To monitor connections between **switch cards, firewalls, servers, network switches, routers, and mainframes** in your on-premises ISO 8583 infrastructure, you can integrate **open-source network monitoring tools** into your existing architecture. Below is a structured plan that aligns with your current setup while ensuring visibility, alerting, and compliance:

**1. Network Monitoring Tools & Techniques**

**A. Layer 3/4 Connectivity Checks**

| **Tool** | **Purpose** | **How It Works** |
| --- | --- | --- |
| **Prometheus + Blackbox Exporter** | Check HTTP/HTTPS, TCP, ICMP (ping) availability of endpoints. | Probes targets (e.g., firewall IPs, switch ports) and reports success/failure. |
| **SmokePing** | Track latency, packet loss, and jitter between nodes. | Uses ICMP/TCP to measure network performance over time. |
| **Telegraf (InfluxData)** | Collect SNMP metrics (interface status, bandwidth usage) from network devices. | Polls SNMP-enabled devices (switches, routers) and sends metrics to InfluxDB. |

**B. Layer 7/Application Checks**

| **Tool** | **Purpose** |
| --- | --- |
| **Apache Kafka** | Monitor connectivity to message brokers (e.g., consumer lag, broker health). |
| **Custom Scripts** | Validate ISO 8583 message flow between switches and mainframes (e.g., synthetic transactions). |

**C. Log Aggregation**

| **Tool** | **Purpose** |
| --- | --- |
| **Elasticsearch + Filebeat** | Collect and analyze firewall logs (e.g., iptables, Cisco ASA), switch syslogs, and mainframe connection logs. |
| **Graylog** | Centralize and correlate logs for security/network audits. |

**2. Integration with Existing Architecture**

**A. Metrics Pipeline**

[Network Devices (SNMP)] --> [Telegraf] --> [Kafka] --> [Flink] --> [VictoriaMetrics]

[Firewall/Switch Logs] --> [Filebeat] --> [Elasticsearch]

[Blackbox Exporter] --> [Prometheus] --> [Alertmanager]

**B. Key Checks to Implement**

1. **Firewall Rules**:
   * Use **Auditbeat** to track rule changes in firewalls (e.g., unexpected DENY rules).
   * Alert on blocked traffic to critical ports (e.g., ISO 8583 port xxxx).
2. **Switch/Router Health**:
   * Monitor SNMP OIDs for:
     + Interface status (up/down).
     + Bandwidth utilization (alert if >80% for 5 minutes).
     + CRC errors, packet drops.
3. **Mainframe Connectivity**:
   * Use **Blackbox Exporter** to TCP-probe mainframe ports.
   * Log connection timeouts via Elasticsearch.
4. **End-to-End Path**:
   * Deploy **SmokePing** to measure latency between switches and mainframes.

**3. Alerting & Dashboards**

**A. Critical Alerts**

| **Scenario** | **Tool** | **Example Alert** |
| --- | --- | --- |
| Firewall port blocked | Prometheus + Alertmanager | firewall\_blocked\_packets{port="ISO8583"} > 0 |
| Switch interface down | Telegraf + InfluxDB | snmp\_ifAdminStatus{interface="Gi0/1"} == 2 (status=down) |
| High latency to mainframe | SmokePing + Grafana | latency > 100ms for 5 consecutive probes. |
| SNMP polling failure | Prometheus | up{job="snmp"} == 0 |

**B. Dashboards**

* **Grafana**:
  + Network Health Overview: Interface status, bandwidth, latency.
  + Firewall Traffic: Allowed/denied connections by port/IP.
* **Kibana**:
  + Firewall log analysis: Top blocked IPs, geo-location of threats.

**4. Security & Compliance**

* **SNMPv3**: Use encryption/auth for SNMP polling (avoid SNMPv2).
* **Network Segmentation**:
  + Isolate monitoring traffic to a dedicated VLAN.
  + Restrict SNMP/ICMP access to monitoring servers only.
* **Audit Logs**:
  + Use **Elasticsearch** to retain firewall/switch logs for compliance (PCI DSS, ISO 27001).

**5. Hardware/Software Requirements**

**A. Dedicated Monitoring Servers**

| **Component** | **Specs** | **Purpose** |
| --- | --- | --- |
| **Telegraf** | 4 vCPU, 8GB RAM | SNMP polling for 100+ devices. |
| **Prometheus** | 8 vCPU, 16GB RAM | Scrape Blackbox Exporter and SNMP metrics. |
| **Elasticsearch** | 16 vCPU, 64GB RAM | Store firewall/switch logs (hot storage). |

**B. Network Device Requirements**

* Enable SNMPv3 on all switches, routers, and firewalls.
* Allocate 5–10% bandwidth for monitoring traffic.

**6. Open-Source Alternatives**

| **Tool** | **Alternative** | **Difference** |
| --- | --- | --- |
| **Telegraf** | Collectd | Less integrated with InfluxDB/Prometheus. |
| **Prometheus** | Nagios | Pull-based vs. Nagios’s active checks. |
| **Graylog** | Loki (Grafana) | Loki is lighter but less feature-rich. |

**7. Example Workflow**

1. **Switch Port Monitoring**:
   * Telegraf polls SNMP OID IF-MIB::ifOperStatus every 30s.
   * Metrics flow to VictoriaMetrics.
   * Grafana dashboard triggers alerts if status ≠ up.
2. **Firewall Connection Tracking**:
   * Filebeat ships iptables logs to Elasticsearch.
   * Kibana dashboard shows blocked ISO 8583 traffic.
3. **Mainframe Health**:
   * Blackbox Exporter sends TCP probes to mainframe port 1234.
   * Alertmanager notifies if probes fail 3 times.

**8. Why This Works**

* **Unified Stack**: Reuse existing tools (Prometheus, Grafana, Elasticsearch).
* **Cost**: No licensing fees; scales with open-source tools.
* **Compliance**: Log retention and access control align with PCI DSS.

This approach ensures full visibility into network connectivity while leveraging your existing ISO 8583 monitoring infrastructure.