Secure Hybrid Network Monitoring

November 3, 2025

(IETF 124)

Yutaka OIWA

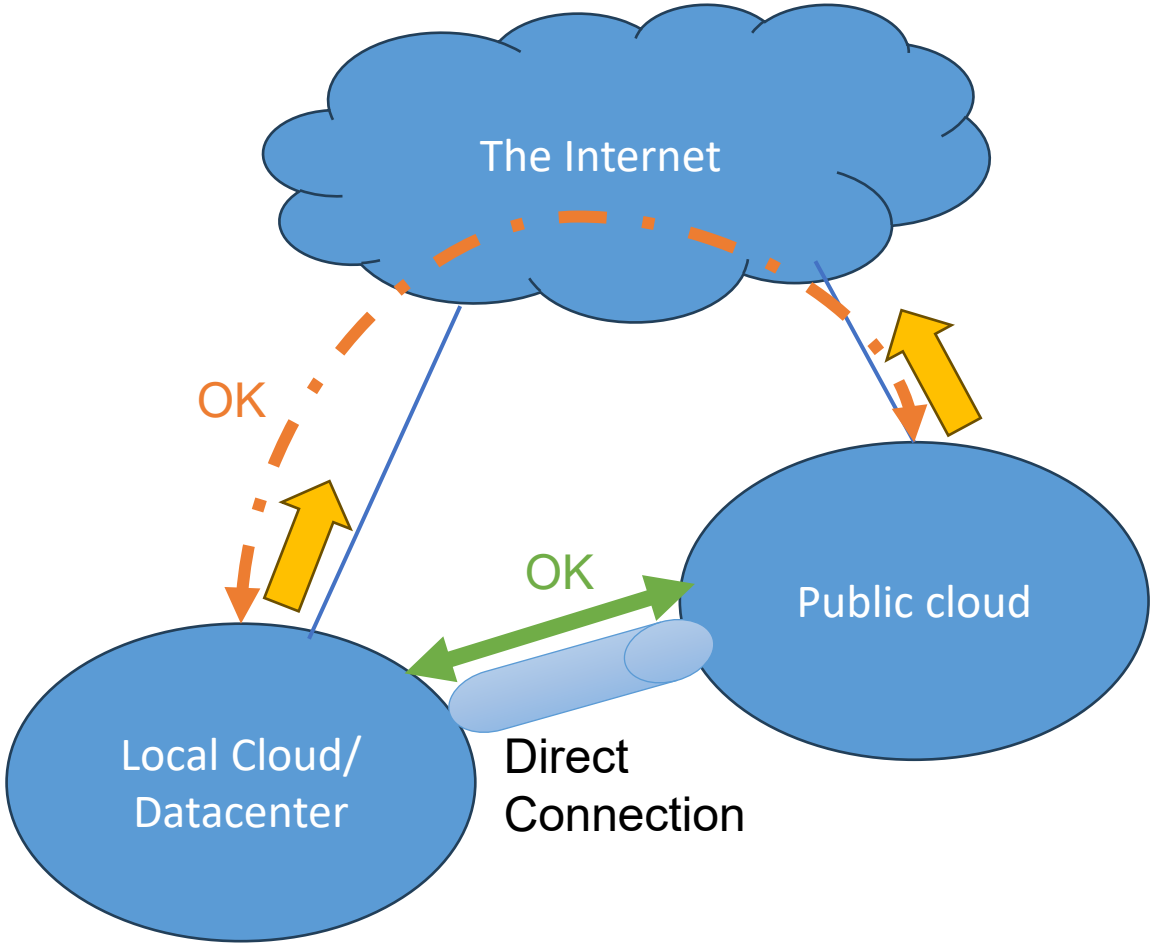
Hybrid Network

- Use of hybrid clouds or network is now common
  - Connect multiple instances of networks and/or cloud services to compose a single system
    - e.g. Use an on-premise cloud for secure data vault, a public cloud for Web frontend
  - Multiple stakeholders
- Monitoring of path properties is important
  - Possible multiple routes for destinations
    - Especially for cloud-base solutions (e.g. via tunnel and via the Internet)
    - Security assumptions only hold for some specific path

Hybrid Network – an example

- Mixed use of two clouds
  - A local cloud - for secure data
  - A public cloud - for frontends
    - Default routes to the Internet
- Dedicated communication path between those

- There are two possible routes between those clouds
- But, only one of those are the valid path



Monitoring Hybrid Networks

- Monitoring of path properties is important
  - There are many possible causes to break path expetations
    - Dynamic Routing – e.g. BGP
    - Misconfigurations
    - Security Intrusions to intermediaries
- Monitoring of path properties is difficult
  - Transparency
    - Existing Internet protocols do not offer path-level guarantees
  - Network complexity
    - Existence of underlay/overlay networks
  - Multiple stakeholders
    - Telemetries and Security Monitors must not be directly exposed to externals

Secure Hybrid Network Monitoring

- Monitoring solutions for (security) properties of communication paths
  - **Gathering** network status using existing telemetries
    - Uses existing protocols / systems
  - **Summarizing** status information among multiple networks
    - Application-layer APIs for actual path characteristics
    - Exchange between multiple network operators
    - Recursion for tunneled network layers (VPN, SDN etc.)
  - **Checking** for policy / SLA satisfaction
    - Detection and application-level alerts for any troubles / anomalies

Design principles

- No/little changes to existing network/devices
  - Add-on / side-car implementation to monitoring/telemetry layers
  - Simple API designs (possibly HTTP-based) for service exchanges
- Mutiple-operator support
  - Cascading query/answers between operators
  - ***Interop needed; needs for standardization***
- Considering various network implementations
  - Conventional IP networks
  - (Proprietary) Software-defined networks
  - VPN / IP-IP tunnels

Materials

- Secure hybrid network monitoring - Problem statement
  https://datatracker.ietf.org/doc/html/draft-oiwa-secure-hybrid-network-02
- Secure Hybrid Network Monitoring - Path Characteristics Service
  https://datatracker.ietf.org/doc/html/draft-oiwa-path-characteristics-service-00
- Demo in Hackathon – ask us for possible presentation

Contacts @ IETF124:

- Yutaka Oiwa
  - y.oiwa@aist.go.jp
- Satoru Kanno
  - kanno@gmo-connect.jp
- Yumi Sakemi
  - sakemi-yumi@gmo-connect.jp

Related works and references

- Possible relations with existing IETF technologies
  - Gathering
    - telemetry framework, defined in RFC 9232
    - local network monitoring – netconf, rats, alternate-marking, nasr, etc.
    - Routing/forwarding monitoring – bgp monitoring, ipfix, rpki etc.
  - Summarizing / managing
    - alto
    - SCION – in panrg