حكومة عجمان
Government of Ajman

هيئة النقل
Transport Authority

Request for Proposal

Project: Fortinet Zero Trust Network Access (ZTNA)

On-Premises FortiClient EMS | 30 Users

1. Project Overview

The Transport Authority seeks proposals from qualified, Fortinet-authorized partners to design, supply, implement, test, document, and support a Fortinet Zero Trust Network Access (ZTNA) solution. The solution will provide secure, application-level remote access for 30 authorized users while keeping protected internal applications inaccessible directly from the Internet.

Deployment Preference: On-premises FortiClient Endpoint Management Server (EMS), integrated with the Authority's existing FortiGate firewall. Supply of a new FortiGate appliance is not part of the base scope.

1.1 Objectives

- **Least-privilege access:** Grant each user access only to approved applications and services, not broad network access.
- **Continuous verification:** Evaluate identity, device certificate, endpoint telemetry, and posture before access is permitted.
- **Centralized control:** Use on-premises EMS to manage FortiClient deployment, profiles, telemetry, Zero Trust tags, and compliance reporting.
- **Secure integration:** Integrate with the existing FortiGate, identity provider, MFA, DNS, certificates, monitoring, and SIEM services.
- **Operational readiness:** Deliver tested configuration, rollback procedures, knowledge transfer, and support for sustainable operations.

1.2 Required Solution Summary

Item	Required Baseline
Users/endpoints	30 production users.
License term	One-year FortiClient ZTNA subscription with on-premises EMS entitlement and applicable FortiCare support. A three-year option shall be quoted separately.
Enforcement	Authority-owned existing FortiGate firewall or HA cluster. No new FortiGate appliance shall be included in the base proposal; the bidder shall confirm model, FortiOS compatibility, licensing, and available capacity.
Endpoint management	Dedicated on-premises FortiClient EMS instance hosted by the Authority.
Application onboarding	All applications/services listed in the Authority-approved application inventory, with no default numerical cap, plus 30 managed endpoints.
Support	Implementation warranty plus one year of partner technical support and software entitlement.

Important: The bidder shall provide the current, valid Fortinet Bill of Materials (BoM) and confirm that every proposed SKU, subscription, version, and support entitlement remains supported at the date of quotation.

2. Scope of Work

- **Discovery and assessment:** Review the current FortiGate model, HA design, FortiOS version, capacity, interfaces, security policies, certificates, DNS, identity sources, MFA, endpoint operating systems, application inventory, network paths, and logging platform.
- **Solution design and architecture:** Conduct design workshops and deliver approved high-level and low-level designs covering traffic flows, security zones, EMS connectivity, certificate trust, identity, posture, application publishing, availability, backup, recovery, and rollback.
- **Licensing and software:** Supply sufficient FortiClient ZTNA licensing for 30 users with on-premises EMS and support for the selected one-year term. Register and activate all entitlements in the Authority-approved account.
- **EMS deployment:** Install and harden FortiClient EMS on the Authority-provided dedicated Linux VM; configure administrators, RBAC, endpoint groups, deployment packages, profiles, telemetry, tags, update settings, audit logging, backup, and certificate management.
- **FortiGate ZTNA configuration:** Configure the Authority's existing FortiGate firewall, including the EMS Fabric connector, ZTNA access proxy/virtual hosts, server mappings, firewall policies, identity groups, certificates, logging, and security inspection in accordance with the approved design.
- **Identity and MFA integration:** Integrate with the Authority's approved AD/LDAP/Entra ID, SAML, OIDC, RADIUS, FortiAuthenticator, or other supported identity service. MFA shall be enforced for remote access unless a documented exception is approved.
- **Endpoint posture:** Create agreed posture rules and Zero Trust tags, including device management status, domain membership, supported OS, endpoint protection/EDR status, firewall status, disk encryption, patch status, certificate presence, and critical vulnerability state where technically supported.
- **Application onboarding:** Publish, configure, and test all applications/services in the Authority-approved application inventory agreed during discovery. No default numerical cap shall apply. Access shall use application-specific policies and shall not expose unrestricted internal network connectivity. Any unsupported application, protocol, or proposed exclusion shall be documented with a secure alternative and submitted for Authority approval.
- **Pilot and rollout:** Complete a controlled pilot, resolve findings, deploy FortiClient to 30 endpoints using an approved method, migrate users in batches, validate user experience, and maintain a tested rollback plan.
- **Monitoring and reporting:** Forward relevant FortiGate and EMS events to the existing FortiAnalyzer/SIEM platform; configure operational alerts and deliver reports for access, posture, failures, and administrator actions.
- **Training and handover:** Provide administrator training, operations training, knowledge transfer, as-built documentation, configuration backup, troubleshooting guide, renewal details, and formal handover.

Change control: All production changes, including any FortiOS upgrade, shall be performed only after compatibility validation, configuration backup, approved maintenance window, documented rollback steps, and Authority approval.

3. Proposed Architecture and Prerequisites

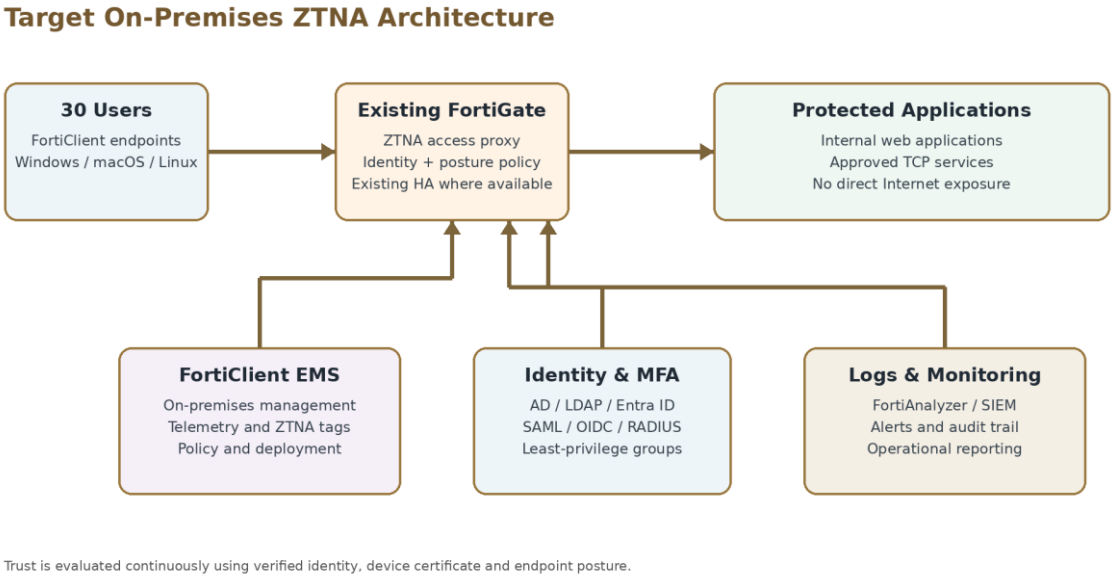

Figure 1 - Logical target architecture. The final design shall be validated against the Authority's installed FortiGate/FortiOS versions and approved network topology.

3.1 Design Principles

- **Application-level access:** Publish only approved applications and ports; do not provide unrestricted network access.
- **Continuous trust:** Evaluate user identity, MFA, device certificate, EMS telemetry, and endpoint posture for every policy decision.
- **On-premises control:** Keep EMS administration, endpoint telemetry, policy, and audit information within the Authority's environment.
- **Existing security integration:** Use the existing FortiGate enforcement layer and integrate logs with FortiAnalyzer/SIEM.

3.2 Integration and Application Readiness

The Authority will provide the agreed on-premises hosting platform and approved enterprise services. The bidder shall validate and document the following implementation dependencies before configuration begins.

Readiness Area	Bidder Validation / Authority Dependency
Network placement	Confirm the required EMS network placement, routing, security zone, management sources, and least-privilege access paths. The Authority will allocate the approved addressing and access.
Time and notifications	Identify NTP and SMTP requirements for system time, alerts, enrollment notices, reports, and certificate-expiry notifications. The Authority will provide approved enterprise services where required.
Network connectivity	Submit a complete connectivity matrix covering EMS, FortiClient endpoints, FortiGate, identity services, protected applications, FortiAnalyzer/SIEM, DNS, NTP, SMTP, and FortiGuard, including source, destination, FQDN/IP, port, protocol, direction, purpose, and TLS-inspection requirements.
Internet and FortiGuard	Disclose all required external domains, cloud dependencies, update services, and documented TLS-inspection exclusions for installation, entitlement validation, FortiGuard services, signatures, and updates. The Authority will approve permitted outbound access.
Certificates and PKI	Submit the certificate inventory and requirements for ZTNA FQDNs, EMS/FortiGate trust, and endpoint authentication, including CSR details, trust chains, private-key handling, renewal ownership, expiry alerting, revocation, and emergency replacement. The Authority will approve or issue certificates through its approved process.
Identity and MFA	Design and document the authentication flow, user/group mappings, MFA method, conditional-access dependencies, test accounts, and least-privilege service accounts or application registrations. The Authority will provide access to the approved identity services.
Endpoint readiness	Validate compatibility for 30 managed endpoints and supply approved deployment packages and rollout requirements. The Authority will provide endpoint inventory, pilot users, deployment access, endpoint-security details, and agreed maintenance windows.
Logging and monitoring	Define the EMS and FortiGate events, secure transport, fields, alerts, reports, and incident-response use cases to be integrated. The Authority will provide the approved FortiAnalyzer/SIEM destination, retention requirements, and operations contacts.
Change and testing	Submit the implementation, test, communication, rollback, and escalation plans. The Authority will provide approved change windows, pilot participants, business validators, and production approval.
Data handling	EMS configuration, endpoint telemetry, logs, credentials, and backups shall remain on premises unless the Authority gives prior written approval. The bidder shall identify any telemetry, licensing, support, or update data sent externally.

Readiness sign-off: Before production implementation, the Authority and bidder shall jointly approve the compatibility report, connectivity matrix, certificate plan, application inventory, pilot plan, and rollback procedure. Gaps shall be recorded with an owner and target date.

4. Technical and Functional Requirements

The bidder shall complete the Vendor Response column for every requirement. 'Partial' or 'No' responses must include the limitation, proposed alternative, licensing impact, and remediation roadmap. M = Mandatory; O = Optional.

Ref.	Area	Requirement
F-01	**Licensing**	Provide current FortiClient ZTNA/VPN subscription licensing for at least 30 endpoints with on-premises EMS entitlement and FortiCare/partner support for one year.
F-02	**Licensing**	Register entitlements to the Authority-approved Fortinet account and provide the complete current SKU-level BoM, renewal date, support level, and license certificate.
F-03	**EMS**	Deploy EMS on premises; cloud/SaaS management or external storage of endpoint telemetry shall not be used without prior written approval.
F-04	**EMS**	Support centralized endpoint registration, deployment packages, profiles, grouping, telemetry, policy, version control, upgrade rings, audit logs, and reporting.
F-05	**FortiGate**	Integrate EMS with the existing FortiGate through a secure connector using supported, CA-signed certificate trust.
F-06	**Access**	Provide application-level ZTNA access proxy capability for internal web applications and approved TCP services without granting broad network access.
F-07	**Access**	Support policies based on user/group, destination application, device certificate, EMS telemetry, posture tags, source context, and schedule where supported.
F-08	**Identity**	Integrate with the approved enterprise identity source and enforce MFA for remote access, subject to approved emergency-access procedures.
F-09	**Certificates**	Deploy and document endpoint/client certificates, server certificates, trust chains, renewal ownership, expiry monitoring, and revocation process.

4.1 Technical and Functional Requirements (Continued)

The bidder shall complete every response and provide supporting evidence where requested.

Ref.	Area	Requirement
F-10	**Posture**	Implement agreed ZTNA tagging for device management, domain membership, supported OS, endpoint protection/EDR, firewall, disk encryption, patch status, and vulnerability state.
F-11	**Posture**	Deny or restrict non-compliant devices and present a clear remediation path without revealing sensitive internal information.
F-12	**Endpoints**	Deploy and validate FortiClient for 30 production endpoints using silent installation and approved endpoint-management tools where available.
F-13	**Applications**	Onboard, configure, and test every application/service in the Authority-approved application inventory. No default numerical cap or unapproved exclusion shall apply.
F-14	**Operations**	Provide controlled policy change, configuration backup, restore, rollback, certificate renewal, troubleshooting, and upgrade procedures.
F-15	**Reporting**	Provide dashboards/reports for endpoint registration, compliance posture, ZTNA access, denials, failed authentication, administrator actions, and license utilization.
F-16	**Integration**	Forward relevant EMS and FortiGate events to the existing FortiAnalyzer/SIEM with timestamps synchronized to the Authority's NTP source.
F-17	**Experience**	Provide consistent user access from approved external networks without requiring direct exposure of internal application servers to the Internet.
F-18	**Scalability**	Allow future expansion beyond 30 users and onboarding of additional applications without architectural redesign.

5. Security and Non-Functional Requirements

Ref.	Area	Requirement
N-01	**Availability**	Preserve the existing FortiGate HA capability where available and design EMS backup/recovery to meet agreed operational recovery objectives.
N-02	**Performance**	Demonstrate acceptable access latency and user experience for 30 concurrent authorized users; identify sizing assumptions and FortiGate resource impact.
N-03	**Encryption**	Use supported strong encryption and TLS 1.2 or later for management and application access; weak/deprecated protocols and ciphers shall be disabled unless formally approved.
N-04	**Hardening**	Apply Fortinet and OS hardening guidance, least privilege, RBAC, MFA for administrators where supported, restricted management access, and secure service accounts.
N-05	**Logging**	Record successful/failed access, policy decisions, posture status, administrative changes, connector health, and system errors with sufficient context for investigation.
N-06	**Retention**	Integrate with the Authority's monitoring platform and retain logs in accordance with internal policy; the bidder shall state storage and licensing dependencies.
N-07	**Privacy**	Keep EMS configuration, telemetry, logs, and credentials on premises unless written approval is provided. Disclose all vendor cloud dependencies and outbound destinations.
N-08	**Vulnerability**	Deliver currently supported releases, identify known relevant vulnerabilities, remediate critical findings before acceptance, and provide a patch/upgrade process.

5.1 Security and Non-Functional Requirements (Continued)

Ref.	Area	Requirement
N-09	**Resilience**	Document failure modes, certificate expiry risks, service dependencies, backup frequency, restoration steps, and tested rollback for each production change.
N-10	**Compliance**	Comply with applicable UAE requirements, Authority security policies, change management, data classification, incident handling, and ISO/IEC 27001-aligned controls.
N-11	**Support**	Provide 24x7 response for Severity 1 incidents and 8x5 support for lower severities, with escalation to Fortinet where required.
N-12	**Documentation**	Provide editable and PDF copies of HLD, LLD, as-built, IP/port matrix, policy matrix, certificate register, backup/restore, SOP, troubleshooting, and support details.
N-13	**Training**	Provide instructor-led administrator and operations training, recorded only if approved, plus training material and hands-on knowledge transfer.
N-14	**Warranty**	Provide at least 30 calendar days of post-go-live implementation warranty for configuration defects at no additional cost.

5.2 Minimum Support Service Levels

Priority	Initial Response	Target / Expectation
Severity 1 - Critical	30 minutes, 24x7	Continuous effort; workaround/restore target within 4 hours
Severity 2 - High	2 business hours	Workaround or action plan within 1 business day
Severity 3 - Medium	4 business hours	Resolution plan within 3 business days
Severity 4 - Low / Request	1 business day	Resolution or planned date within 5 business days

6. Implementation, Deliverables and Acceptance

6.1 Indicative Implementation Plan

Phase	Workstream	Key Outputs	Target
1	Discovery and design	Kickoff, assessment, application/user inventory, HLD/LLD, prerequisites and change plan	Week 1
2	Platform build	EMS installation/hardening, licensing, RBAC, backup, certificates and FortiGate connector	Week 2
3	Policy and pilot	Identity/MFA, posture tags, pilot applications/endpoints, logging and remediation	Week 3
4	Full rollout and handover	All remaining applications and users/endpoints, acceptance testing, documentation, training, cutover and support transition	Approved plan

The bidder shall submit a detailed project plan with dependencies, resource assignments, change windows, risk register, and dates. The final schedule is subject to Authority approval, prerequisite readiness, and the size and complexity of the approved application inventory.

6.2 Required Deliverables

- Project plan, responsibility matrix, risk/issue register, and communication/escalation plan.
- Current Fortinet BoM, license certificate, support entitlement, and renewal schedule.
- Assessment report, compatibility matrix, HLD, LLD, traffic flow, IP/port matrix, and approved rollback plan.
- Hardened EMS build, FortiGate ZTNA configuration, identity/MFA integration, posture/tag policies, policies for every application in the approved inventory, and logging integration.
- Pilot and production test results for all inventoried applications, screenshots/log evidence, vulnerability remediation evidence, and acceptance report.
- As-built document, configuration backups, certificate register, administrator SOP, operational runbook, troubleshooting guide, and training material.

7. BoQ Delivery Date

Please submit the complete BoQ, technical proposal, compliance matrix, and commercial proposal before 15/09/2026

8. Contact Information

For questions or clarifications related to this RFP, please contact:

Financial / Procurement
procurement@ta.gov.ae

Technical
Mohamad Zulfihaar
Mohamed.batcha@ta.gov.ae

Clarifications: All bidder questions and resulting clarifications shall be submitted through the approved procurement channel. Verbal statements will not amend this RFP unless confirmed in writing by the Authority.