

REQUEST FOR INFORMATION (RFI)
SPECIFICATION DOCUMENT

FOR

RFI UJ 01/2024: NETWORK
SECURITY SOLUTION

Table of Contents

1. Overview 3

2. Minimum Requirements..... 3

3. Technical Requirements 3

4. General Information about the Data Centre 9

5. Support requirements 10

6. Additional notes..... 10

7. Technical Evaluations 10

1. Overview

The University of Johannesburg (UJ)'s information and communications systems department (ICS) is responsible for providing IT services to enable UJ to meet its strategic objectives of research, teaching, and learning. To achieve this, a very stable, reliable, high performance and secured wired and wireless network is required. The university has over 50000 full-time students across the four campuses and employs over 5000 staff connected to the network.

The ICS department is undertaking a process of investigating Network Security technology solutions that are available to ensure that the network can meet the demands of both students and staff, in-line with the global trends in technology developments within affordable budget. The network security solution includes:

- Firewalls (Perimeter and DMZ, Internal [LABS, Wi-Fi, Staff LAN, Voice, IoT], and Data Centre).
- Central logging systems (with reporting capabilities).
- DDoS solution (Appliance). To secure and protect against attacked targeted at the university's public facing systems/DMZ.
- SSL VPN Solution with MFA capabilities. For staff and third-party consultants [should be scalable to include students in future)

The ICS department is therefore looking for hardware vendors to work with as a key strategic partner. ICS requests the technology manufacturers to submit their proposals as per specifications and requirements stated below.

2. Minimum Requirements

Should any vendor not meet these requirements, they will automatically be disqualified and will not be evaluated further. The vendors:

- Must certified local South African partners or resellers within the region of the Gauteng Province. This is to cater for effective support and maintenance. (Proof to be provided, i.e., Partner list indicating certification levels. [minimum 5])
- Must have hardware life span of at least 6 years. This is to ensure viability and support for the chosen technology for the duration required by the university. (*EOS (support), EOS (sale), End of Renewal, and/or EOL dates to be provided for each hardware*)
- Must recommend hardware appliance with a valid life span from the year 2026 to 2031. Should there be newer hardware please recommend.
- Must have easily accessible release notes, troubleshooting guides, CLI references, and support forums for efficient management and troubleshooting of the firewall solution.
- Must allow the university to have access to the support portal for call logging for timely issue resolution.
- Must be able to offer professional services to ensure successful implementation and ongoing support of the firewall solution. (*This could include installation, configuration, customisation, and optimisation services, as well as comprehensive training programs for administrators.*)
- Must be able to offer training directly, or through distributor, partners, and resellers.
- Must be identified as leaders and challengers in the Gartner Magic Quadrant.
- Must be compliant with industry standards. (*Proof of certification to be provided, i.e., ISO etc.*)
- Must be willing to do a POC for any of the solutions proposed.

3. Technical Requirements

The Network Firewall equipment (Perimeter, Internal, DC) must be able to meet the following basic requirements and features:

Requirements.	Comply: YES/NO	Comment/Justification
Must allow GUI and CLI admin access.		
Must provide user-friendly UI i.e., drag and drop capabilities, ability to display the actual firewall rule sequence, ability to see used and unused rules, ability to see unused address objects etc.		

Next Generation Firewall with UTM features including IPS, AV/Malware protection, Botnet Scanning, Application control, DDoS/DoS attack prevention, and visibility, SSH/SSL inspection, and prevention.		
Must utilise purpose-built security processors and threat intelligence to provide high-speed threat protection.		
Must deliver low latency and high throughput, ensuring optimal performance even under heavy traffic loads.		
Must support stateful packet inspection, deep packet inspection, and application-layer inspection.		
Must support IPsec and SSL VPN for secured and encrypted remote access over the internet, NAT, and policy-based routing.		
Must provide remote access VPN and site-to-site VPN capabilities.		
Must detect and block network-based attacks using signature-based and anomaly-based detection methods.		
Must be able to regularly update new threat signatures to protect against emerging threats.		
Must be able to Identify and control applications running on the network, regardless of port, protocol, or IP address used.		
Must provide granular control over applications, enabling administrators to allow, block, or limit specific applications.		
Must be able block access to malicious and inappropriate websites based on URL categories and reputation.		
Must enforce acceptable use policies and protect users from web-based threats.		
Must utilise both signature-based and heuristic-based detection methods.		
Must optimise and secure Wide Area Network (WAN) traffic across multiple connections.		
Must be able to provide intelligent path selection, application steering, and bandwidth management.		
Must be able to integrate with Sandbox (on-prem or cloud) for advanced malware analysis and detection.		
Must be able to detect and mitigate advanced persistent threats (APTs) and zero-day attacks.		
Must seamlessly integrate with other products and solutions, to enhance visibility and control across the entire security infrastructure.		
Must support automated threat response and coordinated defence mechanisms.		
Must Provide detailed logs and reports on network activity, security events, and user behaviour.		
Must be able to Integrate with the proposed central logging system for centralised logging, analysis, and reporting.		
1G, 10G ports, up to 100G.		
Must use proprietary SFP modules, if otherwise – Please indicate.		
Multi-gigabit speeds for large traffic volumes		

Must be Scalable, meaning that the Physical Firewall appliance must be able to host at least 10 virtual systems/firewalls.		
Must be Rack Mount capable.		
Full compatibility with Network open standards and Wi-Fi technology.		
Must fully support integration with directory services like LDAP, RADIUS, and Active Directory.		
Must have SSO (Single Sign On) capabilities i.e., User Visibility – AD authenticated users, AD integration etc.		
Must enforce security policies based on user identity and roles.		
Must support trusted host implementation for admin access and firewall management.		
Must support SNMP v3. <i>E.g., 3DES or AES</i>		
Must support hot swappable redundant power supplies and fans.		
Must be able to feed to SIEM solution and/or syslog server.		
Must be able (and compatible) to do remote backups to backup solutions e.g., SolarWinds Kiwi Catt.		
Must have at least 4x 10 gig interfaces.		
Must support minimum throughput of the below in bullets:		
• At least Firewall Throughput (1518 / 512 / 64-byte UDP packets): Up to 70 Gbps.		
• At least Firewall Throughput (Packets Per Second): Up to 78 million pps.		
• At least IPsec VPN Throughput: Up to 20 Gbps.		
• At least Next-Generation Firewall (NGFW) Throughput: Up to 10 Gbps.		
• At least Threat Protection Throughput: Up to 6 Gbps.		
Must support high availability (HA) configurations to ensure continuous operation and failover capabilities i.e., must offer features like active-passive and active-active clustering for redundancy.		
Must have 2x dedicated management interfaces.		
Must support security zones (LAN, WAN, and DMZ)		
Must support Dynamic Routing i.e. OSPF.		
Must support virtual interfaces i.e., 802.1Q VLAN.		
IP multicasting with PIM sparse and dense mode support, DVMRP as secondary support.		
NetFlow/sFlow/IPFIX (in/out traffic on physical and logical interfaces) capable.		
QoS Capable i.e., must manage bandwidth and prioritise network traffic to ensure the performance of critical applications e.g., voice traffic. Must also be able to implement traffic shaping, rate limiting, and bandwidth reservation.		
Must fully support IPv6, enabling the university to transition to the new IP addressing scheme without compromising security.		
Must have SDN and SDWAN Compatibility.		

Must support the implementation of learning firewall policy rules. To learn the kind of traffic that passes through different segments I.e., Staff LAN and DC.		
Orchestration and Automation integration Virtual Firewalls and cost model for these VLAN Traffic encryption and VLAN isolation.		
Must be compatible with Session border controller (SBC)		

The Central Logging Solution must be able to meet the following basic requirements and features:

Requirements.	Comply: YES/NO	Comment/Justification
Must be able to aggregate logs from various Fortinet devices (Firewalls, DDoS, SSL VPN, etc.) for centralised management.		
Must support a wide range of log types, including traffic logs, event logs, security logs, and system logs.		
Must utilise threat intelligence to detect and correlate security incidents.		
Must be able to identify patterns and anomalies that indicate potential security threats.		
Must provide pre-built and customisable reports to meet compliance and auditing requirements.		
Must offer a wide range of report types, including executive summaries, detailed traffic analysis and security incident reports.		
Must have scheduled and on-demand reporting capabilities.		
Must be able to correlate events across different devices and log sources to identify multi-vector attacks.		
Must use predefined correlation rules and allow for the creation of custom rules to match specific needs.		
Must support alerting and notification mechanisms to inform administrators of security incidents in real-time.		
Must have the ability to integrate with SIEM for streamlined incident response.		
Must have dashboards and visualisation tools for real-time monitoring of network activities and security events.		
Must allow administrators to drill down into specific logs and events for detailed analysis.		
Must be scalable to cater for growing network demands, supporting large volumes of log data.		
Must offer high availability configurations to ensure continuous operations and data integrity.		
Must support long-term log storage to meet regulatory and compliance requirements.		
Must provide tools for data archiving, retrieval, and purging based on retention policies.		
Must seamlessly integrate with other (same vendor) products and solutions to provide a holistic security ecosystem.		
Must be able to provide visibility and control across the entire security infrastructure (based on this RFI).		

Must support trusted hosts and role-based access control to ensure that only authorised personnel can access for system management and admin access.		
Must allow for creation of custom roles and permissions.		
Must support automated actions based on predefined criteria to mitigate threats without human intervention.		
Must be able to trigger scripts or workflows to respond to security incidents.		

The DDoS Solution must be able to meet the following basic requirements and features:

Requirements.	Comply: YES/NO	Comment/Justification
Must be a physical appliance that will be first point of entry to the UJ's network infrastructure.		
Must be designed for high performance with custom ASICs that provide low latency and high throughput.		
Must be scalable to handle very high traffic volumes, suitable for large enterprises and service providers.		
Must be equipped with at least 4 pairs x 10 GE SFP+ DDoS Defence Ports, 2x GE RJ45 Management Ports, Dual AC Power Supplies, and includes at least 500 GB SSD storage.		
Must offer at least up to 5 Gbps full-duplex throughput with bidirectional attack mitigation.		
Must adapt to changes in network traffic patterns over time, improving accuracy and reducing false positives.		
Must use behaviour-based algorithms to detect deviations from normal traffic patterns, identifying both known and unknown attack vectors.		
Must support automatic attack mitigation, once an attack is detected, the DDoS solution must automatically mitigate it in real-time without requiring manual intervention.		
Must provide protection across multiple layers, including network (Layer 3), transport (Layer 4), and application (Layer 7).		
Must be able to defend against a wide range of DDoS attacks, including volumetric, protocol, and application-layer attacks.		
Must profile traffic to establish baselines for normal behaviour, enabling accurate detection of anomalies.		
Must provide comprehensive visibility into attack details with granular reporting and analytics.		
Must have real-time dashboards that display current traffic patterns, detected attacks, and mitigation actions.		
Must supports out-of-band deployment for monitoring traffic via network taps or SPAN ports.		
Must support multi-tenant environments with logical isolation of traffic, ensuring that policies and protections are applied separately for each tenant.		
Must allow for individual policy settings and reporting per tenant.		

Must support centralised management interface for configuring, monitoring, and managing multiple DDoS appliances.		
Must provide granular access control for different administrative roles. This must also include the ability to implement trusted hosts.		
Must support seamless integration with other security products (of the same technology/vendor) to enhance the overall security posture through coordinated defence mechanisms.		
Must offer customisable reports for compliance auditing and security monitoring.		
Must be able to rate limit and throttle i.e., must be able to control the rate of traffic to mitigate volumetric attacks.		
Must be able to shape traffic to prioritise legitimate traffic during an attack.		
Must leverage global threat intelligence to stay updated on the latest DDoS attack vectors and methodologies.		
Must receive dynamic updates for emerging threats and attack patterns.		

The SSL VPN Solution must be able to meet the following basic requirements and features:

Requirements.	Comply: YES/NO	Comment/Justification
Can be a dedicated appliance or a Feature on the Firewall appliance.		
Must provide secure, encrypted remote access to the corporate network via SSL VPN, ensuring that data transmitted between the endpoint and the network is secure.		
Must support IPsec VPN for secure, site-to-site and client-to-site VPN connections.		
Must support 2FA using a combination of something the user knows (password) and something the user has (a secondary token or device). Or must be compatible with other third-party MFA solutions, allowing flexibility in authentication methods.		
Must have built-in antivirus and anti-malware protection to prevent endpoint infections.		
Must be able to enforces web filtering policies to block access to malicious or inappropriate websites.		
Must be able to monitor and control application traffic to prevent unauthorized access.		
Must have easy-to-use client interface for setting up and managing VPN connections.		
Must support SSO to streamline the authentication process and enhance user experience.		
Must have the ability to be managed centrally for streamlined deployment, configuration, and monitoring.		
Must ensure security policies are consistently applied across all endpoints, including VPN access policies and endpoint security configurations.		

Must ensure that endpoints comply with security policies before allowing VPN access, reducing the risk of non-compliant devices connecting to the network.		
Must provide detailed logs and reports on VPN usage, connection attempts, and security events for auditing and compliance purposes.		
Must integrate with Sandbox for advanced threat detection and protection, analysing suspicious files in a secure environment.		
Must use behavioural analysis to detect and block suspicious activities on the endpoint.		
Must perform compliance checks to ensure endpoints meet security requirements (e.g., up-to-date antivirus, OS patches) before granting VPN access.		
Must be able to quarantine non-compliant or infected devices to prevent them from accessing the corporate network.		
Must support load balancing to distribute VPN connections across multiple FortiGate devices, ensuring high availability and reliability.		
Must be designed to scale to support a large number of remote users and devices.		
Must be available for various operating systems, including Windows, macOS, Linux, iOS, and Android, providing consistent protection across all user devices.		
Must use strong encryption protocols (at least TLS v 1.2 or above) to protect data in transit and ensure the confidentiality and integrity of communications.		
Must allow administrators to configure encryption levels and protocols based on security requirements.		
Must support certificate-based authentication for enhanced security.		
Must be able to verify the identity of devices in addition to users, providing an additional layer of security.		
Must fully support integration with LDAP directory services such as Microsoft Active Directory (AD) and other LDAP-compliant directories.		
Must be able to authenticate users against the LDAP directory, ensuring that only authorized users can establish VPN connections.		
Must be able to apply VPN access policies based on user groups defined in the LDAP directory. This allows for granular control over who has access to specific resources.		
Must be able to automatically adjust user permissions based on changes in group membership within the LDAP directory.		

4. General Information about the Data Centre.

- The current virtual server environment consists of 85% Hyper-V, 15% VMware.
- Active Directory is in use.
- Oracle Databases in use.
- SQL Clusters.
- Application Servers are in use.

- File Servers are in use.
- Storage hosted within the DC.
- NVR's (Network Video Recorder) are hosted within the Data Centre.

5. Support requirements.

- The hardware manufacturer must be able to provide direct support (Hardware swop, Software upgrades and TAC support)
- Onsite replacement device delivery and collection or through distributors, partners, and resellers.
- TAC support must be available 24X7.

6. Additional notes.

- This RFI is not for procurement purposes, but rather to identify technology that can be used for future procurements.
- This is not a procurement promise and not binding the university to procure any service.
- Adding to the above, no order will be issued from the outcome of this exercise.
- The successful manufacturer should be able to assist with network designs and advise on new technology when required to do so.
- An account manager should be assigned.
- This RFI is for equipment manufacturers or appointed distributor only (resellers acting on behalf of vendors are prohibited).
- Local technical training for UJ technical resources must be available. Training centres and costing must be provided as an appendix.
- Manufacturer local skills must be available.
- The manufacturer must be able to do a POC.
- Warrantees must be indicated (with terms and conditions).
- Provide at least 2 References and case studies from existing customers i.e., Vendor's experience and expertise in delivering similar solutions to similar organisations. (Exposure to educational environment will be added advantage).
- Equipment data sheets to be attached to the response.
- Budgetary Pricing (Price for Appliances, modules etc. must be based on a per item cost. Prices must be accurate as this affects the decision directly).
- Must have a budgetary pricing for each solution (I.e., Firewalls, DDoS, Central Logging, and SSL-VPN solution) separately [as appendices] indicating the following:
 - Detailed breakdown of costs, including initial acquisition, licensing, maintenance, and support.
 - Estimated TCO over a specified period (e.g., 3 years, 5 years).
 - Description of available pricing models (e.g., subscription, perpetual license).
- The manufacturer must have local technology roadshows/events in South Africa yearly to inform customers of new technologies or emerging threats.
- The manufacturer must attend compulsory briefings and presentations.

7. Technical Evaluations.

This RFI will be evaluated as below. Only those meeting requirements in section 2, 3, 5, and 6 above will move to evaluation phase. It is important that the vendor clearly indicate how below requirements will be addressed. The evaluation of each network security solution will be based on the level of compliance with the defined technical requirements. Each solution category—Firewall, DDoS Protection, Central Logging, and SSL VPN—has a set of specific criteria that are weighted according to their importance to the overall performance and security of the solution.

The below tables provide a structured way to evaluate and compare different solutions, ensuring that the scoring is transparent and based on key criteria.

Firewall Solution:

Criteria	Max Points	Points Earned
Hardware Life Span	20	
- Expected Lifespan and Durability	20	
Pricing	20	

- TCO cost	10	
- Yearly cost	10	
Security Features	18	
- Threat Prevention	6	
- Application Control	3	
- URL and Web Filtering	3	
- Advanced Threat Protection	3	
- VPN Capabilities	3	
Performance and Reliability	15	
- Throughput	6	
- Latency	3	
- High Availability	3	
- Redundancy	3	
Management and Usability	12	
- Centralized Management	6	
- User Interface	3	
- Logging and Reporting	3	
Network Capabilities	9	
- NAT and PAT	3	
- IPv6 Support	3	
- Routing	3	
Support and Maintenance	6	
- Vendor Support	3	
- Firmware and Software Updates	2	
- Training and Documentation	1	
Overall Compliance Score	100	

DDoS Solution:

Criteria	Max Points	Points Earned
Hardware Life Span	20	
- Expected Lifespan and Durability	20	
Pricing	20	
- TCO cost	10	
- Yearly cost	10	
Attack Detection and Mitigation	24	
- Real-Time Mitigation	9	
- Multi-Layer Protection	6	
- Behaviour-Based Detection	6	
- Adaptive Learning	3	
Performance and Scalability	12	
- High-Performance Hardware	6	
- Scalability	3	
- Low Latency	3	
Management and Visibility	12	
- Centralized Management	6	
- Detailed Reporting and Analytics	6	
Deployment and Integration	6	
- Flexible Deployment Options	3	
- Integration with Existing Infrastructure	3	
Support and Maintenance	6%	
- Vendor Support	3	
- Firmware and Software Updates	2	
- Training and Documentation	1	
Overall Compliance Score	100	

Central Logging Solution:

Criteria	Max Points	Points Earned
Hardware Life Span	20	
- Expected Lifespan and Durability	20	
Pricing	20	
- TCO cost	10	
- Yearly cost	10	
Data Collection and Aggregation	18	
- Multi-Source Data Collection	6	
- Real-Time Data Aggregation	6	
- Log Normalization	6	
Analysis and Reporting	18	
- Advanced Analytics	6	
- Customizable Reporting	6	
- Compliance Reporting	6	
Scalability and Performance	12	
- High Throughput	6	
- Scalability	6	
Management and Usability	6	
- User Interface	3	
- Centralized Management	3	
Support and Maintenance	6	
- Vendor Support	3	
- Firmware and Software Updates	2	
- Training and Documentation	1	
Overall Compliance Score	100	

SSL VPN Solution:

Criteria	Max Points	Points Earned
Hardware Life Span (if applicable)	20 (if applicable = 20)	
- Expected Lifespan and Durability	20	
Pricing	20 (if hardware appliance = 10)	
- TCO cost	10 (or =5)	
- Yearly cost (e.g., year1, 2, 3 etc)	10 (or =5)	
Security Features	30	
- Multi-Factor Authentication (MFA)	10	
- Endpoint Security Integration	10	
- Data Encryption	5	
- Network Access Control (NAC)	5	
User Authentication and Management	20	
- LDAP Integration	10	
- Single Sign-On (SSO)	5	
- User and Group Management	5	
Performance and Reliability	10	
- High Availability	5	
- Scalability	5	
Management and Usability	10	
- Centralised Management	2	
- User-Friendly Interface	7	
Support and Maintenance	10	
- Vendor Support	5	
- Firmware and Software Updates	3	

- Training and Documentation	2	
Overall Compliance Score	100	

Aggregated Score:

Solution	Earned Points	Comment (Appointable or Not)
Firewall		
DDoS		
Central Logging		
SSL VPN		
Total Ave Score		

Conclusion

The evaluation process will rigorously assess each solution's compliance with the technical requirements. By weighting each criterion appropriately and calculating an overall compliance score, we can ensure that the chosen solutions meet the highest standards for network security and performance. This structured approach facilitates objective comparison and informed decision-making, ultimately enhancing the security posture of our network infrastructure.