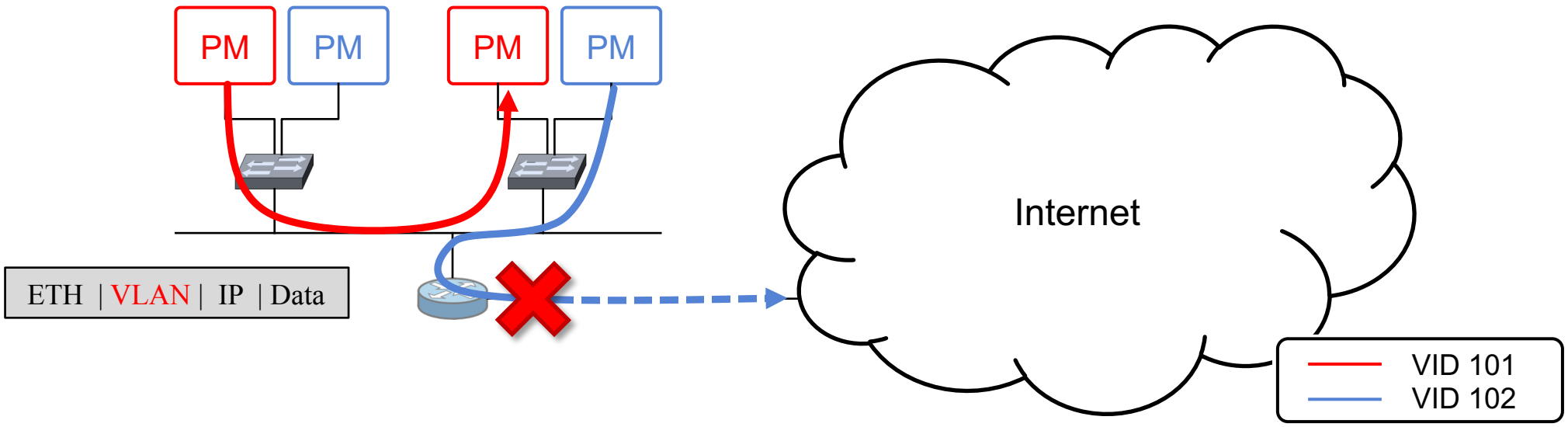
ETH zürich

SVLAN: Secure & Scalable Network Virtualization

Jonghoon Kwon, Taeho Lee, Claude Hähni, Adrian Perrig
ETH Zürich, Network Security Group

NDSS SYMPOSIUM

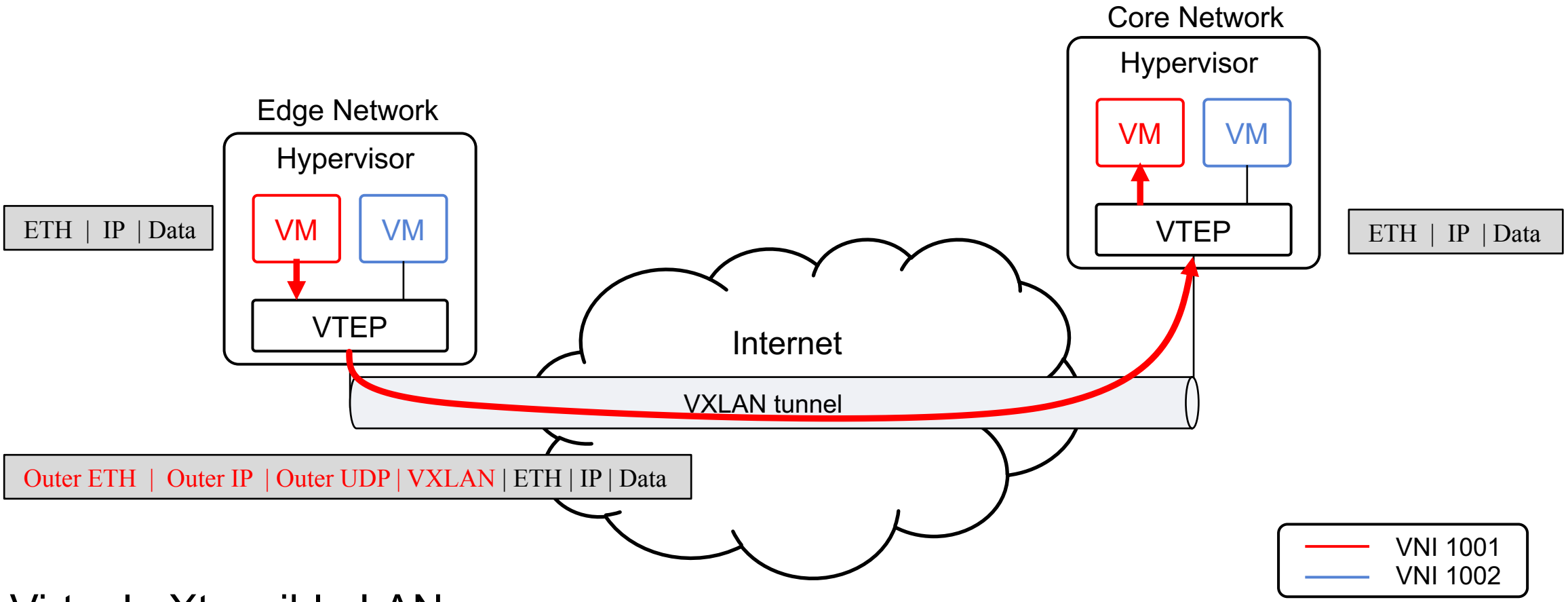
Current Inter-domain Network Virtualization: VLAN



Virtual LAN (IEEE 802.1q)

Layer-2 bridging
Supporting apx. 4 K virtual networks with a 12-bit VID value

Current Inter-domain Network Virtualization: VXLAN



Virtual eXtensible LAN

Supporting 16 M virtual networks with a 24-bit VNI value
Interconnecting layer-2 networks over an underlying layer-3 network

Adversarial Model and Desired Properties

Compromise Network Isolation

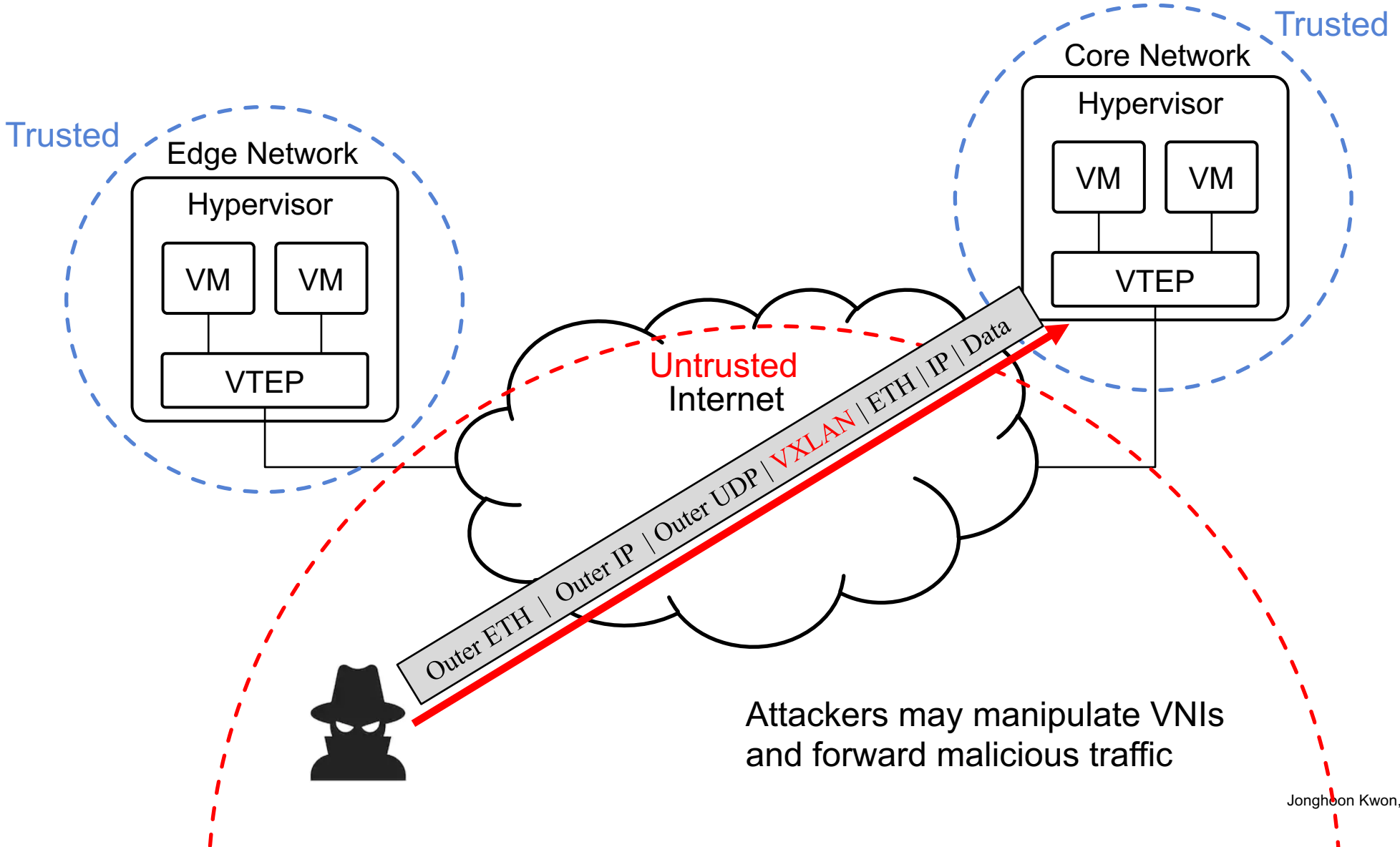
Disrupt Virtual Network

Security

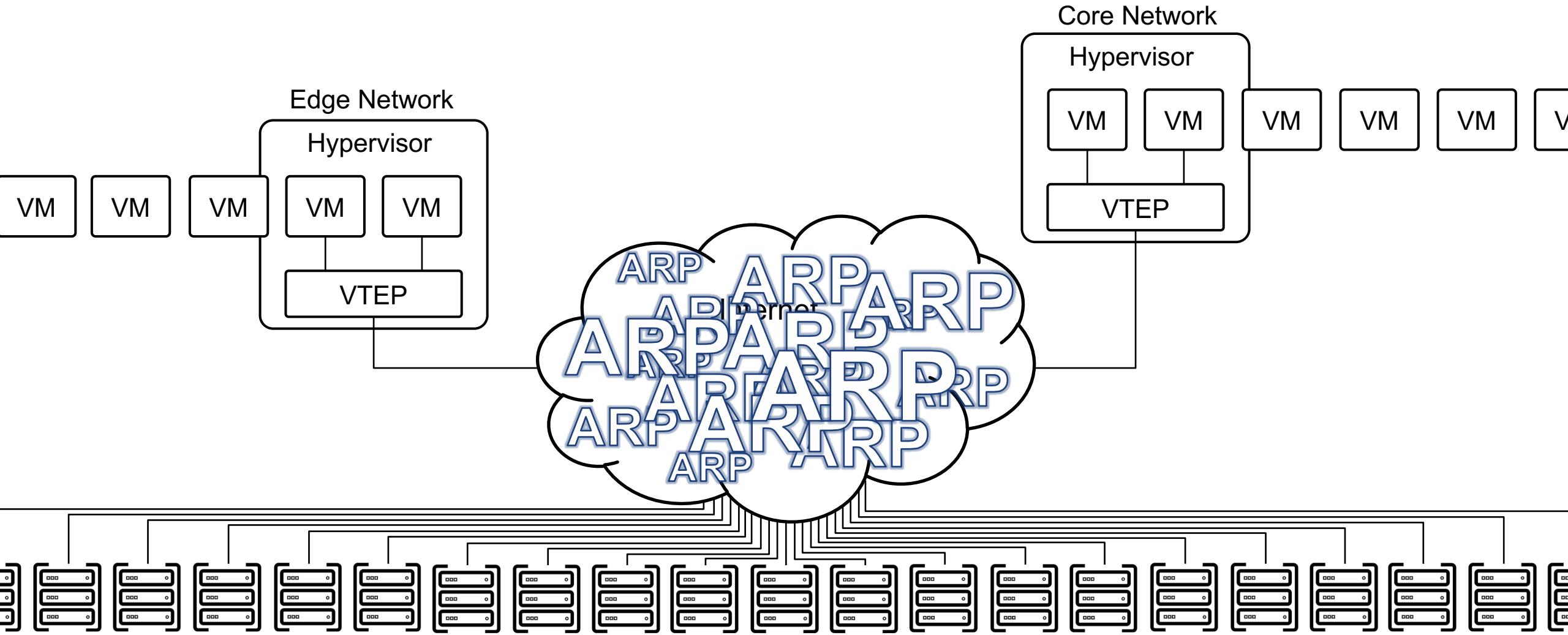
Scalability

Flexibility

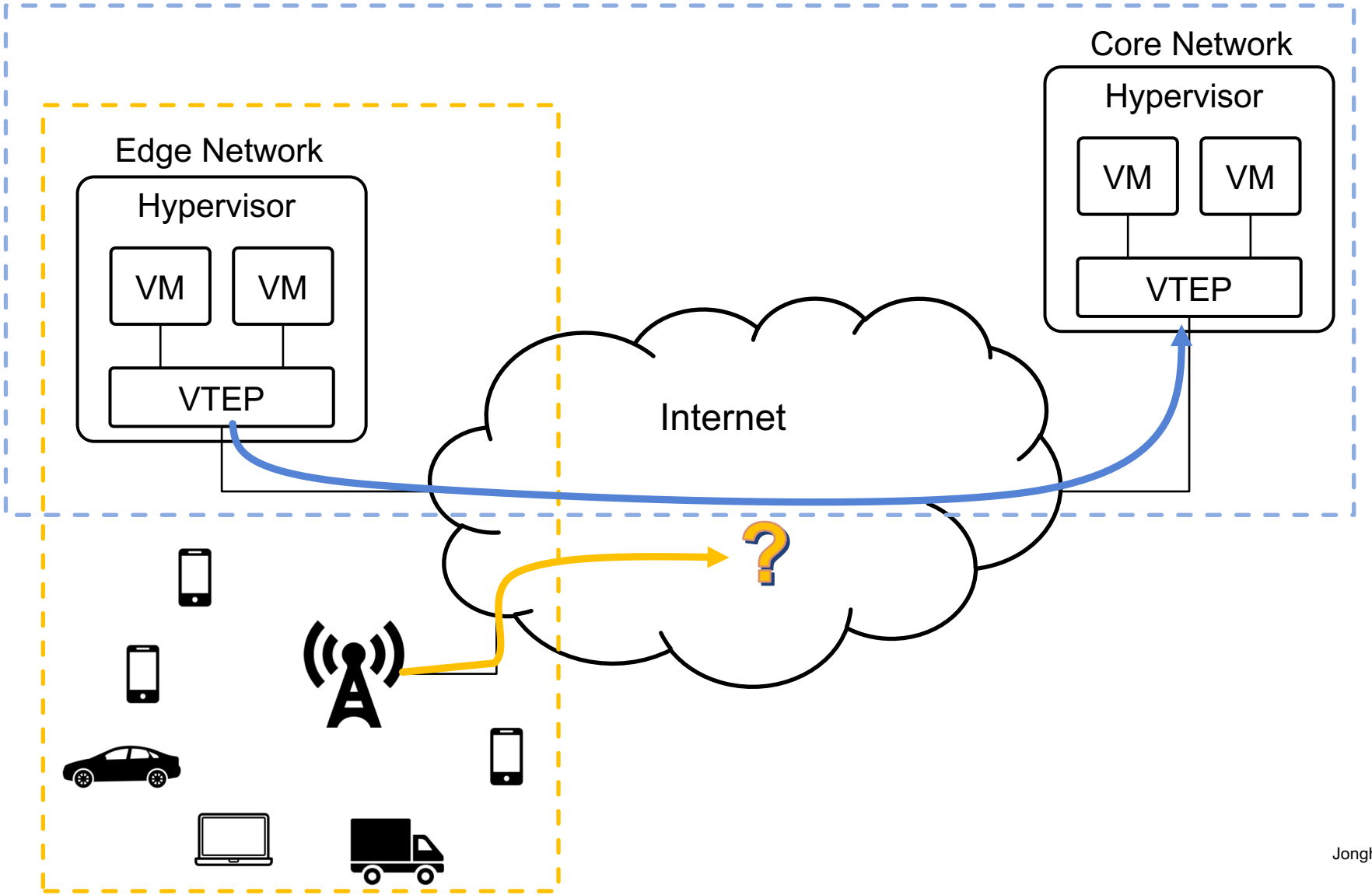
VXLAN: Insufficient Security



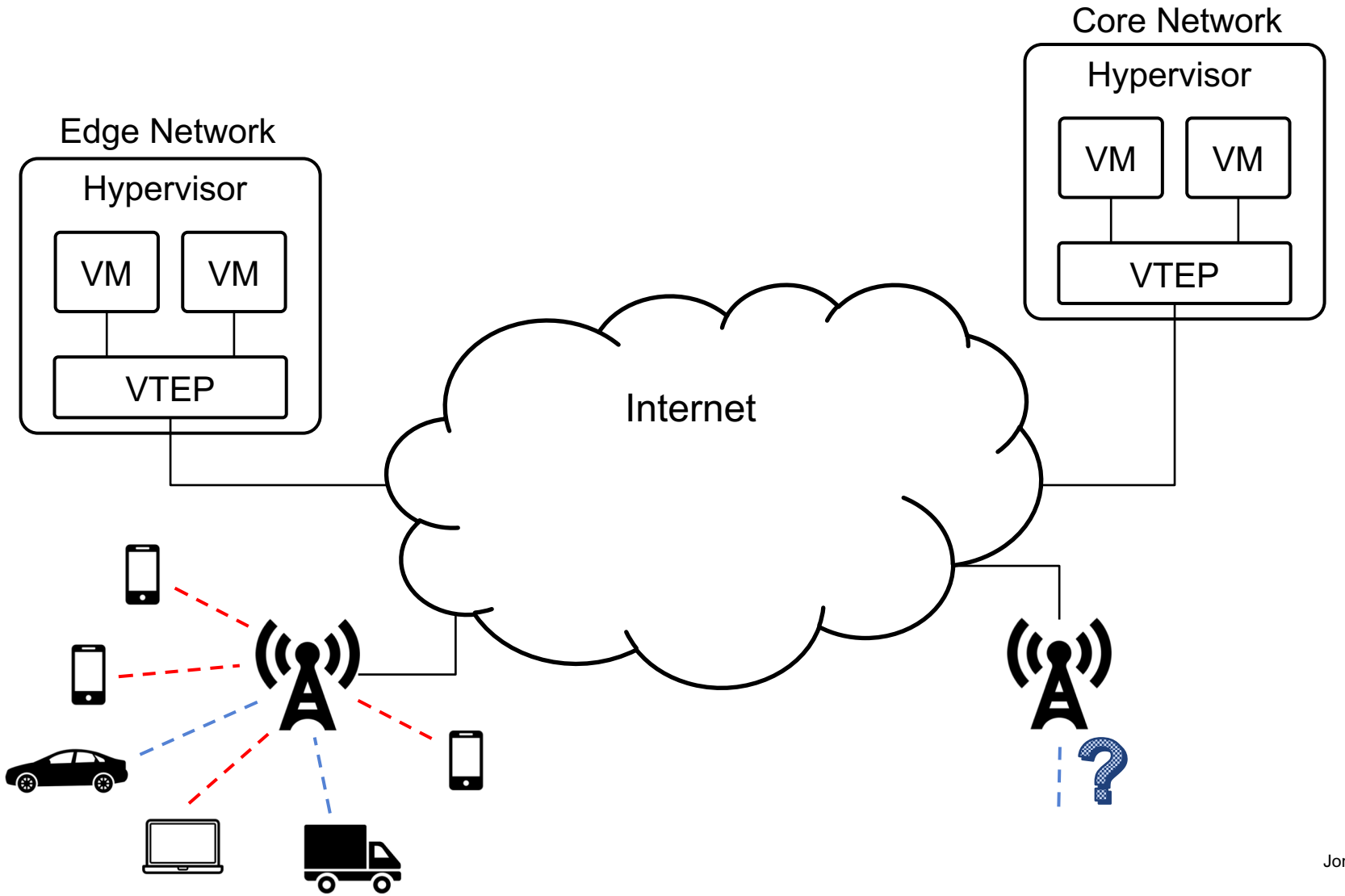
VXLAN: Scalability Constraints



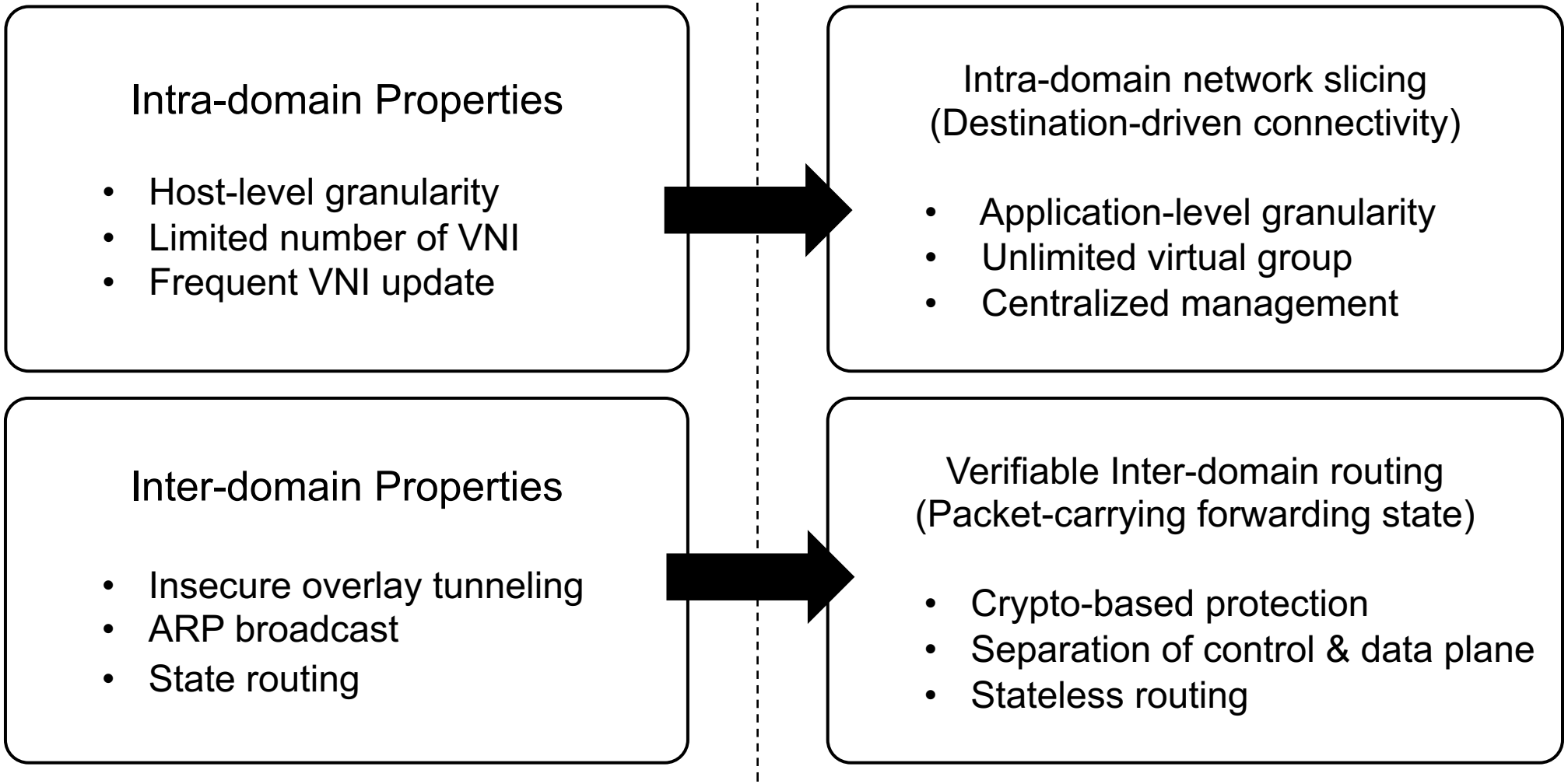
VXLAN: Insufficient Flexibility



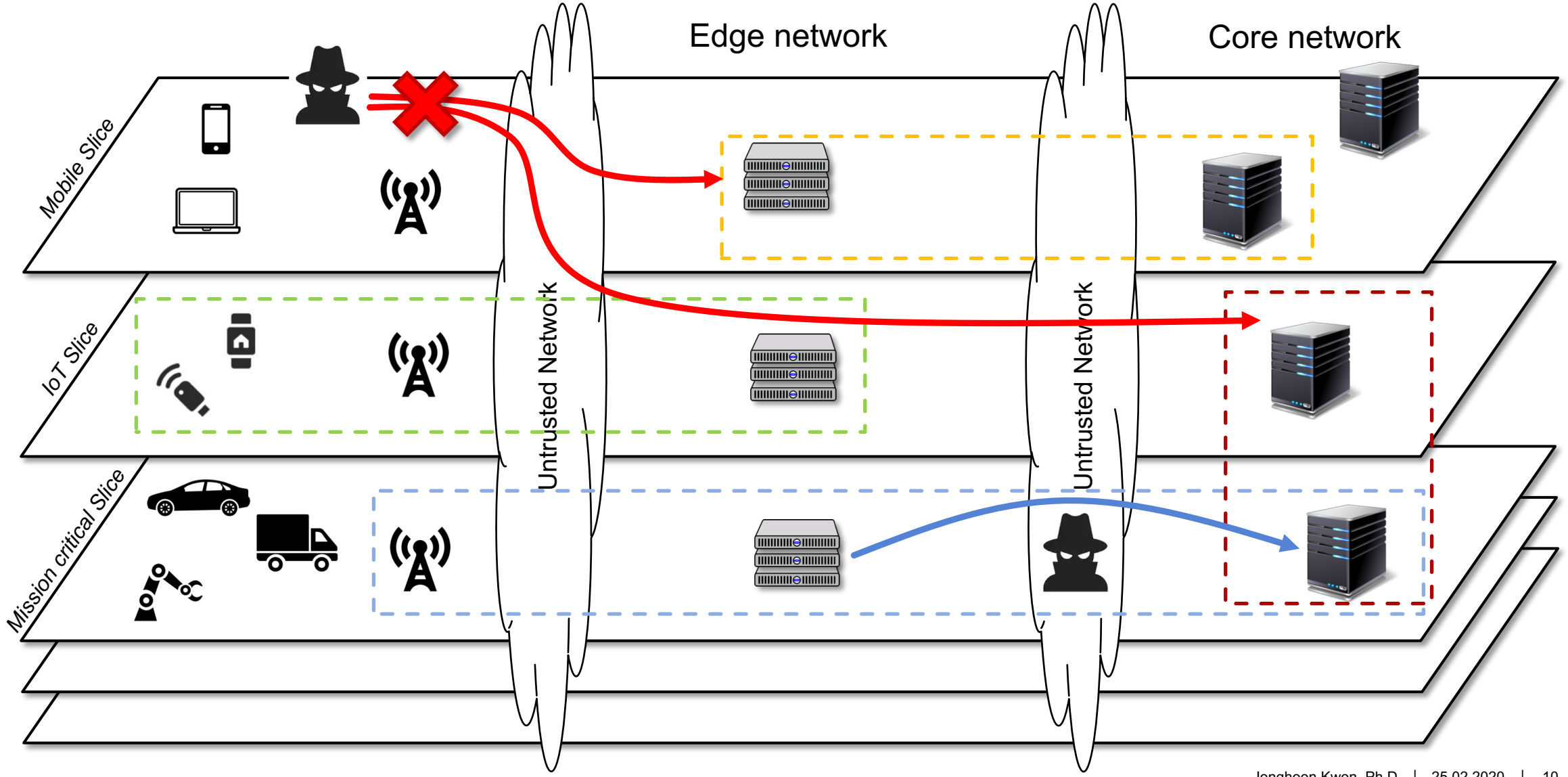
VXLAN: Insufficient Flexibility



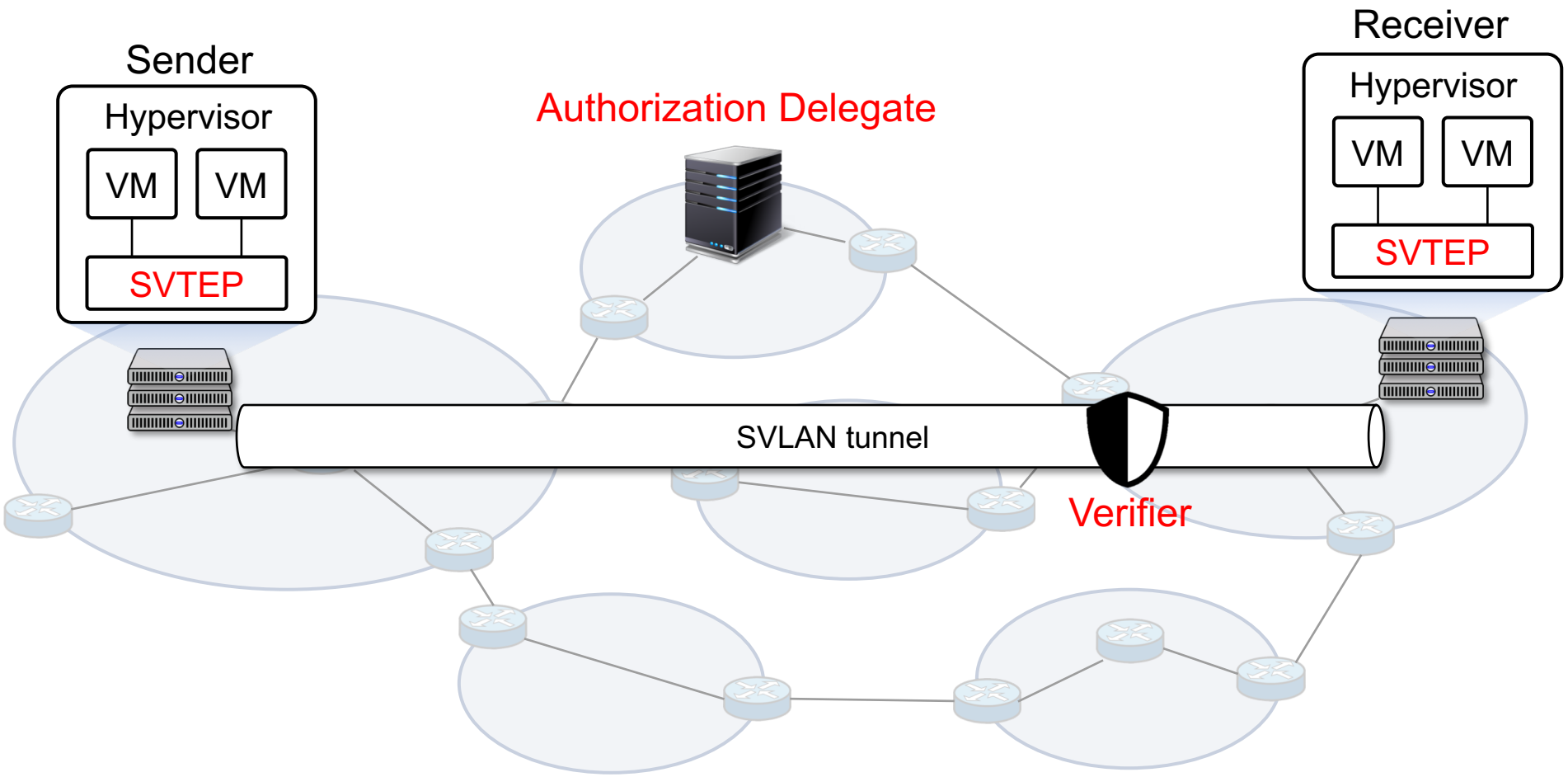
Challenges and Countermeasures



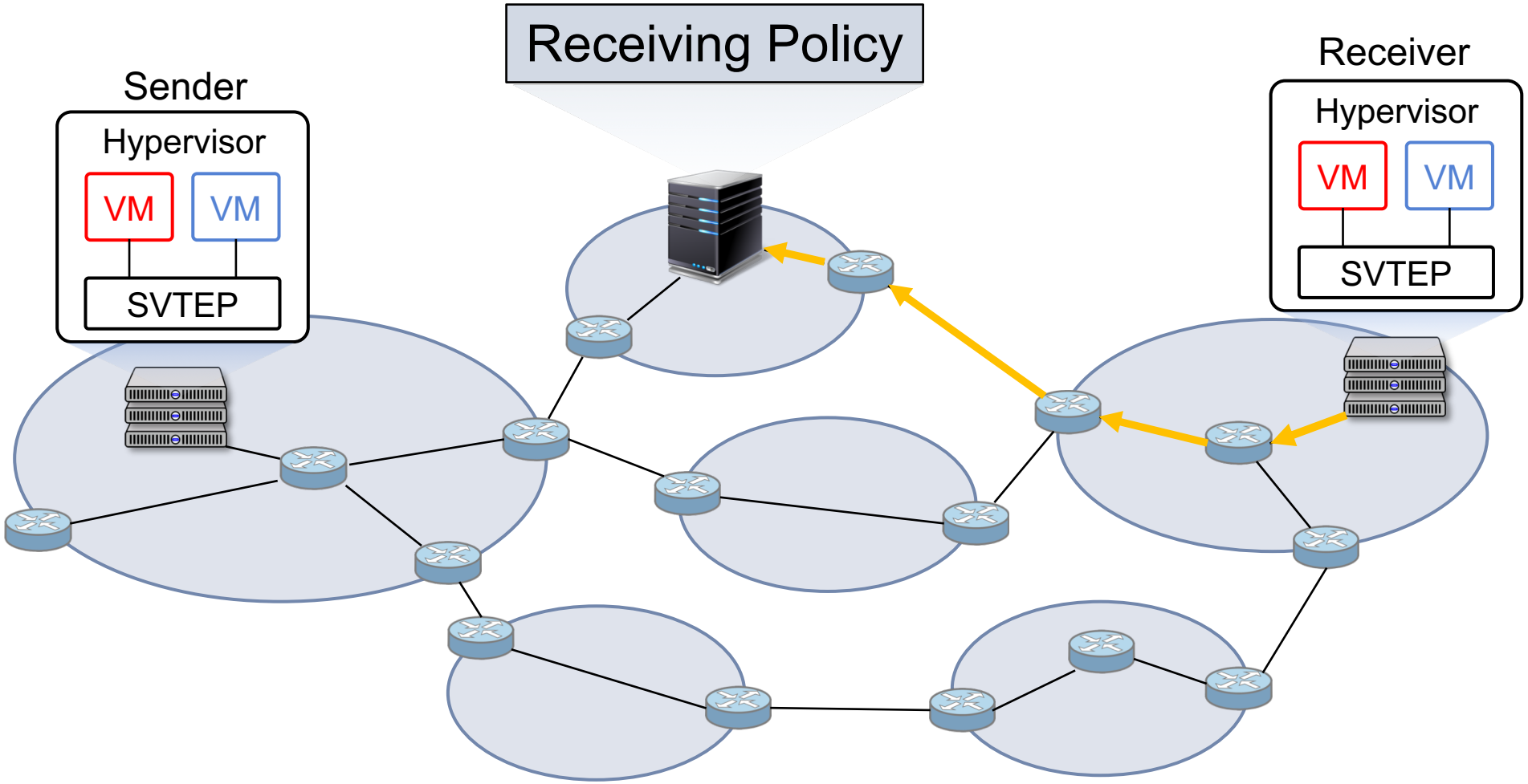
Our Vision on Secure and Scalable Network Virtualization



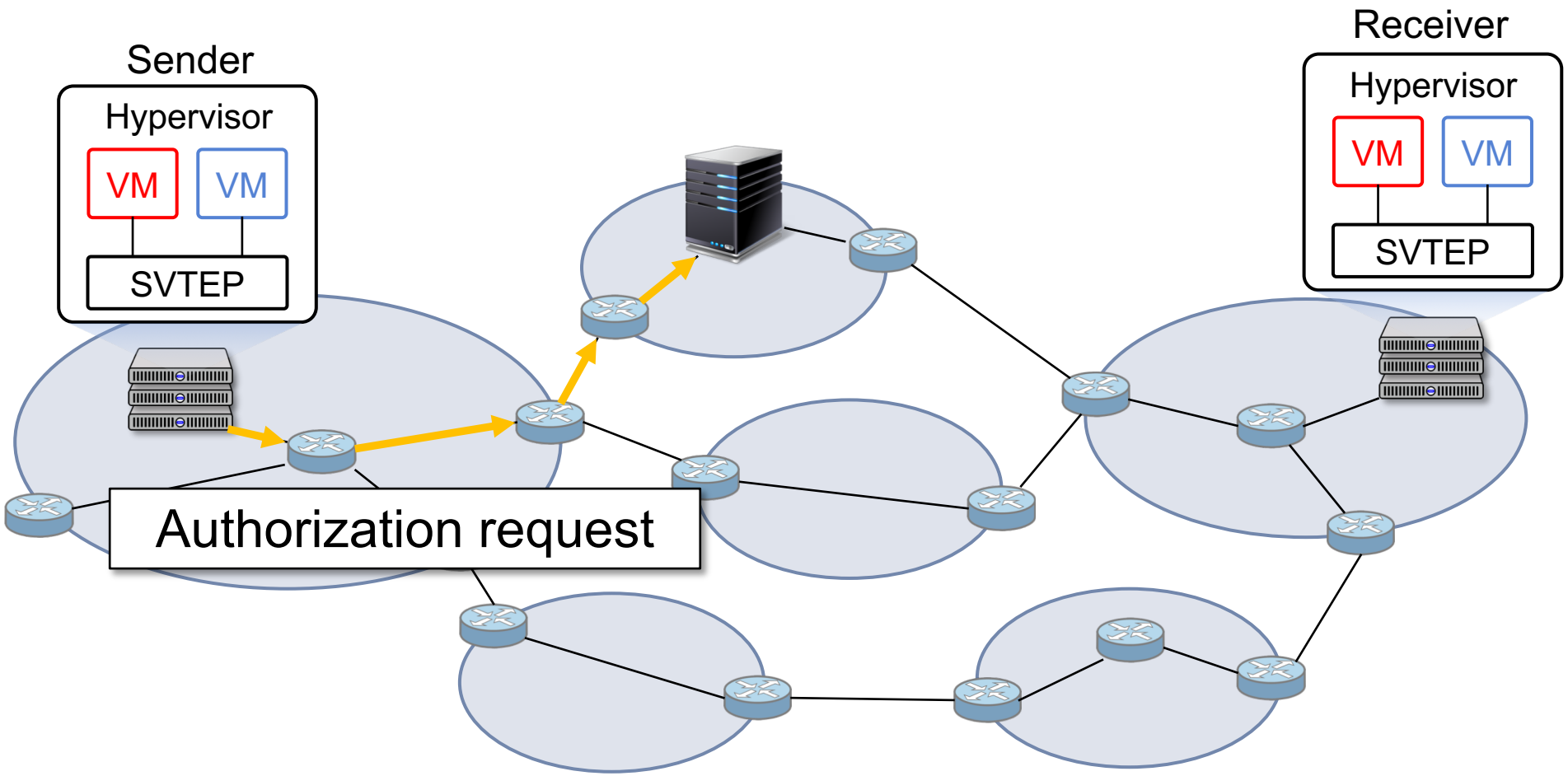
SVLAN (Secure & Scalable Virtual LAN) Overview



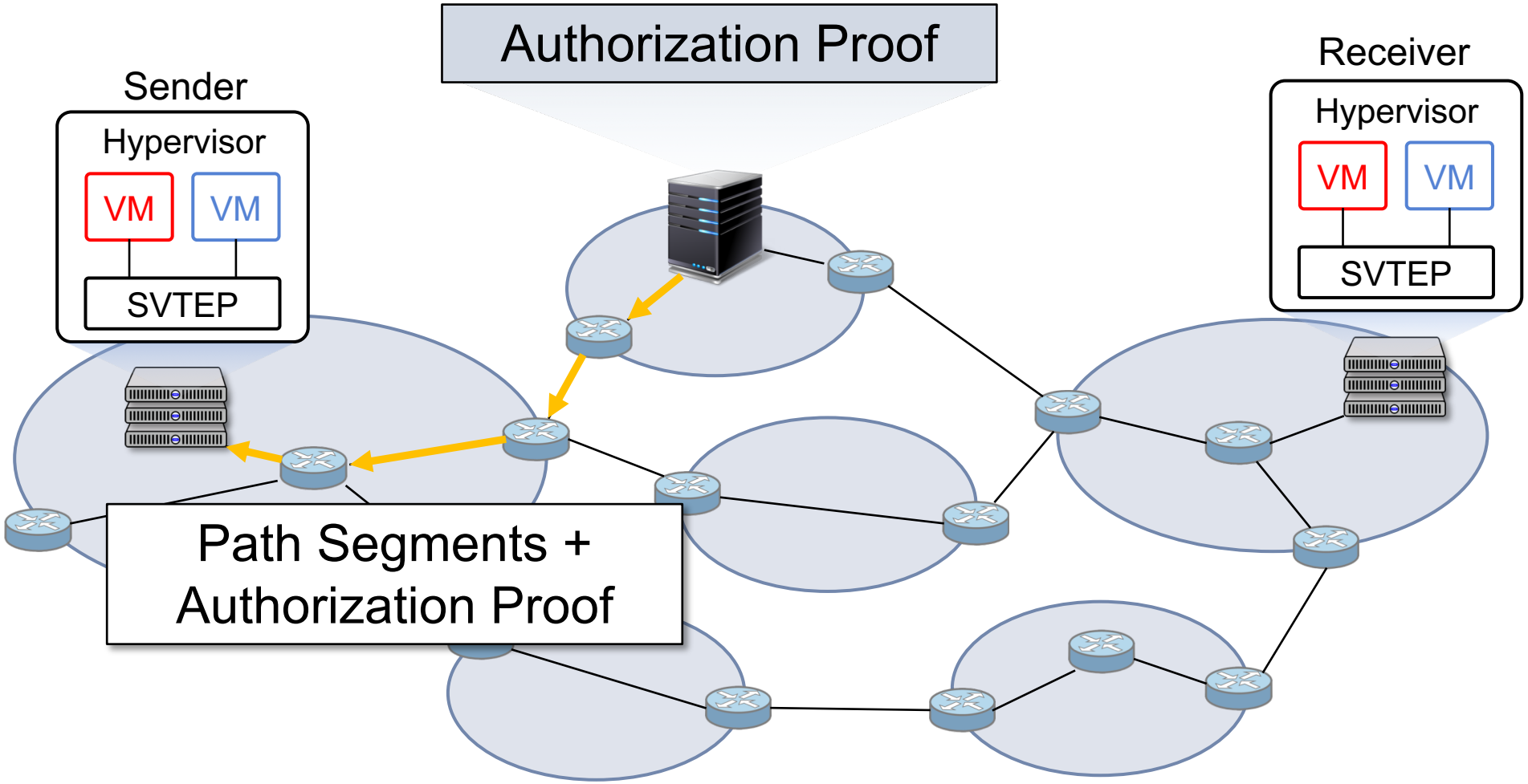
Express Receiver's Consent



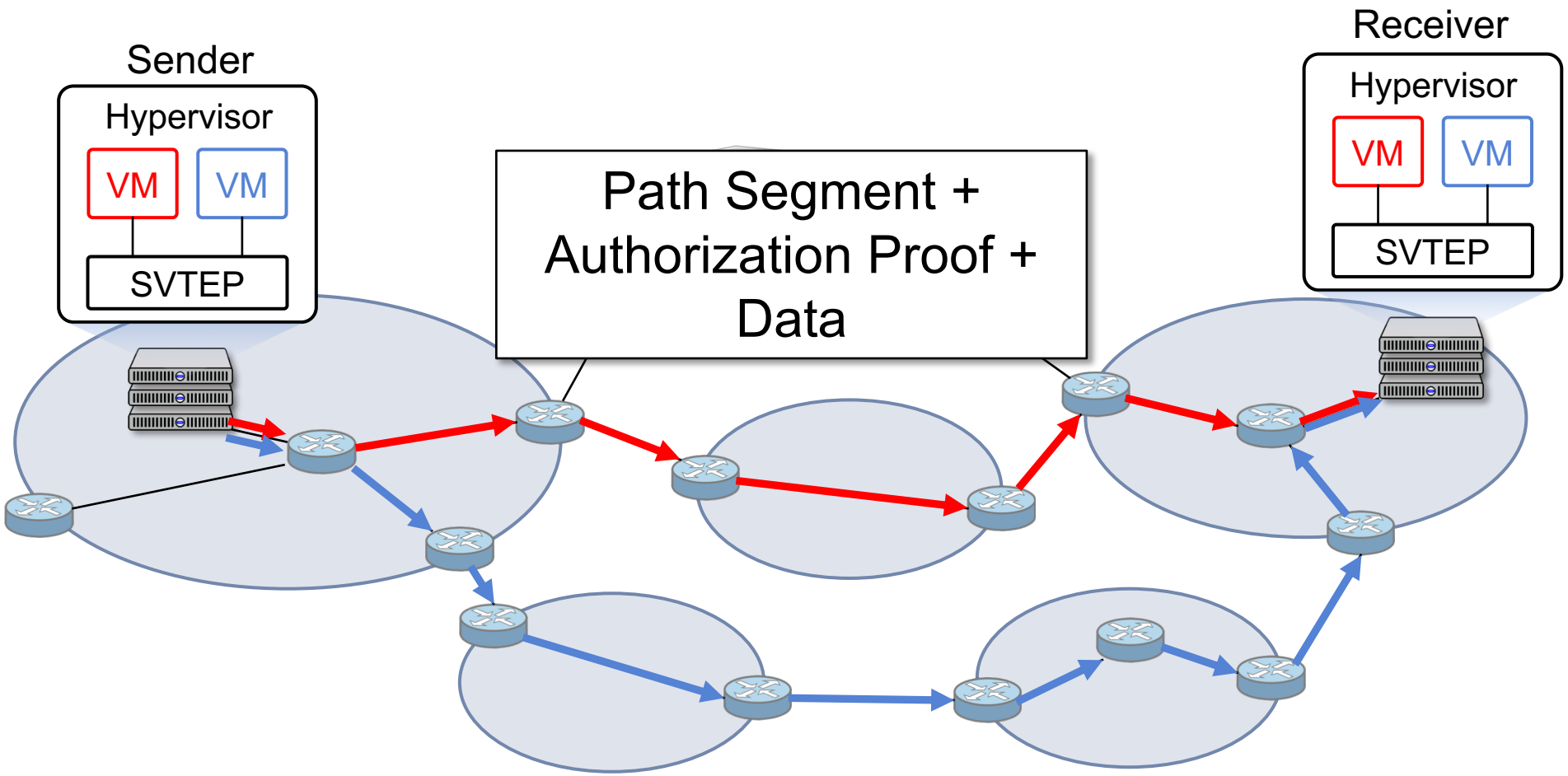
Acquiring Receiver's Consent



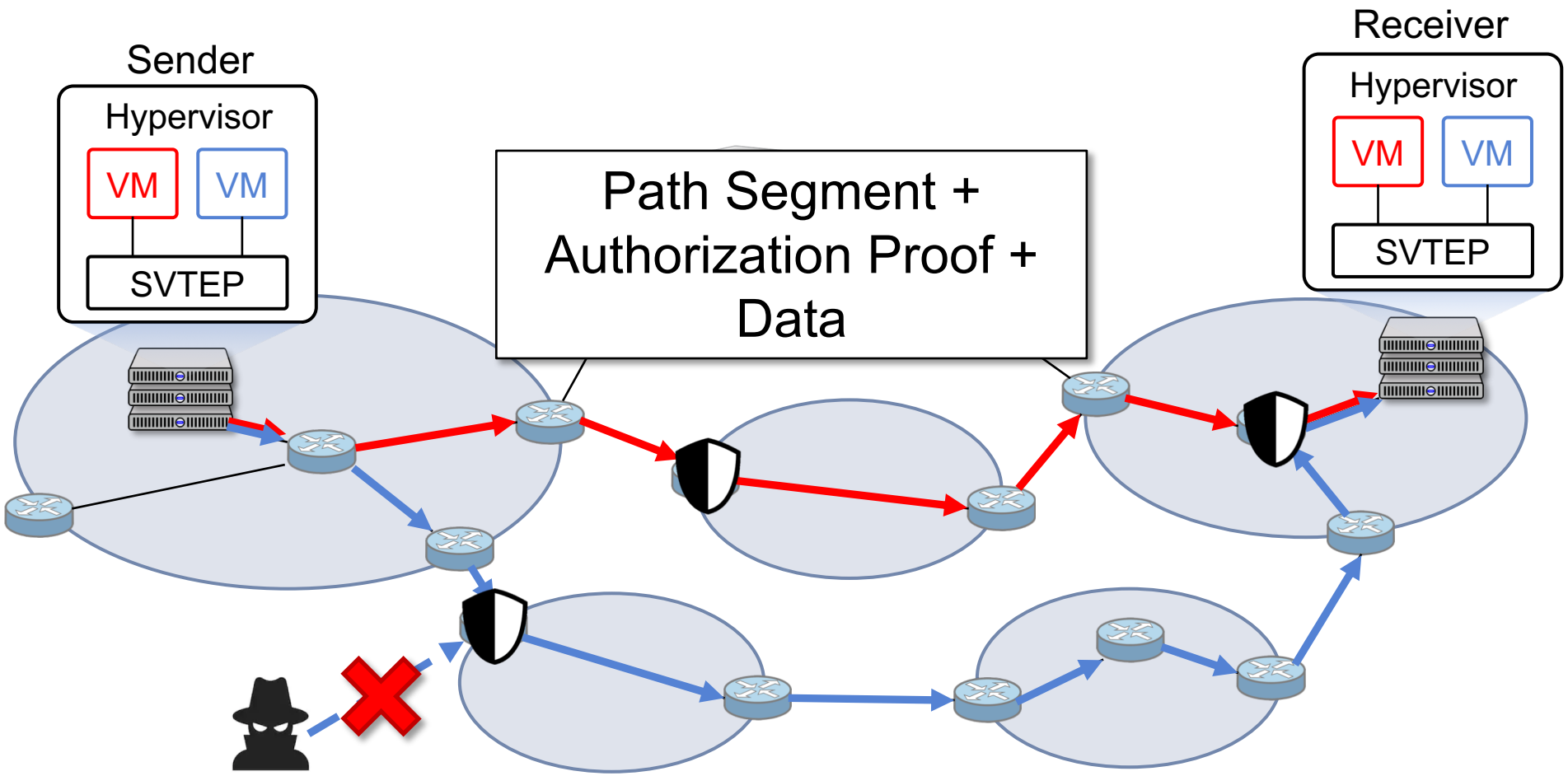
Acquiring Receiver's Consent



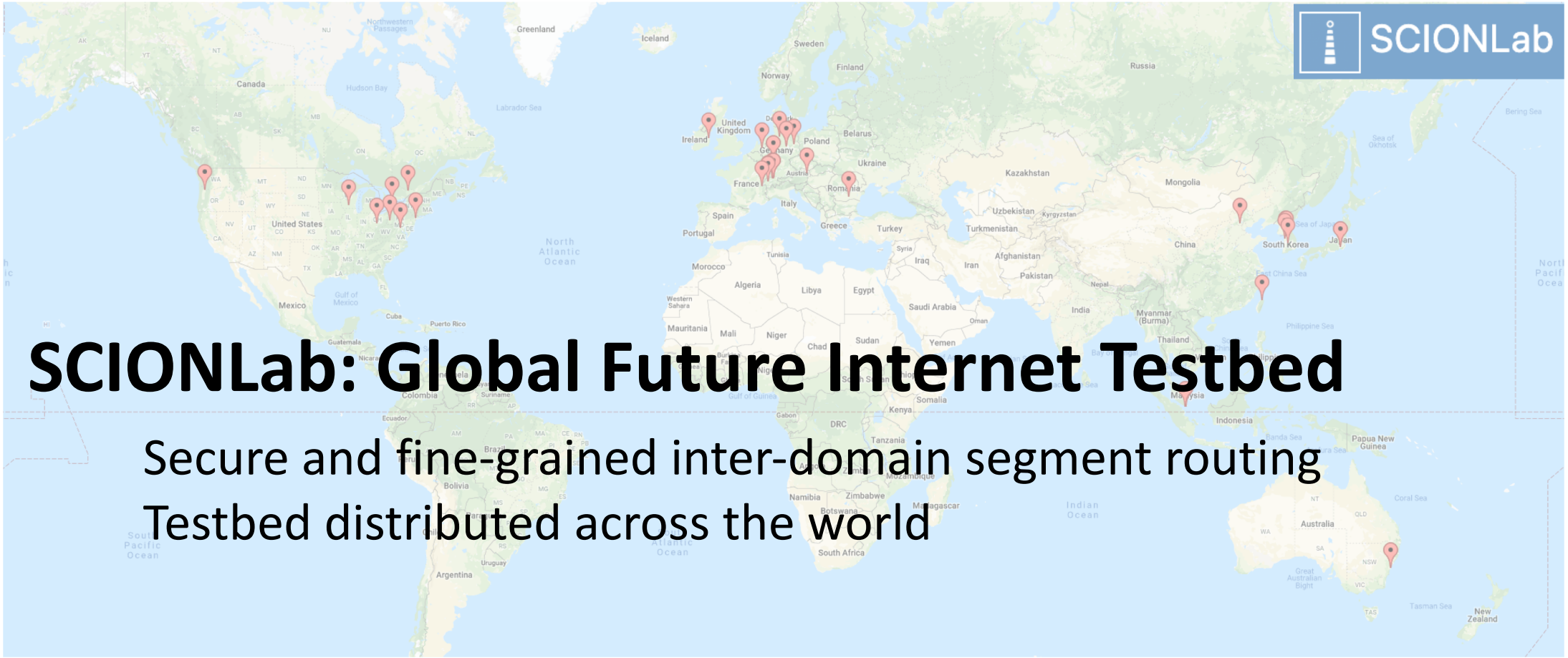
SVLAN Packet Forwarding



Verifying the Validity of Packets



Proof-of-Concept Implementation in SCIONLab



https://github.com/scionproto/scion
https://www.scionlab.org

Cracking the Authorization Proof is Impractical

TABLE III: The number of packets per second (PPS) and the required time to brute-force the SVLAN MAC (in years) for different link bandwidths.

	64-bit MAC		128-bit MAC	
Link	PPS	Time [years]	PPS	Time [years]
1Gbps	976562	5.99e6	919177	1.17e25
10Gbps	9765625	5.99e5	9191176	1.17e24
100Gbps	97656250	5.99e4	91911764	1.17e23

Brute-force attack would require 60000 years on 100 Gbps line to break 64-bit MAC

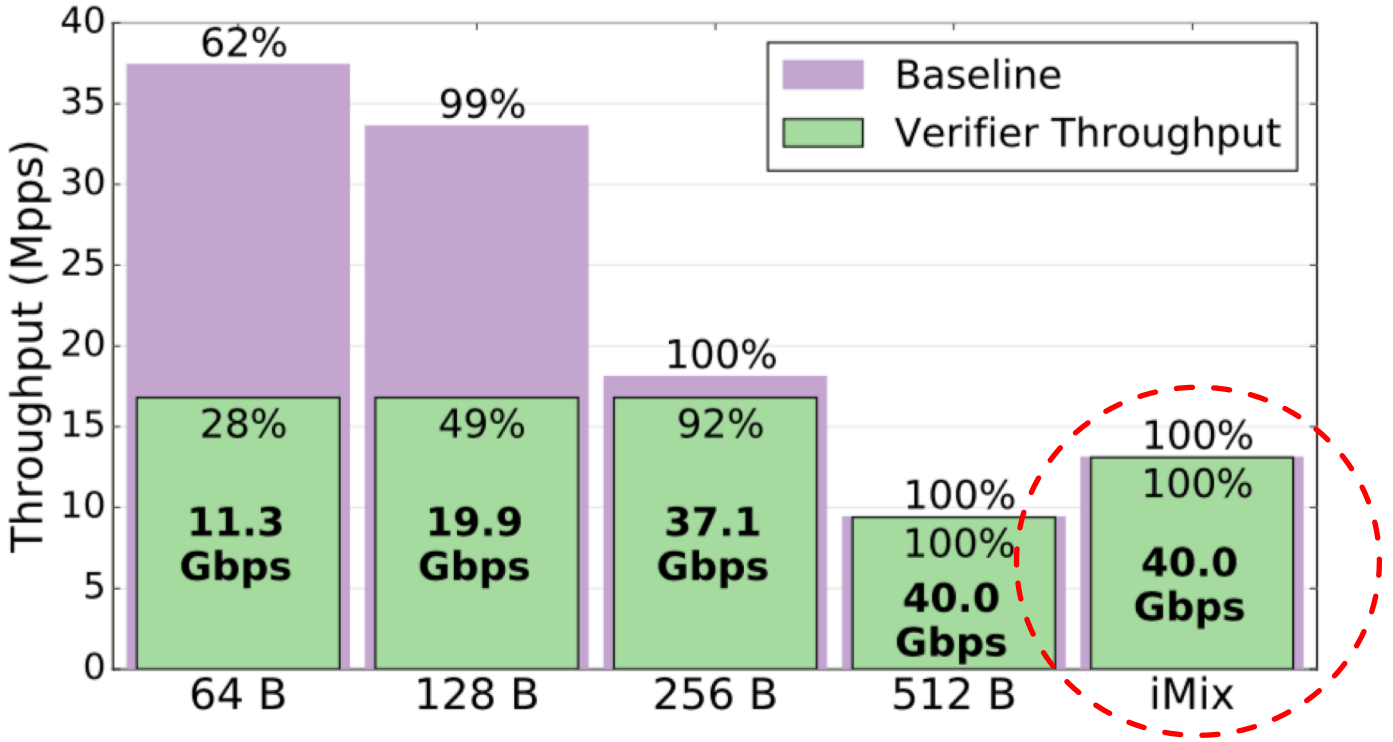
No Significant Bandwidth Overhead

TABLE II: Comparison of the header sizes, maximum payload, and network performance on a 1Gbps link. The SVLAN header contains three segment labels and one authorization proof.

			SVLAN	
	Ethernet	VXLAN	SR-MPLS	SCION
Extra header (bytes)	-	50	36	60
Max payload (bytes)	1460	1410	1424	1400
Max goodput (Mbps)	949	916	926	910

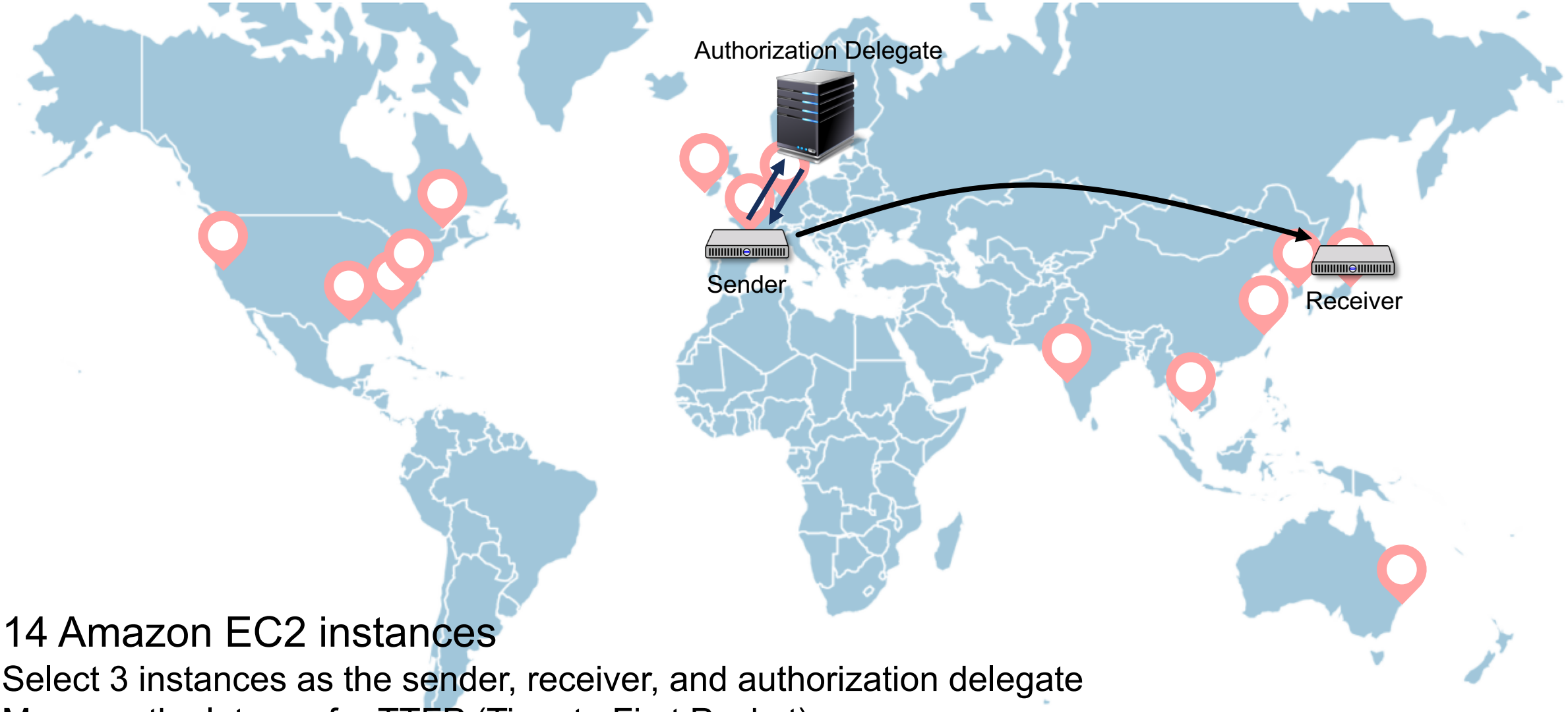
- SR-MPLS
  - 36 bytes of additional header
    - 12 bytes of MPLS labels (three labels)
    - 24 bytes of proof
- SCION
  - 60 bytes of additional header
    - 24 bytes of forwarding paths (three labels)
    - 32 bytes of extra header

Small Forwarding Performance Overhead



iMIX profiles the proportion of packets of a certain size based on statistical sampling from actual Internet traces

Latency Inflation Measurements in Cloud



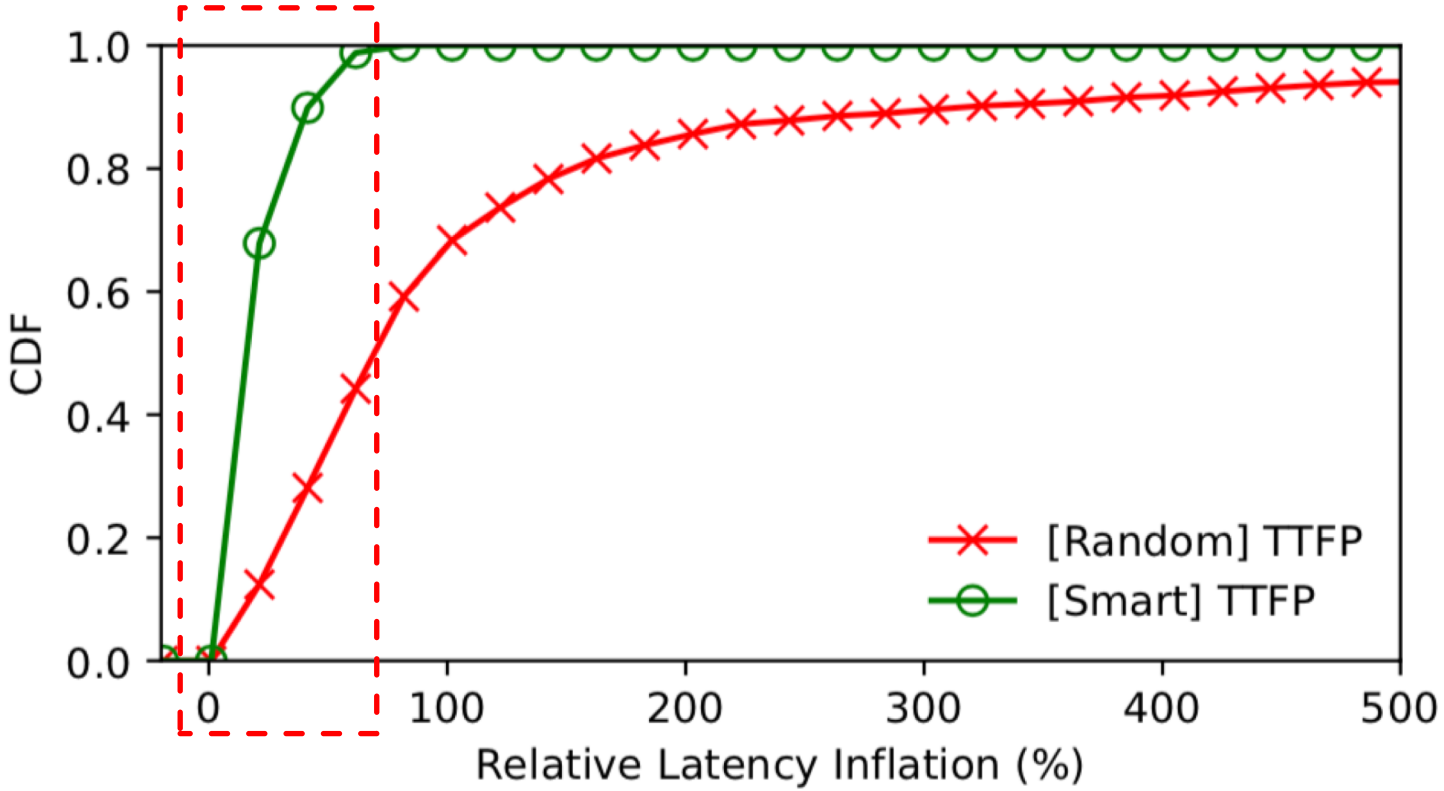
14 Amazon EC2 instances

Select 3 instances as the sender, receiver, and authorization delegate

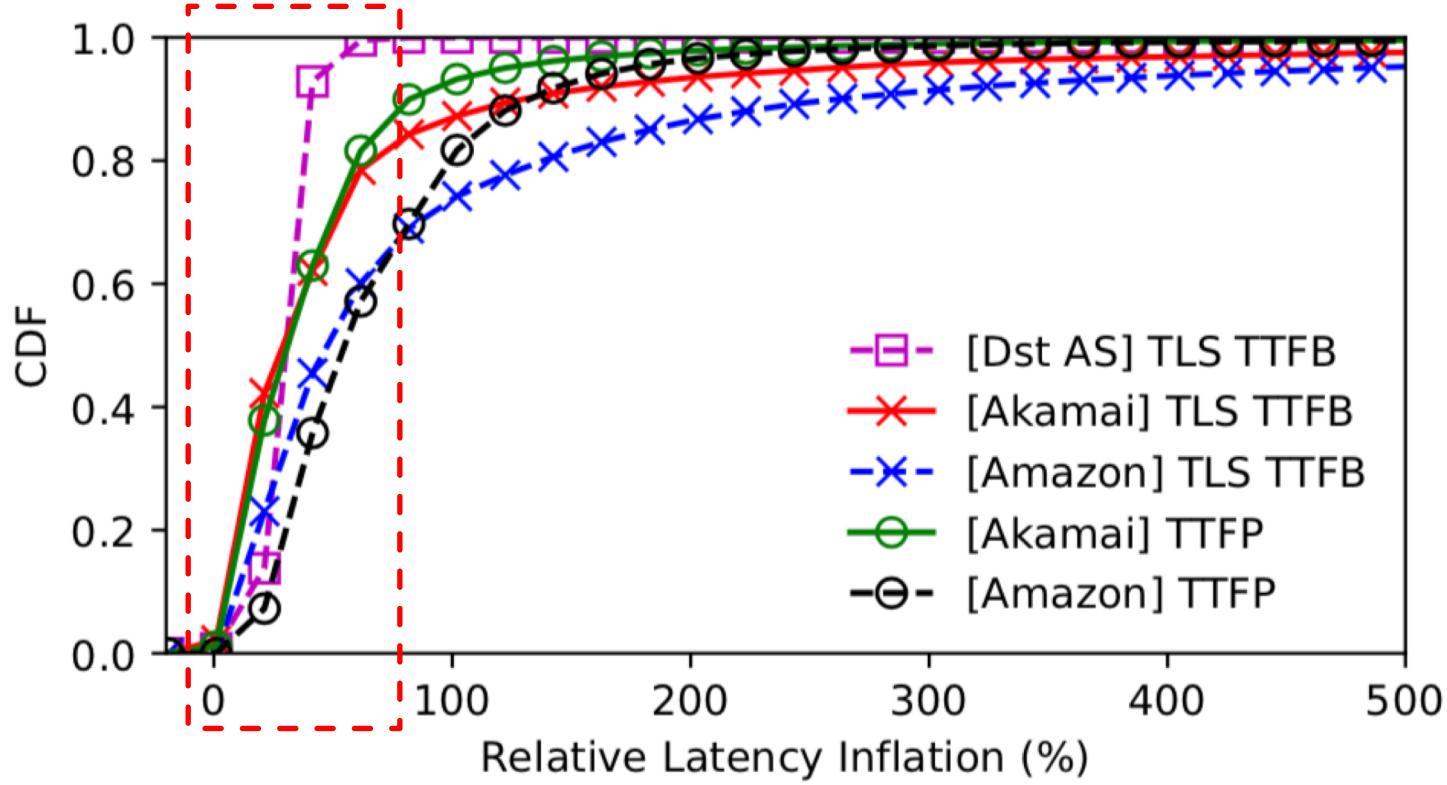
Measure the latency for TTFP (Time to First Packet)

Latency Inflation with AD on Amazon Cloud

< 75% of latency inflation



Large-scale Simulation



SVLAN, Expected Benefits

Scalability

- Highly scalable network virtualization
  - Unlimited number of VNI
  - Stateless VTEP

Flexibility

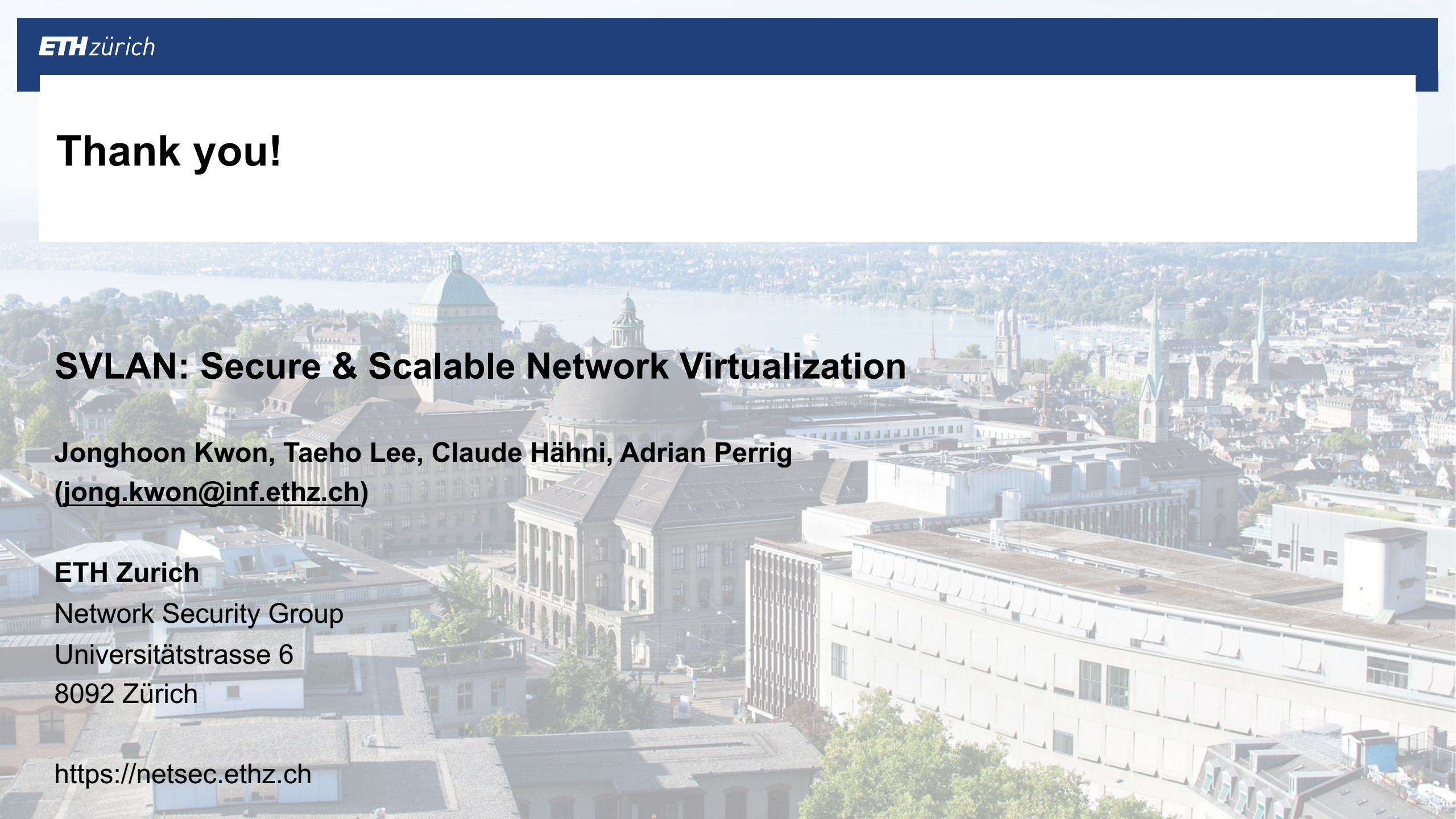
- Flexible network management
  - Receiving policy at different granularity
  - Easy update for virtual network

Security

- Secure isolation from unwanted traffic
  - Only authorized packets get forwarded
  - Adversaries cannot impersonate authorized senders

Performance

- Reducing network overhead
  - No ARP flooding
  - Negligible latency influence



Thank you!

SVLAN: Secure & Scalable Network Virtualization

Jonghoon Kwon, Taeho Lee, Claude Hähni, Adrian Perrig
(jong.kwon@inf.ethz.ch)

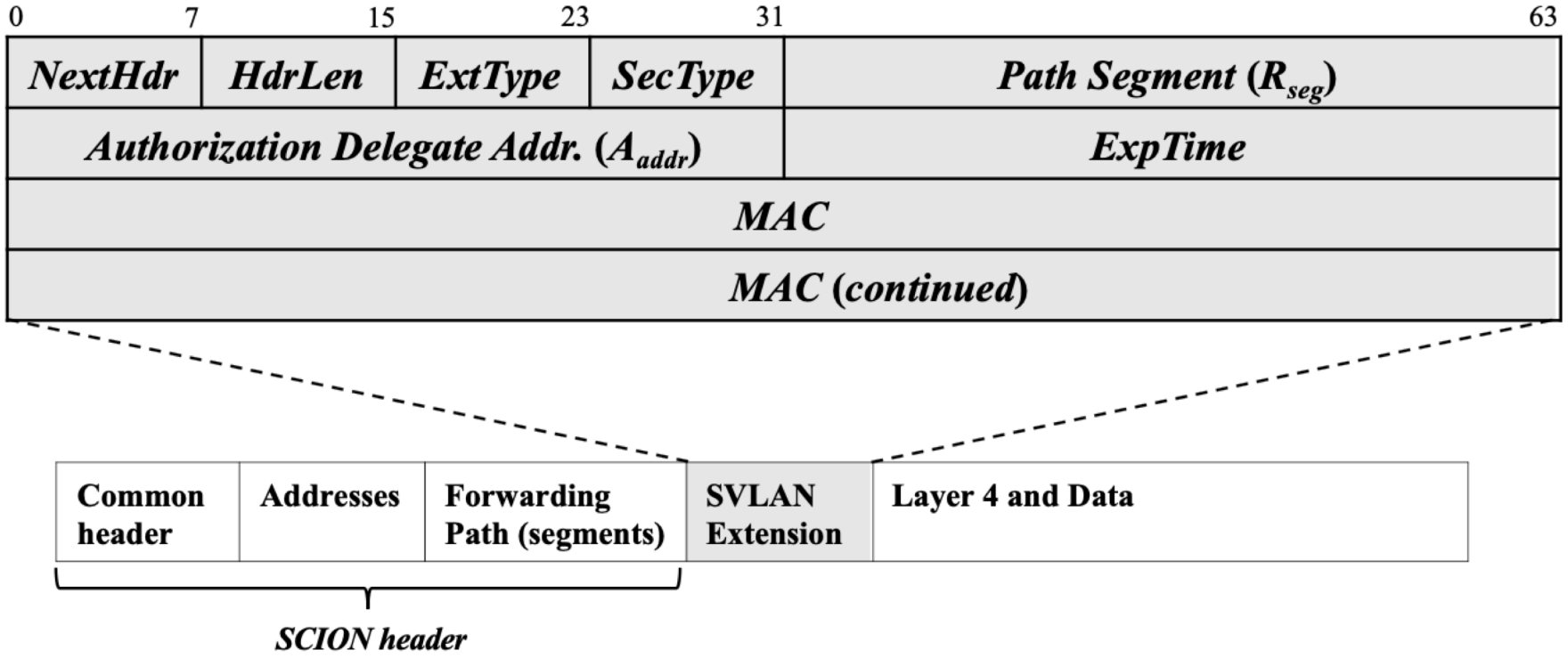
ETH Zurich
Network Security Group
Universitätstrasse 6
8092 Zürich

https://netsec.ethz.ch

Backup Slides

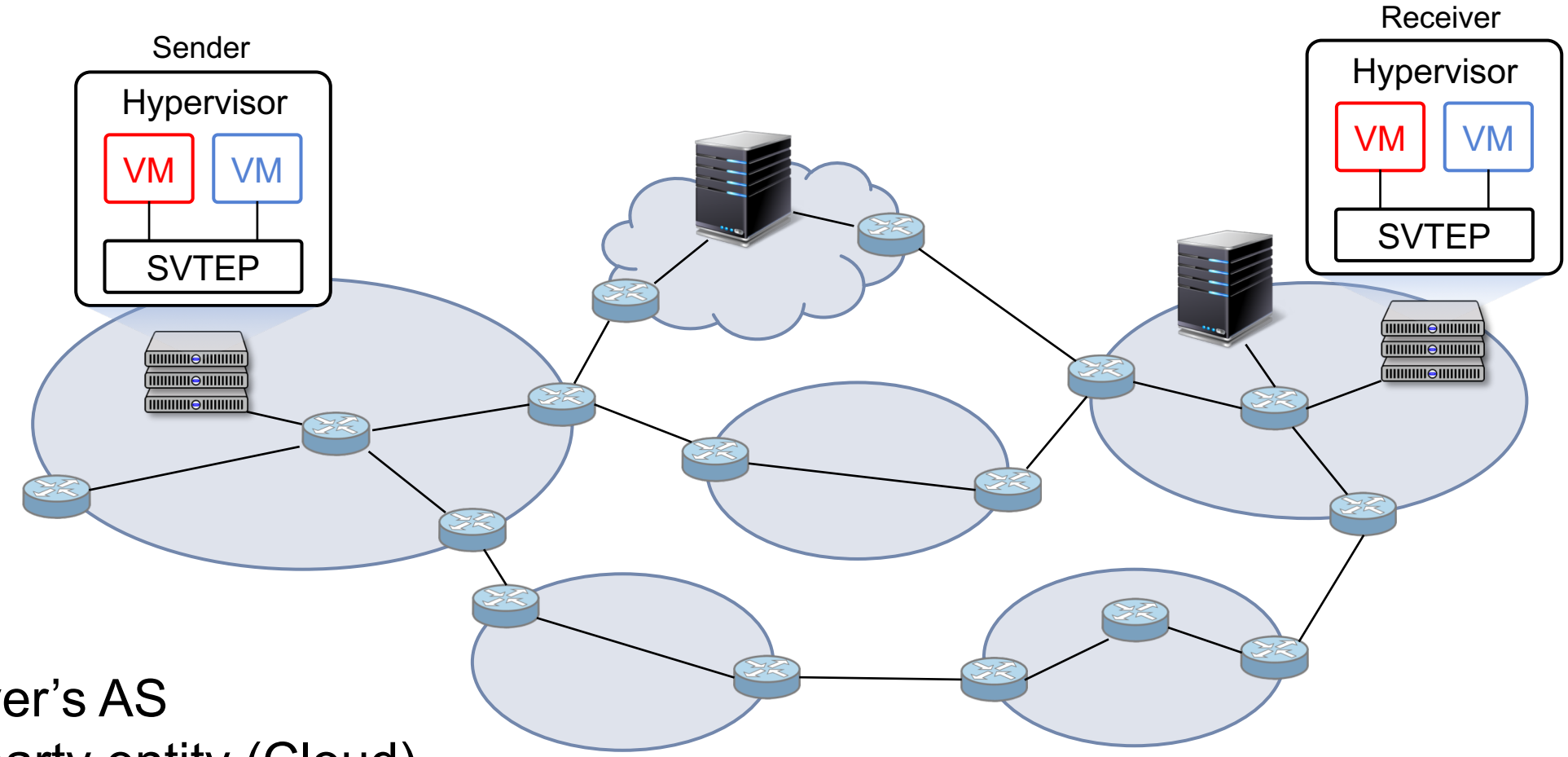
Implementation Example

SVLAN header format on SCION



Practical Consideration

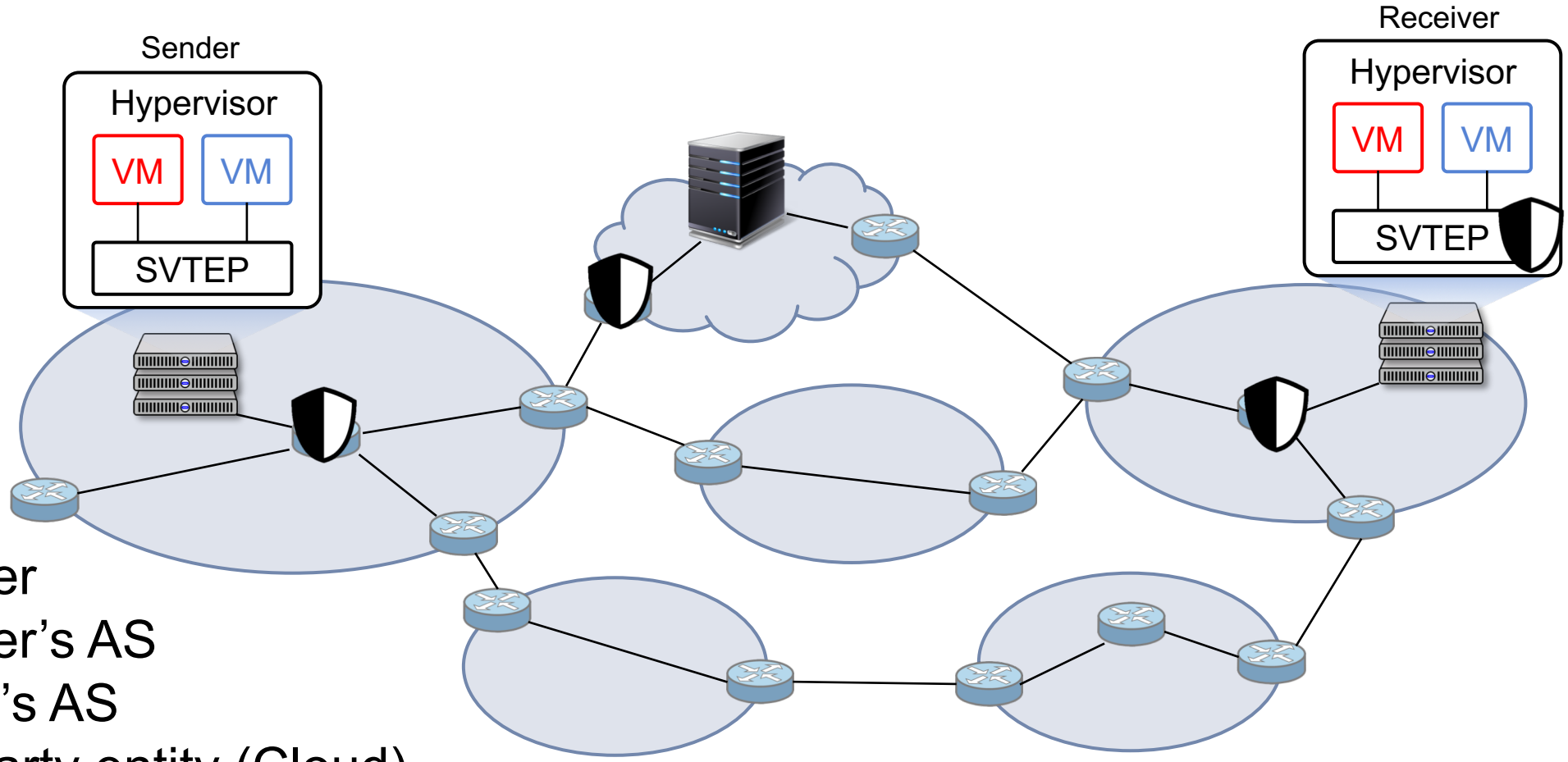
Location of Authorization Delegates



Receiver's AS
Third party entity (Cloud)

Practical Consideration

Location of Verifiers



Receiver
Receiver's AS
Sender's AS
Third party entity (Cloud)