BID NO:

RAF/2024/000045

BID DESCRIPTION**:**

THE ROAD ACCIDENT FUND (RAF) SEEKS TO APPOINT AN EXPERIENCED AND SUITABLE SERVICE PROVIDER FOR PROCUREMENT OF A FIREWALL ASSURANCE SOLUTION FOR A PERIOD OF THREE YEARS FOR A PERIOD OF THREE (3) YEARS.

Questions and Answers

1. How many firewalls does RAF intend to monitor with the tool?

20 devices that need to be managed.

2. How many administrators will need access to the tool? Can we assume the 10 personnel that will need to be trained?

    5 security personnel would need to work on this system but all 10 would need to be trained.

3. Please provide a breakdown on how many firewalls will be on-premises, how many cloud-based firewalls and from those how many will be in public cloud e.g. AWS, Azure, etc., and how many in private cloud e.g VMWare, Hyper-V, etc.

On Premises

1. 2 x Cisco Meraki UTM Firewalls in an active-active/active-passive configuration each in each of the 6 RAF sites. **Each site has 2 of these Cisco Merakis leading to a total of 12 x Cisco Meraki UTM firewalls (i.e. 6 x Cisco Meraki high availability clusters).**
2. 2 x Cisco FTD Firewalls in an HA configuration at the primary Data Center.
3. 1 x Cisco FTD Firewall at the disaster recovery site.

Cisco Meraki Models:

- MX250 x 4
- MX67 x 4
- MX75 x 8

Cloud Environments – The rest of the firewalls will be based in cloud environments, using cloud-native firewalls (e.g. AWS/Azure Firewall)

- AWS
- Azure

4. Also, we need the full specification if the required firewalls - throughput, users, etc. for each one of the 20 firewalls.

OFFICE	Estimated Number of Users	Device Brand	Firewall Throughput	VPN Throughput
Head Office	± 1000	Meraki MX250 x 2 (Active-Active/Active-Passive High Availability cluster)	7.5 Gbps	3.5 Gbps
Site 1	± 800	Meraki MX250 x 2 (Active-Active/Active-Passive High Availability cluster)	7.5 Gbps	3.5 Gbps
Site 2	± 300	Meraki MX75 x 2 (Active-Active/Active-Passive High Availability cluster)	1 Gbps	900 Mbps
Site 3	± 350	Meraki MX75 x 2 (Active-Active/Active-Passive High Availability cluster)	1 Gbps	900 Mbps
Site 4	± 15	Meraki MX67 x 2 (Active-Active/Active-Passive High Availability cluster)	700 Mbps	300Mbps
Site 5	± 500	Meraki MX75 x 2 (Active-Active/Active-Passive High Availability cluster)	1 Gbps	900 Mbps
Site 6	± 220	Meraki MX75 x 2 (Active-Active/Active-Passive High Availability cluster)	1 Gbps	900 Mbps
Site 7	± 15	Meraki MX67 x2 (Active-Active/Active-Passive High Availability cluster)	700 Mbps	300Mbps
Data Center 1	-	Cisco FTD 2130 x 2 (Active-Active/Active-Passive High Availability cluster)	10 Gbps	1.9 Gbps
Data Center 2	-	Cisco FTD 2130 x 1	10 Gbps	1.9 Gbps
Data Center 1	-	Meraki MX250 x 2 (Active-Active/Active-Passive High Availability cluster)	7.5 Gbps	3.5 Gbps

Cloud Native Firewalls (1 x AWS Firewall and 1 x Azure Firewalls) are also activated in their respective cloud environments.

Please note that the limit of firewalls to be managed by the Firewall Assurance Solution will remain at a maximum of the 20 firewalls mentioned in the RFP requirements and RAF will decide which of the firewalls will be prioritised for onboarding onto the Firewall Assurance Solution.

5. Firewall Assurance Solution and VDOM Licensing - Firewall Assurance Solution for twenty (20) firewalls

Could you provide details on the number of VDOMs associated with the 20 firewalls, as some solutions may have licensing models based on VDOM usage?

Answer 4…. RAF does not use the VDOM licensing model. The following firewalls are deployed On Premises.

Cloud Native Firewalls (1 x AWS Firewall and 1 x Azure Firewalls) are also activated in their respective cloud environments.

Please note that the limit of firewalls to be managed by the Firewall Assurance Solution will remain at a maximum of the 20 firewalls mentioned in the RFP requirements and RAF will decide which of the firewalls will be prioritised for onboarding onto the Firewall Assurance Solution.

6. Security Policy Enforcement - The proposed solution must have the capability to continuously enforce security policies (based on RAF security policies and security best practices) on managed firewalls including firewall access and configurations.

Is the solution expected to automatically enforce changes directly on the firewalls, or should it instead offer detailed guidance for the security team to implement necessary policy adjustments based on identified criticality?

The intention is to get a solution that would be able to monitor firewalls against security requirements. As this would be more from a detective control with recommendations rather than enforcement.

7. Cloud-Based Solution and Hosting Costs - The proposed Cloud Based Firewall Assurance Solution must be delivered as Software as a Service (SaaS) Solution, hosted in RAF'S Amazon Web Services (AWS) Cloud

Will RAF assume responsibility for hosting costs within its AWS environment, including network expenses for transmitting syslog data from on-premise firewalls to the cloud instance? Should we only include pricing for licensing and support services?

RAF will own the license and manage infrastructure costs. However, we are unclear about how syslog transmission from on premises firewalls feature in this context as RAF already has a SIEM solution and is not intending to introduce yet another second syslog destination. Perhaps the bidder must unpack this in their response.

8. Firewall Vulnerability Remediation - The proposed solution must have the capability to remediate discovered firewall vulnerabilities

Is the solution expected to perform direct patch installations on the firewalls, or is it sufficient to provide detailed vulnerability information along with recommended remediation actions for the security team to implement?

Bidders must respond with what their solution offers, and this will be evaluated against the requirements.

9. Training and Knowledge Transfer:

Could you kindly confirm the number of personnel who will require training for the proposed solution?

10 would need to be trained.

10. Support & Maintenance:

Regarding the support hours, the pricing schedule allocates 20 hours; however, on page 21, under section 4.1.2 (Support & Maintenance), only 10 hours are listed. Could you please provide clarification on the correct number of support hours?

There is a mistake with section 4.1.2. This was supposed to be 20 hours and not 10 hours. Bidders must cater for 20 hours per month, payable on a usage basis.

11. Could you please clarify if it is a renewal for the firewall license you are looking for? And if so, please state what is the current firewall solution you are using?

This has nothing to do with firewall licenses.