Secure Hybrid Network Monitoring

Yutaka OIWA (AIST Japan)

IETF 123 – HotRFC
19–20 Jul 2025
Madrid, Spain

Hybrid Network

- Use of hybrid clouds or hybrid 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
  - Connected by various means of interconnection paths, like VPN-secured path, overlay networks or leased physical line
    - e.g. Direct Connect for AWS, ExpressRoute for Azure
  - Some hidden security assumptions for those interconnections
    - VPN strength, operators, geo-locations etc.

Monitoring Hybrid Network

- 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 paths
- Monitoring of path properties is difficult
  - Transparency
    - IP paths are transparent to applications
    - Existing Internet protocols do not offer path-level guarantees
  - Network complexity
    - Existence of underlay/overlay networks

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
- Considering various network implementations
  - Conventional IP networks
  - (Proprietary) Software-defined networks
  - VPN / IP-IP tunnels

Roadmap

- During IETF 123 (hackathon and following days)
  - Initial design of architecture, first I-D
- After IETF 123
  - Requests for various comments
  - Initial service implementation
- Present some demo on IETF 124 or 125?

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

Persons / contacts

Team members @ IETF 123:

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

Materials:

- An existing draft: https://datatracker.ietf.org/doc/html/draft-oiwa-secure-hybrid-network-01
- New draft - TBP