Network Working Group
Internet-Draft
Intended status: Informational
Expires: 10 April 2026

Y. OIWA
AIST Japan
S. Kanno
Y. Sakemi
GMO CONNECT

7 October 2025

Secure hybrid network monitoring - Problem statement
draft-oiwa-secure-hybrid-network-02

Abstract

This document describes a problem statement regarding the challenges and requirements for ensuring and monitoring the security status of networks operating in complex environments, such as hybrid or mixed cloud systems.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 April 2026.

Table of Contents

1. Introduction

Recently, virtualized resources such as cloud computing infrastructure rapidly replace traditional types of network/computing environments such as local servers or on-premises computer clusters. In such kind of infrastructure, information of physical resources such as servers, local network, network routers, etc. are hidden from users in trade with flexibility, service redundancy and costs as well. Cryptographic communications such as TLS, IPsec, etc. are typically used to protect communication into/out of such systems from eavesdropping and tampering.

However, there are many use cases where service still depends on the security nature of underlying physical resources, instead of just encrypting the communication:

* Traffic analysis on encrypted communication may reveal partial information of the payload;

* Juridical requirement (such as personal data protection) demands some specific property (such as governing laws, geological positions, operators) to be checked;

* Denial-of-service and several other attacks may not be prevented by encryption only.

For such high-security applications, we need some technical infrastructure for continuously checking the properties and statuses of underlying network and intermediate nodes. In a non-virtualized, self-managed setting, there are several existing technologies (e.g. NETCONF, path validation, etc.) for acquiring such statuses. However, these are not enough for virtualized, multi-stakeholder setting of modern cloud infrastructure.

This document gives a first-stage problem analysis for ensuring and monitoring the security status of the network used under complex network environments such as hybrid cloud or mixed cloud settings.

This document provides (1) a problem statement and gap analysis, and (2) a non-normative outline of potential solution directions. It does not define protocol requirements.

1.1. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Background

2.1. Multi-cloud and Hybrid Cloud Systems

Concepts of multi-cloud and hybrid clouds are defined in [ISO-IEC-5140]; in short, multi-cloud is a system where a single service is implemented using two-or-more independently operated cloud services. Hybrid cloud systems compose two or more computation environments having different nature of operation, security level or other aspects, at least one of which is typically a public cloud service. Often, subsystems on privately-operated cloud, on-premises, or edge networks are connected with public cloud infrastructure by network to construct a single hybrid cloud system.

Hybrid cloud systems are, in general, constructed when the security or other provisions of public cloud systems are not sufficient for a part of information or a subsystem component (if not, a simple public or multi-cloud environment is sufficient). At the same time, there are often requirements where some benefits (scalability, costs, resilience, maintainability etc.) of public cloud systems are beneficial (if not, simple on-premises deployment is enough). This mixed, seemingly conflicting requirement makes it difficult to ensure the monitoring of security for hybrid cloud systems.

2.2. Security Implications of Hybrid Clouds

Multi-cloud and hybrid cloud systems require system-internal communications flowing beyond the boundary of single cloud systems. In the simplest case, it can be implemented using authenticated TLS or HTTPS communications via public Internet infrastructure. For high-security systems, it is often implemented using dedicated channels of communications, such as VPNs, private peering, or even dedicated optical fiber channels. To maintain the security of whole systems, monitoring integrity of such dedicated channels is mandatory.

Furthermore, with IP-based software systems, there is lot more dependency to ensure such secure communications. In other words, there are a lot more surfaces for attacks. For example, if a DNS record is either tampered or misconfigured, communication intended to go through a secure channel might be routed to public channels. If there is a misconfiguration for routing, the traffic might go public. Enumerating and collecting status of such dependency is undermined currently.

3. Problem Statement

There is a lot of technology already available and useful for such purposes.

* SAVNET (Source Address Validation in Intra-domain and Inter-domain Networks) [SAVNET-CHARTER] provides a way to ensure validity of incoming traffic and possibly blocking any rogue packets.

* SRv6 [RFC9819] provides control of intended routes for individual IPv6 packets between networks.

* RPKI [RFC6480] provides control and trust anchors for the security or inter-domain routing.

However, to ensure the security of the whole hybrid cloud infrastructure, we still have to address the following aspects, which seem to be lacking solutions currently.

3.1. The Nature of Multiple Operators/Stakeholders

Hybrid cloud systems depend on a lot of resources which are not under the control of the application system operators. Public clouds (both IaaS and SaaS) are operated by external service providers. They have their own policy for their operations, and they have their own decisions for maintaining or replacing any of the providing hardware/ software resources, provided that their service-level agreements (SLAs) are met.

This makes it non-satisfactory to expose information of all intermediate network nodes to the final application operators. First, detailed information on design and implementation of the cloud infrastructure is confidential information and important properties of the cloud providers. Moreover, some extent of independence between application operators (users or cloud infrastructure) and cloud service providers are critical for maintaining cost effectiveness, maintainability, security etc. of the cloud services.

3.2. Determination of the "Correct" States

In a small-scale, hand-crafted network, determining whether the current running state of the network is intended or not is a relatively simple question. However, in the complex multi-cloud systems, it is quite hard or even impossible problem to determine that, even if we had been possible to know all the details of the running state of the whole global network. To determine that, we also have to know about the design principle and hidden assumptions about the operation of each single network.

3.3. Shared Infrastructure and Information Leakage

The infrastructure of the cloud system is deeply shared among several clients. Although some information on the operational status at cloud service side is required to check the reliability of the user-side applications, exposing the raw operational parameters to some clients may reveal security-critical information of other clients. Before exposing the cloud-side status, it must be cooked and filtered so that information only relevant to a specific client is included.

3.4. Virtualized Infrastructure

Many cloud resources, not only computation nodes but also network routers, switches, VPN endpoints, etc., are virtualized and provided via infrastructure-as-code (IaC) systems. Unlike physical routers and switches, determination of virtual intermediate nodes in the traffic path does not mean its physical locations, physical properties, and security natures. (Imagine how we can analyze results of traceroute or ICMP ping via virtual private network.)

If there are any virtual nodes, physical properties of its underlying infrastructure may have to be traced and checked to ensure security and integrity. This requires cooperation of virtual resource providers or cloud providers and integration with their infrastructure management systems.

3.5. Risks Beyond Network Layers

Today, many network systems are managed via complex systems. This means any invasion to the IT-side assets of those management systems will cause severe risks to the network layers. These assets include (and are not limited to) software asset management, software vulnerability, ID management, etc.

To correctly evaluate risks of the whole network operations, we must also care about the risks of these management systems as well.

4. Security Considerations

The lack of comprehensive security monitoring in hybrid cloud environments creates several critical security risks that this document addresses:

4.1. Invisible Attack Vectors

Current hybrid cloud deployments create numerous blind spots where malicious activities can occur undetected:

* *Traffic Misdirection*: DNS tampering or routing misconfigurations can redirect secure traffic through compromised or unintended paths without detection

* *Virtual Infrastructure Exploitation*: Attacks targeting hypervisors or virtual network components remain invisible to traditional network monitoring

* *Cross-Tenant Information Leakage*: Shared infrastructure may enable side-channel attacks or resource-based information disclosure between different cloud tenants

4.2. Compromised Trust Assumptions

The multi-stakeholder nature of hybrid clouds breaks traditional security perimeters:

* *Fragmented Visibility*: No single entity has complete visibility into the security posture, creating gaps that attackers can exploit

* *Unclear Responsibility Boundaries*: Security incidents may go undetected when responsibilities are unclear between cloud providers and users

* *Supply Chain Vulnerabilities*: Dependencies on multiple cloud providers increase the attack surface through potential compromise of any provider

4.3. Persistent Security Degradation

Without proper monitoring capabilities, security posture deteriorates over time:

* *Configuration Drift*: Gradual misconfigurations accumulate, creating vulnerabilities that remain undetected

* *Stale Security Policies*: Security rules become outdated as infrastructure evolves, but changes go unnoticed

* *Delayed Incident Response*: Security incidents remain undetected for extended periods, allowing attackers to establish persistence

4.4. Amplified Attack Impact

The interconnected nature of hybrid clouds amplifies the impact of successful attacks:

* *Lateral Movement*: Compromised components can serve as stepping stones to access other parts of the hybrid infrastructure

* *Cascading Failures*: Security incidents in one cloud provider can propagate to other components of the hybrid system

* *Data Exfiltration*: Sensitive data may traverse multiple untrusted networks without adequate monitoring

Any solution addressing these problems must carefully balance security monitoring requirements with the protection of sensitive infrastructure information and the preservation of multi-stakeholder operational independence.

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

6.2. Informative References

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/rfc/rfc6480>.

[RFC9232] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", RFC 9232, DOI 10.17487/RFC9232, May 2022, <https://www.rfc-editor.org/rfc/rfc9232>.

[RFC9819] Talaulikar, K., Raza, K., Rabadan, J., and W. Lin, "Argument Signaling for BGP Services in Segment Routing over IPv6 (SRv6)", RFC 9819, DOI 10.17487/RFC9819, July 2025, <https://www.rfc-editor.org/rfc/rfc9819>.

[ISO-IEC-5140] ISO/IEC, "Information technology - Cloud computing - Multi-cloud and hybrid cloud vocabulary", ISO/IEC 5140:2024, 2024.

[SAVNET-CHARTER] "Source Address Validation in Intra-domain and Inter-domain Networks (SAVNET) Charter", n.d., <https://datatracker.ietf.org/wg/savnet/about/>.

Acknowledgments

This work is based on results obtained from a project JPNP23013 commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

Authors' Addresses

Yutaka OIWA
National Institute of Advanced Industrial Science and Technology (AIST)
Email: y.oiwa@aist.go.jp

Satoru Kanno
GMO CONNECT Inc.
Email: kanno@gmo-connect.jp

Yumi Sakemi
GMO CONNECT Inc.
Email: sakemi-yumi@gmo-connect.jp