



RFP UJ 41/2025: Provision of a Forticlient VPN, EMS and ZTNA Solution for a Three Year Period

Table of Contents

1. Overview	2
2. Basic requirements.....	2
3. Support requirements.....	2
4. Service Credit Clauses for Non-Compliance with SLA	3
5 FortiClient VPN, EMS and ZTNA Implementation Requirements (Specifications)	4
6 Configuration and implementation Phases and timeline	5
7 Additional notes.....	6
8 Technical Adjudication.....	7
9 Pricing Sheet.....	8
10 Approvals	9

1. Overview

The University of Johannesburg (UJ) has established a robust campus security infrastructure. In 2025, one of our key strategic focus areas is to ensure a robust security posture while enabling seamless and secure corporate resources. To achieve this, the Information and Communication Systems (ICS) department is implementing FortiClient VPN EMS and Zero Trust Network Access (ZTNA). This initiative will enhance secure remote access and endpoint protection.

As part of our ongoing commitment to maintaining the highest security standards, ICS is initiating a tender process for deploying FortiClient VPN EMS and Zero Trust Network Access, leveraging Fortinet technology. Since this technology is within UJ's environment, this initiative aims to maximize existing investments, reduce costs, and enhance the university's overall security posture.

This document outlines the specifications, implementation requirements, and support services necessary to deploy and operate the FortiClient Endpoint Management Server solution successfully.

2. Basic requirements.

The successful service provider must be able to meet the following requirements:

- 2.1 Fortinet approved reseller and Fortinet accredited. (Proof of valid certification to be included in the submission.) -Failure to provide valid proof of partner certification will lead to disqualification.
- 2.2 Local i.e., South African representative and must be around the Gauteng province.
- 2.3 Own In-house Fortinet Engineers. (Proof such as CVs to be supplied in the submission.)
- 2.4 Technical Resources MUST have valid NSE 4 and NSE 5 Certification. (Proof of valid certifications to be supplied.)

3. Support requirements.

The successful service provider must be able to adhere to the following support requirements:

3.1 Support Calls

- UJ working hours are 7:30 am to 5 pm, Monday to Friday, excluding holidays.
- When a support call is initiated, the service provider must respond within 2 hours. If a repair is needed, the service provider must repair it within 4 hours. The hours that will be used can be used from the total amount of hours that is specified for support hours (section 3.2)

Priority	Response Time	Resolution Time
Critical	15 Min	2 Hours
High	30 Min	4 Hours
Medium	1 hour	8 Hours
Low	2 Hours	24 Hours

3.2 Support Hours

- As specialized skills are needed, UJ will need support hours to be included in the submission by the service provider. These support hours can be used for troubleshooting

problems, optimising the configurations of devices, firmware Updates and recommendations, updating new ransomware definitions, expert advice on best practices, etc.

- Furthermore, a certified Fortinet Engineer can provide these consulting/support hours onsite or remotely (UJ will decide).
- Support and Maintenance should be included in the solution for 1 year thereafter.
 - 20 hours for support to be allocated for the year. (during working hours).
 - These hours will be pre-arranged with the successful service provider in advance unless urgent support is needed for a break-fix scenario.
- Monthly report on the balance of hours used and remaining to be supplied. (A Must)

3.3 Afterhours

- Afterhours refers to work outside normal working hours. In certain cases, the service provider must be able to provide service outside working hours indicated in section 3.1.
- After-hours Support and Maintenance should be included in the solution for 1 year period thereafter.
 - 10 after-hours support hours must be quoted.

4. Service Credit Clauses for Non-Compliance with SLA.

4.1 Service Credit Eligibility.

- 4.1.2 If the Service Provider fails to meet the agreed Service Level Agreement (SLA) targets for incident response, resolution, or availability as stipulated in this contract, the Client shall be entitled to claim service credits.
- 4.1.3 Service credits will apply when SLA breaches occur (without in any way impacting UJ's rights in terms of the agreement, in respect of breach) due to the Service Provider's failure and not due to Force Majeure events, Client-induced delays, or scheduled maintenance agreed upon by both parties.

4.2 Service Credit Calculation.

- 4.2.1 Service credits shall be calculated based on the severity of the breach and the time exceeding the agreed resolution period.

SLA Breach Type	Breach Duration Beyond SLA	Service Credit (% of Monthly Fees)
Priority 1 (Critical)	1 - 4 hours	5%
Priority 1 (Critical)	4 - 8 hours	10%
Priority 1 (Critical)	8+ hours	15%
Priority 2 (High)	4 - 12 hours	5%
Priority 2 (High)	2+ hours	10%
Priority 3 (Medium)	24+ hours	5%

- 4.2.2 The total service credit awarded each month shall not exceed 25% of the total service fee.

4.3 Service Credit Application.

- 4.3.1 The Client must formally notify the Service Provider of any SLA breach and intend to claim service credits within ten (10) business days of the breach occurrence.

- 4.3.2 Service credits will be deducted from the next invoice issued to the Client. If the contract is terminated, outstanding service credits will be refunded within thirty (30) calendar days.
- 4.3.3 Repeated SLA breaches (three or more within a rolling six-month period) may trigger a contract review, penalty escalation, or grounds for contract termination.

4.4 Exclusions and Exceptions.

- 4.4.1 Service credits shall not apply if SLA breaches result from.
 - Client-side infrastructure or application failures.
 - Planned and emergency maintenance pre-approved by the Client.
 - Third-party service failures beyond the Service Provider's control.
 - Force Majeure events, including natural disasters, strikes, and regulatory restrictions.

5 FortiClient VPN, EMS and ZTNA Implementation Requirements (Specifications)

The proposed solution must include the following functionalities:

5.1 VPN Implementation (The successful service provider is expected to provide expert advice on the use cases to implement the solution effectively)

- FortiClient VPN should provide secure remote access using SSL-VPN Tunnel.
- VPN Gateway configuration should be setup to terminate on FortiGate.
- Split Tunneling: Configure policies to route only corporate traffic through VPN.
- Authentication should support MFA and identity-based access.
- Configuration optimization to correct and enhance the current implementation.
- Performance optimization ensures that bandwidth and latency requirements are met.
- Support error messages handling in FortiClient application.

5.2 EMS Implementation (The successful service provider is expected to provide expert advice on the use cases to implement the solution effectively)

- Central Management Tools should be cloud hosted.
- Provide Centralised Management for policy enforcement and monitoring.
- Device enrolment Checks for compliance and automatic provisioning.
- Telemetry at Endpoints For risk-based access control, gather information on security posture.
- Provide Role-Based Access Control (RBAC) to restrict administrative privileges based on roles. (RBAC for system administrators and consultants)
- Support Incident Response to automated remediation actions based on threat intelligence.
- Support integration with Microsoft LDAP.
- Enforce user verification using LDAP/SAML server for authentication.
- Hosted on the Fortinet Cloud to ensure redundancy and High Availability (HA) of EMS.
- Provide a quote on Cloud-Hosted solution (MFA Capable).

5.3 Zero Trust Network Access (ZTNA) implementation (The successful service provider is expected to provide expert advice on the use cases to implement the solution effectively)

- FortiGate should be the ZTNA gateway for secure access control.
- Version Control: Identify and address endpoints running outdated versions of applications.
- Must support security posture checking on endpoints, including but not limited to the following:
 - Must determine if the machine is joined to the domain or not.

- Must check if anti-virus is installed, enable, and updated.
- Must be able to the vendor of the AV.
- Must be able to determine which OS the device is running on.
 - Endpoints that have unhealthy security posture must be thrown in to the guest network with only internet access for remediation.
 - Develop custom posture checks for machines joined to the domain, those not joined, and non-UJ endpoints.
 - Endpoint Vulnerability Monitoring.
 - Ensure that staff can only access specific applications or systems they are authorised to use, regardless of whether they are on the LAN, Wi-Fi, or working remotely.
 - Policy Enforcement Granular application-level access based on user identity and device posture.
 - Support Multi-Factor Authentication for all remote and high-privilege access.
 - Deploy FortiClient with ZTNA Configuration to endpoints.
 - Allow application-layer access control instead of full network access. (ZTNA non-access proxy, also known as ZTNA Secure access.
 - Users should receive clear error messages and logs errors for admin review.

5.4 Monitoring and management

- **FortiClient EMS Dashboard:** Centralised endpoint security management.
- **FortiGate Logs & Reports:** Monitor ZTNA access and policy violations. (It should integrate with FortiAnalyzer and existing SIEM)
- **Endpoint Administration:** Manage endpoint registrations by accepting, deregistering, or blocking them as needed
- **Incident Response:** Automated threat response and remediation. (detect threat, enforces security policies and response to security incidents at the endpoint level).
- **Remote Deployment:** Install FortiClient software on Windows PCs from a central location. (The solution can also deploy FortiClient applications to clients for version control.

6 Configuration and implementation Phases and timeline.

Phases	Description	Timeline
Planning	Identify endpoints and Network requirements, Plans FortiClient deployment strategies.	2 weeks
Installation	Install FortiClient EMS and configuring the database on Fortinet Cloud. Ensures network connectivity. Configure licensing and activate endpoint management.	2 weeks
Configuration	Setup Integration between Ems and the firewall. Setup Administrative account and roles. Configure endpoint visibility and posture management and control. Define ZTNA tags and application policies. Set up ZTNA access proxy for applications (Web, RDP, SSH, etc.). Configure authentication using SAML, LDAP, or Forti Authenticator.	3 weeks

Testing and Validation	Test application access through ZTNA policies. Verify endpoint posture enforcement. Ensure logging and monitoring are functional.	1 months
Deployment and Monitoring	Deploy FortiClient to endpoints using EMS or SCCM Server. Roll out ZTNA policies in phases. Monitor logs and enforce compliance dynamically.	4 Months

7 Additional notes.

- 7.1 By responding to this tender, the tenderer agrees to the UJ Standard Terms and Conditions provided in the tender pack.
- 7.2 The response must strictly adhere to the above requirements. Deviations must be clearly mentioned and explained. However, it will be at the sole discretion of UJ to accept or reject such deviations.
- 7.3 The successful service provider is expected to provide onsite support or remotely through VPN service, and access will be provided if needed.
- 7.4 The successful service provider MUST provide expert advice on the use cases to implement each solution effectively or recommend the ideal use cases.
- 7.5 The implementation must align with change and project management principles to ensure smooth adoption across the UJ community.
- 7.6 The existing environment has 8 Firewalls (2x each campus) used as perimeter firewalls for internet access; other campuses network access, including internet access, should not be affected should one site be down.
- 7.7 Total Cost Ownership pricing to be included to show initial and investment costs over 3 three years.
- 7.8 Separate costing (Yearly (year 1, 2, & 3)
- 7.9 The below pricing sheet in section 8 must be used for pricing submission.
- 7.10The successful Service Provider must be willing to enter a 3-year SLA for yearly renewals and support. However, is it UJ's discretion to renew the SLA for the 2 and 3rd year, this will be based on the service provider's performance and quality of service.
- 7.11Training and awareness programs should be included to educate stakeholders on the implemented solution (packaged as part of the support services).
- 7.12 Provide End of Support, End of Sale, and End of Life dates for the solution software
- 7.13The service provider must conduct organizational change management for the adoption of the solution where end-users are affected by change in business processes. (This can be extended to a third-party service provider should the successful service provider not have the capabilities. However, the successful service provider will be accountable for the delivery of the service as the SLA will be between UJ and the successful service provider.)
- 7.14 As-Built document for the solution is a requirement as part of the project deliverables.
- 7.15FortiClient EMS and ZTNA standard document is a requirement as part of the project deliverables (linking to all applicable UJ policies [or standards]) – UJ to provide the policy documents to the successful service provider.

8 Technical Adjudication.

The Tender will be evaluated in three stages:

Stage 1 – Tender Compliance Evaluation

Stage 2 – Functionality Evaluation

Stage 3 – Financial and B-BBEE

Stage 2: Functionality Evaluation

Requirement	Maximum points																											
- Fully Priced BOQ. (Year 1, 2, and 3) =15 points	15																											
- Solution Functionality (Meets all the listed Specifications)	30																											
<table><tr><td>Functionality(i.e.)</td><td>YES</td><td>NO</td></tr><tr><td>Centralized Endpoint Management – 4 points</td><td></td><td></td></tr><tr><td>Endpoint Compliance Enforcement & Posture Checking – 4 points</td><td></td><td></td></tr><tr><td>Zero Trust Network Access (ZTNA) – 4 points</td><td></td><td></td></tr><tr><td>Secure VPN & Remote Acss – 4 points</td><td></td><td></td></tr><tr><td>Role-Based Access Control (RBAC) – 3 points</td><td></td><td></td></tr><tr><td>FortiAnalyzer and SIEM (Elastic) Integration – 3 points</td><td></td><td></td></tr><tr><td>Single Agent for all functionality – 4 points</td><td></td><td></td></tr><tr><td>Endpoint Vulnerability Monitoring – 4 points</td><td></td><td></td></tr></table>	Functionality(i.e.)	YES	NO	Centralized Endpoint Management – 4 points			Endpoint Compliance Enforcement & Posture Checking – 4 points			Zero Trust Network Access (ZTNA) – 4 points			Secure VPN & Remote Acss – 4 points			Role-Based Access Control (RBAC) – 3 points			FortiAnalyzer and SIEM (Elastic) Integration – 3 points			Single Agent for all functionality – 4 points			Endpoint Vulnerability Monitoring – 4 points			
Functionality(i.e.)	YES	NO																										
Centralized Endpoint Management – 4 points																												
Endpoint Compliance Enforcement & Posture Checking – 4 points																												
Zero Trust Network Access (ZTNA) – 4 points																												
Secure VPN & Remote Acss – 4 points																												
Role-Based Access Control (RBAC) – 3 points																												
FortiAnalyzer and SIEM (Elastic) Integration – 3 points																												
Single Agent for all functionality – 4 points																												
Endpoint Vulnerability Monitoring – 4 points																												
Key 2x Technical resources with Minimum experience of over 3 years in NSE 4 and NSE 5 Certification of Similar FortiClient EMS VPN ZTNA deployment. (Valid Proof and cv to be attached). – 10 points per resource	20																											
Contactable Reference Letters on a client letterhead (3 References not older than 5 years and relevant to the deployment, support, and maintenance of FortiClient EMS VPN ZTNA or similar products) – 5 points per valid letter.	15																											
Implementation Strategy for Project Management and Org Change Management Approach or Framework based on UJ Solution Deployment 20 points – Excellent: A well-developed, tailored implementation Strategy for Project Management and Org Change Management Approach or Framework based on UJ Solution Deployment that aligns directly with the project's objectives. Clearly outlines project management structures, resource planning, risk mitigation, and implementation strategies. 10 points – Satisfactory: Methodology is generally adequate but lacks specificity or adaptation to the project context. Some elements of project management are addressed, but with limited depth. 0 points – Unsatisfactory: Methodology is vague, generic, or not aligned with the objectives. Key components are missing or inadequately addressed.	20																											
Total Points awarded	100																											

All tenderers require a minimum of 70 points before further evaluation. All tenderers who achieve 70 points or

more will be evaluated equally in terms of stage 3.

8.1 Stage 3 - Financial and B-BBEE

- Price (80 points)
- BBEE (20 points)

9 Pricing Sheet.

NB: Quotations must be based on an exchange rate of R19.00 to \$1.00 for evaluation purposes.

Items					
Description	QTY	Year 1	Year 2	Year 3	Total Cost for 3 Years
Solution Licensing Costs:					
• Per-user or per-device licensing fees	5000				
Implementation Costs:					
Support & Maintenance Costs:					
• Standard support (20)	20				
• After-hours critical support (10)	10				
Other Costs:					
Sub Total					
VAT					
Total Including VAT					
ROE used					

The table below indicates the number of devices UJ has.

	Count	OS Type
Staff	5000	Windows, Linux, and macOS
Total	5000	Windows, Linux, and macOS

