Zero Trust Network Access (ZTNA) for Network Cloud Interface

Network Operations for Telecom Clouds
draft-dunchihi-neotec-zerotrust-access-dm-00

Houda CHIHI @IETF 122, Bangkok

Problem Statement

- ➢Dynamic Nature of Cloud Services : requirement of dynamic policies ➔ Neotec (Network Operations for Telecom Clouds)
- ➢Network cloud coordination lacks security mechanisms.
  - ❑Cloud and Network telemetry data may be exposed to unauthorized entities.
  - ❑Lack of Standardized Security Policies framework for enforcing ZTNA principles in network-Cloud coordination.
  - ❑No standardized model to secure exposure of Cloud and Network resources dynamically.

Why ZTNA is Needed for Telecom Edge Clouds

Telecom operators own both the Edge Clouds and the networks interconnecting them.

- Even within operator-owned environments, insider threats, misconfigurations, and compromised devices pose security risks.
- A single compromised edge cloud or network node can expose multiple interconnected services.
- ZTNA ensures real-time policy enforcement, dynamically adapting to latency-sensitive services (e.g., MEC, private 5G, AI workloads). .
- ZTNA ensures end-to-end security monitoring, reducing compliance risks and enforcing access controls.

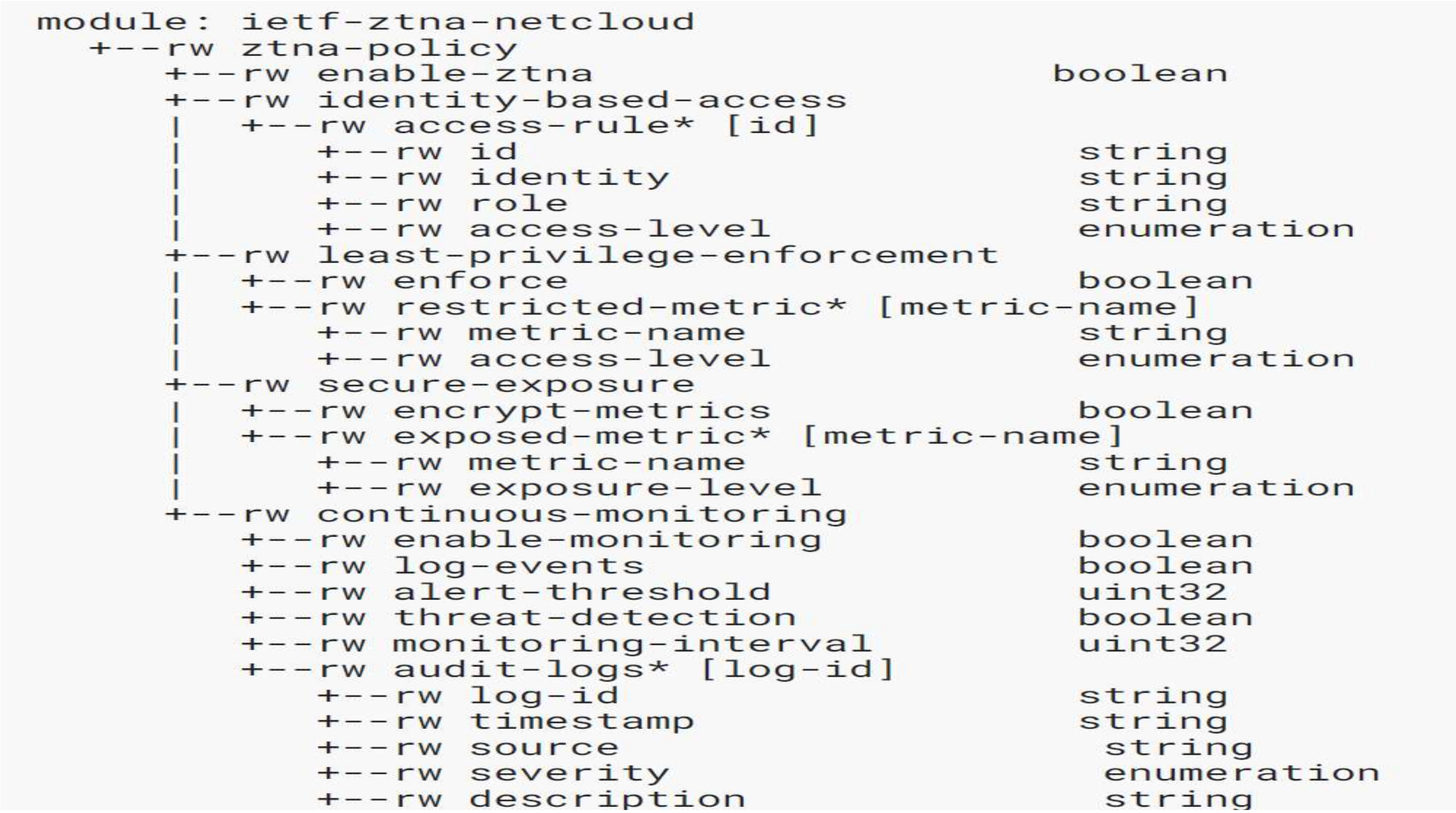
Gap Analysis

- Previous IETF initiatives primarily focus on policy-based network orchestration, telemetry, and capability-aware routing.
- Previous initiatives do not adequately address real-time ZTNA policy enforcement for network- cloud interfaces.
- Lack of identity-based access control mechanisms between Cloud Service Orchestrators and Network Controllers.
- Absence of least privilege enforcement to restrict access to network and Cloud telemetry.

Proposed Solution

- YANG data model implementing ZTNA principles at the network-cloud interface and integrating ZTNA policies into the Neotec (NM4EC) framework.
- High Level Objective of the ZTNA YANG DM for Neotec:
  - **Establish identity-based access control** to secure network-cloud interactions.
  - **Enable least privilege principles**, ensuring entities only access necessary resources.
  - **Secure network and cloud telemetry exposure,** preventing unauthorized access.
  - **Enable continuous monitoring** to detect unauthorized access attempts and security anomalies.
  - **Ensure real-time, policy-driven security coordination** between cloud-aware orchestrators and network controllers.
  - **Provide a scalable and extensible structure** for future security enhancements.

ZTNA YANG Model major components

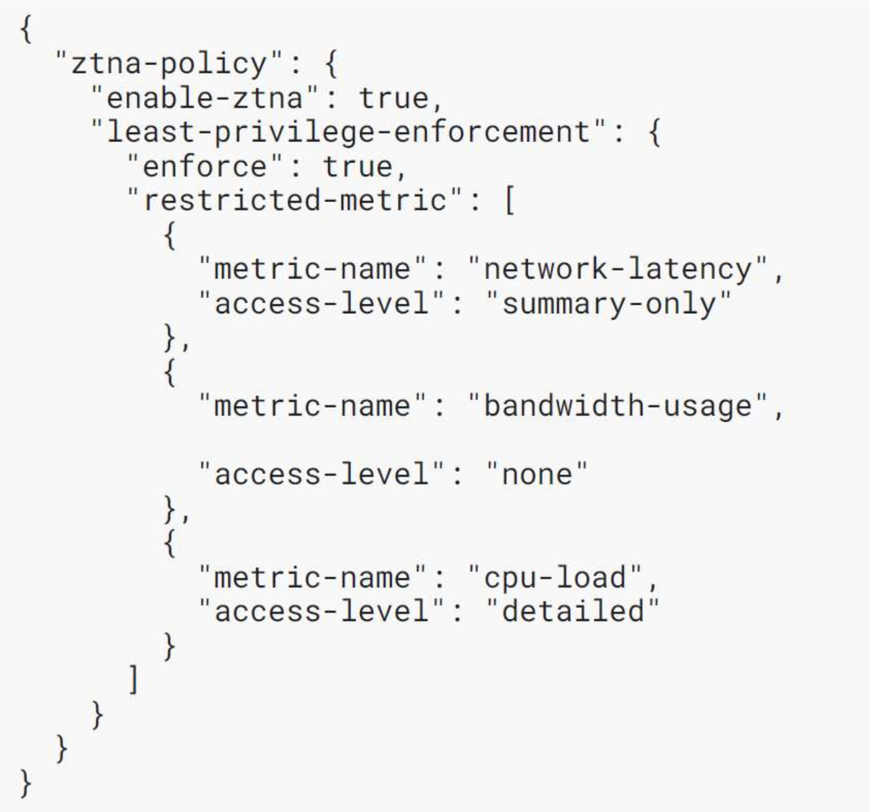


```
module: ietf-ztna-netcloud
  +--rw ztna-policy
     +--rw enable-ztna                  boolean
     +--rw identity-based-access
     |  +--rw access-rule* [id]
     |     +--rw id                      string
     |     +--rw identity                string
     |     +--rw role                    string
     |     +--rw access-level            enumeration
     +--rw least-privilege-enforcement
     |  +--rw enforce                    boolean
     |  +--rw restricted-metric* [metric-name]
     |     +--rw metric-name             string
     |     +--rw access-level            enumeration
     +--rw secure-exposure
     |  +--rw encrypt-metrics            boolean
     |  +--rw exposed-metric* [metric-name]
     |     +--rw metric-name             string
     |     +--rw exposure-level          enumeration
     +--rw continuous-monitoring
        +--rw enable-monitoring          boolean
        +--rw log-events                 boolean
        +--rw alert-threshold            uint32
        +--rw threat-detection           boolean
        +--rw monitoring-interval        uint32
        +--rw audit-logs* [log-id]
           +--rw log-id                  string
           +--rw timestamp               string
           +--rw source                   string
           +--rw severity                 enumeration
           +--rw description              string
```

Utilizing ZTNA YANG Module

Least Privilege Enforcement:

- Latency data: Accessible in summary-only mode,
- Bandwidth usage: Completely restricted (no access).

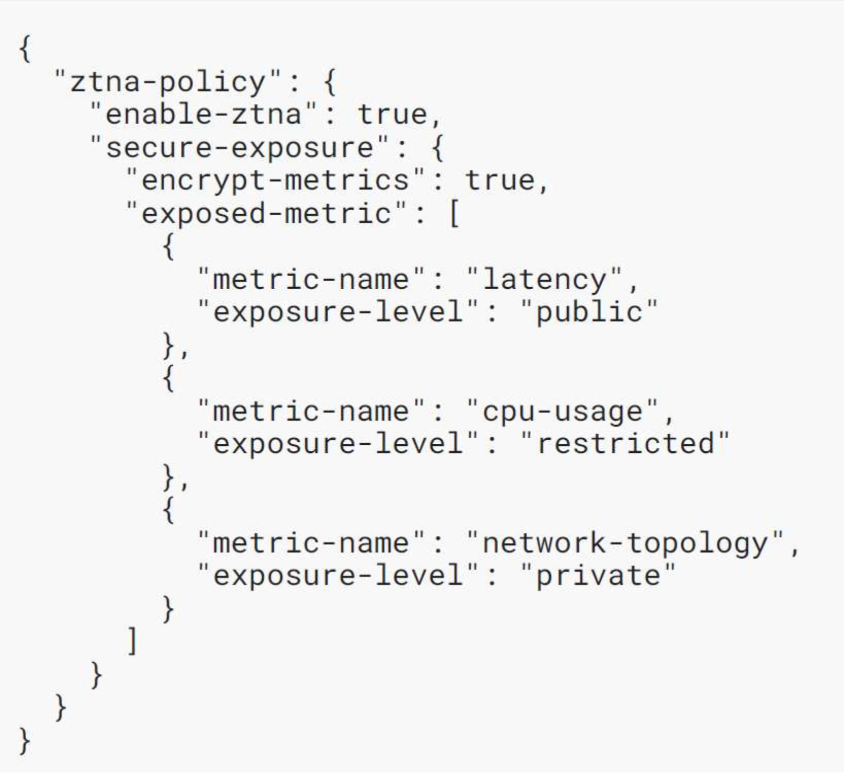


```
{
  "ztna-policy": {
    "enable-ztna": true,
    "least-privilege-enforcement": {
      "enforce": true,
      "restricted-metric": [
        {
          "metric-name": "network-latency",
          "access-level": "summary-only"
        },
        {
          "metric-name": "bandwidth-usage",

          "access-level": "none"
        },
        {
          "metric-name": "cpu-load",
          "access-level": "detailed"
        }
      ]
    }
  }
}
```

Secure Exposure:

- CPU usage: Restricted access to authorized entities.
- Network topology: Marked as private and hidden



```
{
  "ztna-policy": {
    "enable-ztna": true,
    "secure-exposure": {
      "encrypt-metrics": true,
      "exposed-metric": [
        {
          "metric-name": "latency",
          "exposure-level": "public"
        },
        {
          "metric-name": "cpu-usage",
          "exposure-level": "restricted"
        },
        {
          "metric-name": "network-topology",
          "exposure-level": "private"
        }
      ]
    }
  }
}
```

Thank you ! Stay Connected !

IETF

For additional information, please contact:

Houda.chihi@supcom.tn