Tender #47/2026/S

Centralized Log Management & Security Analytics Appliance (Forti Analyzer) QTY 1

Technical Requirement	Comply (Yes / No)
1. The proposed solution shall be a dedicated centralized log management, security analytics, event correlation and reporting appliance, providing centralized visibility across security and network devices.	
2. The appliance shall support a log ingestion capacity of 25 GB per day.	
3. The appliance shall sustain an analytics processing rate of 500 logs per second without degradation of the analytics database and system performance.	
4. When operating in Collector mode, the appliance shall sustain a log collection rate of 750 logs per second.	
5. The appliance shall support 50 -100 managed devices / virtual domains (VDOMs) and up to 90 days of analytics retention when receiving logs continuously at the specified sustained analytics rate.	
6. The hardware appliance shall provide two (2) Gigabit Ethernet RJ45 interfaces.	
7. The appliance shall include 4 TB raw local storage using two (2) 2 TB drives, with 2 TB usable storage after the default RAID configuration. RAID 0 and RAID 1 shall be supported, with RAID 1 as the default level.	
8. The appliance shall be supplied in a compact desktop form factor and support 100–240 VAC, 50–60 Hz input power.	
9. The solution shall support both Analyzer and Collector operational modes. It shall support real-time or near-real-time log forwarding to another analyzer, Syslog server, or CEF server while retaining a local copy of logs.	
10. The solution shall provide centralized NOC/SOC visibility with real-time log and threat information, drill-down investigation, customizable dashboards, event monitoring, correlation and configurable event handlers. (Optional)	
11. The solution shall support multi-tenancy using administrative domains (ADOMs) with quota management, and enterprise-grade High Availability with support for a cluster of up to four nodes for redundancy and disaster recovery.	
12. The solution shall support security automation through REST API, scripts, connectors and playbooks, integration with security-fabric components, and comprehensive reporting capabilities including more than 60 report templates, 800+ datasets and 750+ charts, with report export/output in PDF, HTML, CSV and XML formats.	

Hosted Cloud Email Security Gateway Service (Forti Mail) QTY 100

Technical Requirement	Comply (Yes / No)
1. The proposed solution shall be a fully hosted and managed cloud email security gateway service designed to protect organizations against phishing, spear phishing, spam, malware, ransomware, impersonation, targeted attacks and Business Email Compromise (BEC).	
2. The service shall provide a managed cloud infrastructure with a service level target of at least 99.99% availability and a spam capture rate of at least 99.97%.	
3. The service shall provide advanced multi-layer malware detection and shall inspect both inbound and outbound email traffic.	
4. The service shall include enterprise-grade Antivirus, AntiSpam and Virus Outbreak Prevention capabilities as standard security services.	
5. The service shall include cloud-based sandboxing for advanced detection and analysis of suspicious or previously unknown email-borne threats.	
6. The service shall provide Content Disarm and Reconstruction (CDR) capabilities to sanitize supported email content and attachments before delivery to end users.	
7. The service shall provide URL click protection to inspect and protect users from malicious or compromised links contained in email messages.	
8. The service shall provide impersonation analysis capabilities for detecting spoofing, identity-based attacks and Business Email Compromise attempts.	
9. The service shall support secure message delivery using TLS and shall provide Identity-Based Encryption (IBE) for secure email communications.	
10. The service shall support integration with the customer directory through LDAP for recipient/user validation and shall provide message tracking and reporting capabilities for administrative visibility and investigation.	
11. The service shall support up to ten (10) protected primary email domains, with the ability to associate additional alias email domains with the protected domains.	
12. The service shall be licensed on an annual per-mailbox subscription basis and shall include 24x7 technical support. The proposed subscription tier shall be selected according to the required number of active mailboxes.	

Privileged Access Management (PAM) Specification QTY 7

Section	Minimum Technical Requirement	Comply (Yes/NO)
Solution Architecture	The proposed solution shall be an enterprise-grade PAM virtual appliance providing centralized privileged credential vaulting, privileged access control, session management, auditing, reporting, and secure remote access from a unified management platform. The solution shall support deployment on industry-standard virtualization infrastructure.	
High Availability & Capacity	The solution shall be deployed using two virtual appliances in a High Availability (HA) architecture with automatic failover and configuration/data synchronization between nodes. The proposed licensing shall support a minimum of seven (7) named privileged administrator users across the HA deployment. Any vendor-specific minimum license increment required for an HA/DR node shall be included in the proposed bill of materials without additional cost to the customer beyond the submitted offer.	
Credential Vault & Password Management	The solution shall provide secure centralized storage of privileged credentials using AES-256 encryption or stronger. Privileged passwords shall be protected from disclosure to end users and the solution shall support password verification, scheduled and policy-based password rotation, password complexity enforcement, and automatic password change after use or check-in where applicable.	
Privileged Access & Protocol Support	The solution shall provide controlled and proxied privileged access to target systems using commonly used protocols, including at minimum RDP, SSH, SFTP/SCP, SMB and web-based access. The platform shall support browser-based/clientless access and controlled native application access where applicable, while preventing unnecessary exposure of managed credentials to the end user.	
Session Monitoring & Control	The solution shall provide real-time monitoring of active privileged sessions, session recording and playback, administrative session termination, and detailed activity auditing. The solution shall support granular activity controls, including command filtering for SSH sessions and/or application-level restrictions for Windows privileged sessions.	
File Transfer Security	The PAM platform shall provide native security controls for privileged-session file transfers, including anti-malware/antivirus inspection and Data Loss Prevention (DLP) capabilities. The solution shall support inspection and enforcement based on file attributes such as file type and size, and shall provide the ability to integrate with advanced malware sandboxing or equivalent threat-analysis services.	
Access Governance & Approval Workflow	The solution shall provide Role-Based Access Control (RBAC), policy-based authorization, privileged access request and approval workflows, multiple approval levels or approvers, secret/account check-out and check-in controls, time-restricted access, and emergency or break-glass access for authorized personnel.	
Authentication & Identity Integration	The solution shall integrate with enterprise identity sources and support at minimum Microsoft Active Directory/LDAP, RADIUS and SAML. It shall support Multi-Factor Authentication (MFA) and Single Sign-On (SSO), either natively or through integration with enterprise authentication services.	

Account Discovery, Service Accounts & Zero-Trust Controls	The solution shall support discovery, onboarding and policy-based management of privileged and service accounts, including automated credential rotation. It shall also support endpoint/device posture or equivalent Zero-Trust access controls to restrict privileged access based on the security or compliance status of the connecting endpoint.	
Audit, Reporting, Integration & Support	The solution shall provide centralized and tamper-resistant audit logging for authentication events, privileged account access, secret operations, administrative actions and recorded sessions. It shall provide compliance-oriented reporting and integration with external SIEM/SOC or automation platforms through REST API and/or standard integration mechanisms. The proposed solution shall include the required vendor support and subscription services for the full contract period. CSV, PDF, HTML, exportable reports (users, sessions, anomalies)	

The bidder shall provide an enterprise-grade Privileged Access Management (PAM) solution meeting or exceeding the following minimum requirements. The proposed solution shall be delivered as virtual appliances in a High Availability (HA) architecture and shall support a minimum of seven (7) named privileged administrator users.

Infrastructure Provisioning Note:

All infrastructure resources required to deploy and operate the proposed PAM solution in the required HA architecture shall be included within the bidder's scope and commercial offer, with both PAM virtual appliances hosted on the same underlying compute platform, without reliance on additional customer-provided infrastructure.

Other Notes

Support & Local Delivery	1–3-year support local partner with 7+ years of experience and government references.	
Price	Provide us for 1-year subscription, 3-year subscription	
	The solution should be complied with NPC local network	
Certifications	3+ Engineer Certified for Above solutions	
Training	2- 4 NPC Staff	
Instruction/ Guideline for Installation	NPC HQ- Amman & Documentation (AR/EN)& SLA	
Reports	All Reports should be satisfied for NPC Staff	