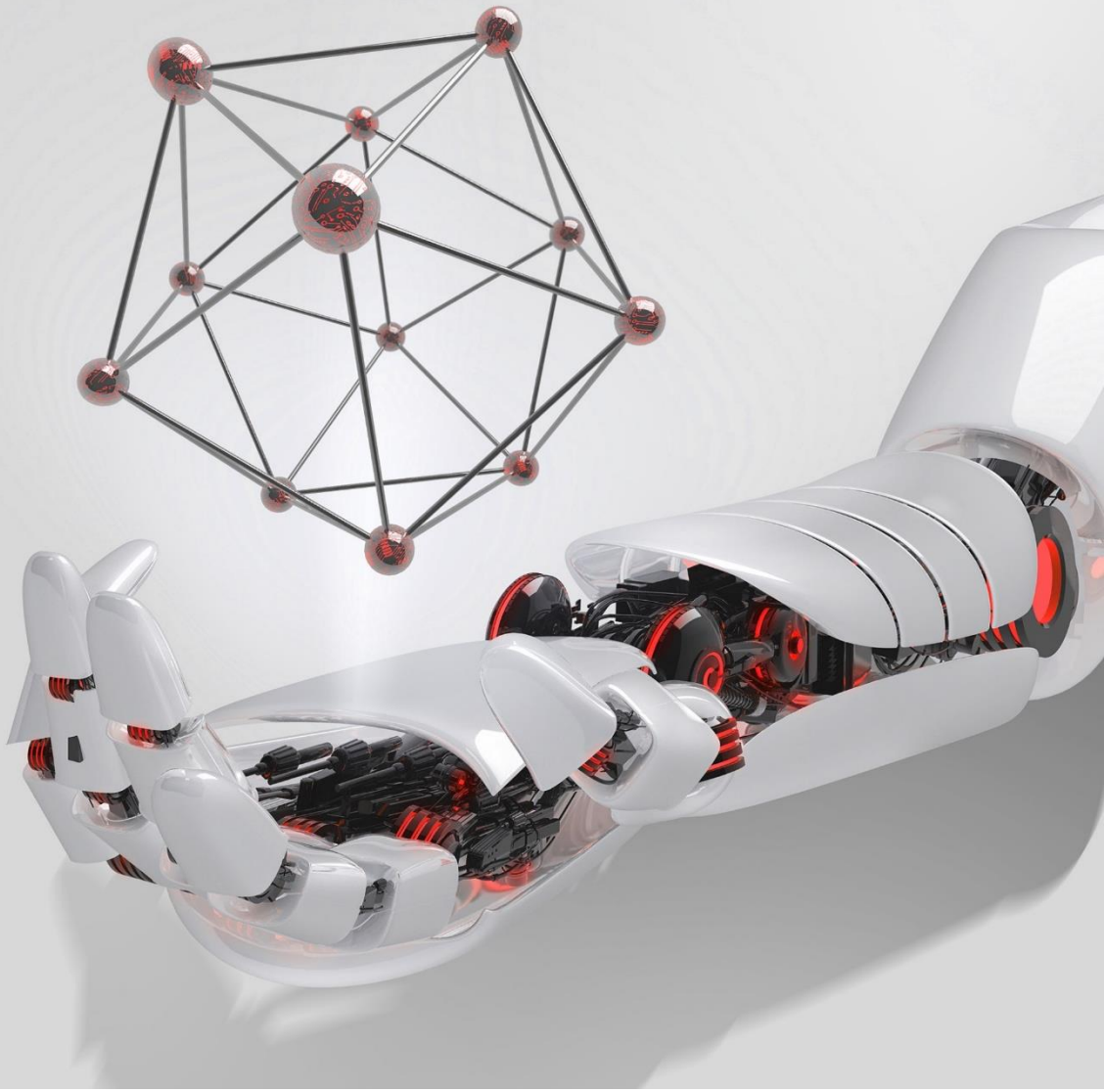
Zero Trust Networking



David Lou, Chief Researcher, Huawei Technologies

Zhe.lou@Huawei.com

HUAWEI

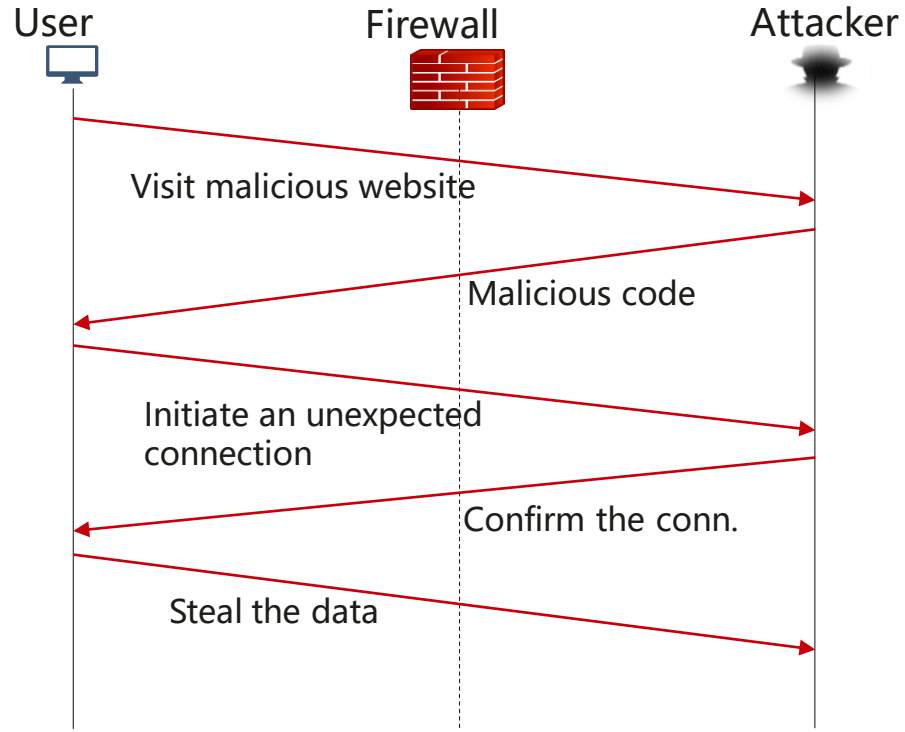
Outline

- Zero Trust Model Overview
- SASE and Potential Solution
- The Impact on the Network: Overlay vs Underlay
- Network Based Authentication and Authorization
- Anonymous Communication

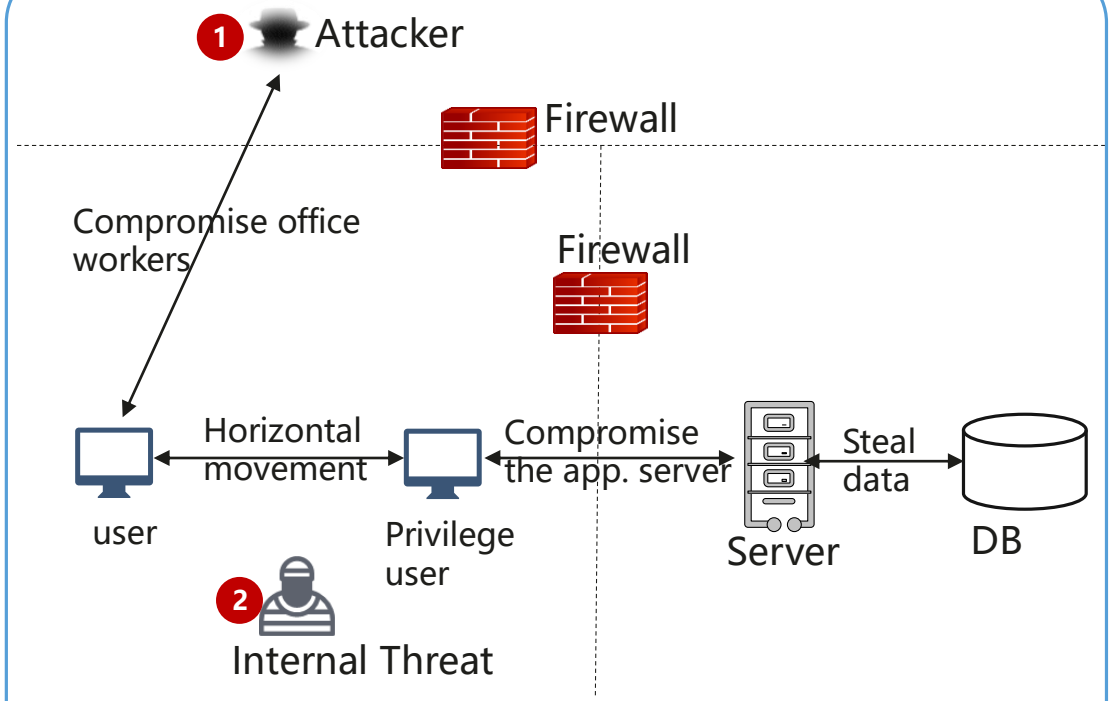
We built fortresses following the **castle-and-moat** model…


… the cloud has come…
… accompanied by IoT, edge computing and swarm computing…

The Problems of the "Castle-and-Moat" Model



Issue: the attacker could break the firewall by embedding malicious code in the response message



Once the attacker compromises one user/device, it can penetrate horizontally to other devices for illegal purposes

HUAWEI

The Concept of Zero Trust Model

- The concept of zero trust was first proposed by Forrester's chief analyst John Kindervag in 2010.
- "Never Trust, Always Verify" is the core of Zero Trust.
- The initial security posture has no implicit trust between different entities.

5 Assumptions

① The network is always a dangerous environment

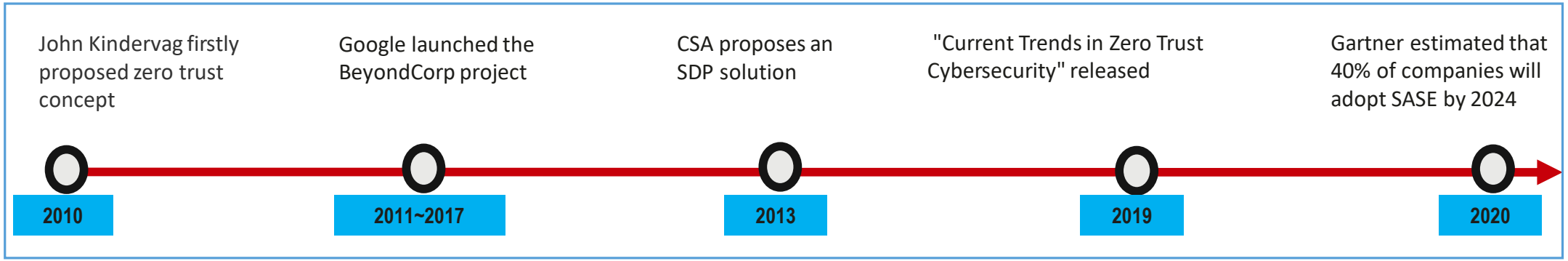
② There are external and internal threats throughout the network

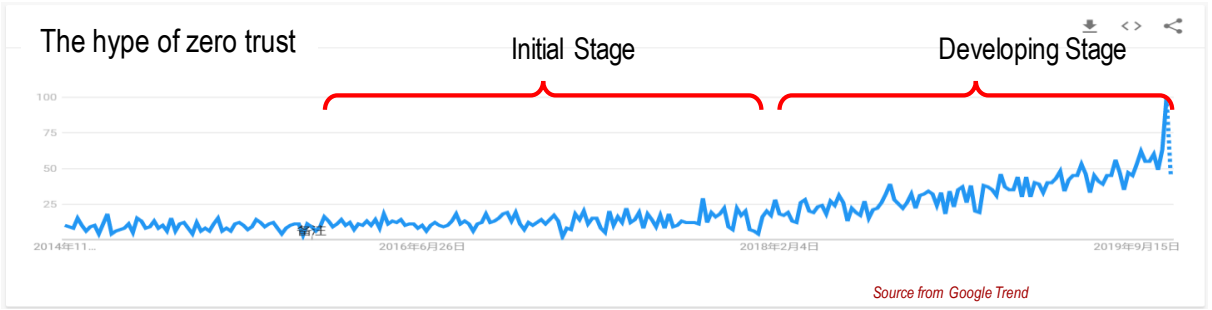
③ The location (inside or outside) is not sufficient to determine the credibility of the network

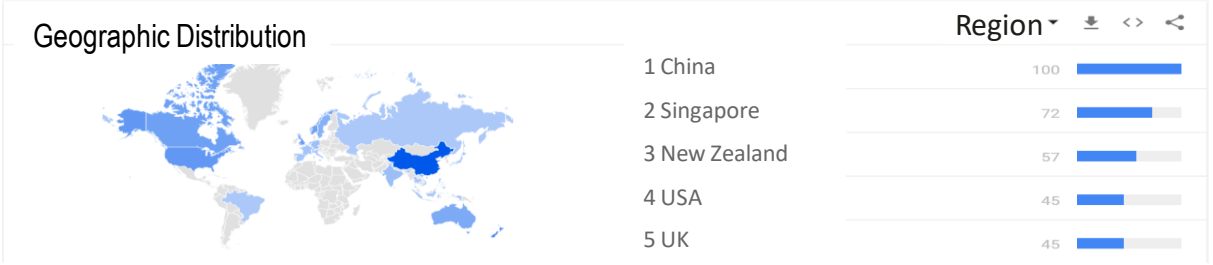
④ All equipment, users, and network traffic should be authenticated and authorized

⑤ The security policy must be dynamic and determined based on as many data sources as possible

The Development of Zero Trust Model







Zero Trust is currently in a period of rapid development, and it is expected that it will gradually enter a mature period in the next 3 to 5 years.

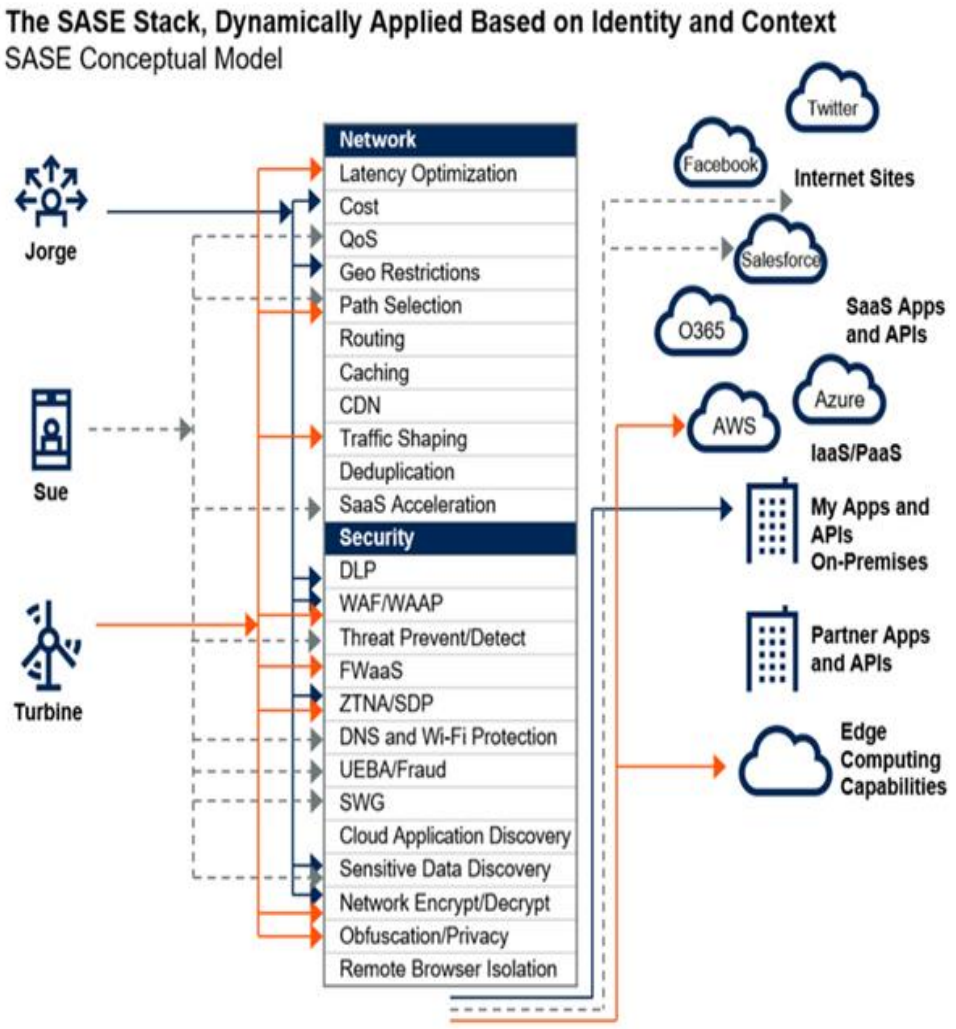
The popularity of zero trust is soaring, and the driving force behind it is the peak of the development of big data.

HUAWEI

Outline

- Zero Trust Model Overview
-  **SASE and Potential Solution**
- The Impact on the Network: Overlay vs Underlay
- Network Based Authentication and Authorization
- Anonymous Communication

SASE Overview



Zero Trust（ID Driven）

- User/Device auto-recognition
- Supporting multi-factor authentication and authorization

Cloud Oriented

- flexibility, self-adaptability, self-recovery and self-maintenance
- Provide a platform that can share customer expenses and provide maximum efficiency

Support Hetero. NW

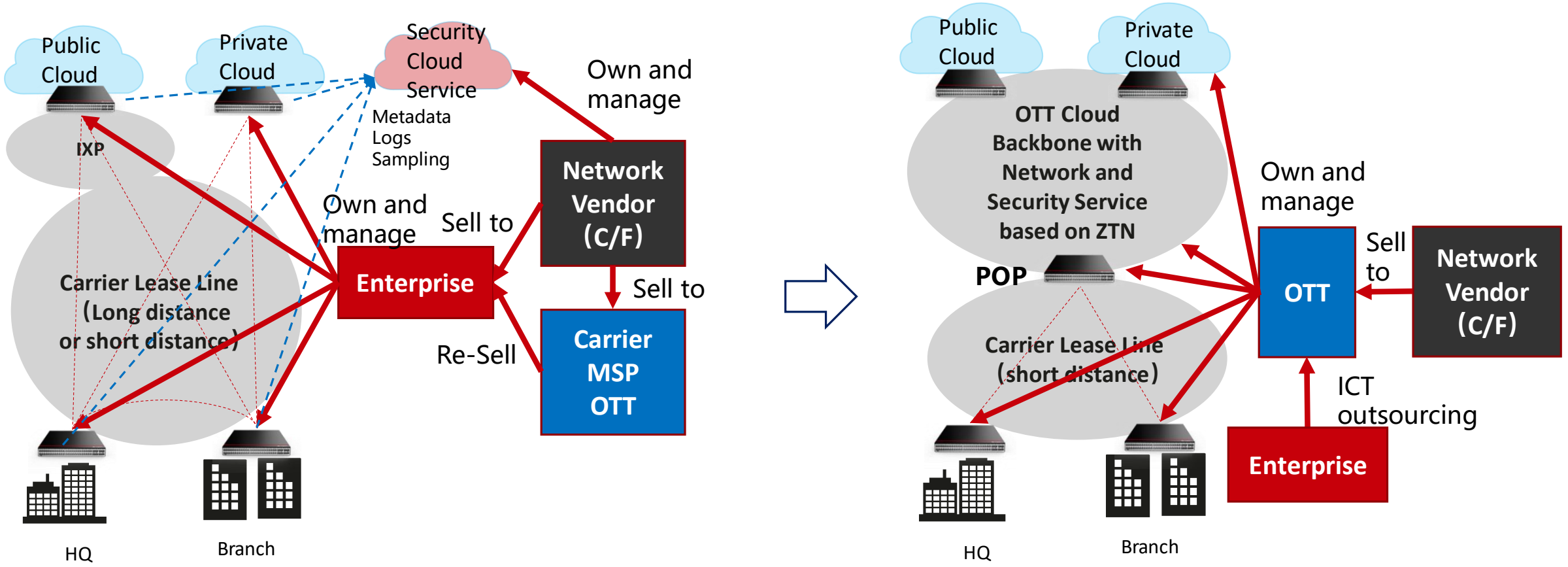
- Created a network for all resources -data centers, branch offices and cloud resources
- Support both physical and logical edges

Global Distribution

- To ensure that all network and security functions are available everywhere
- It must expand its coverage and deliver low-latency services to the edge of the enterprise

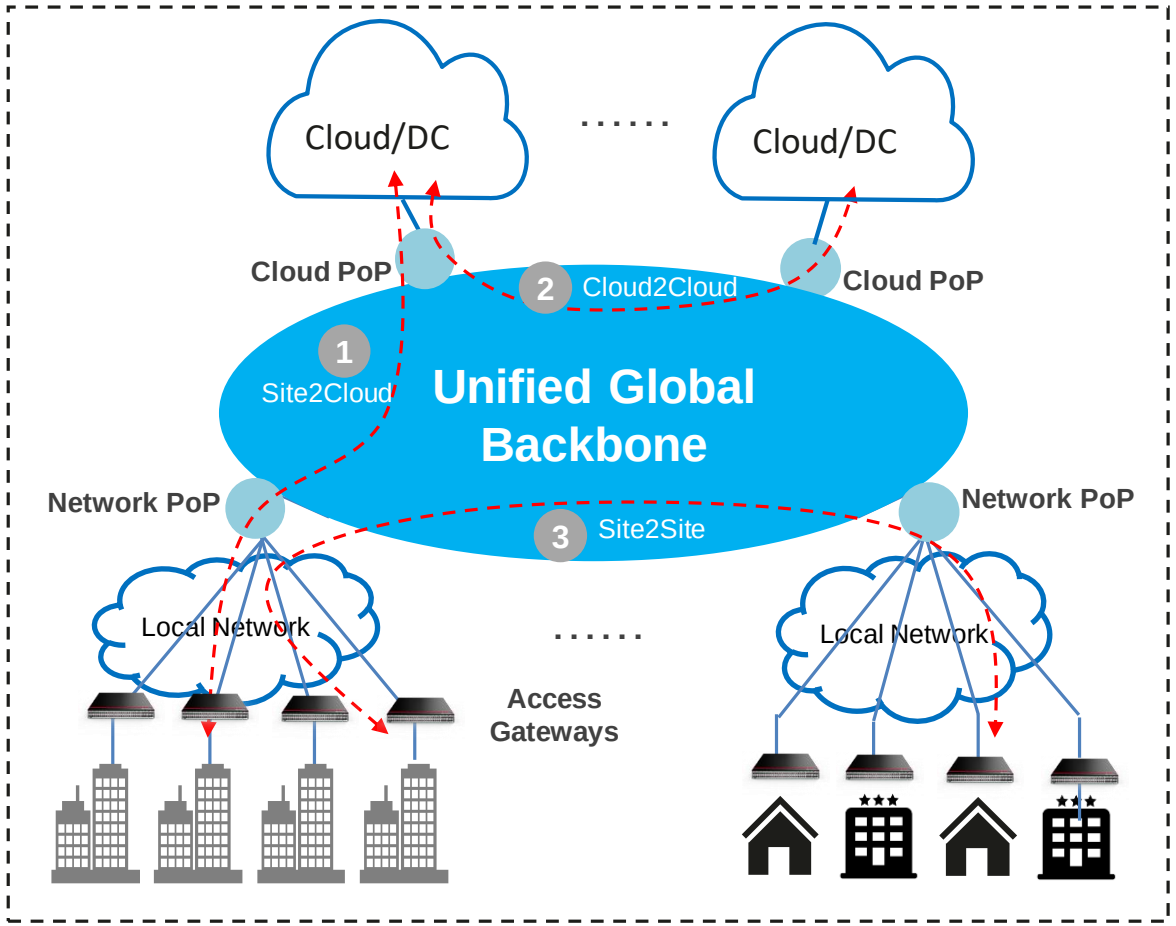
HUAWEI

SASE is Changing the Market



HUAWEI

A Unified Global Backbone



	Deployment	Key Feature
Cloud and Network PoPs	**Virtual software**	• SD-WAN • **Client VPN gateway（such SSL VPN， or L2TP over IPSec VPN）for personal** • DCI • Service Chain • SLA Measurement, Application Visibility, Experience Assurance, Intelligent Troubleshooting
Value-added Service	**Physical Hardware or Virtual software**	• AAA • **Access control** • **Identity-based and application-based dynamic policy control** • Security-as-a-service (such as FWaaS, IPS, URL filtering, Anti-Virus, **Anti-DDoS**, SWG, DNS filtering, security sandbox, AMP) • ZTN based Traffic Security analysis
Access gateway	**Physical Hardware or Virtual software**	• SD-WAN • SLA Measurement • Application Visibility • Experience Assurance • Intelligent Troubleshooting • **Basic security** (such as IPSec, **device authentication, basic Anti-DDoS**)

HUAWEI

Outline

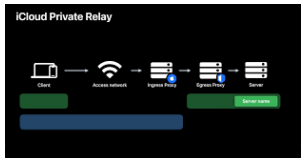
- Zero Trust Model Overview
- SASE and Potential Solution
-  **The Impact on the Network: Overlay vs Underlay**
- Network Based Authentication and Authorization
- Anonymous Communication

Overlay Implementations

Pros

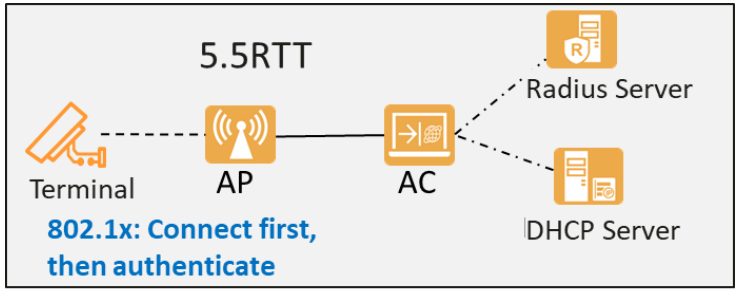
- Software based modular design and development
- Can be deployed easily with an appropriate business case.
- Can be upgraded and maintained easily

BeyondCorp

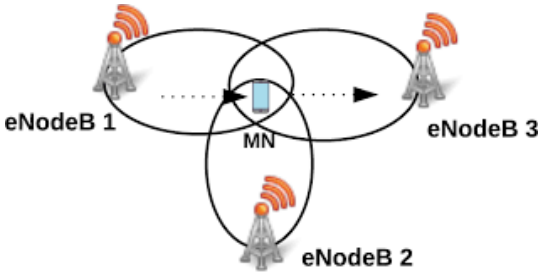


Cons

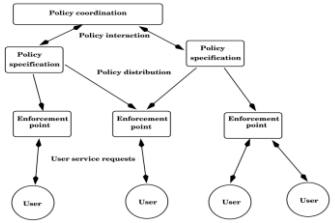
- Relative low performance and high latency, might not be suitable for a number of scenarios
  - power-limited scenarios like IoT
  - mobile services/applications



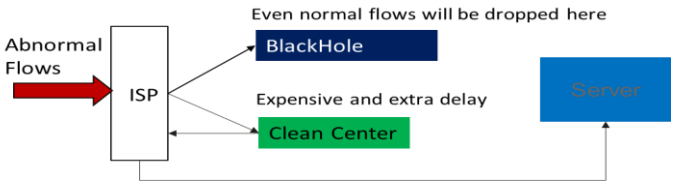
IEEE 802.1X



Ref: F. Abdullah, "Handover authentication latency reduction using mobile edge computing and mobility patterns"
K. Park, "Authentication Latency Reduction Technique for Secure and Seamless Ubiquitous Services"



Ref: A. Keromytis, "Requirements for Scalable Access Control and Security Management Architectures"



HUAWEI

Offload Capabilities to the Underlay

WHY

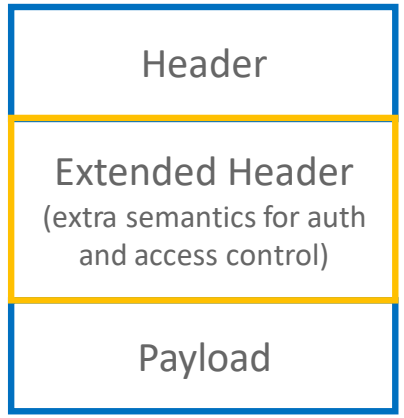
- Performance consideration for time sensitive applications
- Deployment issues
- Underlay visibility is critical to the overlay solutions
- Leverage the in network computation

WHAT

- Identity and Device Authentication
- Network/Service/Application Access Control
- DDoS Attack resiliency and mitigation
- Anonymous Networking and Communication
- …

HOW

- Implement required changes in the network protocols



Outline

- Zero Trust Model Overview
- SASE and Potential Solution
- The Impact on the Network: Overlay vs Underlay
-  **Network Based Authentication and Authorization**
- Anonymous Communication

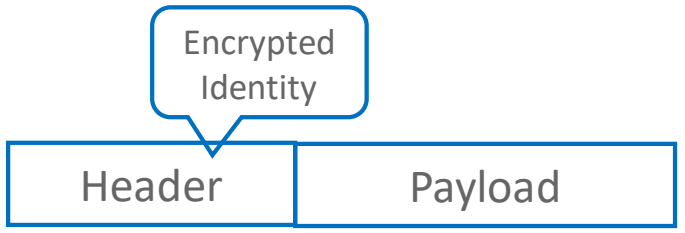
Network Based Security Technologies

a. TECH 1: Network based Authentication

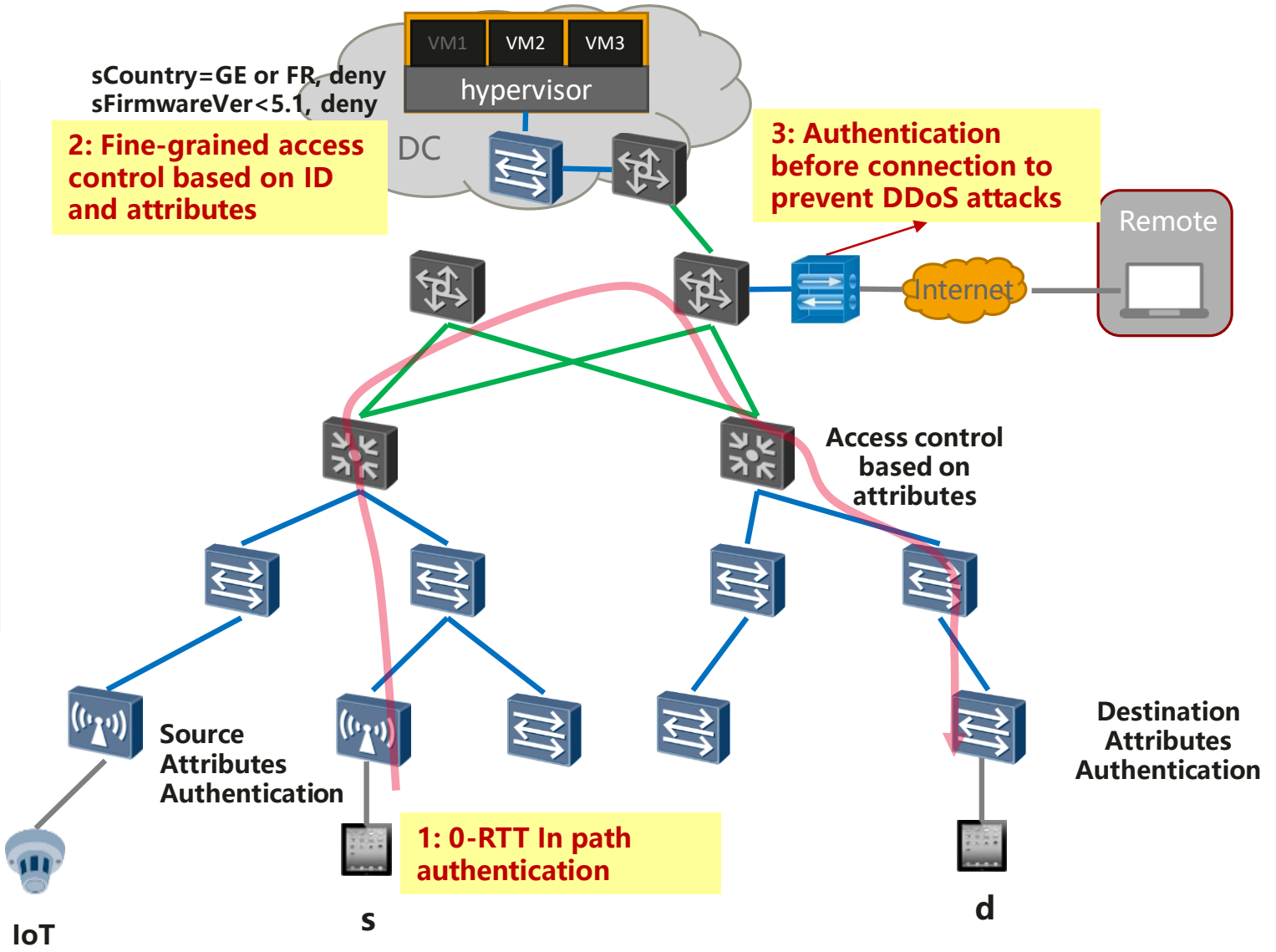
b. TECH 2: Network based Access Control

c. TECH 3: ID based DDoS Defense Mechanism

d. …



Network layer protocol

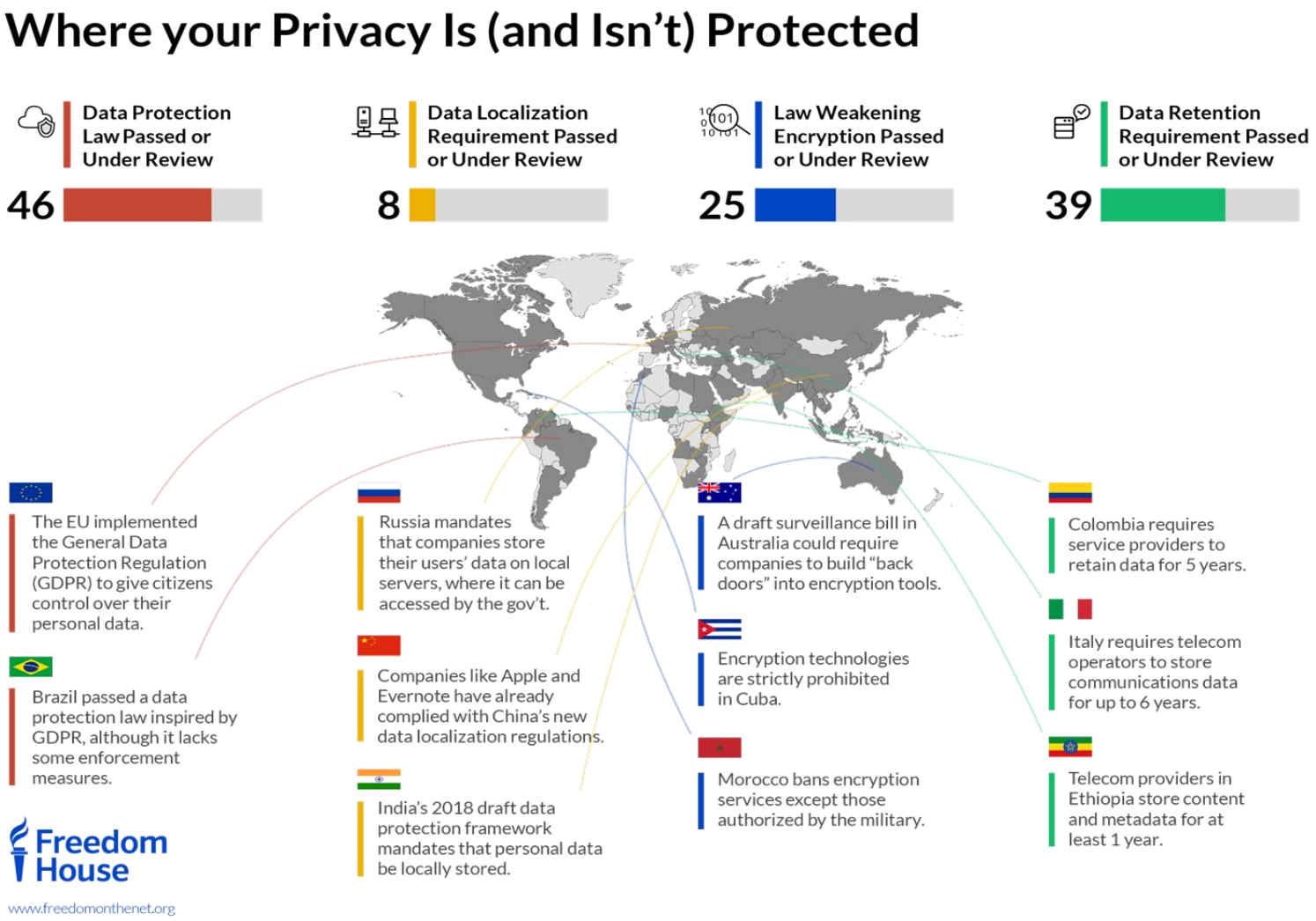


HUAWEI

Outline

- Zero Trust Model Overview
- SASE and Potential Solution
- The Impact on the Network: Overlay vs Underlay
- Network Based Authentication and Authorization
- **Anonymous Communication**

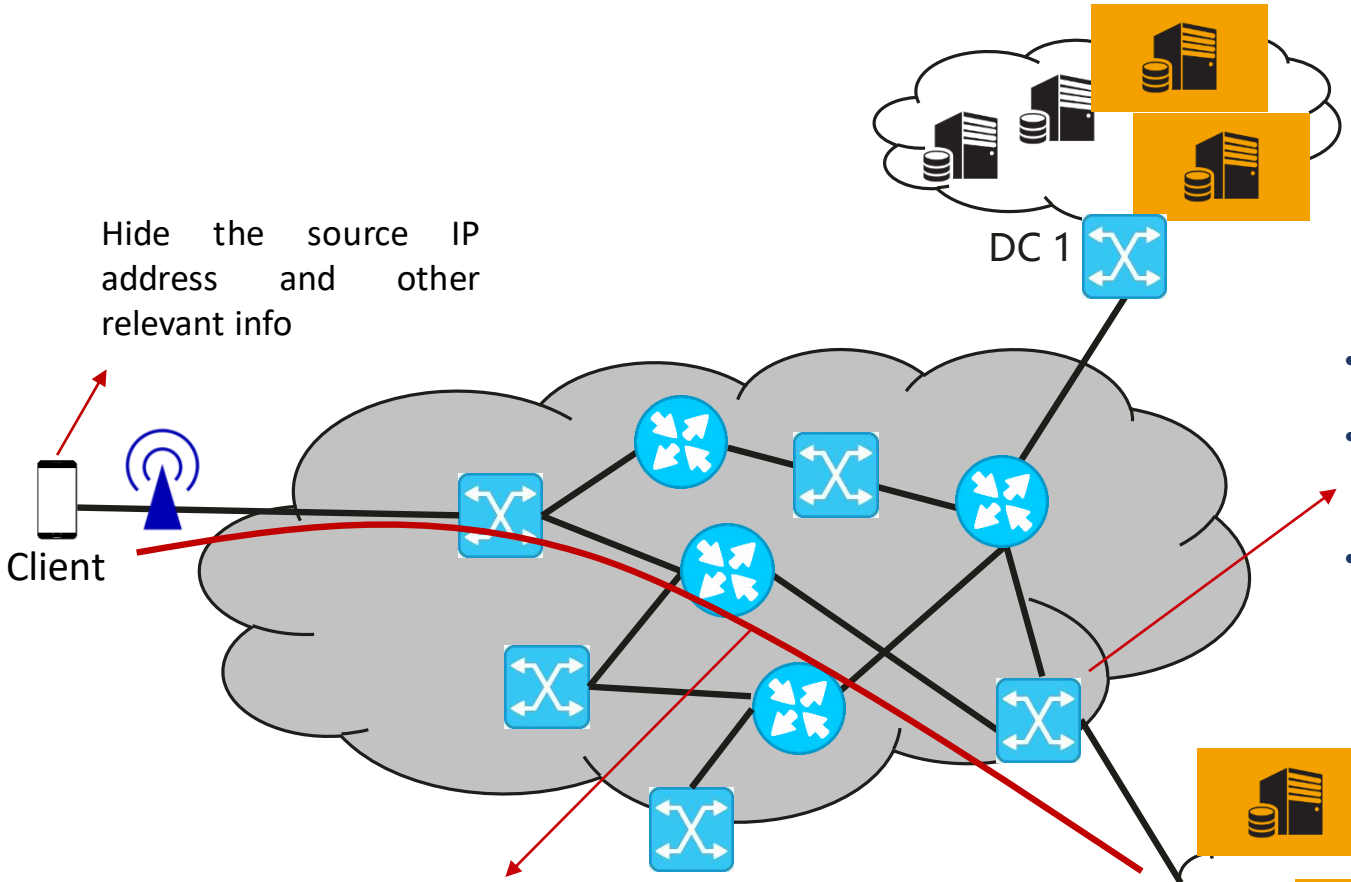
Privacy: A global regulatory concern



- Laws passed all over the world to protect citizen's privacy
  - GDPR in Europe
  - Cybersecurity Law in China with privacy protection guidelines
  - …
- Difficult balance
  - Data protection is sometimes considered as a potential danger for national security

HUAWEI

Privacy protection from a network perspective



Hide the source IP address and other relevant info

- Ideally there should ZERO trusted 3rd party
- The routing and forwarding performance should not be impacted by the security means
- Compromising one node should not collapse the whole system

Hide the destination IP address and services if necessary

DC 2

Protect the path so that:

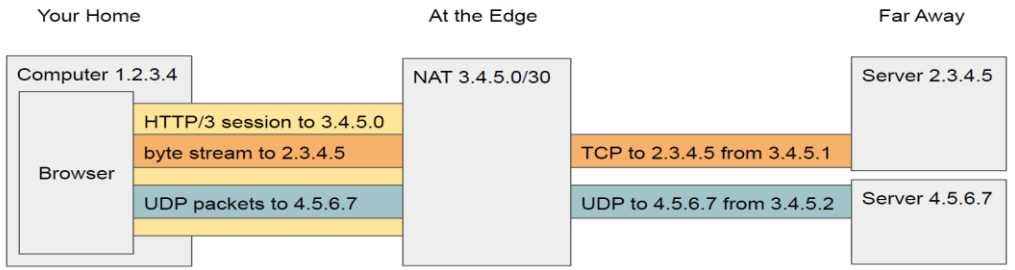
- Source is not associated with the destination
- Protect the underlay network from attacks

HUAWEI

Existing Solutions

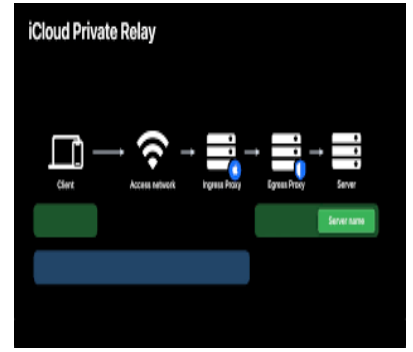
GnatCatcher from Google

- **Near-Path NAT** effectively hiding their IP addresses from the site host.
- **Willful IP Blindness** allows access to IP addresses for legitimate purposes



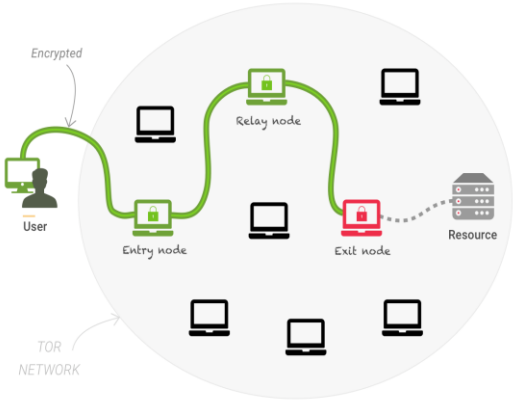
iCloud + Private Relay from Apple

- Use of a chain of 2 proxies to ensure source-destination unlinkability
- Traffic tunneled in QUIC - HTTP/3 tunnels
- Traffic protected using temporary public / private key pairs given by a Private Relay Access Token Server
- Access token are made unlinkable by use of cryptographic blinding
- Quite heavy from a cryptographic standpoint



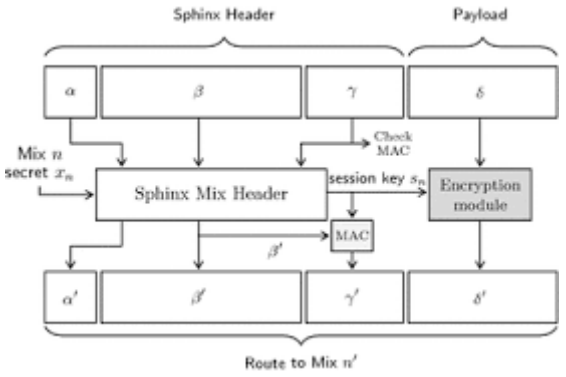
The Onion Router

- Use of proxies and relays to anonymize TCP traffic
- Data sent among a set of relay nodes in the form of recursively encrypted cells. Each node on the path decrypts the cell and relays it to the next node.
- Lightweight system



Sphinx Mix Network

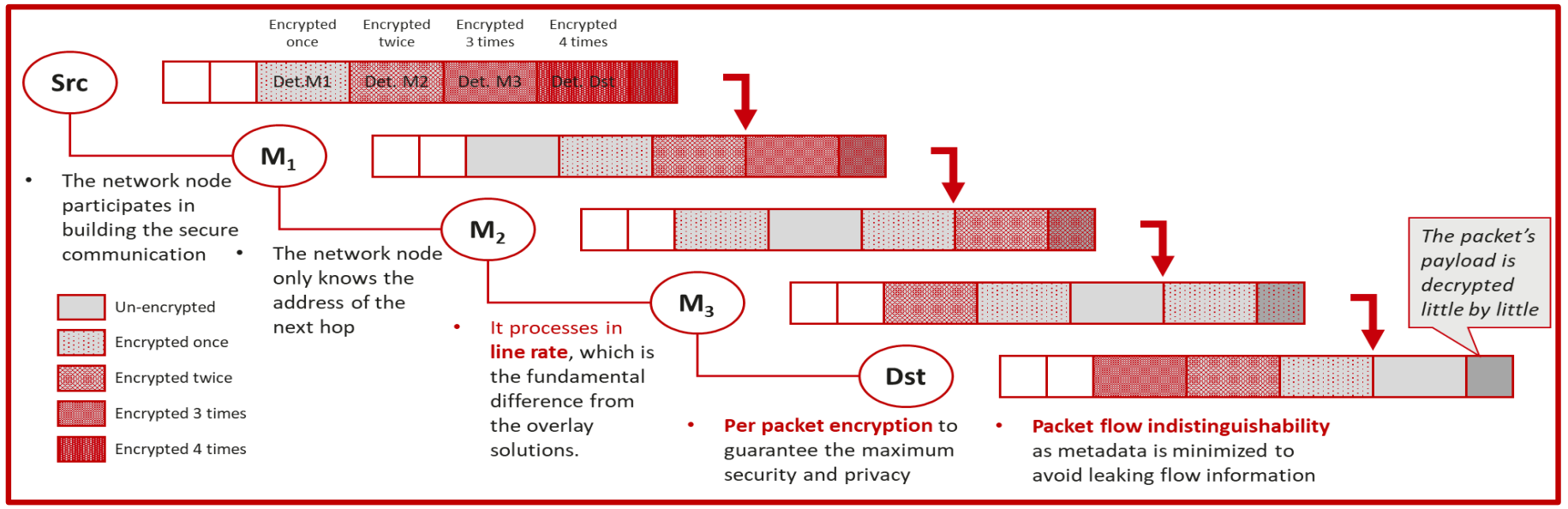
- Provably secure format: Sphinx's anonymity properties are ensured as soon as the cryptographic primitives used by Sphinx are secure.
- Quite strong attack resistance despite 10 years of efforts (1 attack published in 2020 [2], hard to put in place).



HUAWEI

Source Routing Based Secure Network Communication

- Source routing model to overcome the scalability limit of the VPN solution
- Sequential encryption of a packet to protect all nodes on the path
- Topological anonymity to enhance privacy
- Reduction of traffic metadata to reduce the risk of DDoS attacks and deanonymization
- Per packet encryption to make the packet flow indistinguishable
- Required to have no impact on the routing and forwarding performance



HUAWEI

Conclusions

- The core of Zero Trust Networking is “never trust, always verify”
- Overlay solutions are flexible and easy to maintain and upgrade
- Underlay solutions could be complementary and support restricted devices and environment

Thank you.