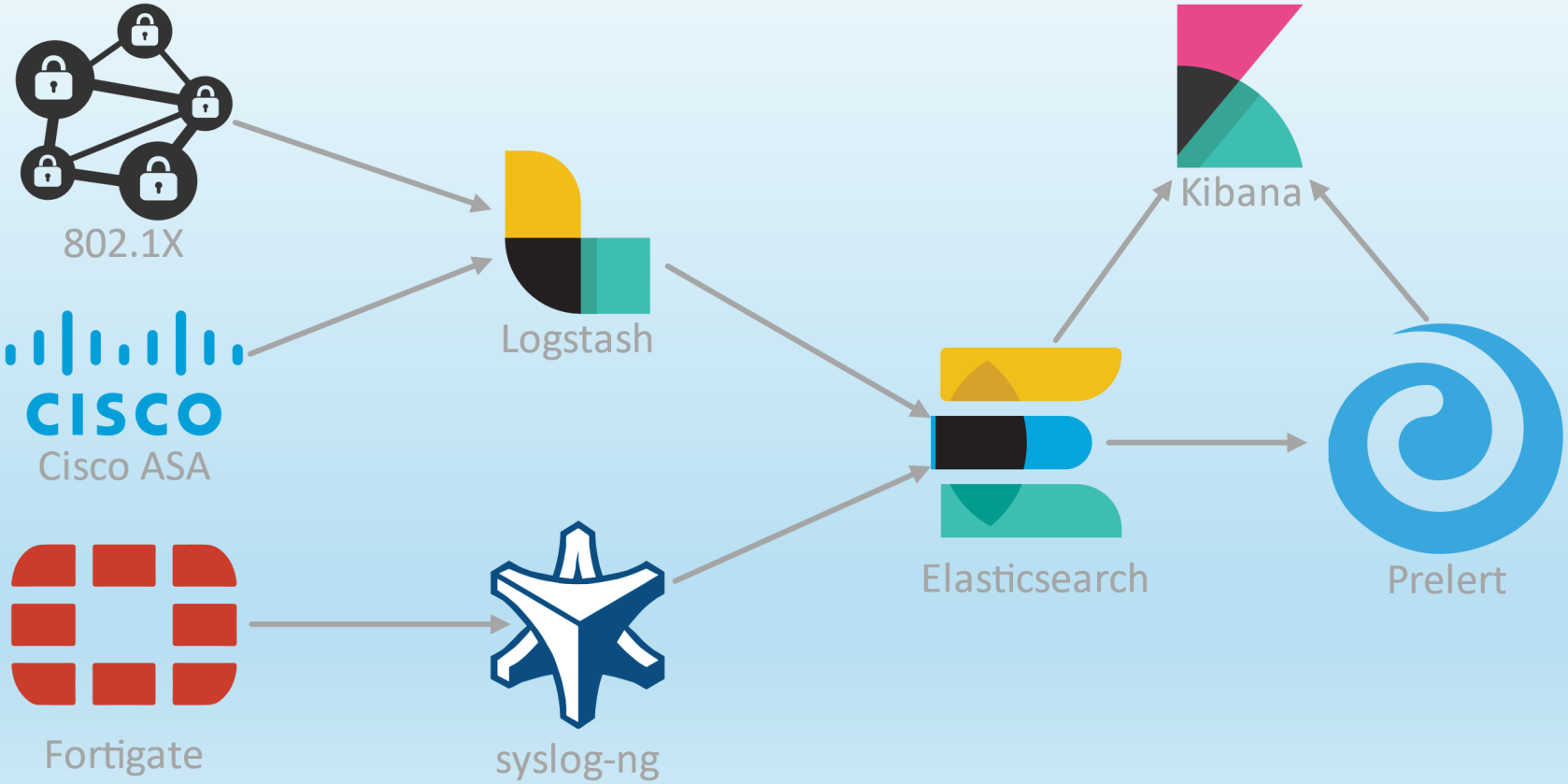
kv.srcip: Descending	Sum of kv.rcvdbyte	Sum of kv.sentbyte
10.14.75.189	48.315GB	890.355MB
10.2.45.30	26.802GB	489.322MB
10.14.79.185	24.569GB	293.154MB
10.0.0.114	24.09GB	1.397GB
10.14.78.229	22.071GB	419.981MB
10.2.45.28	16.889GB	318.188MB
10.14.82.208	15.785GB	303.934MB
10.2.61.59	14.892GB	57.95MB
10.14.76.31	11.962GB	240.256MB
10.14.80.182	11.764GB	252.867MB

Die Projektidee :: Schritt 1

- Typische Fragestellungen
  - Surferguy des Tages?
  - Top IP-Adressen
  - Top Googel-Suchwörter?
  - Anzahl von gleichzeitigen Sessions
  - „Lasterverteilung“ WLAN – „Festnetz“
  - Social Media Traffic

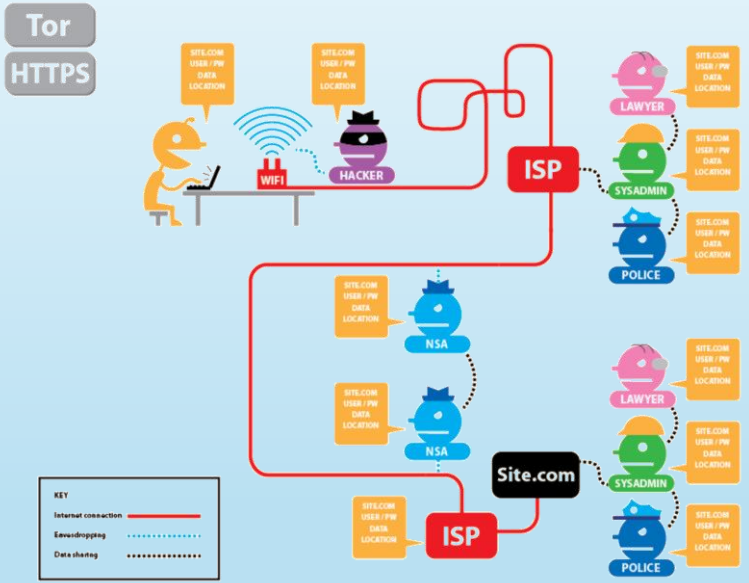
Send in more servers…




802.1X
CISCO
Cisco ASA
Fortigate
Logstash
syslog-ng
Kibana
Elasticsearch
Prelert

Die Projektidee :: Schritt 2

- Suchen wir Signaturen
  - Die Nadel im Heuhaufen!
  - Noch mehr syslogging
- Typische Fragestellungen
  - DNS Tunneling
  - Browsergames
  - Verschlüsselter Traffic?
  - Torrents?



Deep Learning

Ausblick

- Erweiterung auf weitere Standorte
  - Wer möchte dabei sein?
  - christian@schoendorfer.cc
- Suche nach leistungsfähiger Serverinfrastruktur
  - SAP
- Partnerschaft mit Herstellern
  - Know How Transfer: CISCO Systems
- IOT Security
  - KMX Bussysteme