DDoS Defense Mechanisms

Motivation

Distributed Denial of Service (DDoS)

Einfach in der Anwendung

Millionen Angriffe pro Tag und es werden mehr

Gliederung

IXP Scrubber [11]

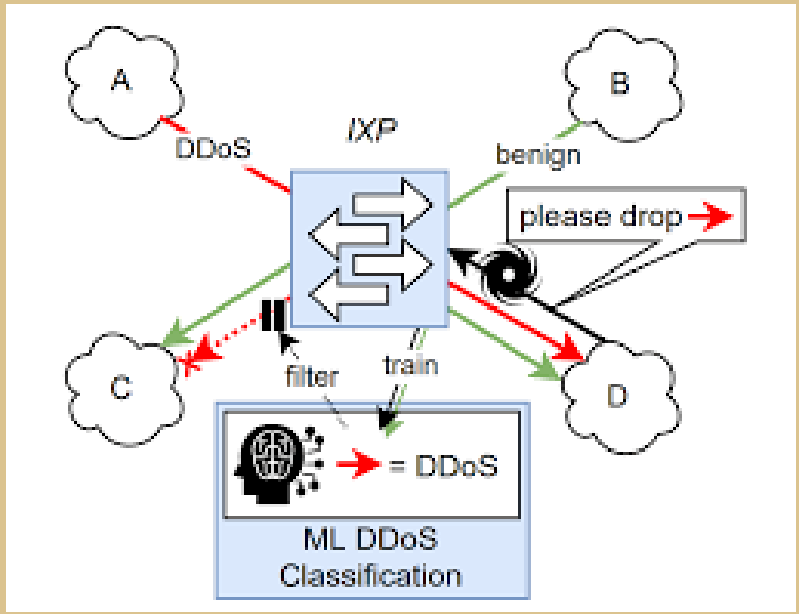


Abbildung 1

Gliederung

IXP Scrubber [11]

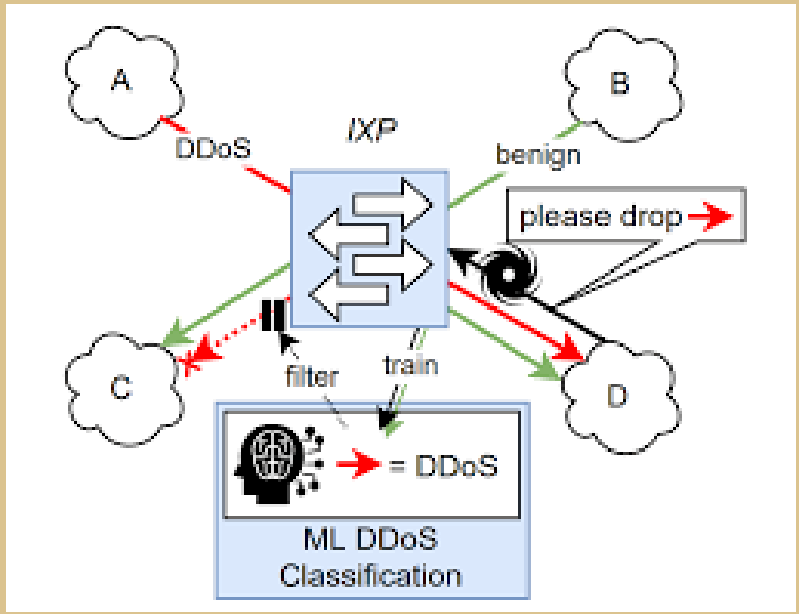
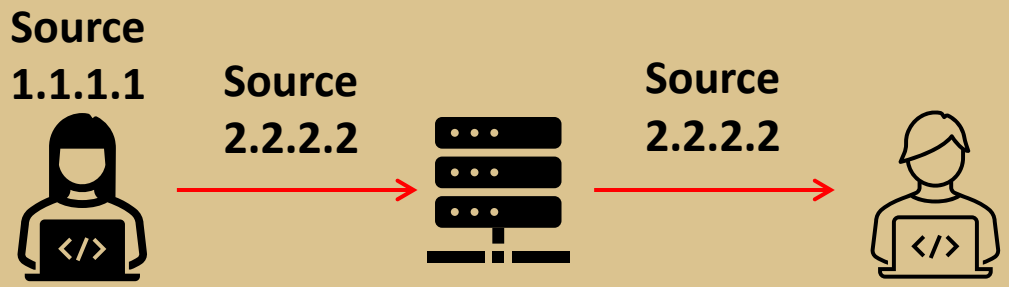


Abbildung 1

Source Address Validation



Überblick Internet

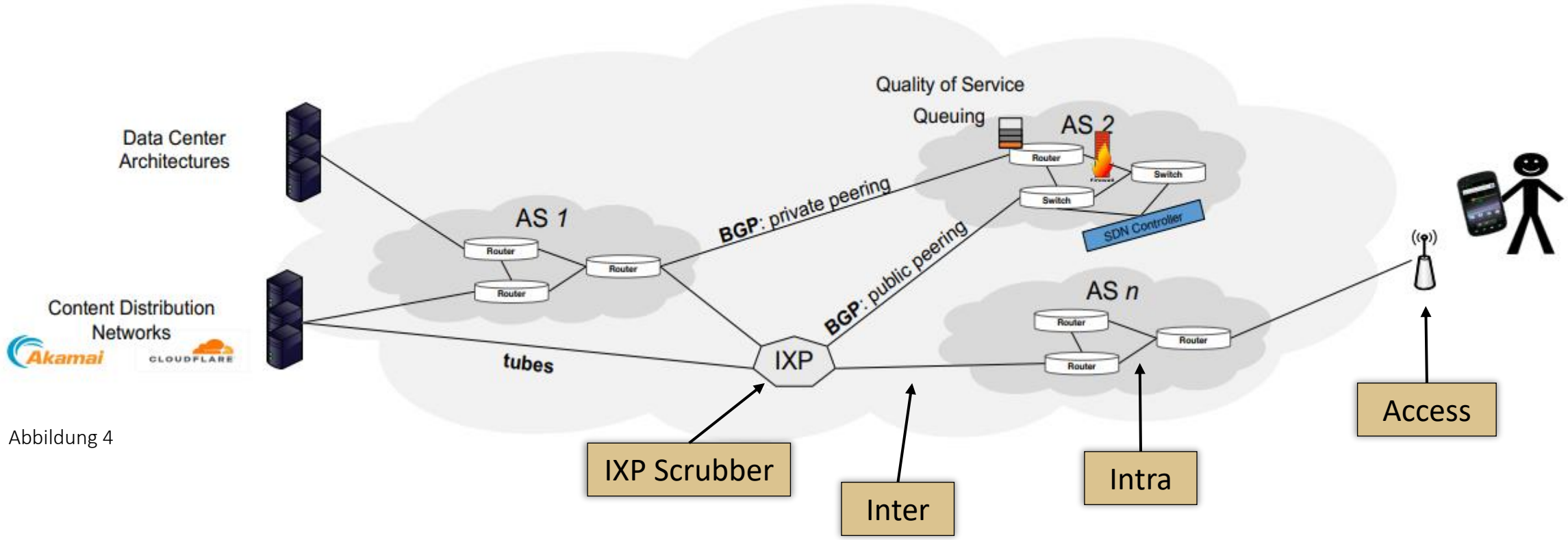


Abbildung 4

Training

ML Trainingset

- Daten von 5 IXPs
  - 3 Monate bis 2 Jahre
  - EU und US
- 200M Daten nach Vorverarbeitung

Trainiert das Model

trainieren

Training

ML Trainingset

- Daten von 5 IXPs
  - 3 Monate bis 2 Jahre
  - EU und US
- 200M Daten nach Vorverarbeitung

Self Attack Set

- Selbst erzeugte Daten
  - dedizierte Infrastruktur
  - DDoS-for-hire-services
- 700k Daten

Trainiert das Model

trainieren → validieren

Validiert Model auf Trainingsset, um Bias zu reduzieren

Klassifikation

Klassifikation

Mikroskopische Ebene

Ziel: blackhole anfällige Anfragen erkennen

- Association Rule Mining (ARM)

Bsp: {src_port=12;packet_size=5} -> {blackhole}

- Regeln werden minimiert
- Experten können korrigieren mit UI
- Hyperparameter

Klassifikation

Mikroskopische Ebene

Ziel: blackhole anfällige Anfragen erkennen

- Association Rule Mining (ARM)

Bsp: {src_port=12;packet_size=5} -> {blackhole}

- Regeln werden minimiert
- Experten können korrigieren mit UI
- Hyperparameter

Makroskopische Ebene

Ziel: Angegriffene Hosts erkennen => Verkehr stoppen

- Weight of Evidence (WoE):
  - oft in blackhole => positiver score
  - nicht in blackhole => negativer score

Evaluation

Leistung

- Fünf verschiedene ML Klassifikatoren
- XGBoost: höchste Leistung

Retraining

- Tägliches neu lernen, um Leistung beizubehalten

=> neue Angriffsvektoren lernen

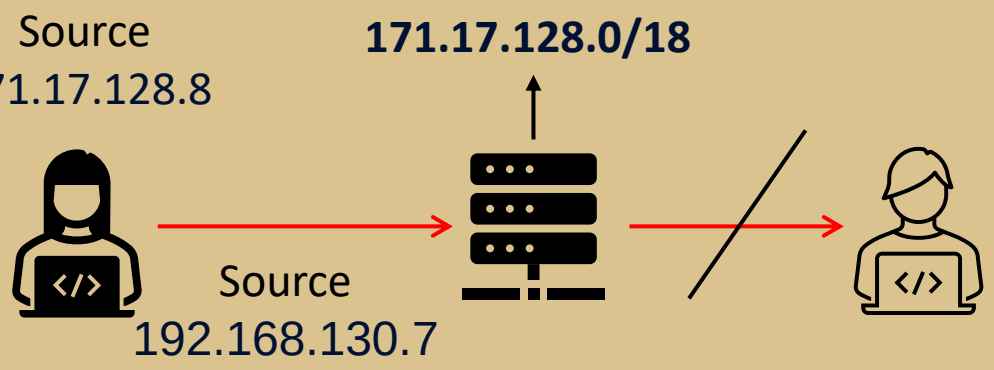
Geographische Lage

- Klassifikator bleibt
- WoE wird lokal generiert

=> sehr wenig Einbüse

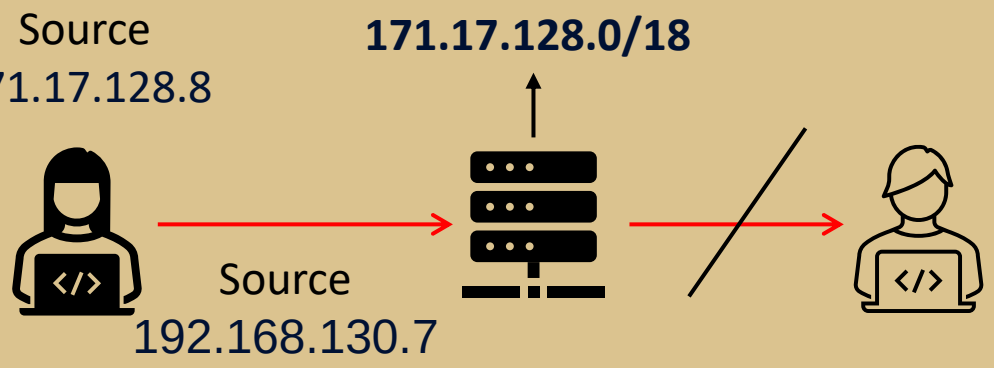
Source Address Validation – IP Spoofing

BCP 38 – Ingress Filter [19]



Source Address Validation – IP Spoofing

BCP 38 – Ingress Filter [19]



BCP 84 – IF for Multihomed Networks [20]

- Access Control Lists
  - Steht Präfix in der Liste?
- Strict Reverse Path Forwarding
  - Forwarding Information Base (FIB)
  - Richtige Schnittstelle

outbound SAV

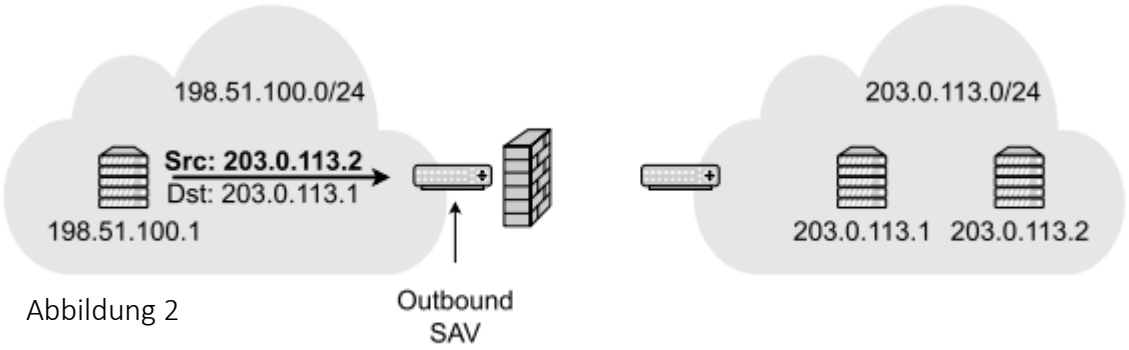


Abbildung 2

inbound SAV

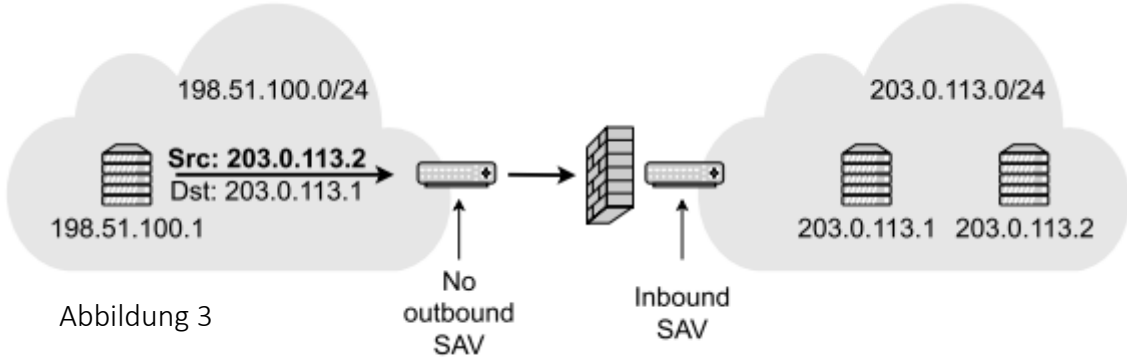


Abbildung 3

Aktueller Stand

Nicht weit verbreitet [2] [13] [23]:
- fehlender Wirtschafsreiz
- Ressourcenintensiv
- keine Regularien
- zu viel Filtern
- hängen hinterher

Aktueller Stand

Nicht weit verbreitet [2] [13] [23]:
- fehlender Wirtschafsreiz
- Ressourcenintensiv
- keine Regularien
- zu viel Filtern
- hängen hinterher

Mutually Agreed Norms for Routing Security
- Initiative aus Experten
- Bietet Lösungen für Bedrohungen
- Reichweite für SAV

Aktueller Stand

Nicht weit verbreitet [2] [13] [23]:
- fehlender Wirtschafsreiz
- Ressourcenintensiv
- keine Regularien
- zu viel Filtern
- hängen hinterher

Mutually Agreed Norms for Routing Security
- Initiative aus Experten
- Bietet Lösungen für Bedrohungen
- Reichweite für SAV

SAV in China [14] [22] [23]
- großes Ziel für DDoS-Angriffe
- viele Angriffe kommen her
- wenig Schutz vor Spoofing

Die Zukunft

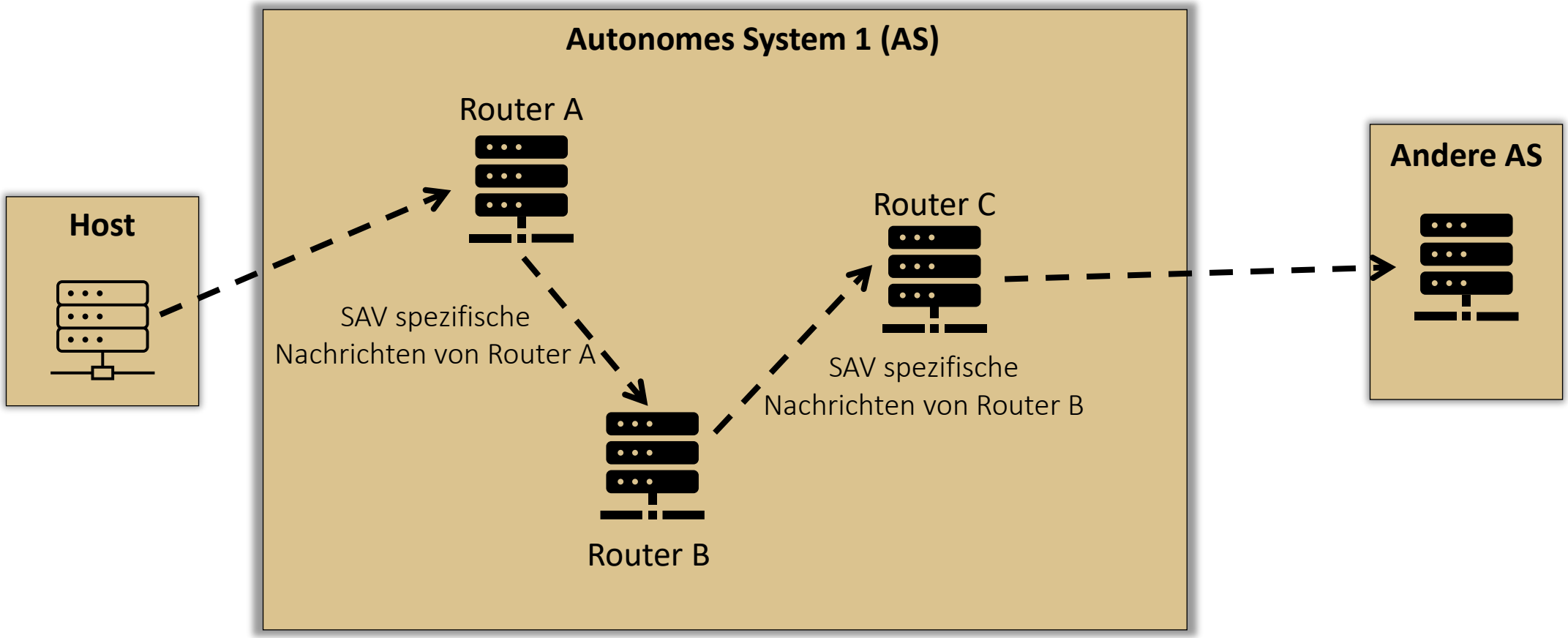
Internet Engineering Task Force
- regelmäßige Treffen
- neue Internetstandards
- Internet sicherer machen

Die Zukunft

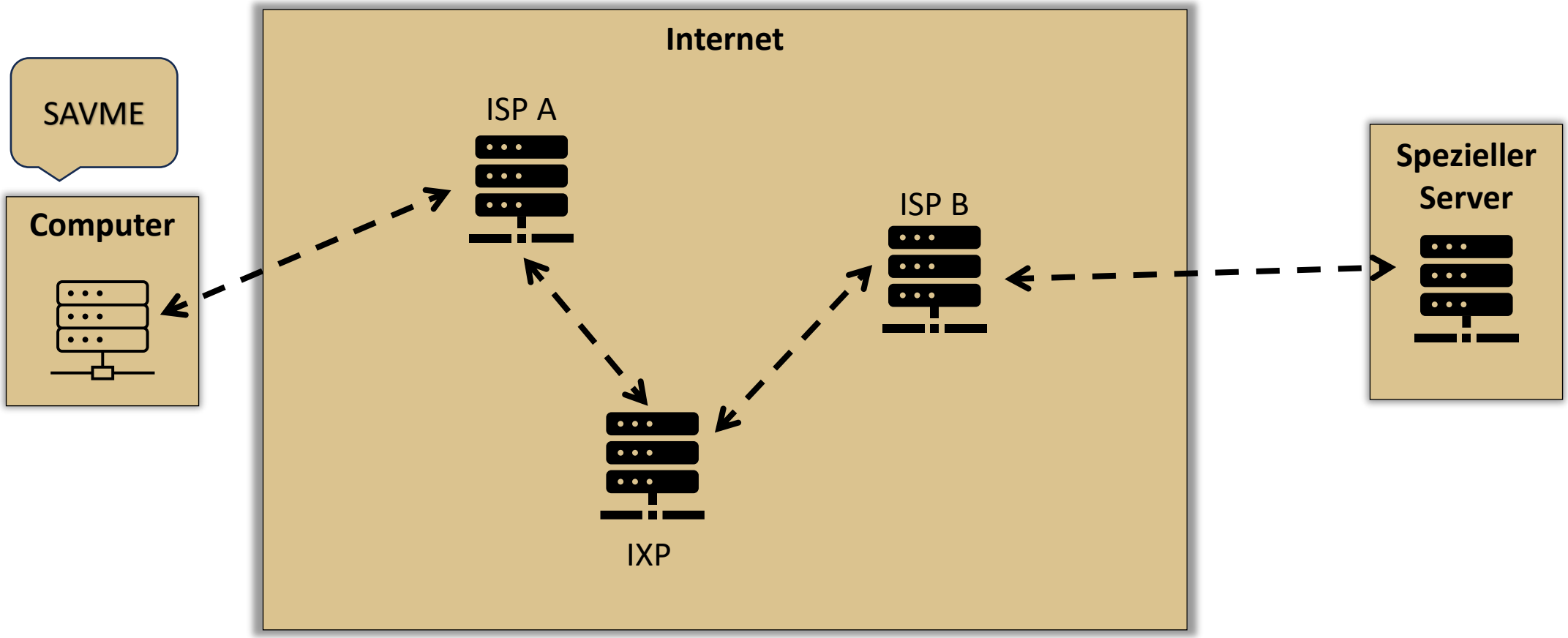
Internet Engineering Task Force
- regelmäßige Treffen
- neue Internetstandards
- Internet sicherer machen

Anforderung für neue SAV-Methoden [5]
- automatisch Aktualisieren
- präzise Validierung
- Effektiv, auch wenn nicht vollständig implementiert
- IPv4 und IPv6
- keine neuen Sicherheitslücken
- weniger Arbeit

Intra-domain SAV (SAVNET) Architecture [6]



A Large-scale Measurement of IP Source Spoofing on the Internet [23]



Fazit

Aktueller Stand
- Herausforderung DDoS-Angriffe
- BCP 38 und 84 weisen Schwächen auf [5]
- IXP Scrubber
- SAV wenig im Einsatz

SAV braucht mehr Reichweite
- MANRS
- mehr SAV Einsatz

=> weniger DDoS-Angriffe

weitere Forschung
- IEFT
- neue und bessere SAV-Methoden
- einfacher in der Anwendung
- Internet wird Sicherer

Referenzen

Abbildung 1: Matthias Wichtlhuber (u.a.) IXP Scrubber auf Seite 1 https://doi.org/10.1145/3544216.3544268
Abbildung 2 und 3: Yevheniya Nosyk (u.a.) The Closed Resolver Project auf Seite 3 https://doi.org/10.1109/TNET.2023.3257413
Abbildung 4: Moodle Kurs „Architektur und Dienste des Internets SoSe 2023“ https://moodle.uni-kassel.de/course/view.php?id=9032