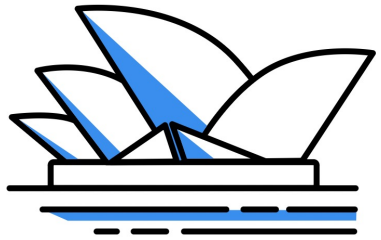
Enabling Trustworthy Network Outsourcing

Guyue Liu

Peking University

2024.8

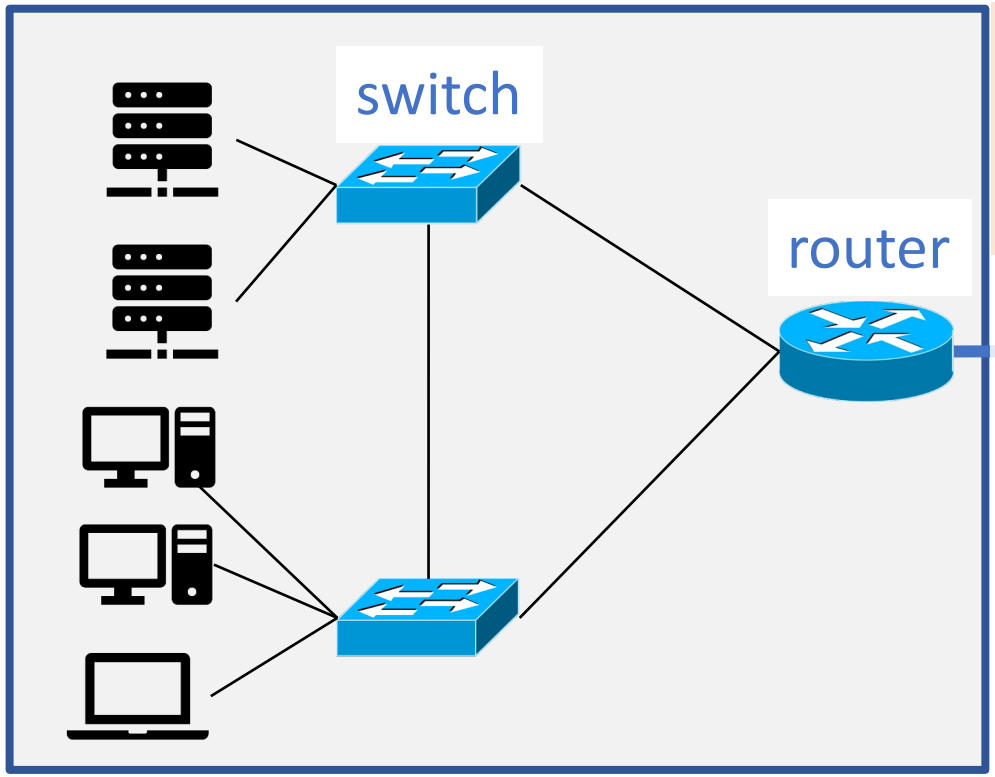
北京大学
PEKING UNIVERSITY



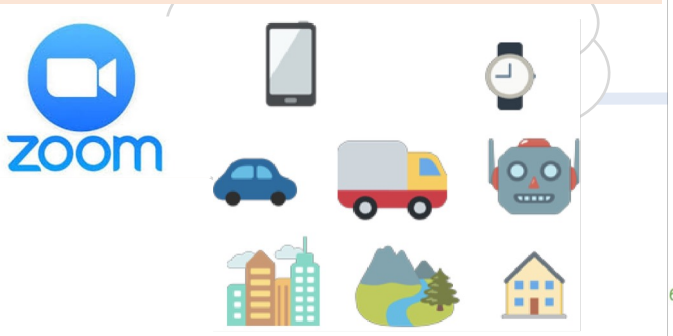
APNet
2024

New Challenges for the Network

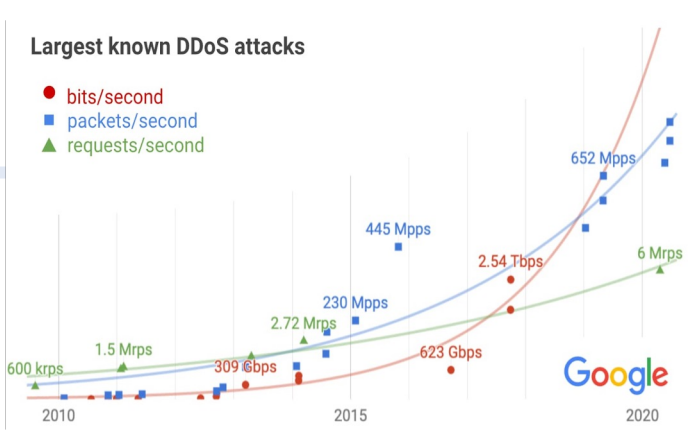
Enterprise Network



New applications and devices
e.g., video, IoT

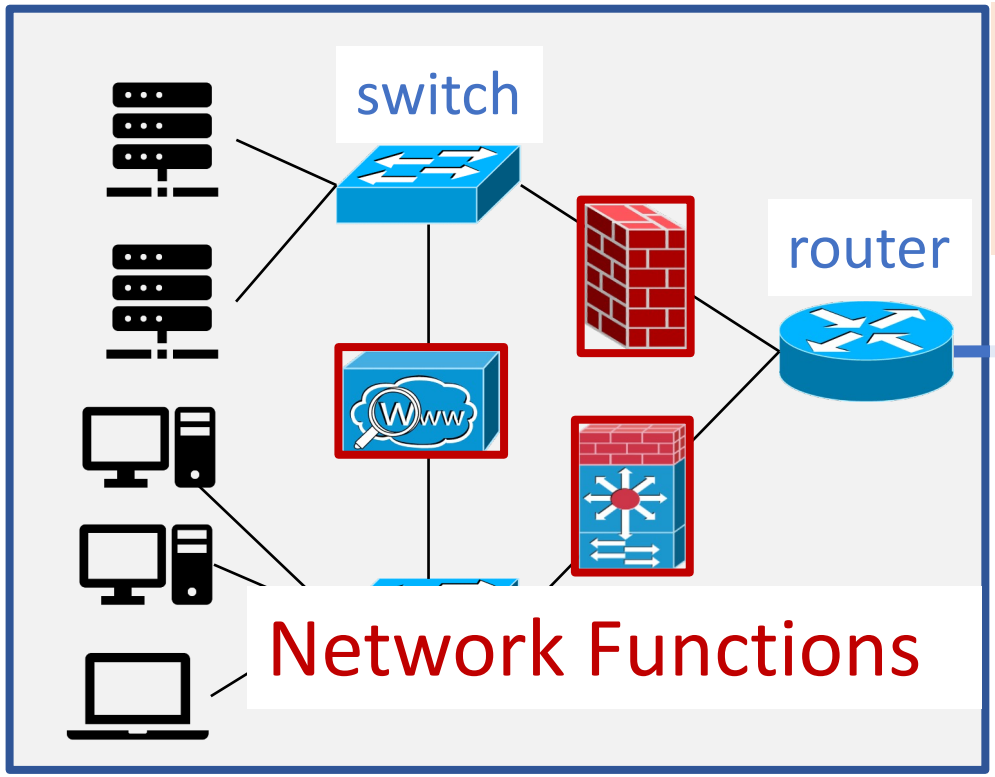


New vulnerabilities and attacks

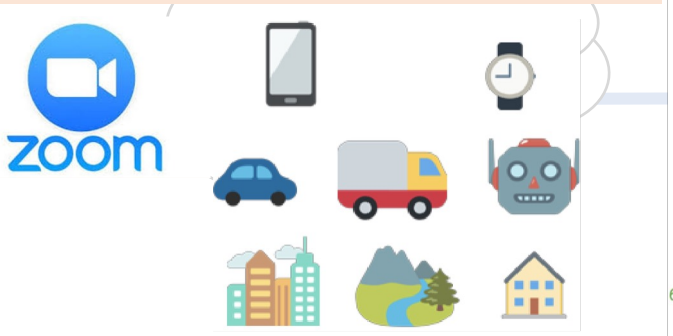


Increasing Complexity of the Network

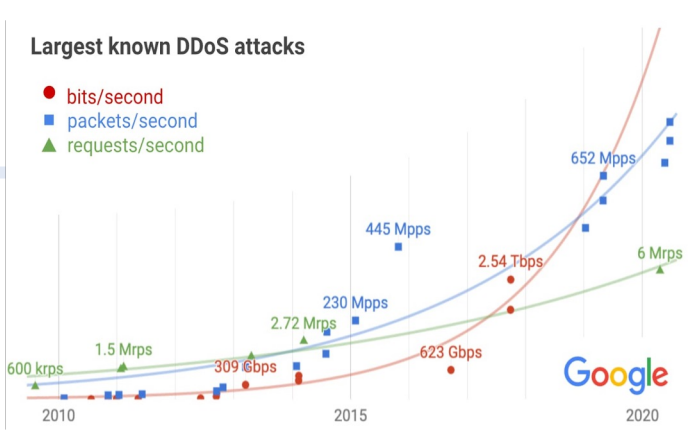
Enterprise Network



New applications and devices
e.g., video, IoT



New vulnerabilities and attacks



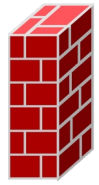
Enterprises Are Outsourcing Network Tasks

Costs

Outsourcing
reduces operational
and capital costs

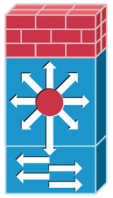
Popular Outsourcing Models

1. Outsourcing Network Functions



Firewall

Load Balancer



VPN

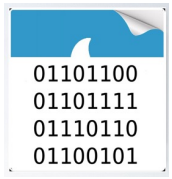
2. Outsourcing Network Services

Troubleshooting

Configuration

Monitoring

3. Outsourcing Network Data

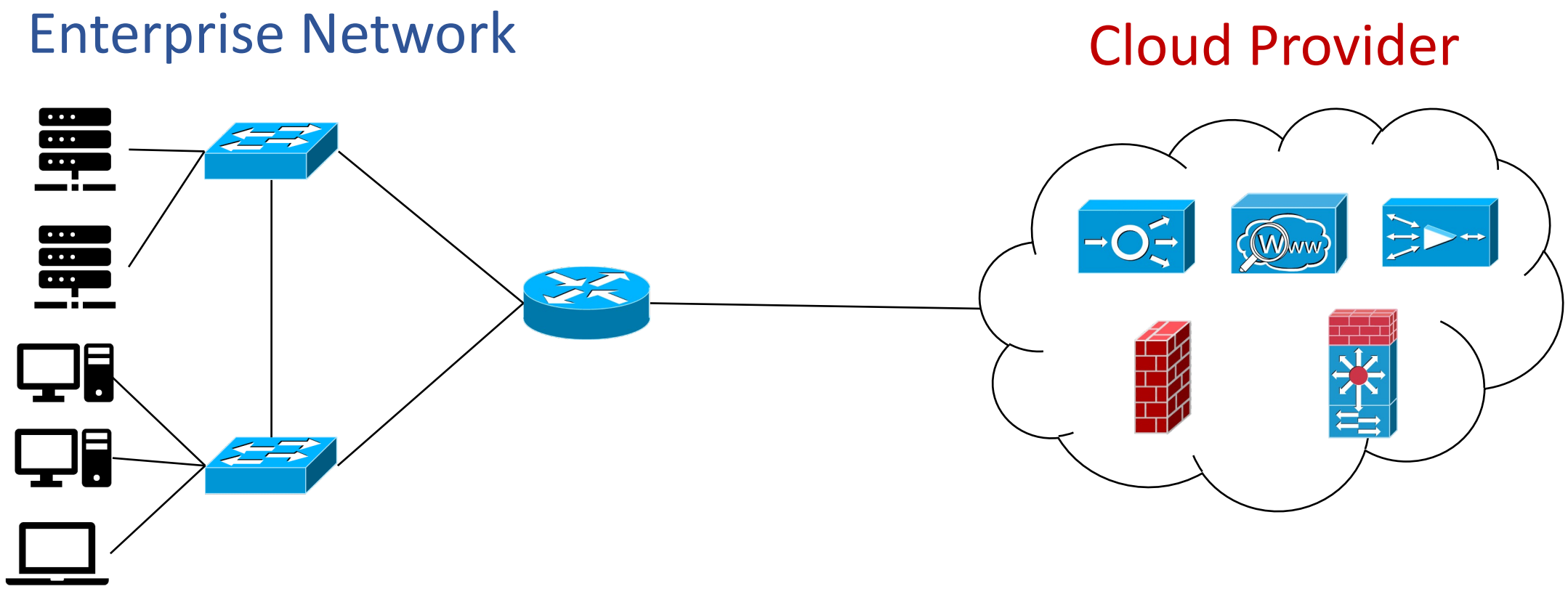


Trace

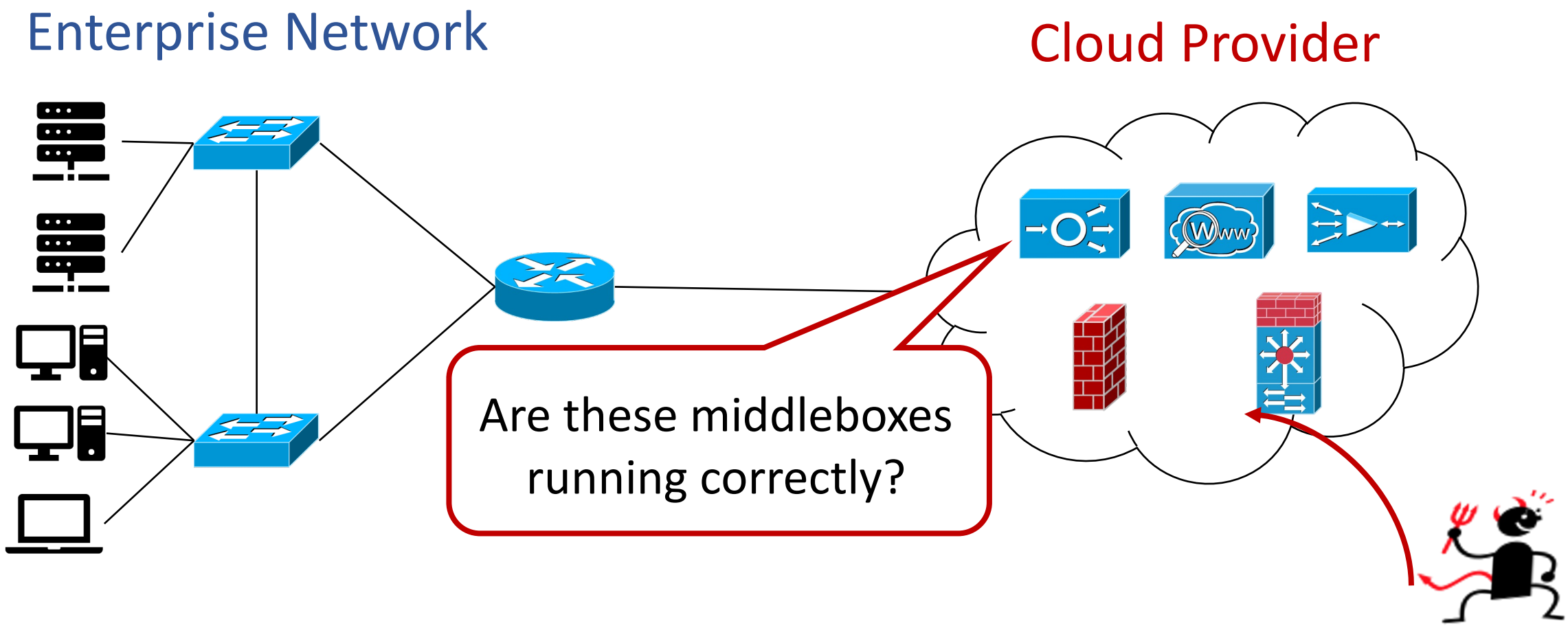
Log

Configuration

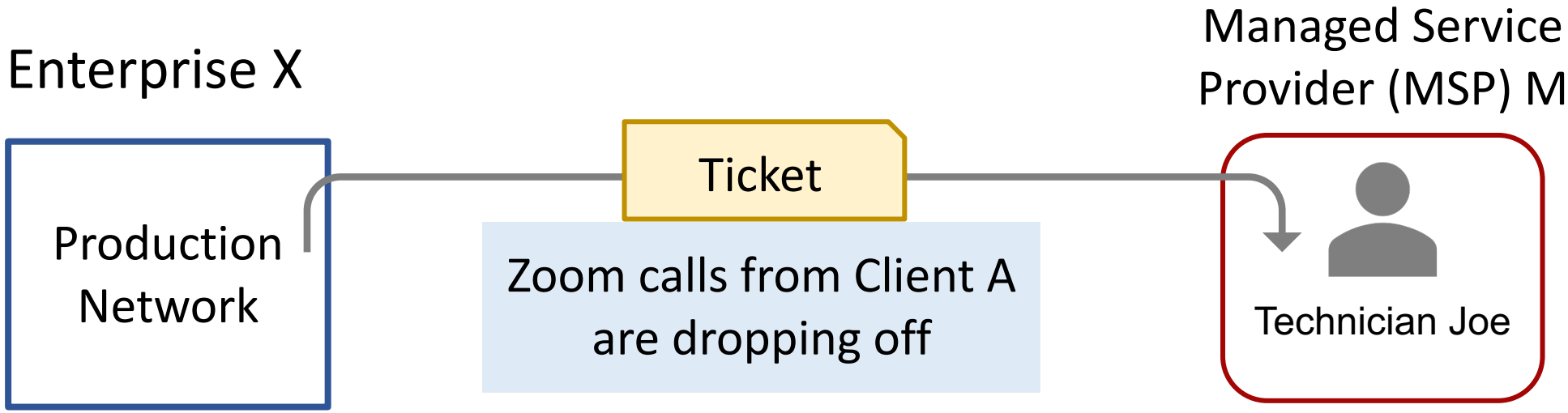
Scenario #1: Outsourcing Network Functions



Valuable, but raises security concerns



Scenario #2: Outsourcing Network Services

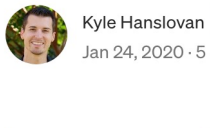


356.24 billion dollars market size by 2025

(Statista)

Outsourcing Workflows Today Are Not Secure

Validating the SolarWinds N-central "Dumpster Diver" Vulnerability



Kyle Hanslovan Follow

Jan 24, 2020 · 5 min read

ZDNet

VIDEOS WINDOWS 10 5G BEST V

MUST READ: Ransomware as a service is the new big problem for business

Ransomware gang hacks MSPs to deploy ransomware on customer systems

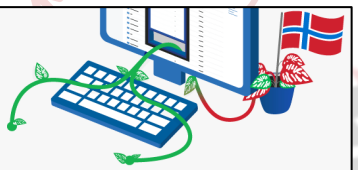
Hackers breach MSPs and use Webroot SecureAnywhere console to infect customer PCs with the Sodinokibi ransomware.

By Catalin Cimpanu for Zero Day | June 20, 2019 -- 23:49 GMT (16:49 PDT) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
Chrome will s

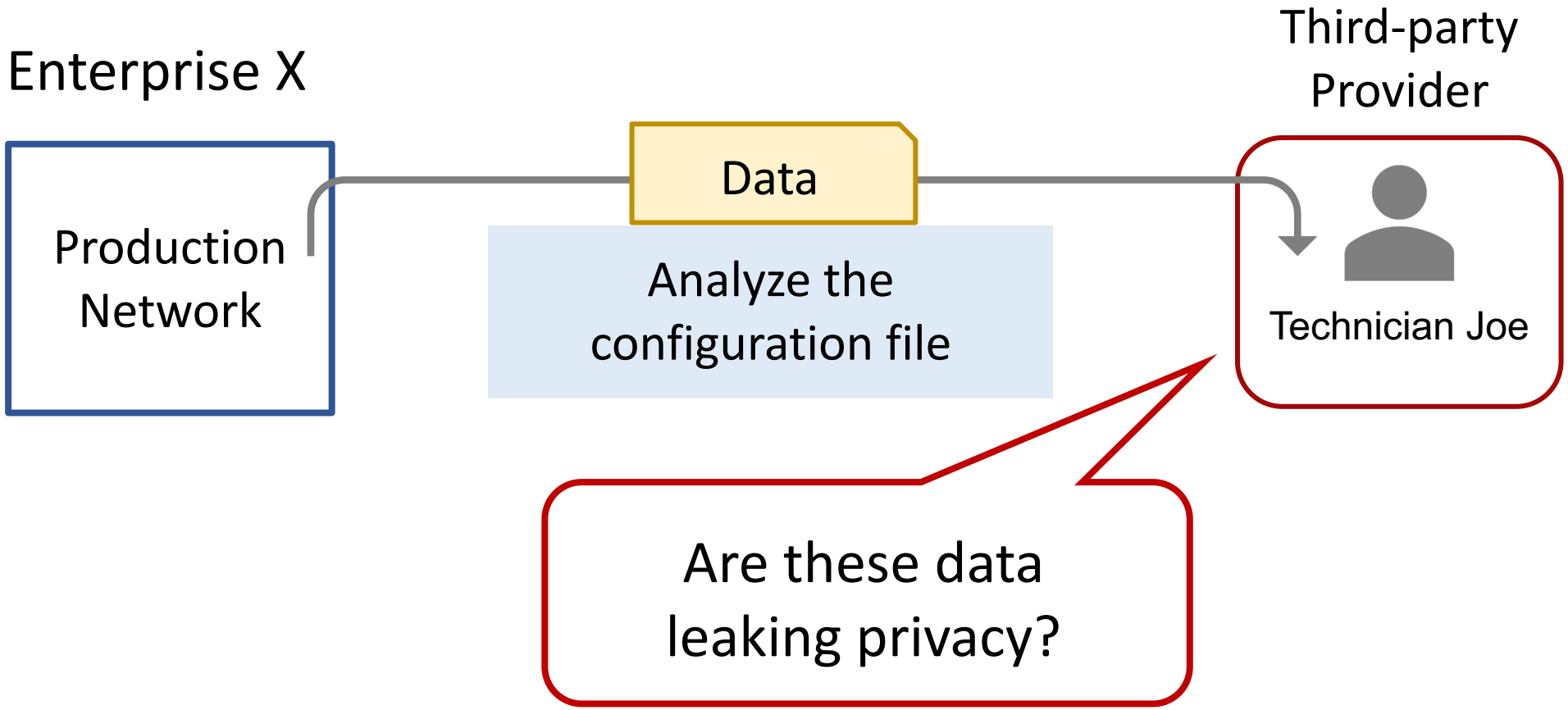
Recorded Future®



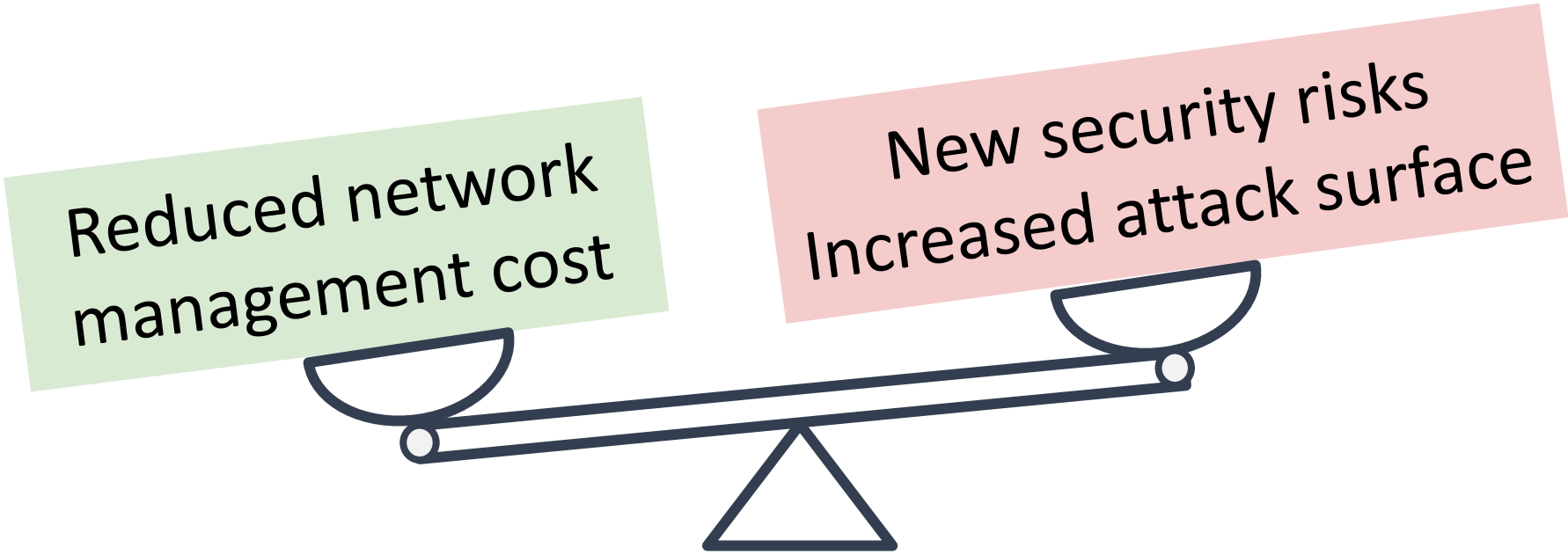
APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign

FEBRUARY 6, 2019 • INSIKT GROUP

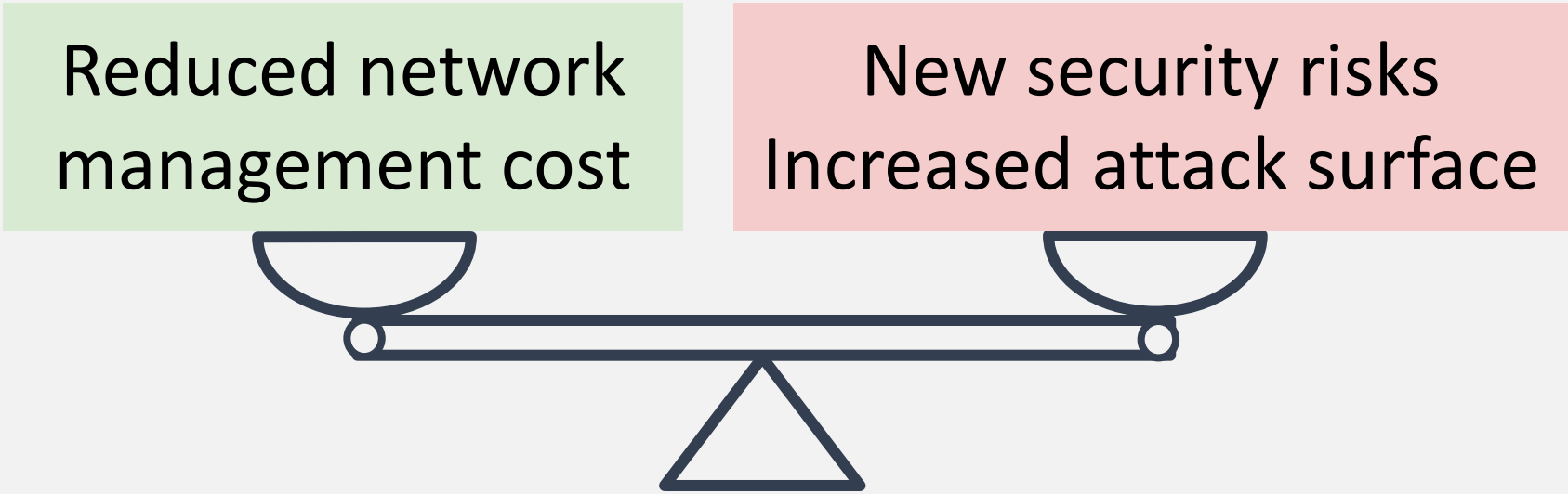
Scenario #3: Outsourcing Network Data



The Reality


Reduced network management cost
New security risks
Increased attack surface

My Vision


Reduced network management cost
New security risks
Increased attack surface

Trustworthy Network Outsourcing

Building systems that enable trustworthy network outsourcing

- Practical systems with
- Correctness guarantees

This Talk

AuditBox (NSDI' 21)

Auditing virtualized network functions

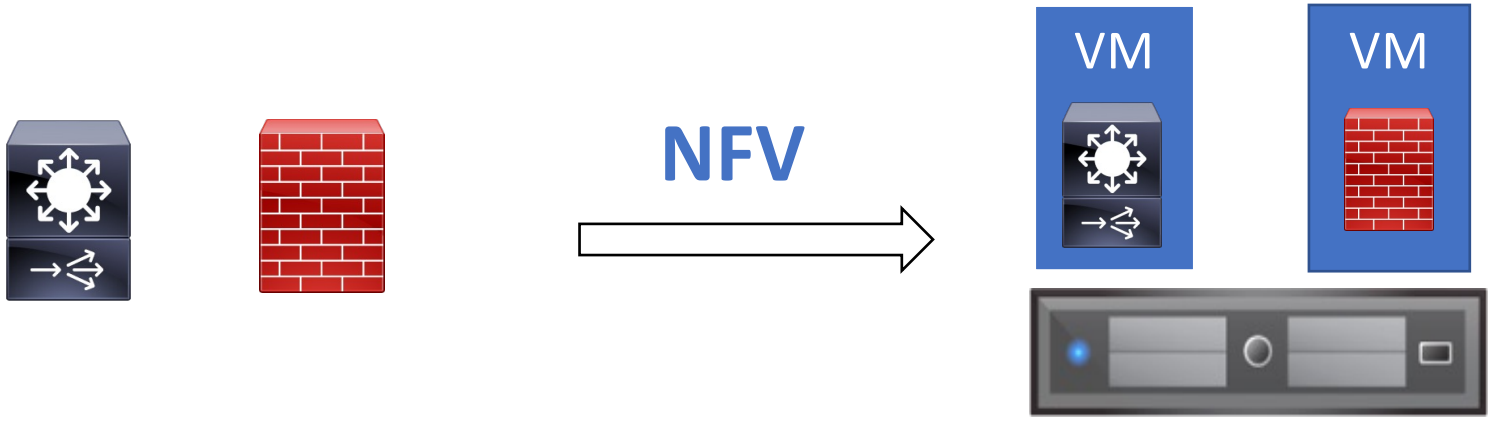
Heimdall (NDSS'24*)

Risk-aware outsourcing of configuration management

ConfMask (SIGCOMM'24)

Privacy-preserving configuration sharing via anonymization

Network Function Virtualization (NFV)



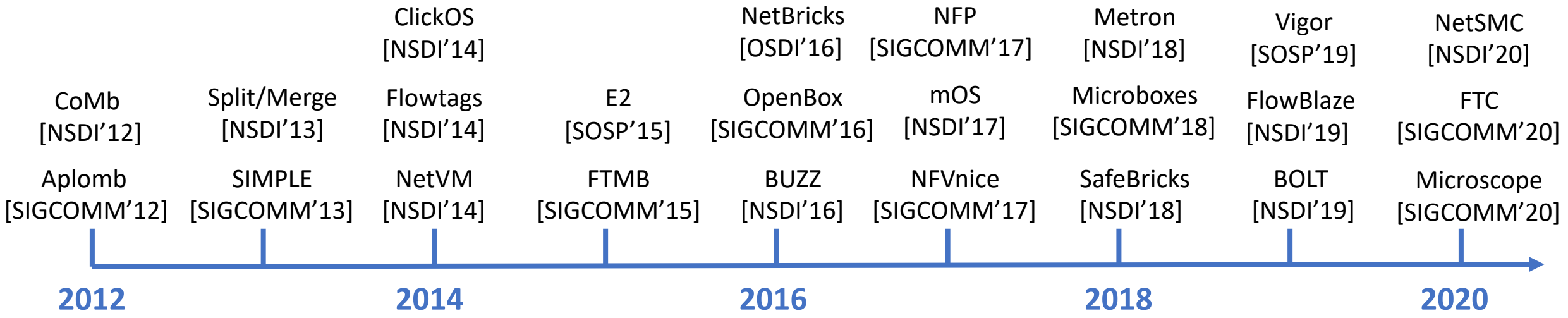
Specialized Appliances

— Closed, proprietary
— High Costs
— Inflexible deployment
— Hard to extend

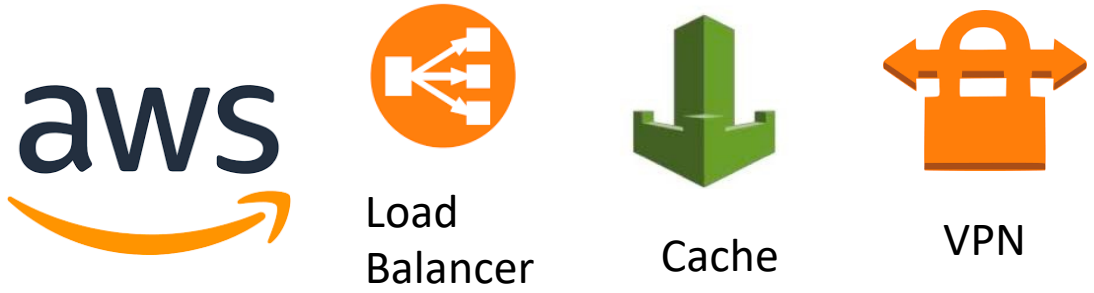
Commodity Server

+ Open, standard based
+ Reduce Costs
+ Easy to deploy
+ Extensible

Academia Efforts To Promote NFV



Cloud-based Network Functions



Enterprises Are Reluctant To Adopt NFV

NFV

Current NFV Deployments Are Not Auditable

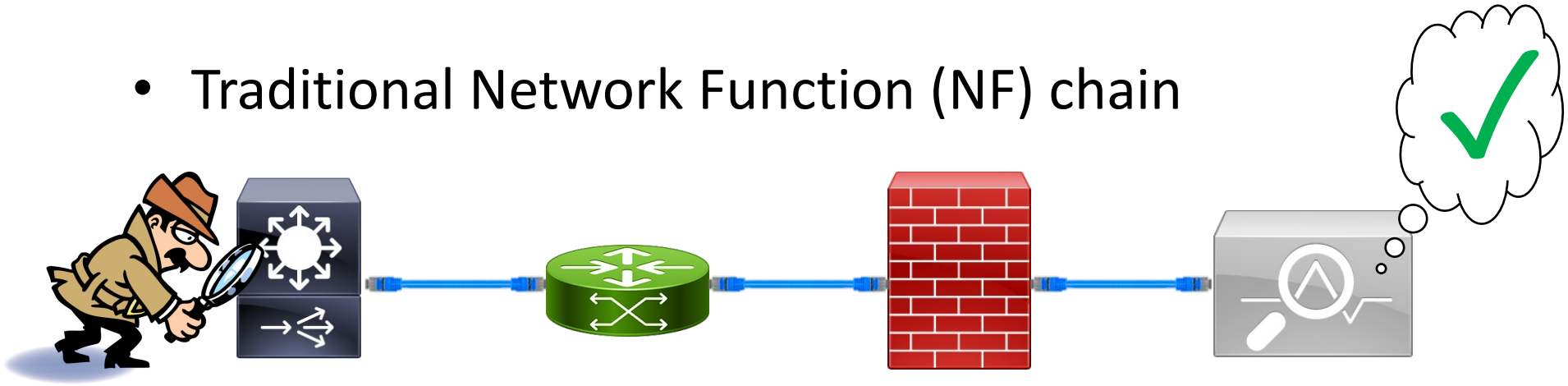
NFV

Why?

Cannot meet government and industrial regulations requirements, e.g., HIPAA, FERPA, GDPR, and PCI.

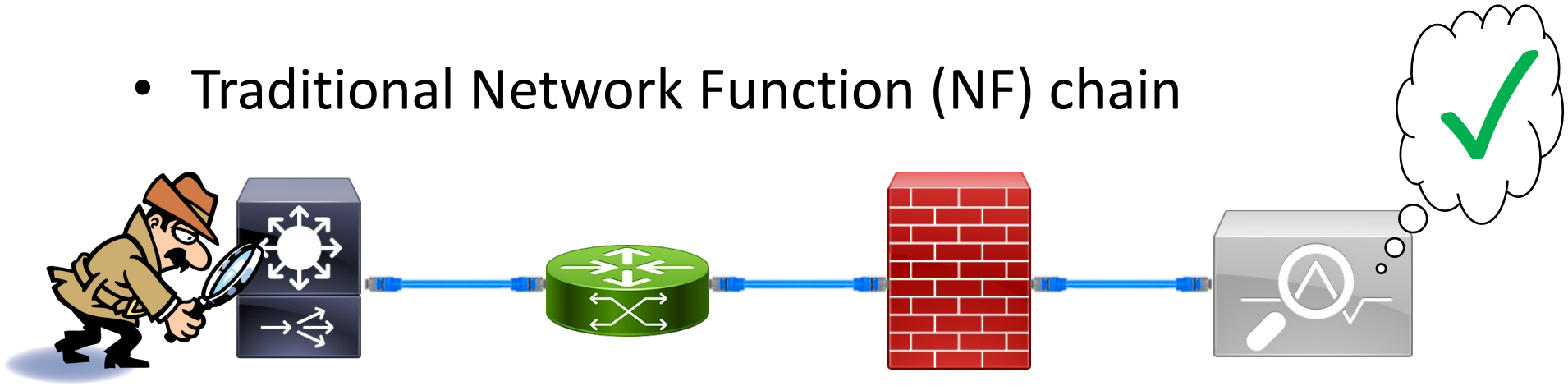
Traditional Auditing Approach

- Traditional Network Function (NF) chain

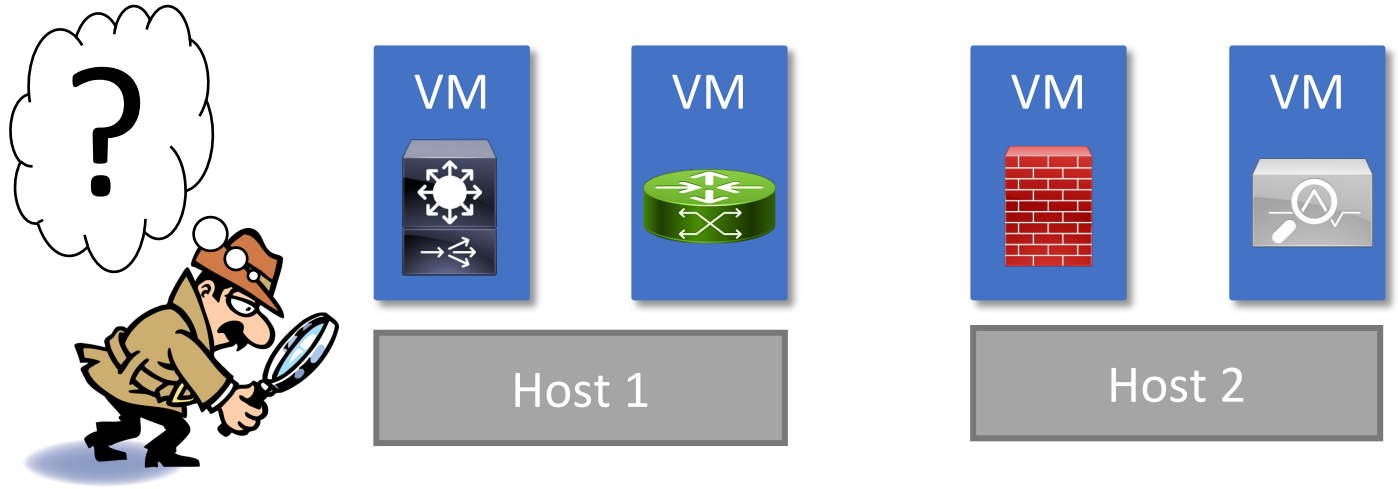


No Existing Tools To Audit Virtualized NFs

- Traditional Network Function (NF) chain



- Modern virtualized NF chain



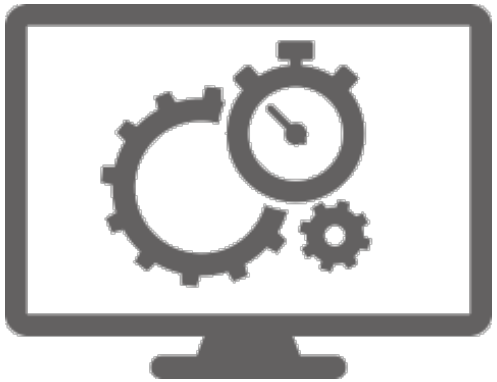
AuditBox Contribution

Offer missing capabilities to audit NFV deployments

Time-of-check-to-time-of-use vulnerabilities

Coarse, manual correctness checks

Provable, continuous assurance of correctness



AuditBox Contribution

- Offer missing capabilities to audit NFV deployments

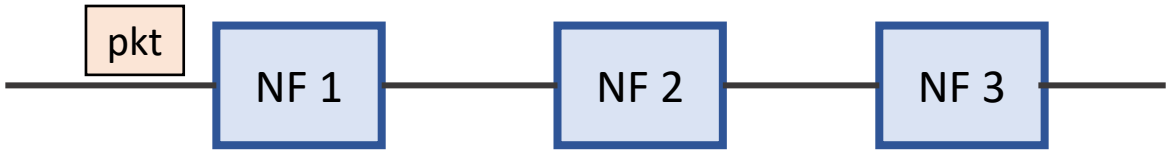
Coarse, manual correctness checks

Provable, continuous assurance of correctness

correctness?

What Does Correctness Mean?

- **Runtime Correctness** = Network implements the intended NF forwarding policies
  - **Packet correctness**
  - **Flow correctness**



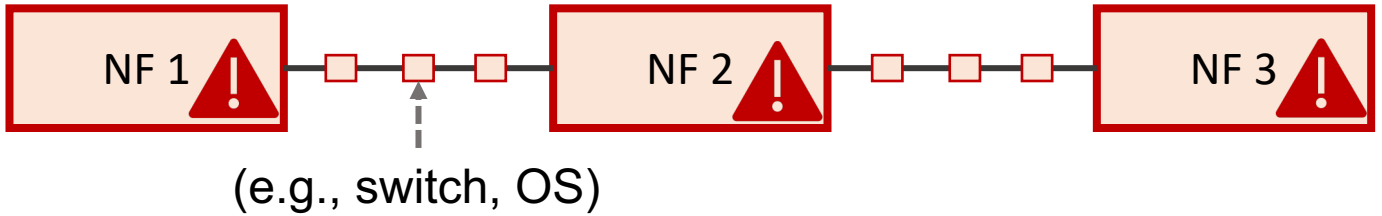
- **Offline Auditability** = Must provide a **tamper-proof** 'audit trail'

Outline

1. Motivation
2. Our Insight
3. AuditBox Design
4. Evaluation

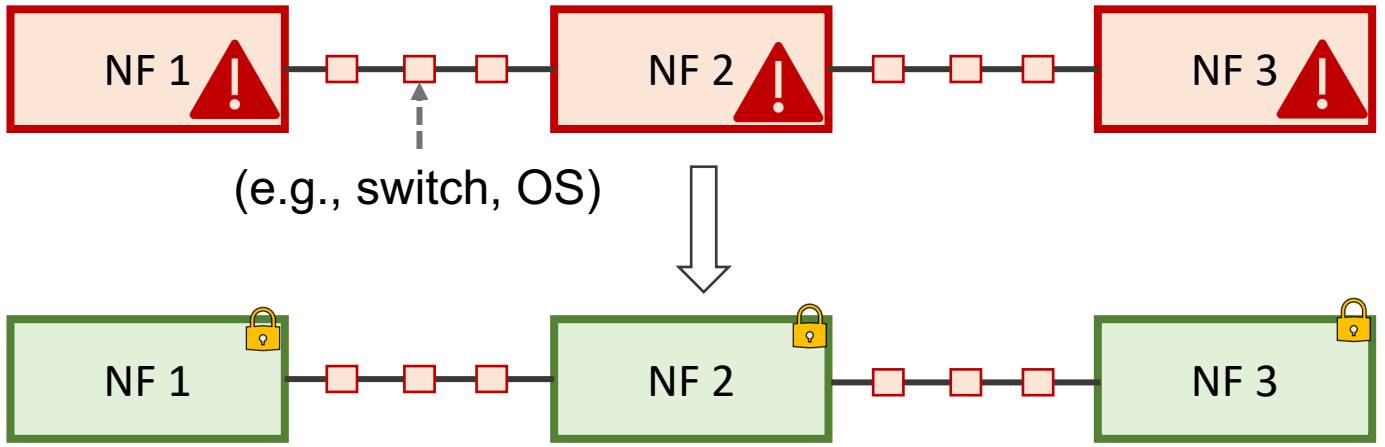
Our Observation

The complexity of auditing comes from NFs' internal processing



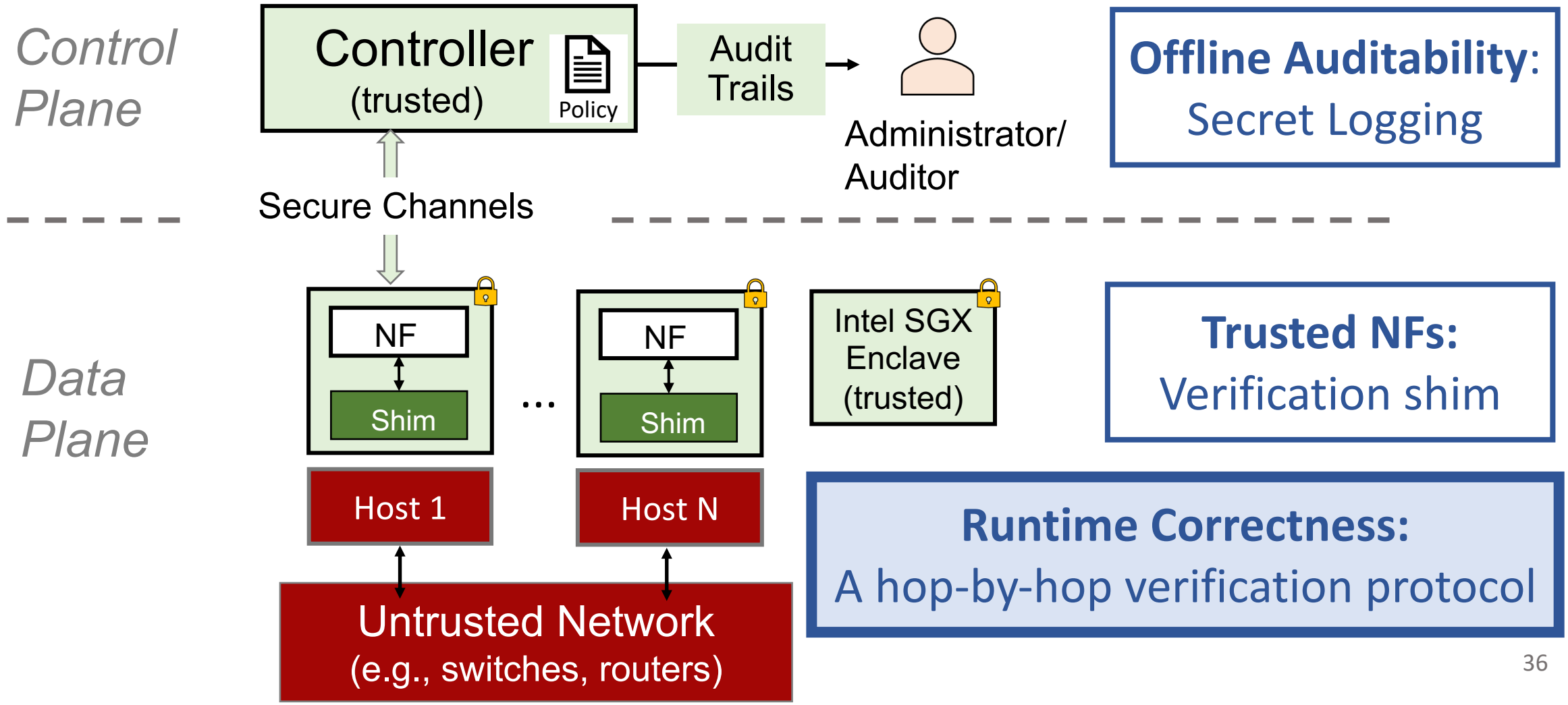
Our Insight

The complexity of auditing comes from NFs' internal processing



Run NFs within Trusted Execution Environment (TEEs), and only audit actions between NFs over the untrusted network.

Design Overview



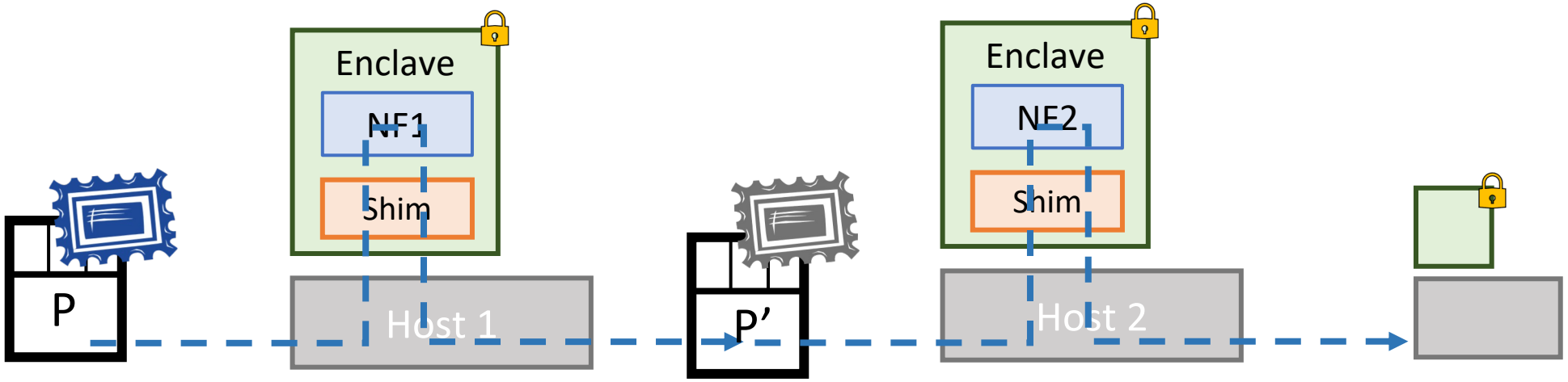
Offline Auditability: Secret Logging

Trusted NFs: Verification shim

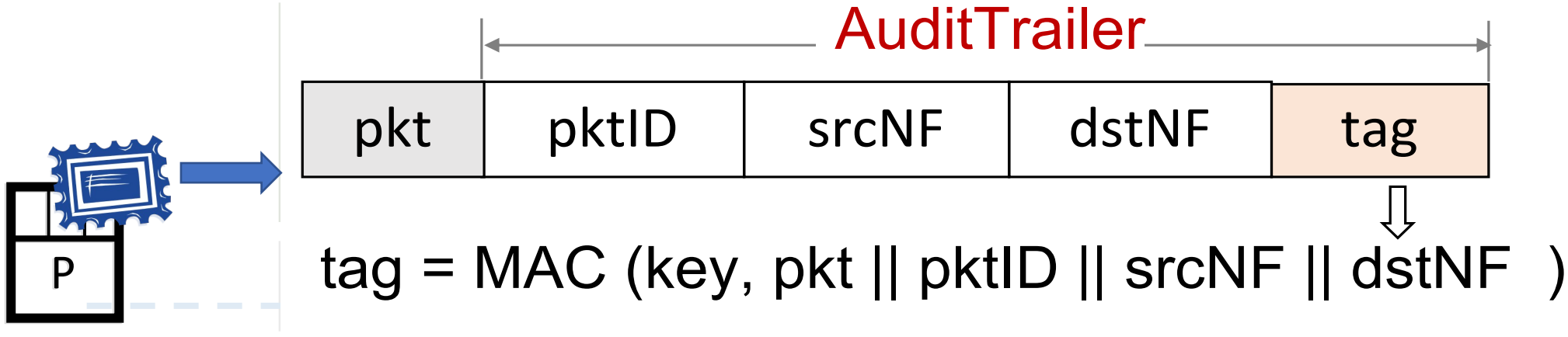
Runtime Correctness: A hop-by-hop verification protocol

NF Hop-by-hop Verification Protocol

- A **shim** in each enclave implements the protocol
- Leverage **transitive trust** to verify packets and enforce policy

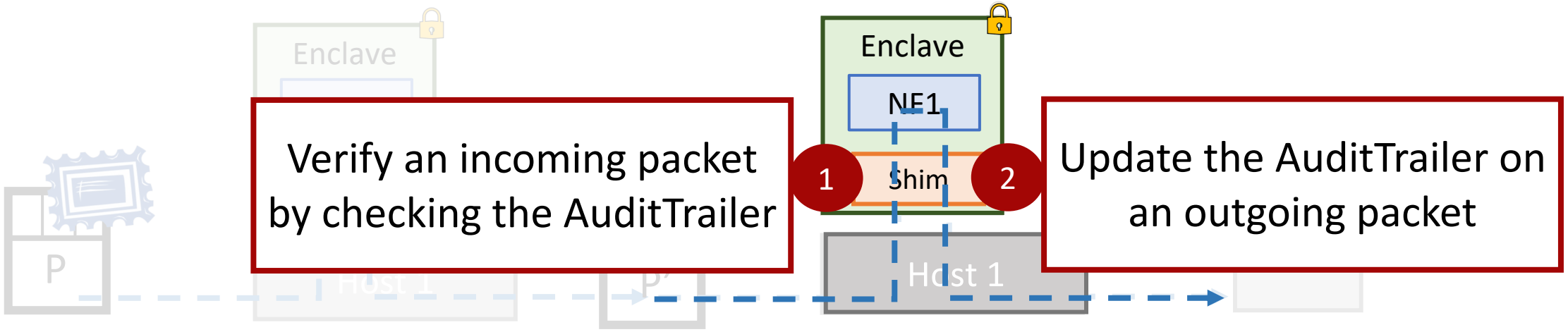


Optimization 1: Simple AuditTrailer



Optimization 2: Updatable GMAC

Reuse the first GMAC when computing the second GMAC to reduce overheads



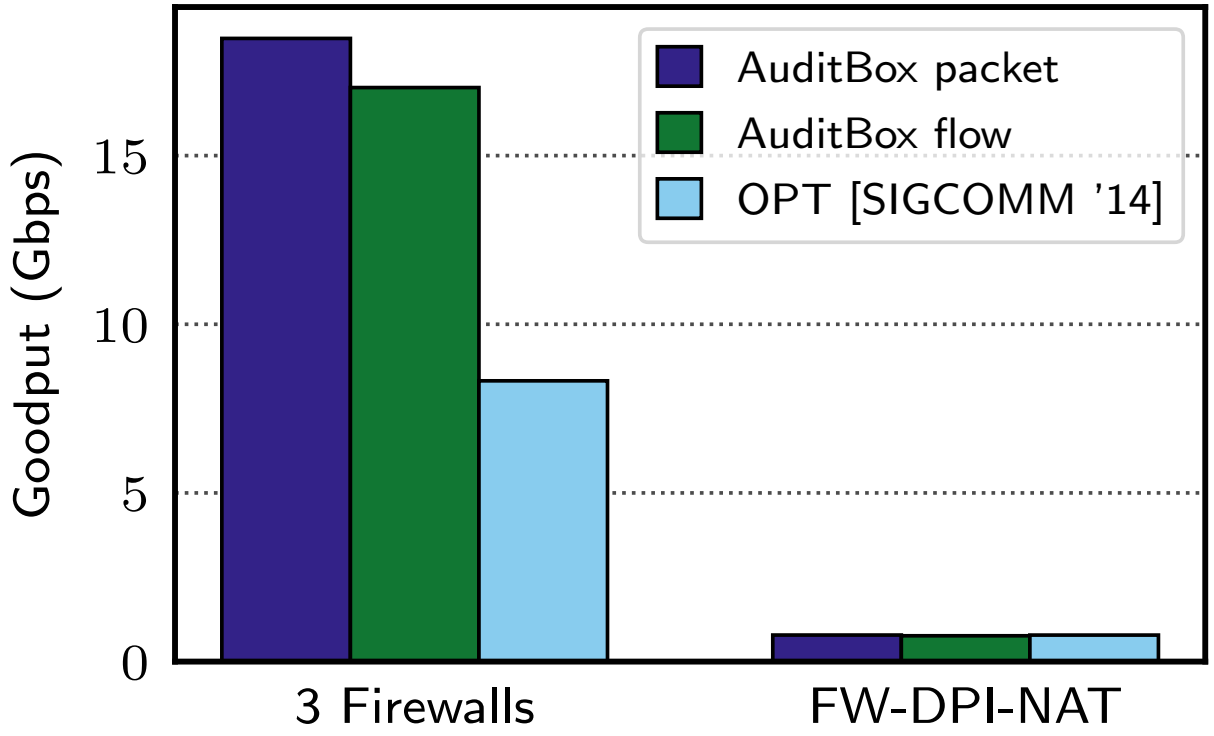
Evaluation

- **Proofs:** We provide **security proofs** that AuditBox can achieve both runtime correctness and offline auditability

- **Functionality Evaluation:** AuditBox correctly detects a broad class of policy violations

- **Performance Evaluation**: AuditBox enables **auditing** for unmodified NFs with **low overhead**

Evaluation: NF Chain Goodput



Achieves 18 Gbps goodput for a simple NF chain

AuditBox Summary

- **1st NFV auditing system**
- Leverages trusted execution environments to provide
  - **Runtime correctness** guarantees and offline **auditability**
  - And still achieve a good performance
- **Industry Impacts:**
  - Promote the adoption of NFV for security-sensitive enterprises
  - Potential deployments: VMware and Intel

nsdi'21

Don't Yank My Chain: Auditable NF Service Chaining

Guyue Liu, Hugo Sadok, Anne Kohlbrenner, Bryan Parno, Vyas Sekar, Justine Sherry*

Carnegie Mellon University **Princeton University*

This Talk

AuditBox (NSDI' 21)

Auditing virtualized network functions

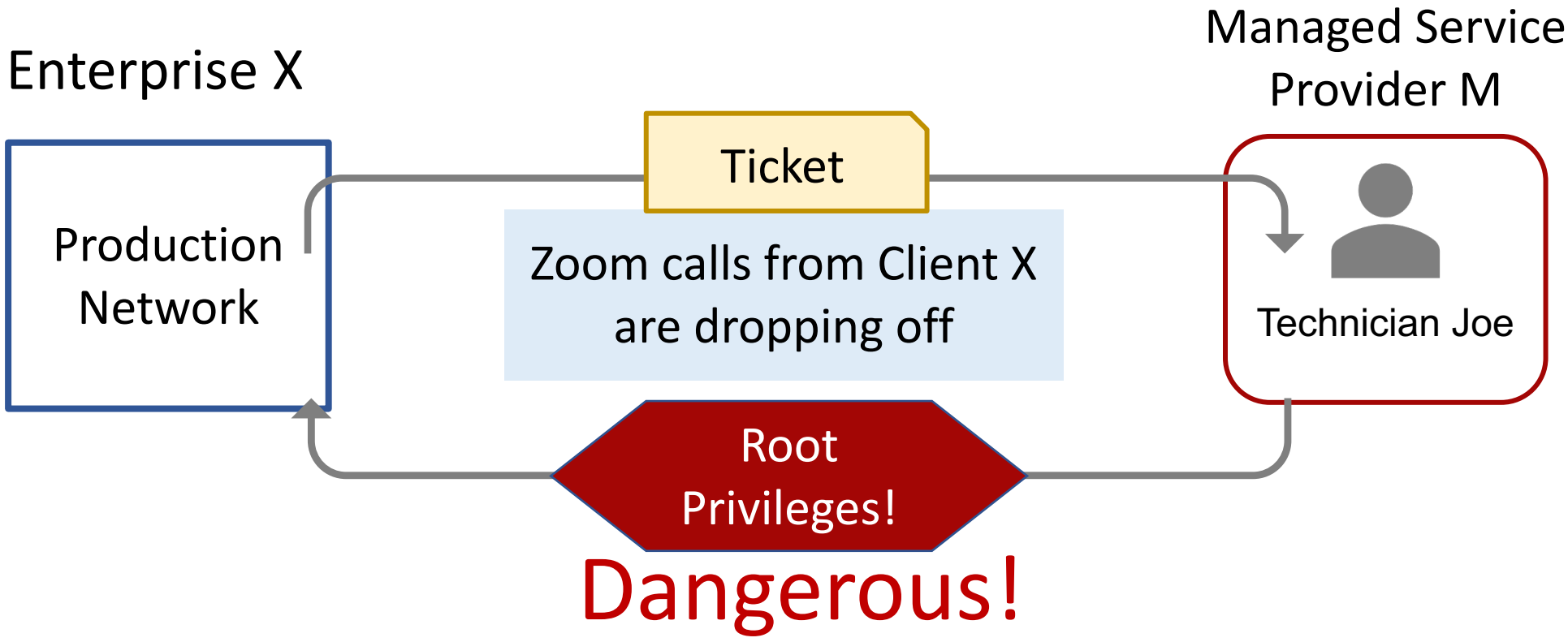
Heimdall (NDSS'24*)

Risk-aware outsourcing of configuration management

ConfMask (SIGCOMM'24)

Privacy-preserving configuration sharing via anonymization

Why Is Current Workflow Insecure?



Large Scale Networks Outage

- Unsafe network management are not uncommon in big companies

On October 4th , 2021 Facebook's apps — which include Facebook, Instagram, WhatsApp, Messenger and Oculus — began displaying error messages around 11:40 a.m. Eastern time, users reported. Within minutes, Facebook had disappeared from the internet. The outage lasted over five hours.

More than 3.5 billion people around the world use these apps. --- New York Times

Network outsourcing scenarios in practice

Outsourced Tasks	Frequency (/day)	Outsource Reason	Access Type
Troubleshooting	10^4	*Costs*	Virtual
Network turn-up and upgrade	10^3	*Costs*	Physical, Virtual
Hardware repair and replacement	10^3	*Geo-proximity*	Physical
Fiber leasing and maintenance	10^2	*Geo-proximity*	Physical, Virtual

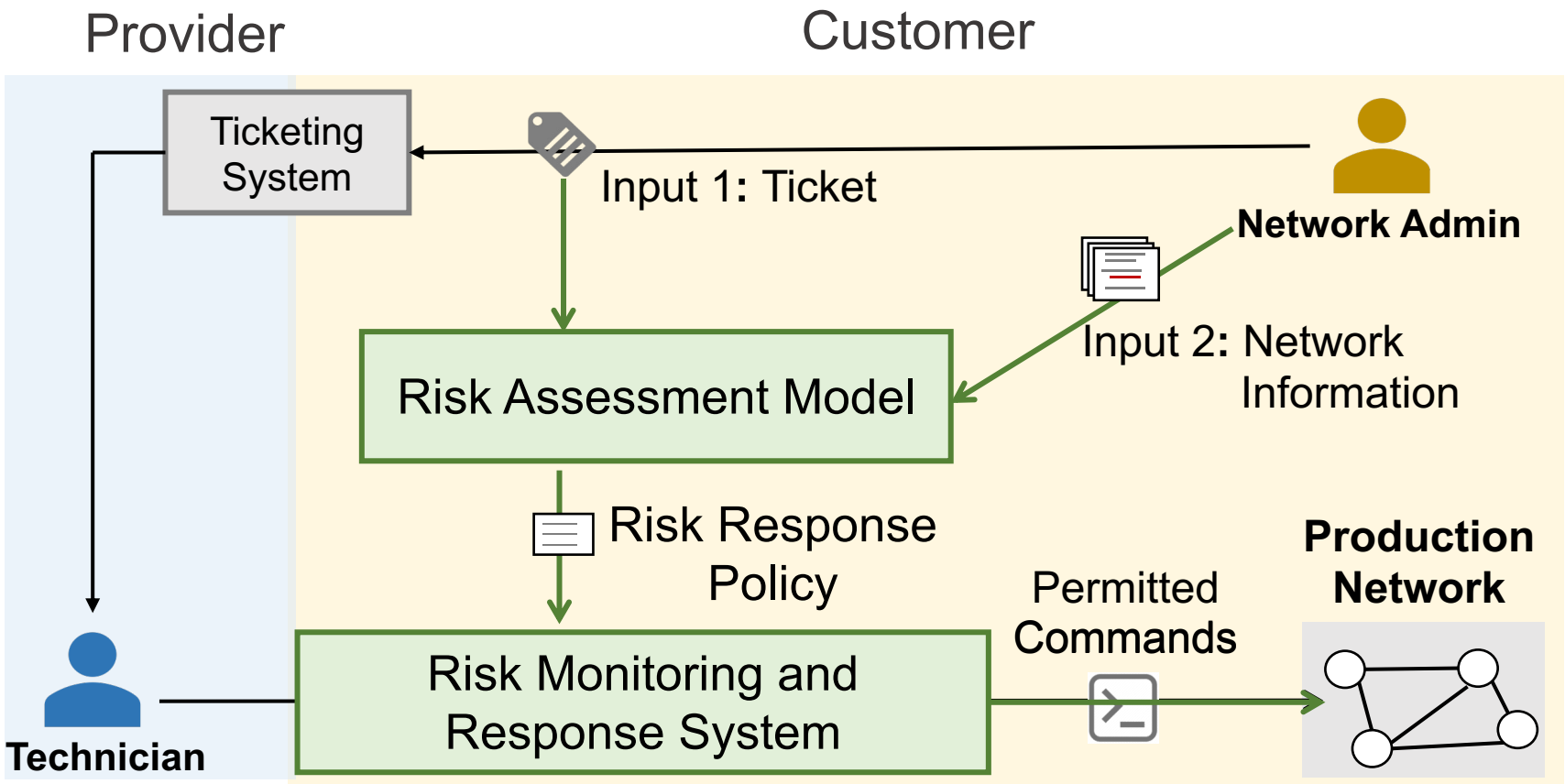
TABLE I: Network outsourcing scenarios in practice based on a hyperscaler network survey

Limitations of Existing Approaches

- **Approach 1: Router built-in privilege management**
  - Cisco IOS allows customizable commands for different privilege levels
  - Difficult to determine required commands for a specific task
  - “All-or-nothing” by either giving root or read-only privilege

- **Approach 2: Use a verification tool to validate configuration changes**
  - Require a formal, complete, and correct specification
  - Cannot handle any implicit or unforeseen policies

Risk-aware Management Workflow



Design Challenges

- How to quantify risk?
- How to accurately assess the risk associated with a ticket?
- How to monitor and respond to risk in real-time?

How to Quantify Risk?

- **Traditional Command-based View of Risk:**
  - Use the number of allowed router commands to quantify risks
  - **Problem 1**: different commands may imply different risks, e.g., show VS. shutdown
  - **Problem 2**: the same command may imply different risks for different tickets

Quantitative Risk Model

- Risk = Probability of occurrence * Consequence

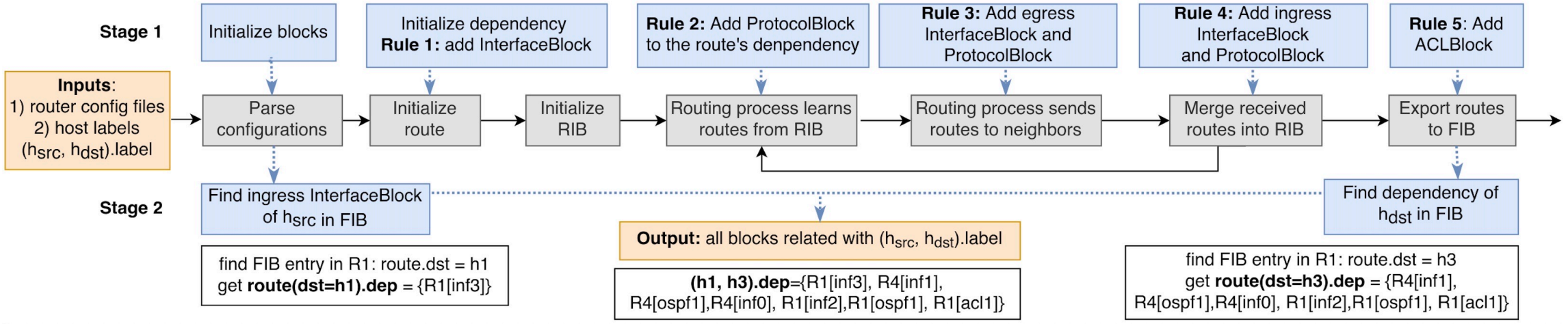
$$\text{Risk (E)} = \sum_{e \in E} P\ (e) * C\ (e)$$

- **Our asset-based risk model:**
  - Assets are the primary concerns of an enterprise

$$\text{Risk (ticket)} = \sum_{s \in Assets} P\ (S|Ticket) * S.value$$

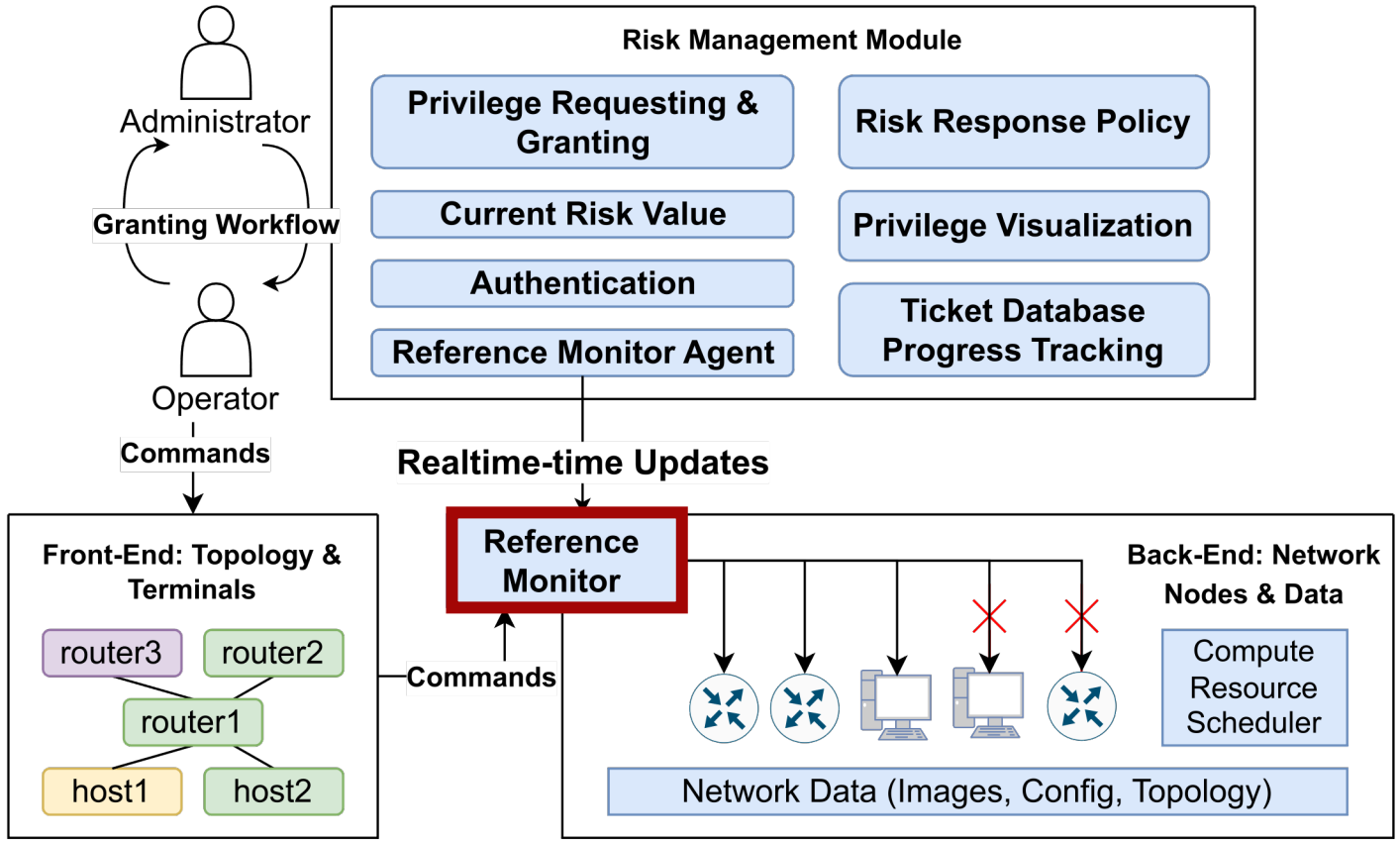
How to Assess the Risk with A Ticket?

- Build connections between assets and each configuration block
- Five set of rules for different types of configuration blocks: interface, protocol, ingress, egress, ACL



How to Monitor and Respond to Risk in Real-time?

- Risk monitoring and response system

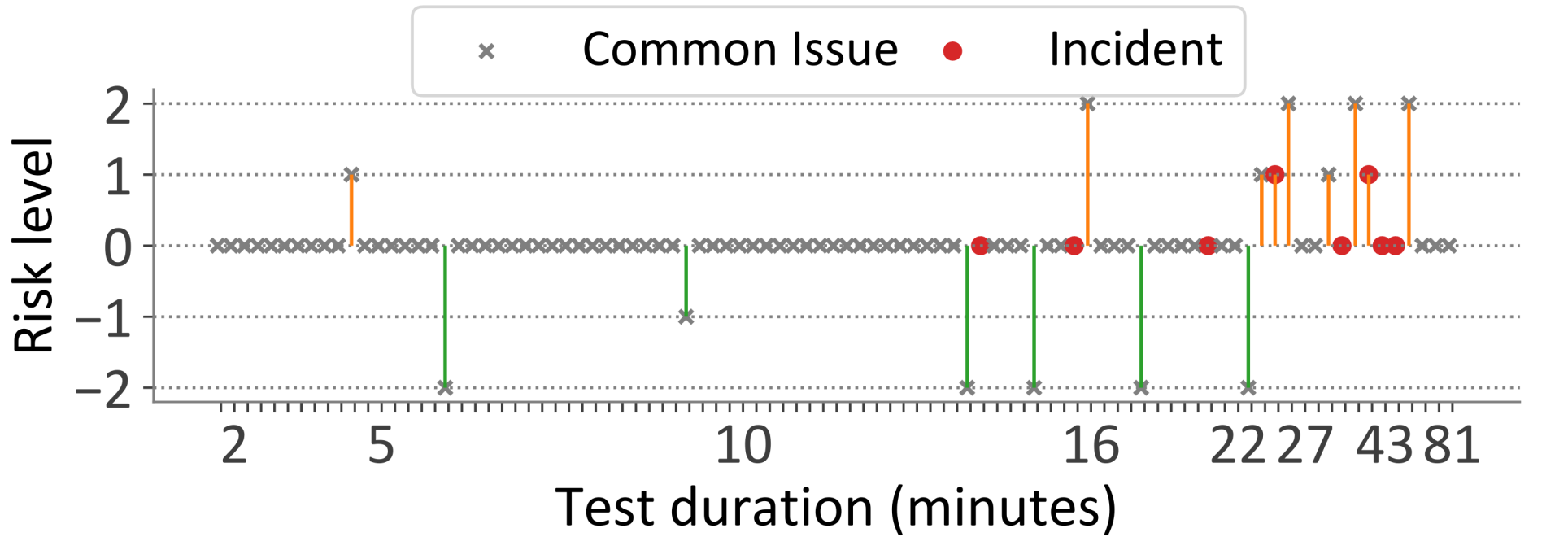


Evaluation Setup

- 8 networks including campus, backbone, data center
- 10 network operators from third-party providers
- 33 types of network configuration tickets
- 99 rounds of test (93 valid tests) lasting for 41 hours

Evaluation Results

Risk control: 92% tasks can be resolved at the lowest risk level



This Talk

AuditBox (NSDI' 21)

Auditing virtualized network functions

Heimdall (NDSS'24*)

Risk-aware outsourcing of configuration management

ConfMask (SIGCOMM'24)

Privacy-preserving configuration sharing via anonymization

Enterprises Hesitate to Share Configurations

When sharing configurations on online forums…

Enterprises Hesitate to Share Configurations

When sharing configurations on online forums…

Problem #1
privacy concerns

Full Sharing — Leaks sensitive organization data

Enterprises Hesitate to Share Configurations

When sharing configurations on online forums…

Problem #1 **privacy concerns**	*Full* Sharing	Leaks sensitive organization data
Problem #2 **low efficiency**	*Partial* Sharing	Requires multiple rounds of replying on the forums to solve an issue

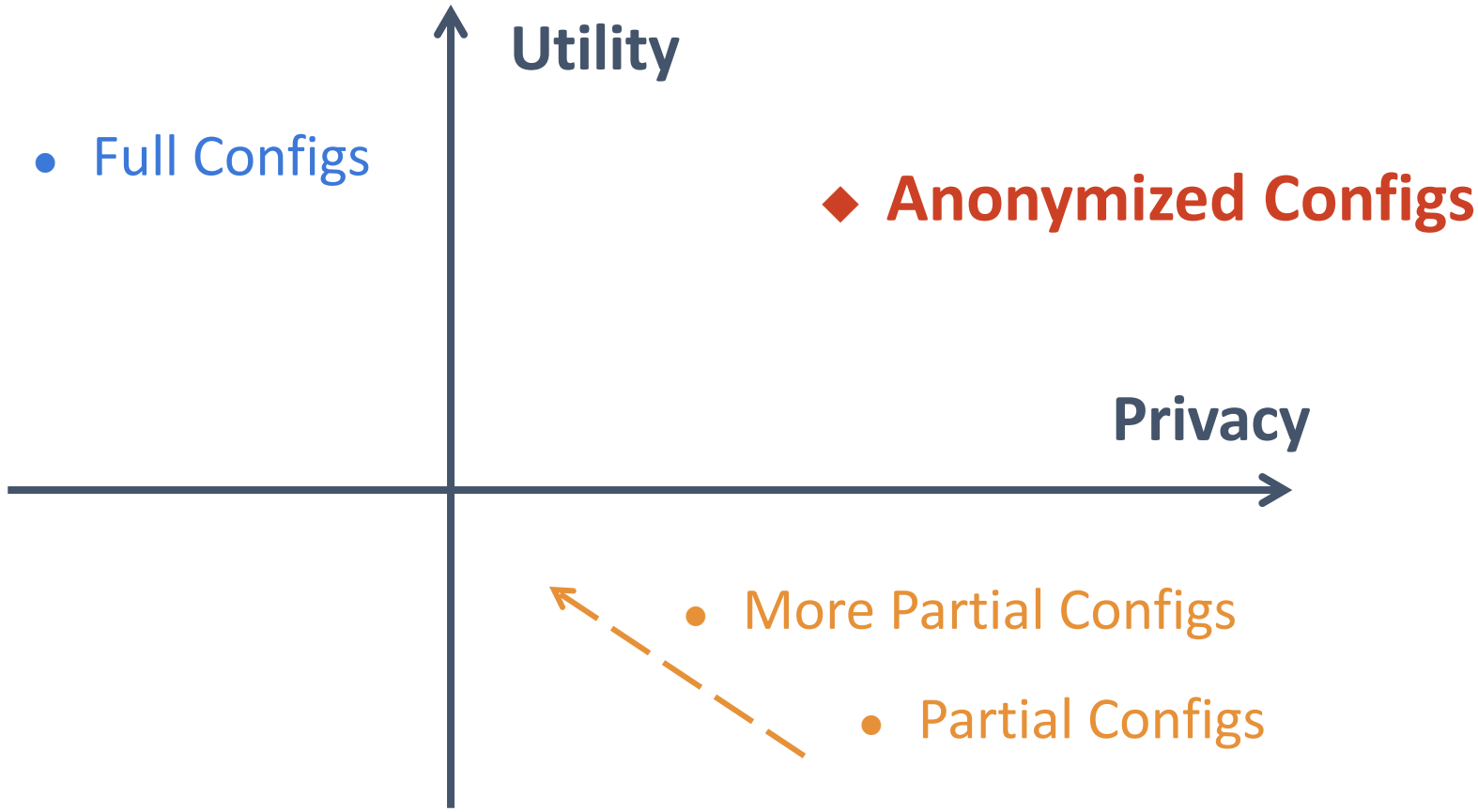
Enterprises Hesitate to Share Configurations

When sharing configurations on online forums…

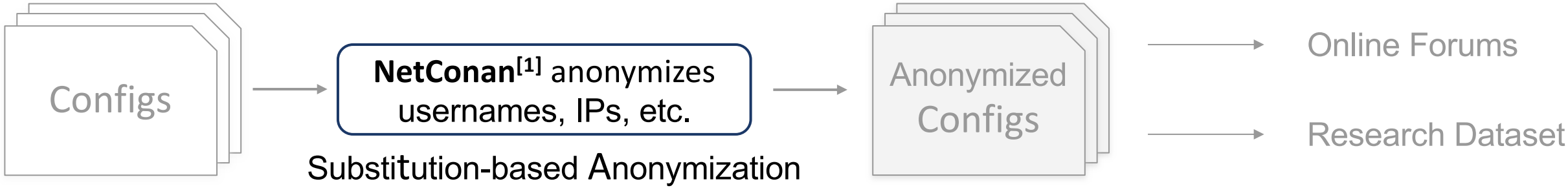
Problem #1 **privacy concerns**	*Full* Sharing	Leaks sensitive organization data
Problem #2 **low efficiency**	*Partial* Sharing	Requires multiple rounds of replying on the forums to solve an issue

Collaborative debugging is ***inefficient*** due to ***privacy concerns*** in configuration sharing

Intuition – Share With Anonymization



Limitations of Existing Approaches

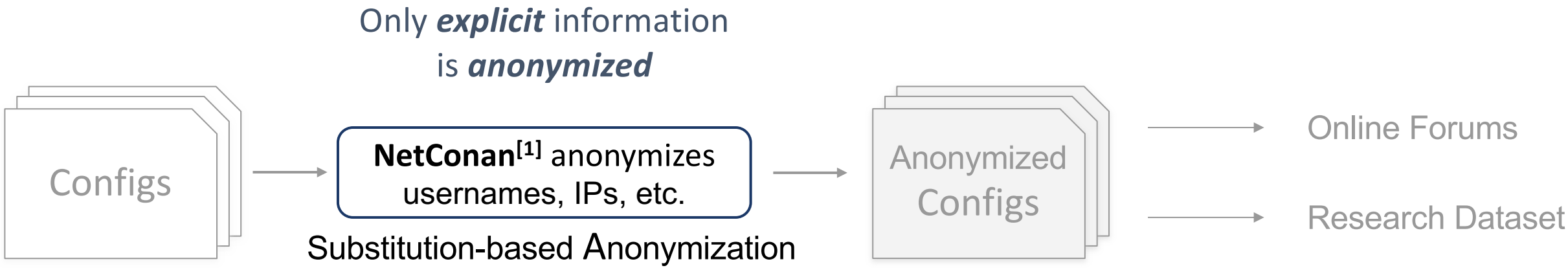



```
username admin password 7
122A001901
!
tacacs-server host 1.2.3.4 key
pwd1234
ip address 10.10.20.30/24
ip address 2001:2002::9d3b:1
!
route-map sea-to-lax ...
route-map sea-to-atl ...
```

```
username admin password 7
09424B1D1A0A1913E012724322D3765
!
tacacs-server host 7.227.130.88 key
netconanRemoved2
ip address 10.72.218.183/24
ip address cd7e:83e:af:2a:753:1e:6d47:a4b8
!
route-map e69ceb-to-880ac2 ...
route-map e69ceb-to-5d37ad ...
```


[1] NetConan: a Network Configuration Anonymizer https://github.com/intentionet/netconan

Limitations of Existing Approaches

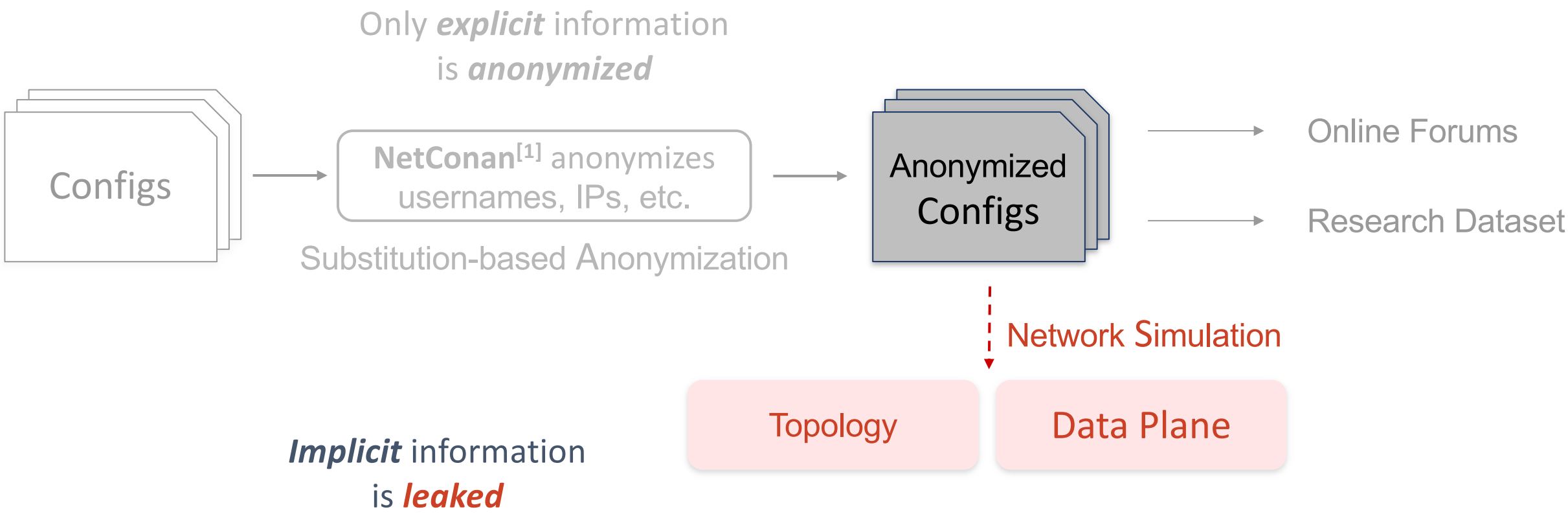



```
username admin password 7
122A001901
!
tacacs-server host 1.2.3.4 key
pwd1234
ip address 10.10.20.30/24
ip address 2001:2002::9d3b:1
!
route-map sea-to-lax ...
route-map sea-to-atl ...
```

```
username admin password 7
09424B1D1A0A1913E012724322D3765
!
tacacs-server host 7.227.130.88 key
netconanRemoved2
ip address 10.72.218.183/24
ip address cd7e:83e:af:2a:753:1e:6d47:a4b8
!
route-map e69ceb-to-880ac2 ...
route-map e69ceb-to-5d37ad ...
```

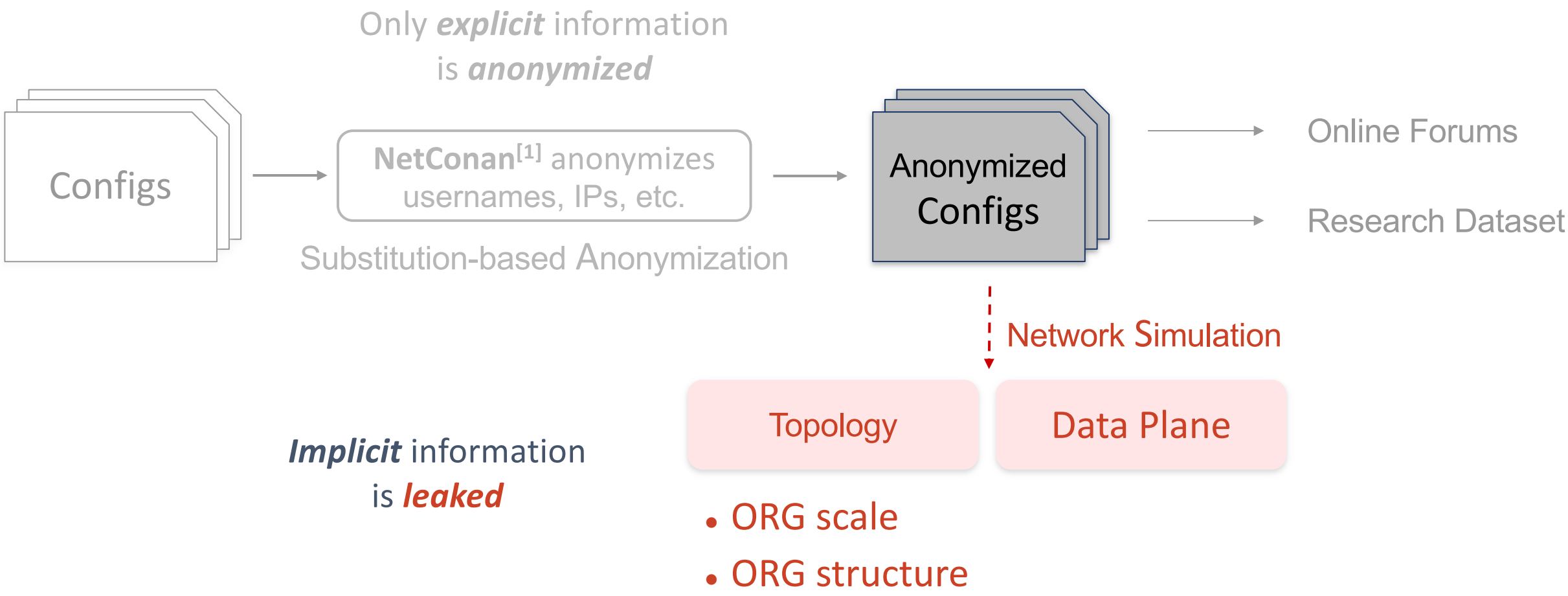

[1] NetConan: a Network Configuration Anonymizer https://github.com/intentionet/netconan

Limitations of Existing Approaches



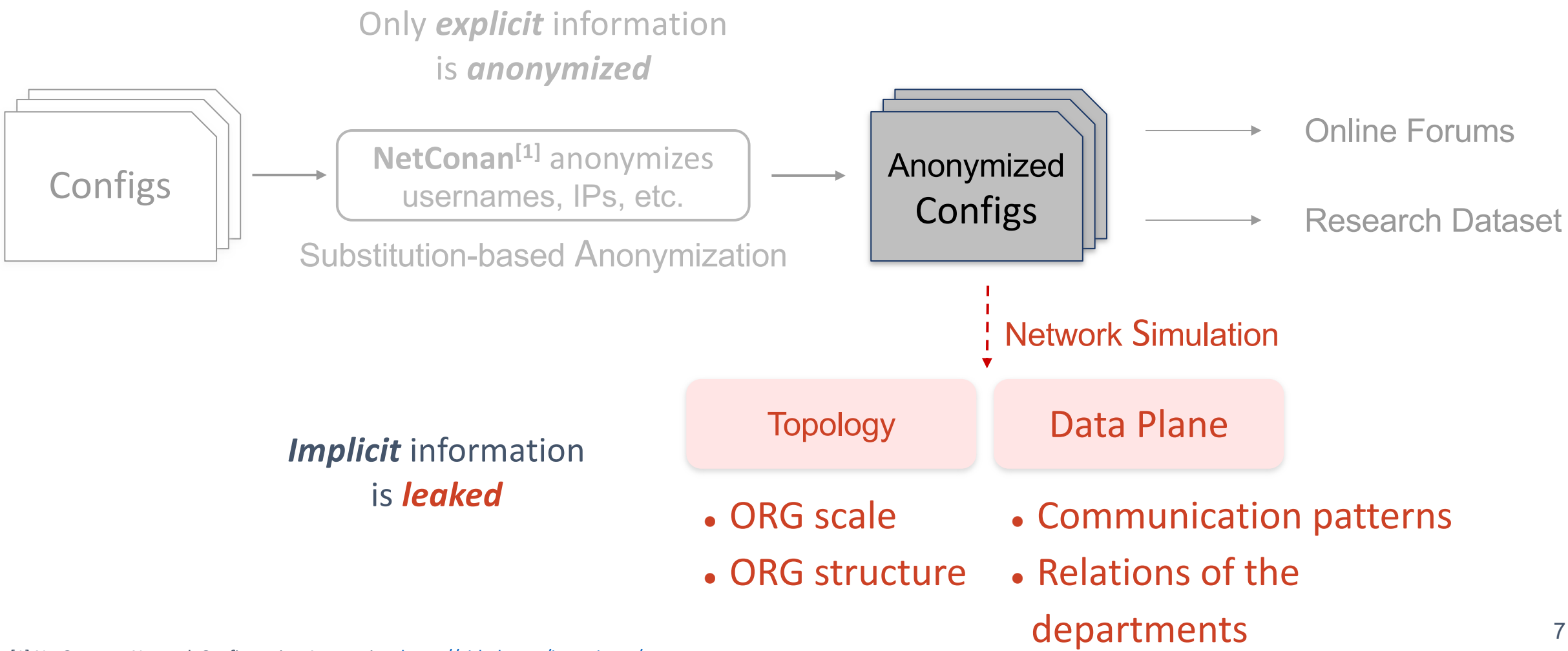
[1] NetConan: a Network Configuration Anonymizer https://github.com/intentionet/netconan

Limitations of Existing Approaches



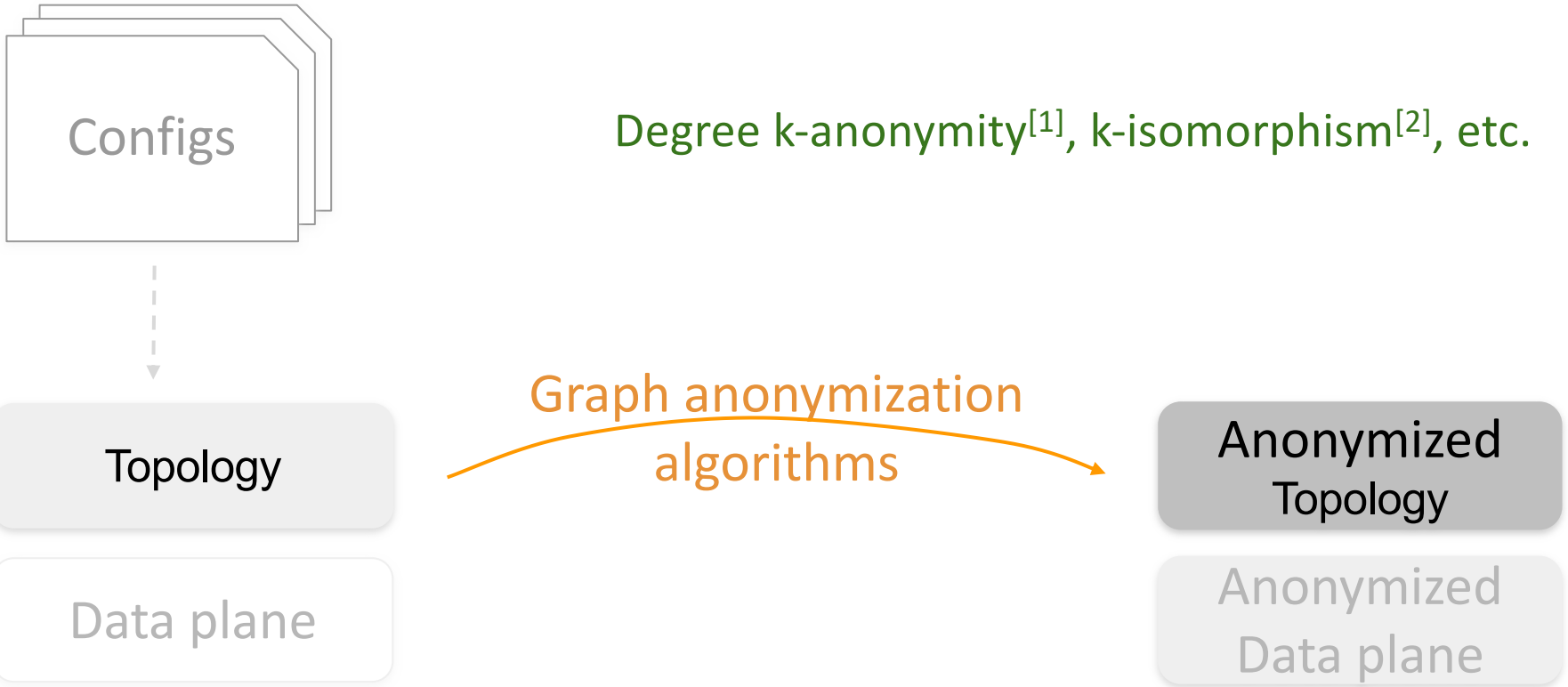
[1] NetConan: a Network Configuration Anonymizer https://github.com/intentionet/netconan

Limitations of Existing Approaches



[1] NetConan: a Network Configuration Anonymizer https://github.com/intentionet/netconan

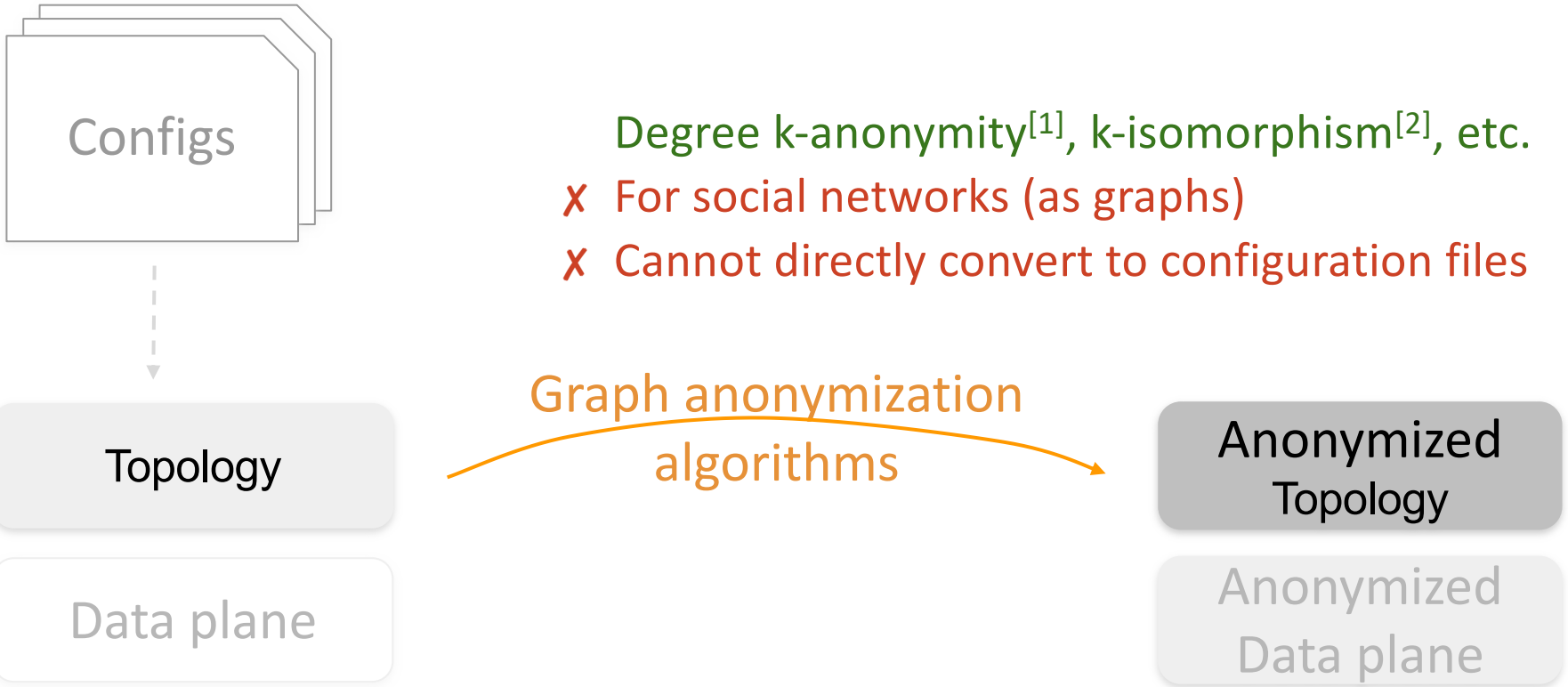
Existing Topology Anonymization



Degree k-anonymity[1], k-isomorphism[2], etc.

[1] Sweeney L. k-anonymity: A model for protecting privacy. International journal of uncertainty, fuzziness and knowledge-based systems. 2002 Oct;10(05):557-70.
[2] Cheng J, Fu AW, Liu J. K-isomorphism: privacy preserving network publication against structural attacks. In SIGMOD 2010 (pp. 459-470).

Existing Topology Anonymization



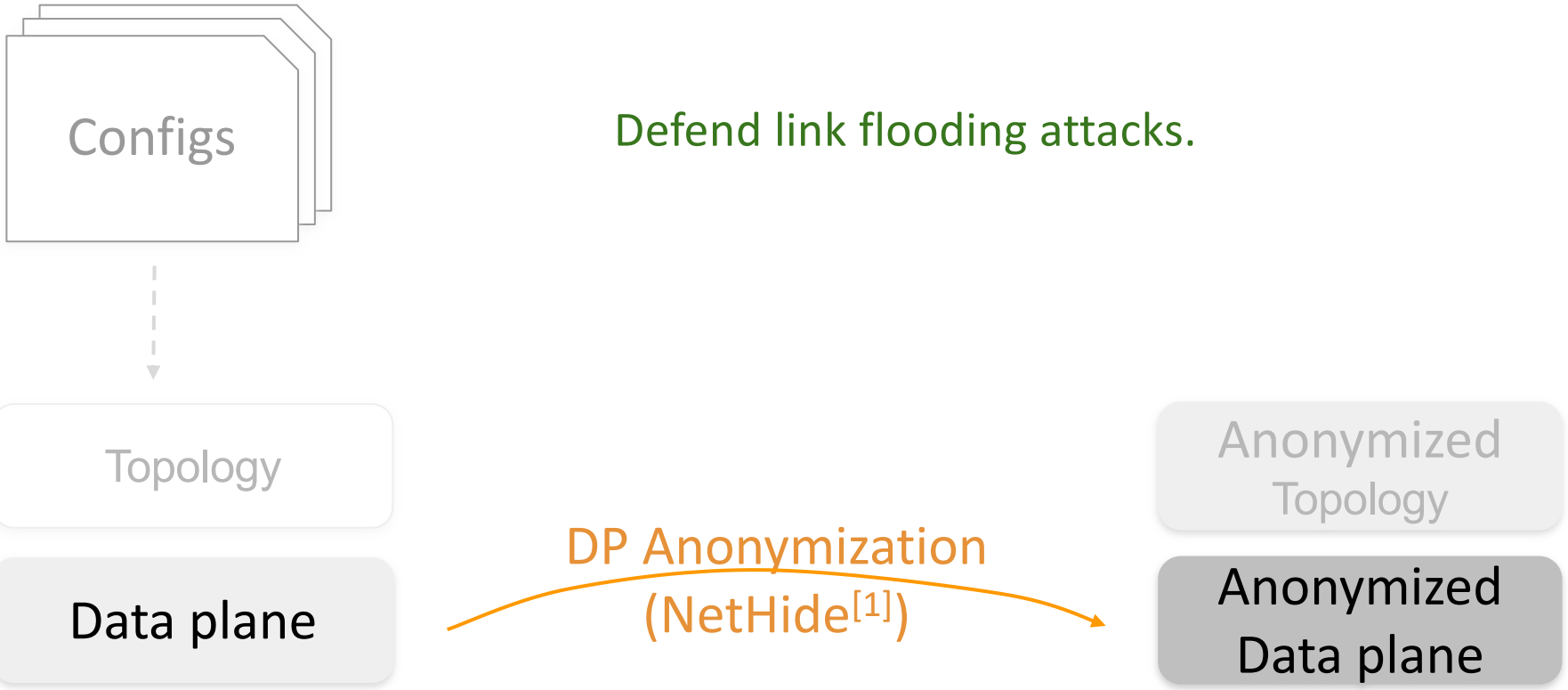
Degree k-anonymity[1], k-isomorphism[2], etc.

✗ For social networks (as graphs)

✗ Cannot directly convert to configuration files

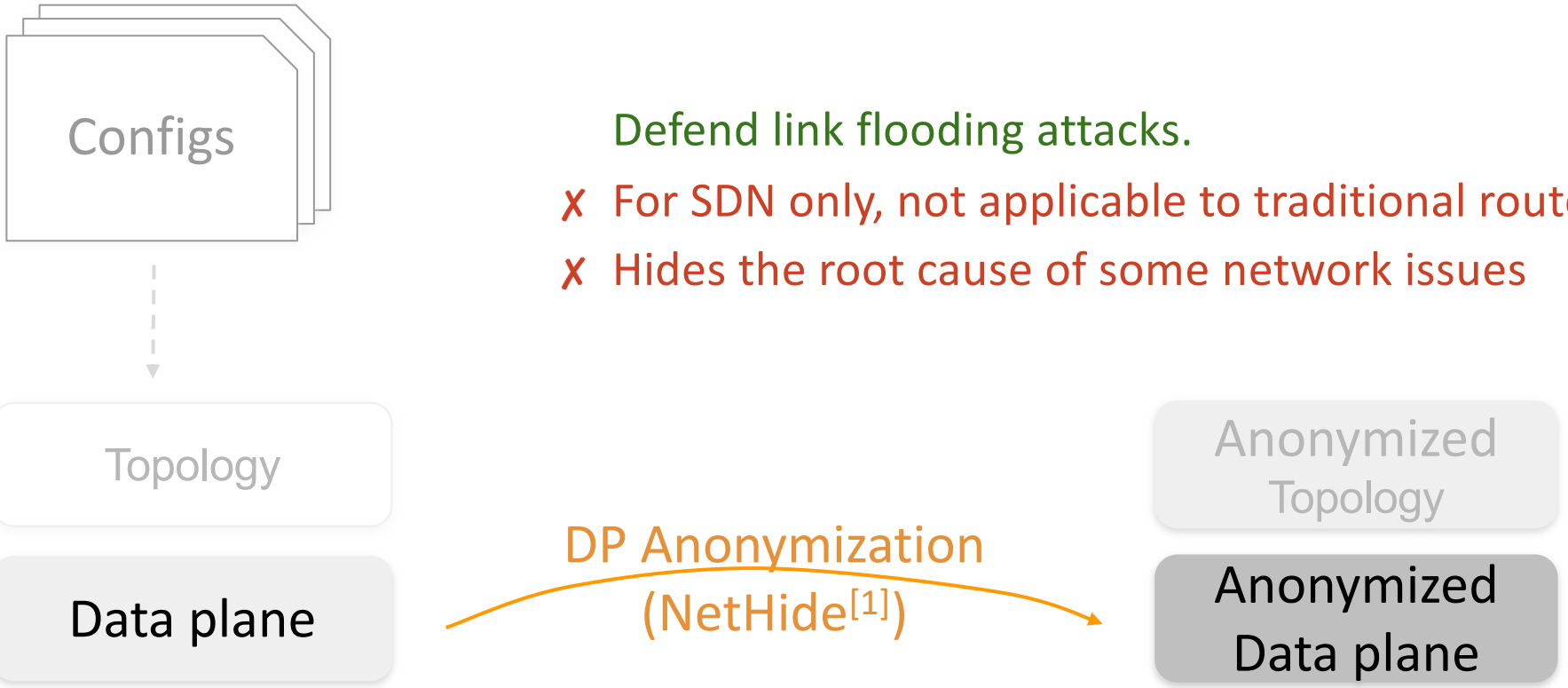
[1] Sweeney L. k-anonymity: A model for protecting privacy. International journal of uncertainty, fuzziness and knowledge-based systems. 2002 Oct;10(05):557-70.
[2] Cheng J, Fu AW, Liu J. K-isomorphism: privacy preserving network publication against structural attacks. In SIGMOD 2010 (pp. 459-470).

Existing Data Plane Anonymization



[1] Roland Meier, Petar Tsankov, Vincent Lenders, Laurent Venbever, and Martin Vechev. 2018. NetHide: Secure and Practical Network Topology Obfuscation. In *27th USENIX Security Symposium (USENIX Security 18)*. 693–709.

Existing Data Plane Anonymization



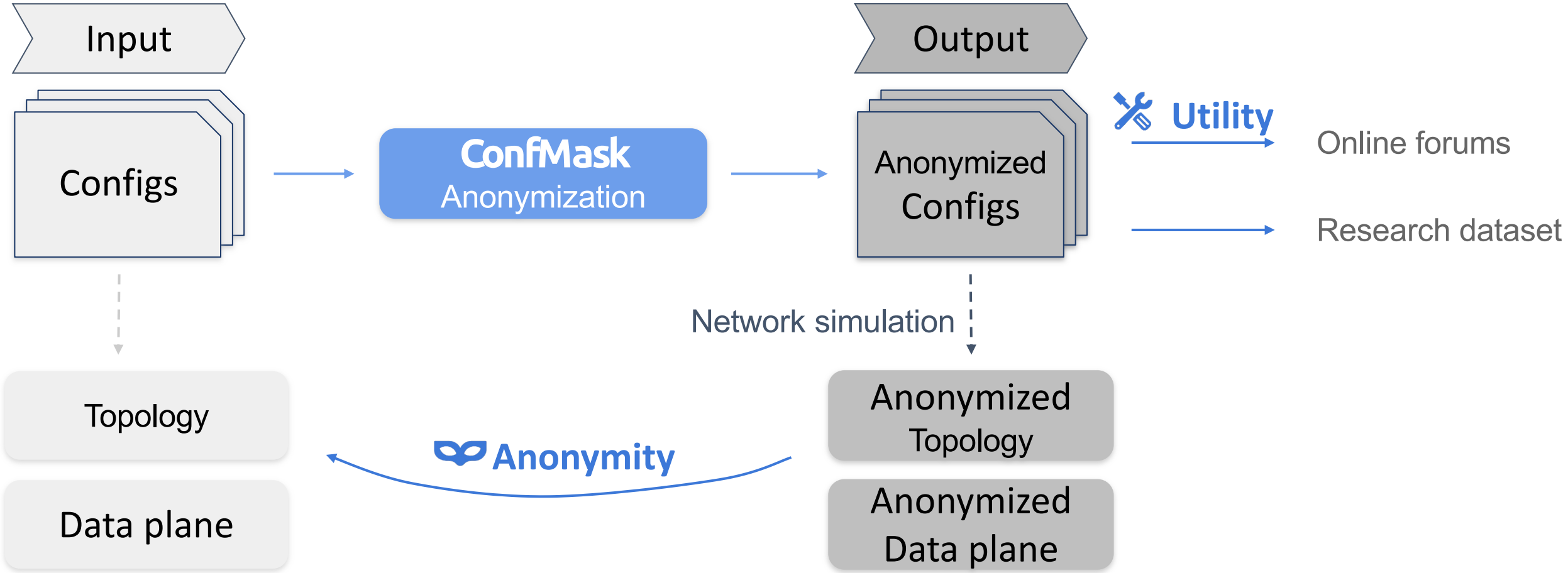
Defend link flooding attacks.

✗ For SDN only, not applicable to traditional routers

✗ Hides the root cause of some network issues

[1] Roland Meier, Petar Tsankov, Vincent Lenders, Laurent Venbever, and Martin Vechev. 2018. NetHide: Secure and Practical Network Topology Obfuscation. In *27th USENIX Security Symposium (USENIX Security 18)*. 693–709.

ConfMask Goals



ConfMask: Privacy-Preserving Configuration Sharing via Anonymization

ConfMask: Enabling Privacy-Preserving Configuration Sharing via Anonymization

Yuejie Wang
Peking University
New York University Shanghai

Qiutong Men
New York University Shanghai

Yao Xiao
New York University Shanghai

Yongting Chen
New York University Shanghai

Guyue Liu
Peking University

ConfMask focuses on **topology and data plane** to enable privacy-preserving configuration sharing while providing high utility.

https://github.com/ConfMask/ConfMask

Trustworthy Network Outsourcing

AuditBox (NSDI' 21)

Auditing virtualized network functions ***by verifying every packet at every hop***

Heimdall (NDSS'24*)

Risk-aware outsourcing of configuration management ***by quantifying risk and continuously measuring risk***

ConfMask (SIGCOMM'24)

Privacy-preserving configuration sharing via **topology and data plane anonymization**