中国移动
China Mobile

Zero Trust and Practice in Telecommunication Networks

China Mobile

Junzhi YAN

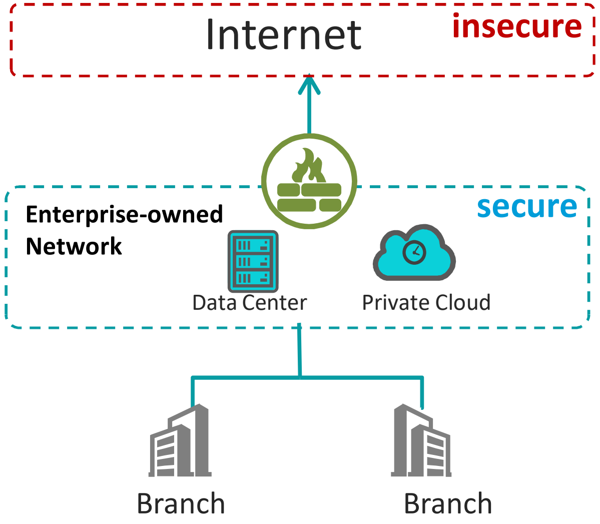
www.10086.cn

Background

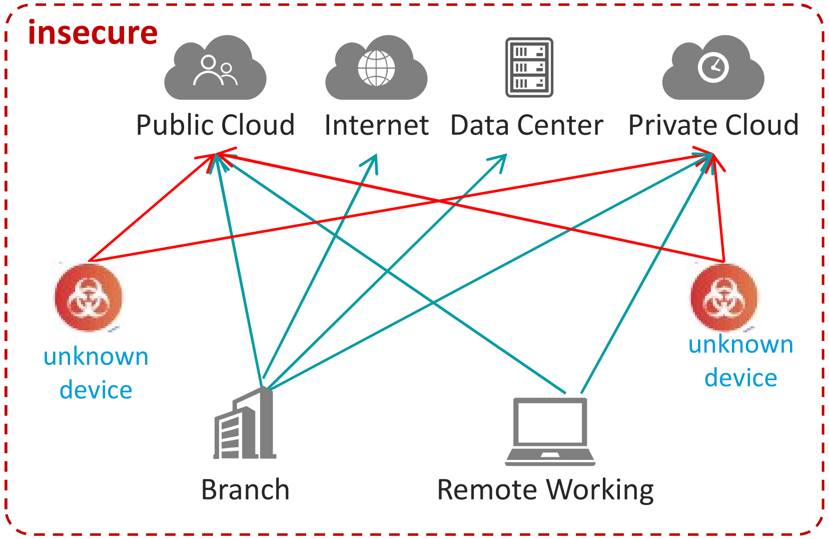
Security boundary and security threat has changed:

- **Boundary protection is not enough:** The boundary can be by passed. Horizontal attacks and permission reuse are difficult to prevent.
- **Increase of cybersecurity threat:** Attacker capabilities improve, and static strategies cannot provide effective protection.
- **Complicated access model:** Network access and internal access control becomes more complex, enterprise network boundaries disappear, and the exposure increases.

In the past:
The perimeter is clear.



Nowadays:
The boundary is vague.



Assumptions and Key Tenets of Zero Trust

Assumptions

1 Network is always in an insecure environment.

2 External and internal threats are always exist.

3 Network location alone doesn’t imply trust.

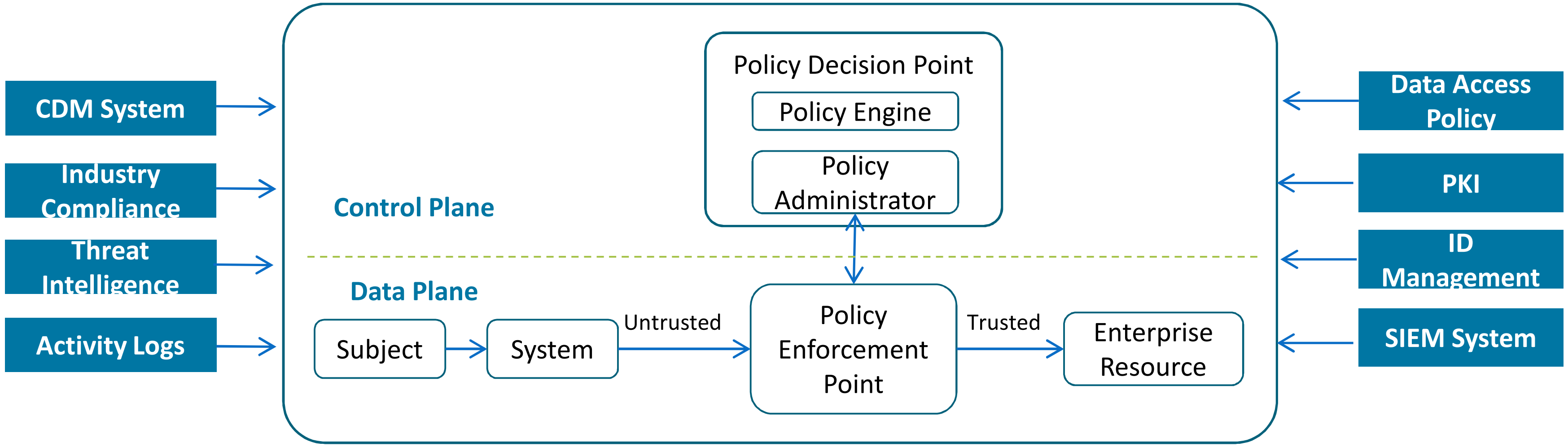
4 Authentication and authorization are needed for all the devices, uses, and workflows.

5 Security policy is dynamic.

Key tenets

Traditional security model	Zero Trust
Network centered	Identity driven
Attack & defence	Resource protection
Boundary protection	No-boundary protection
Trust based protection	No implicit trust, least privilege
Authentication only once, static policy	Continual evaluation, dynamic policy
Passive, static defence	Active, dynamic defence

Example of Zero Trust Architecture

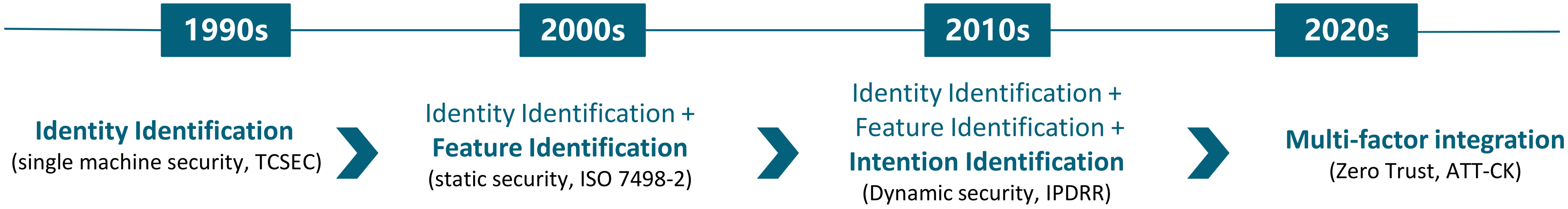


Example of Zero Trust Architecture (NIST SP 800-207)

- **Policy engine (PE):** Responsible for the ultimate decision to grant access to a resource for a given subject.
- **Policy administrator (PA):** Responsible for establishing and/or shutting down the communication path between a subject and a resource.
- **Policy enforcement point (PEP):** Responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

Security Evolution of Telecom Networks

➢ Evolution of security technology: static -> dynamic, passive -> active, multi-factor, fine-grained



1990s

Identity Identification
(single machine security, TCSEC)

2000s

Identity Identification +
Feature Identification
(static security, ISO 7498-2)

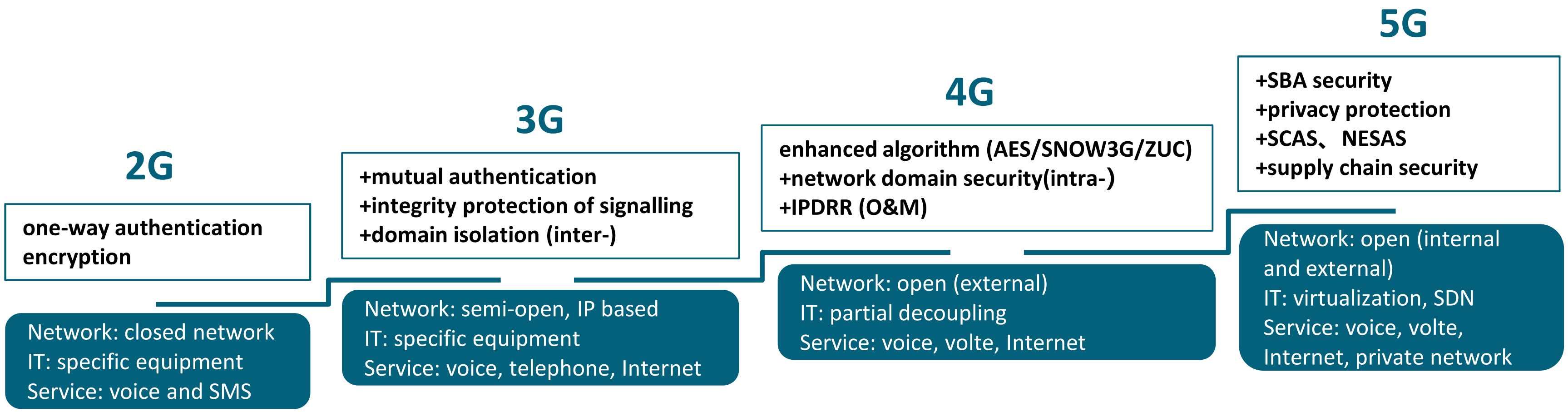
2010s

Identity Identification +
Feature Identification +
Intention Identification
(Dynamic security, IPDRR)

2020s

Multi-factor integration
(Zero Trust, ATT-CK)

➢ Evolution of telecom network faces more attack paths and more complex attack methods



2G

one-way authentication encryption

Network: closed network
IT: specific equipment
Service: voice and SMS

3G

+mutual authentication
+integrity protection of signalling
+domain isolation (inter-)

Network: semi-open, IP based
IT: specific equipment
Service: voice, telephone, Internet

4G

enhanced algorithm (AES/SNOW3G/ZUC)
+network domain security(intra-)
+IPDRR (O&M)

Network: open (external)
IT: partial decoupling
Service: voice, volte, Internet

5G

+SBA security
+privacy protection
+SCAS、 NESAS
+supply chain security

Network: open (internal and external)
IT: virtualization, SDN
Service: voice, volte, Internet, private network

➢ Key elements of 6G & future telecom network security

Identity

interoperation for cross domain

Trust

assessment and evaluation

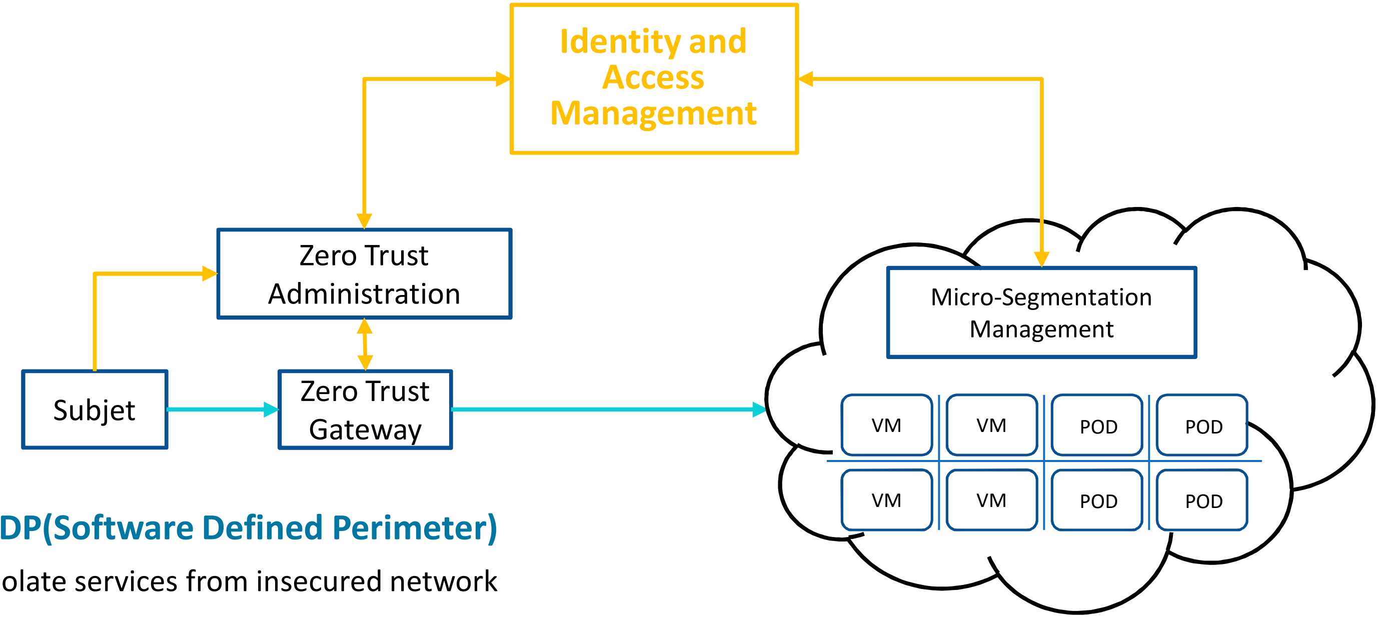
Security

built in security, of security capability orchestration

Approaches of Zero Trust

Enhanced Identity Governance

- Use identity as the key component of policy creation
- Access policies based on identity and assigned attributes
- Multi-factor authentication


Identity and Access Management
Zero Trust Administration
Subjet
Zero Trust Gateway
Micro-Segmentation Management
VM
VM
POD
POD
VM
VM
POD
POD

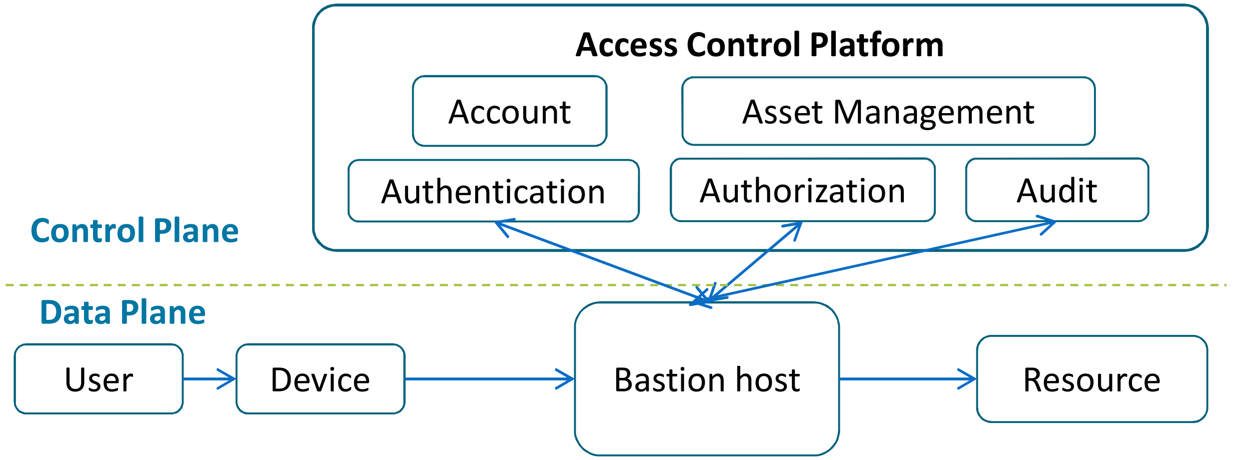
SDP(Software Defined Perimeter)

- Isolate services from insecured network
- Authentication before connection
- Mitigate the exposure of assets
- Least privilege

Micro-Segmentation

- Software devices to protect each resource or small group of related resources

Enhanced Identity Governance for O&M System in Telecom Networks

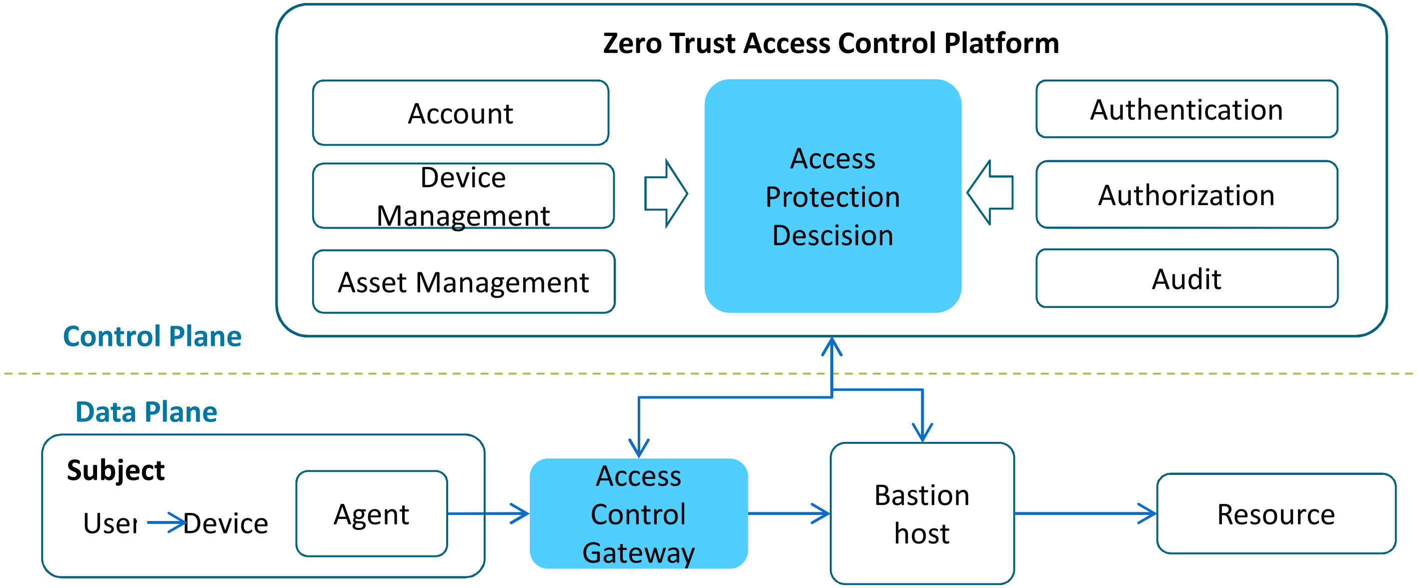


Typical architecture of access control platform in operator's network (ITU-T TR.zt-acp)

Security Challenges

- **Excessive trust.** It believes that users within the security area are trusted by default, which makes users have too high access rights, resulting in excessive trust.
- **Unknown devices.** The user and the device are not bounded during authentication. Authentication just based on user identity is difficult to guarantee the security of the access process.
- **Privilege abuse.** The device state, resource being accessed and network environment may change and become insecure during access process. The risk information are not collected in real time, which may lead to privilege abuse.
- **Exposing resource.** "Connect first, authenticate later" provided by VPN lead to the exposure of intranet resources to the attacker.

Enhanced Identity Governance for O&M System in Telecom Networks

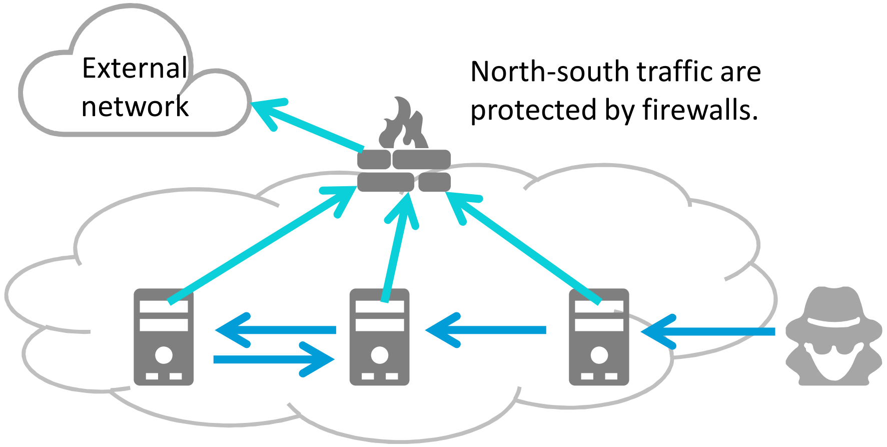


Framework of ZT access control platform (ITU-T TR.zt-acp)

- **Access control gateway:**
  - Authenticates the subject and establishes a security tunnel between the gateway and the agent.
  - Receives dynamic policies from access protection decision module and implement the policies.
- **Access protection decision:**
  - Collects user related information, device related information and network environment information.
  - Continuous trust evaluation: analyses the logs and risk data, evaluates the risk.
  - Makes dynamic access control decision.

Micro-Segmentation for Internal Access inside Data Center

Multiple services in the form of hosts, virtual machines, containers are deployed in data center. The east-west access between services become complex with the frequent business changes. In order to prevent attackers from jumping between services, fine-grained access control is necessary for east-west access.



No detection and access control for east-west traffic

Challenges

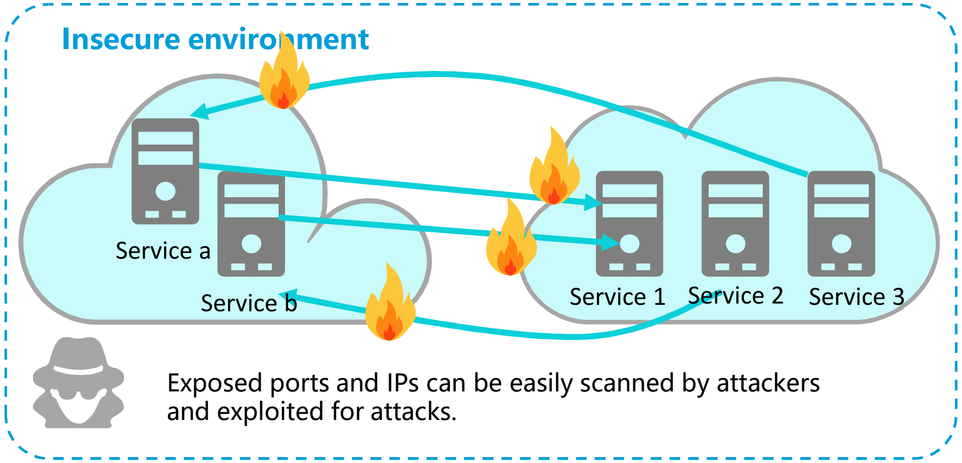
- The traditional boundary protection architecture lacks monitoring and protection against the internal threats.
- Complex relationship between containers and virtualization business, exponentially increased access control policies, making it difficult to manage the policies uniformly.
- Technology leads to frequent IP changes. Traditional access control management models based on physical IP addresses become ineffective.

Zero Trust based Solutions

- **Unified east-west fine-grained access control:** push and execute unified access control policies based on micro-segmentation
- **Instant traffic detection:** achieving adaptive dynamic access control based on the trust evaluation of traffic characteristics and context
- **Access control strategies without IP:** Using label systems or virtual IPs to define business traffic, establishing an identity centric dynamic access control model

SDP for Service Access between Multiple Clouds

For enterprises deploying services in a multi-cloud architecture using a hybrid cloud and distributed data center, fine-grained and centrally controlled access control is needed for the cross clouds access.
SDP (Software Defined Perimeter) is suitable in this scenario.


Insecure environment
Service a
Service b
Service 1
Service 2
Service 3
Exposed ports and IPs can be easily scanned by attackers and exploited for attacks.

Challenges

- The boundary protection architecture of traditional data centers only implements traffic filtering. The service IP and ports are exposed to the external network.
- Unify access control and traffic monitoring is difficult to imployed for the cross cloud access between services.
- Dynamic access control based on traffic characteristics and context is needed., since the rules for the access control policy between services are complicated and changable.

Zero Trust based Solutions

- **Connect first, authenticate later:** Before authentication and authorization, the port is closed by default and denying any access, so as to hide the port and internal structure.
- **Unified monitoring and management of access traffic:** Identity authentication, access control, and real-time monitoring of cross cloud access traffic are implemented unifiedly.
- **Dynamic access control:** Conduct trust evaluation and implement dynamic access control based on traffic characteristics and context between services.

Suggestion for Construction of Zero Trust System

- **Upgrade the legacy service system, and integrate capabilities of legacy architecture with capabilities in new architecture smoothly.**
  - □ Dual mode architecture for both new and old systems, new applications adopting the new security architecture
  - □ Gradual migration of legacy service system
  - □ Integrate the existing security devices as zero trust support components into the new architecture
- **Construction of new service system**
  - □ Following the principle of zero trust
  - □ Continuous and comprehensive assessment of the exposure and external attack risks of the enterprise's service system

中国移动
China Mobile

Thank you !