Appendix 1

---

1. Introduction

1.1 Purpose

This Request for Proposal (RFP) invites qualified vendors to submit proposals for the supply of network equipment required to build an Ethernet VPN (EVPN) Fabric, enterprise firewalls, and centralized management systems. The proposed solutions must ensure high performance, scalability, and resilient data center networking, enabling seamless routing, bridging, and integration with virtualization platforms. All the selected equipment must meet stringent technical specifications to ensure low-latency operations, robust security, and efficient management.

1.2 Background

The AMIO Bank is undertaking a project to modernize its data center infrastructure. The EVPN Fabric will form the backbone of this upgrade, enabling virtualized workloads, multi-tenancy, and high-speed connectivity. Proposals should demonstrate full compliance with the requirements outlined in this document and offer cost-effective, interoperable, sustainable solutions.

1.3 Objectives

- Procure spine, leaf, service leaf/DCI devices that support EVPN/VXLAN for routing and bridging.
- Acquire enterprise-class firewalls for border, data center, Zero Trust Network Access Firewall (ZTNA) / User Access GW and WAN environments.
- Include all necessary optical transceivers (SFP/SFP+/SFP28/QSFP+) and structured cabling.
- Ensure equipment meets performance, reliability, and scalability needs.

- Facilitate network and security integration with software overlays like VMware NSX and Nutanix Flow.
- Prioritize vendors offering comprehensive monitoring, maintenance, and telemetry capabilities.

2. Scope of Work

The vendors are required to supply their appropriate solutions. The scope includes:

- **Network Equipment:** Spine, leaf, and service leaf/DCI switches, meeting the specified port configurations, buffer sizes, and forwarding capacities, also features for EVPN Fabric deployment, including routing, QoS, security, and telemetry.
- **Firewalls:** Enterprise Border, Data Center / Server-Farm, Zero Trust Network Access / User Access GW, and WAN IPsec firewalls.

- **Optical Modules and Cabling:** All necessary SFP/SFP+/SFP28/QSFP+/QSFP28 optical modules and compatible cables for full connectivity between devices, including cable distribution systems (ODFs, horizontal and vertical cable managers).
- **Centralized Management and Logging Systems:** Management and logging appliances.
- **Optional Complimentary Services**: Installation assistance, commissioning, training, and post-deployment support

Each proposal must include:

- Detailed technical specifications and datasheets.
- Pricing for equipment and any optional services.
- All licenses to open the requested functionalities.
- Warranty, support, and software subscription terms.
- Evidence of compliance (certifications, test reports).
- **Optional Complimentary Services:** The bidder ranked first (winning participant) shall submit a Manufacturer Authorization Form (MAF) issued by the manufacturer

---

Technical Requirements

All proposed hardware and software must comply with the following common and device-specific requirements. Vendors must provide documentation confirming support for each item.

3.1 EVPN/VXLAN Fabric Common Requirements

3.1.1 Routing and Bridging

The equipment must support advanced Layer 2 and Layer 3 functionalities for EVPN Fabric deployment, including:

1. Compliance with all necessary EVPN standards (e.g., RFC 7432, RFC 8365).
2. EVPN/VXLAN for routing and bridging, enabling overlay networking.
3. Centralized Routing and Bridging (CRB) design on leaf switches.
4. Multi-Chassis Link Aggregation (MC-LAG) for high availability.
5. Ethernet Segment Identifier (ESI) for multi-homing.
6. Equal-Cost Multi-Path (ECMP) with up to 128 paths, plus Unequal-Cost Multi-Path (UCMP) routing.
7. Border Gateway Protocol (BGP) for dynamic routing.
8. Bidirectional Forwarding Detection (BFD) for fast failure detection.
9. Anycast IP addressing for load balancing and redundancy.
10. Virtual MAC/IP addressing for mobility and flexibility.
11. Policy-Based Routing (PBR) for traffic steering.

3.1.2 Hardware

Hardware components must ensure high performance and reliability:

1. ASIC latency of 800 ns or lower for ultra-low-latency forwarding.
2. Redundant power supplies for fault tolerance.
3. Support for Precision Time Protocol (PTP)/IEEE 1588 for time synchronization.

3.1.3 Quality of Service (QoS)

QoS features must handle traffic prioritization and congestion management:

1. Microburst detection with the ability to mirror dropped traffic for analysis.
2. Support for Explicit Congestion Notification (ECN), Data Center Bridging Exchange (DCBX), and Priority Flow Control (PFC).

3.1.4 Maintenance

Maintenance capabilities must minimize downtime and simplify operations:

1. A common software image across all network models for consistent upgrades.
2. Common monitoring and provisioning tools for unified management.
3. Smart System Upgrade (SSU) functionality, including network maintenance mode during switch reboots to maintain fabric availability.

3.1.5 Telemetry Collection

Telemetry must provide real-time insights into network performance:

4. Support for OpenTelemetry, with the ability to export data to InfluxDB or Prometheus. Scratch interval is 2 seconds or less for all collecting metrics.
5. sFlow/IPFIX sampling at a ratio of 1:500 for flow monitoring.
6. Inband telemetry for detailed packet-level insights.

3.1.6 Security

Security features must protect the network from threats:

1. Control Plane Policing (CoPP) to safeguard control plane resources.
2. IPv4/IPv6 Layer 2/Layer 3/Layer 4 ingress/egress access control lists (ACLs).
3. ACL drop counters and logging for auditing.
4. Integrated packet capture for troubleshooting.
5. Customized event detection and processing, supporting CLI-based and script-based automation.
6. Unicast Reverse Path Forwarding (uRPF) for security against spoofing.
7. DHCP-assisted MAC/IP security.

3.1.7 Monitoring

The monitoring solution must provide a centralized management platform that delivers a simplified network operations experience. It should leverage cloud networking principles for automation, observability, and security. Key requirements include:

- Turnkey management for monitoring, maintaining, and orchestrating network devices across data centers, campuses, and WAN domains.
- Continuous streaming of telemetry data from devices for real-time insights.
- Environmental monitoring with graphical displays for temperature, power supply usage, fan speeds and interfaces status and performance.
- Automation of complex tasks, including configuration management, compliance checks, and zero-touch provisioning.
- Observability features such as inventory tracking (e.g., hostname, management IP, serial numbers), topology visualization, and change control.
- Zero trust security integration, including visibility into VXLAN overlays, and third-party device updates.
- Support for on-premises model.
- Advanced analytics for anomaly detection, performance trending, and predictive maintenance.

3.2 EVPN/VXLAN Fabric Device-Specific Requirements

3.2.1 Spine Devices

- 32 x 100GE QSFP28 ports.
- Virtual Output Queuing (VoQ) architecture.
- 32MB shared buffer.
- Airflow: front-to-rear

3.2.2 Leaf Devices

Two variants required:

- **Variant 1:** 48 x 1/10GE Base-T ports + 4 x 100GE uplinks
- **Variant 2:** 48 x 10/25GE SFP28 ports + 6 x 100GE uplinks
- Both: Virtual Output Queuing (VoQ) architecture.
- Both: 32MB shared buffer.
- Forwarding Information Base (FIB): Up to 288K MAC addresses.
- FIB: Up to 360K routes.
- Airflow: front-to-rear

3.2.3 Service Leaf/DCI Devices

- 48 x 10/25GE SFP28 ports + 6 x 100GE ports.
- Virtual Output Queuing (VoQ) architecture.
- 16GB shared buffer.

- FIB: Up to 256K MAC addresses.
- FIB: Up to 1.5M routes.
- ARP table: Up to 80K entries.
- DCI support: EVPN/VXLAN to EVPN/MPLS handoff for interconnectivity
- Airflow: front-to-rear

3.3.1 Quantities and Support

- **Spine Devices:**
    - 2 pairs (4 devices total) with 5-year support and appropriate software licenses.
    - Advanced hardware replacement (RMA) with 24x7 TAC access.
- **Leaf Switches**
    - **Variant 1:**
        - 4 pairs + 1 spare device (9 devices total) with 5-year support and appropriate software licenses.
        - Advanced hardware replacement (RMA) with 24x7 TAC access.
    - **Variant 2:**
        - 5 pairs + 1 spare device (11 devices total) with 5-year support and appropriate software licenses.
        - Advanced hardware replacement (RMA) with 24x7 TAC access.
- **Service Leaf/DCI Devices (EVPN L3):**
    - 2 pairs (4 devices total) with 5-year support and appropriate software licenses.
    - Advanced hardware replacement (RMA) with 24x7 TAC access.
- **Monitoring and management:**
    - HA pair of on-premise virtual appliance, with 5-year subscription license for evpn/vlxan fabric devices.

4. Enterprise Border Firewalls, DC Firewalls and Zero Trust Network Access

4.1 Enterprise Border Firewall Minimum Requirements

- Form Factor: Rack Mount, 1U 19" standard rack
- Firewall throughput (with App Visibility and logging enabled): 8Gbps
- Threat Prevention throughput (with App Visibility, IPS, AV, AMP and logging enabled): 4Gbps
- Concurrent sessions: 900K

- New sessions per second: 100K
- Virtual Systems/Domains (full virtual slicing with independent management): at least 5
- Virtual Routing and Forwarding tables: at least 10
- Routing: BGP with graceful restart, policy-based forwarding, BFD
- Interface modes: L2, L3, tap, virtual-wire
- Interface types: 8 x 1/10G RJ45, 4 x 1/10G SFP/SFP+, 1 x 1/10G SFP/SFP+ HA
- Clustering: Active/Active, Active/Passive, horizontal scaling (upto 4 devices)
- Onboard Storage: More than 250G SSD
- Dual AC PSU for 1+1 Redundancy: hot swappable
- Airflow: front-to-back

4.2 Data Center / Server Farm Firewall Minimum Requirements

- Form Factor: Rack Mount, 1U 19" standard rack
- Firewall throughput (with App Visibility and logging enabled): 19Gbps
- Threat Prevention throughput (with App Visibility, IPS, AV, AMP and logging enabled): 10Gbps
- Concurrent sessions: 2M
- New sessions per second: 200K
- Virtual Systems/Domains (full virtual slicing with independent management): at least 10
- Virtual Routing and Forwarding tables: at least 10
- Routing: BGP with graceful restart, policy-based forwarding, BFD
- Interface modes: L2, L3, tap, virtual-wire
- Clustering: Active/Active, Active/Passive, horizontal scaling (upto 4 devices)
- VXLAN tunnel inspection
- Interface types: 8 x 1/10G RJ45, 4 x 1/10G SFP/SFP+, 4 x 25G SFP28+, 1 x 1/10G SFP/SFP+ HA
- Onboard Storage: More than 250G SSD
- Dual AC PSU for 1+1 Redundancy: hot swappable
- Airflow: front-to-back

4.3 Campus Zero Trust Network Access Firewall / User Access GW Requirements

- Form Factor: Rack Mount, 1U 19" standard rack
- Firewall throughput (with App Visibility and logging enabled): 19Gbps
- Threat Prevention throughput (with App Visibility, IPS, AV, AMP and logging enabled): 10Gbps
- Concurrent sessions: 2M
- New sessions per second: 200K
- Minimum client ssl vpn tunnels: 1500
- Virtual Systems/Domains (full virtual slicing with independent management): at least 5
- Virtual Routing and Forwarding tables: at least 10
- Routing: BGP with graceful restart, policy-based forwarding, BFD
- Interface modes: L2, L3, tap, virtual-wire
- Interface types: 8 x 1/10G RJ45, 4 x 1/10G SFP/SFP+, 4 x 25G SFP28+, 1 x 1/10G SFP/SFP+ HA

- Clustering: Active/Active, Active/Passive, horizontal scaling (upto 4 devices)
- Onboard Storage: More than 250G SSD
- Dual AC PSU for 1+1 Redundancy: hot swappable
- Airflow: front-to-back

Common Firewalls requirements:

- Built-in machine learning in the core of the firewall for signatureless threat detection
- Real-time SSL inspection (including TLS 1.3) to provide full visibility into users, devices, and applications across the attack surface
- Stateful firewall, intrusion prevention system (IPS), malware protection and application control, security policy enforcement.
- Integration with identity services, such as Active Directory, to enforce security policies based on user identity and group memberships.
- VXLAN tunnel inspection capability.
- Firewall vendor should have VM-based and container-based virtual appliances to protect virtualized environment (ESXi, KVM, HyperV, AHV) and container environment (Kubernetes). Optional

Additional Requirements for Campus Zero Trust Firewalls

common firewall requirements plus:

- Identity-based access enforcement
- Least privilege access model
- Continuous trust evaluation during sessions
- Centralized policy-based access control
- Application-level micro-segmentation
- Integration with multi-factor authentication (MFA)
- Support for SAML, OIDC, and OAuth2-based SSO
- Integration with LDAP, AD, Azure AD, and identity providers
- Multiplatform support (Windows, macOS, Linux, iOS, and Android)
- Device posture assessment and compliance validation

4.4 Quantities and Support

- **Enterprise Border Firewalls:**
  - 2 pairs of NGFW (4 devices total) in HA configuration.
  - 3-year or 5-year support with full security subscriptions (TP, URL, DNS, cloud sandboxing).
- **Data Center / Server Farm Firewalls:**
  - 2 pairs of NGFW (4 devices total) in HA configuration.
  - 3-year or 5-year support with VXLAN inspection enabled.

- **Campus Zero Trust Network Access Firewalls:**

    - 2 pairs (4 devices total) in HA configuration.
    - 3-year or 5-year support with SSL VPN and host information collection.

---

5. Centralized Management and Logging

5.1 Requirements

- Form Factor: Virtual Appliance.
- Supported hypervisors: VMware ESXi, KVM, Nutanix, Microsoft Hyper-V.
- Clustering: Active/Passive.
- Log retention: ≥ 3 months.
- Log collection: ≥ 25,000 logs/sec per instance.
- Distributed log collector deployment support.
- Variables for configuration components defined on the templates
- Multilevel device grouping to centrally manage the policies and objects across all deployments.
- Role-based access control, reporting, and software/license update management for controlled devices.
- Common administration, monitoring and log collection for hardware appliances, virtual appliances and container appliances.

5.2 Quantities and Support

- **Centralized Management and Logging:**

    - 1 HA pair for device management (up to 25 devices).
    - 1 HA pair for dedicated log collection.
    - 5-year support for both device manager and log collector.

---

6. Enterprise WAN IPsec Firewalls

6.1 Firewall Requirements

- Rack-mount up to 2U, 19” standard
- IPsec VPN throughput: ≥ 45 Gbps (AES256-SHA256)
- Site-to-Site VPN tunnels: ≥ 15,000
- Concurrent sessions: ≥ 9M
- New sessions per second: ≥ 500K
- Virtual Systems: up to 250
- Routing: BGP, PBF, BFD

- Interface modes: L2, L3
- Interfaces: 16 x GE RJ45, 8 x GE SFP, 12 x 10/25G SFP+/SFP28, 4 x 40/100G QSFP+/QSFP28
- Dual hot-swappable PSUs
- front-to-back airflow

6.2 Centralized Management and Logging

- Form Factor: Virtual Appliance.
- Supported hypervisors: VMware ESXi, KVM, Nutanix, Microsoft Hyper-V.
- Active/Passive clustering.
- Distributed log collection and full policy-based administration

6.3 Quantities and Support

- **Enterprise WAN Firewalls:**
    - 2 pairs (4 devices total) with 5-year support.
- **Centralized Management and Logging:**
    - 1 HA pair managing up to 100 devices with 5-year support.

---

7. Optical Transceivers

7.1 Optical Modules

The participants must supply all necessary optical transceivers to ensure end-to-end connectivity:

- SFP+ (10G), SFP28 (25G), QSFP+/QSFP28 (40G/100G).
- Modules must match switch and firewall interface requirements and be compatible with corresponding devices.
- Support for short-reach (SR) and long-reach (LR) optics depending on deployment design.

7.2 Quantities

- **10GBASE-T SFP+ Copper (min 30m):**
    - 20 units totally - 16 units compatible with **4.4** devices, 4 units compatible with **3.3.1** devices
- **10GBASE-LR SFP+ Duplex LC/UPC SMF:**
    - 200 units totally – 160 units compatible with **3.3.1** devices, 20 units compatible with **4.4** devices, 20 units compatible with **6.3** devices
- **25GBASE-LR SFP28 Duplex LC/UPC SMF:**

    - 160 units totally - 30 units compatible with **4.4** devices, 40 units compatible with **6.3** devices, 90 units compatible with **3.3.1** devices

- **100GBASE-DR QSFP28 Duplex LC/UPC SMF:**
    - 64 units totally - 56 units compatible with **3.3.1** devices, 8 units compatible with **6.3** devices
- **100GBASE-PSM4 QSFP28 MPO-12 SMF:**
    - 24 units totally - compatible with **3.3.1** devices