بسم الله الرحمن الرحيم

Ministry of Environment, Climate Change and Technology
Male', Republic of Maldives

TERMS OF REFERENCE

SUPPLY, INSTALLATION AND CONFIGURATION OF A NEXT GENERATION FIREWALL

Advertisement No.: (IUL)438-ICTU/438/2022/156
Advertisement Date: 21st April 2022

SCHEDULE OF CRITICAL DATES

Activity	Action Date
Advertised date	21st April 2022
Bid queries submission timeline	21st April 2022to 26th April 2022 at1200hrs
Bid clarification deadline	27th April 2022 at 1200hrs
Proposal submission deadline	11th May 2022 at 1100hrs

SUBMISSION REQUIREMENTS

The following related documents shall be submitted for the bids to be considered sufficiently responsive.

Applicants should submit their proposals containing the following documents and applicable Technical Proposal – Standard Forms and Financial Proposal – Standard Forms under ANNEX 1.

a. Technical Proposal – Standard Forms

1. Proposal submission form **(signed by the owner of the entity or person with power of attorney to sign) – (Tech Form 1)**
2. Compliance Checklist – **(Tech Form 2)**
3. Technical Specifications of the proposed product.
4. Copy of Business (company/partnerships/institutions) registration certificate.
5. Copy of GST Registration certificate issued by MIRA (Maldives Inland Revenue Authority) – if registered
6. Tax payer registration Certificate(If registerd) / Notification Copy
7. SME Registration Certificate (If any)
8. Work experience – Only reference letters for supply and configuration of firewalls will be deemed acceptable for evaluation.

b. Financial Proposal – Standard Forms

1. FIN FORM 1 – Financial Proposal Submission Form (**signed by the owner of the entity or person with power of attorney to sign**)
2. FIN FORM – 2 Financial Breakdown Form
3. FIN FORM 3: Details Financial Situation (if applicable)
4. Financial statements of the business for the year 2019, 2020 & 2021 (if applicable)
5. Business entities that have not completed one year (from the date of business registration to date of bid announcement) are required to submit the bank statement of the business's bank account. (Bank statement should be from the date of account opening to date of bid announcement)
6. FIN FORM – 4: Average Annual Turnover
7. FIN FORM -5: Financial Resources
8. FIN FORM -6: Line of Credit Letter
9. FIN FORM -7 Current Contract Commitments / Work in Progress

Note 01: If bidder fails to submit any of the above listed document, their proposal may not be considered for further evaluation.

Note 02: After the evaluation, highest scoring party will be notified to submit tax clearance report. Tender will be awarded upon submission of tax clearance report.

1. INTRODUCTION

The Ministry of Environment, Climate Change and Technology (MECCT) is seeking bids from authorrized suppliers who are experienced in supplying and configuring Next Generation Firewalls.

2. SCOPE OF WORKS

The tasks to be undertaken by the selected party under this Terms of Reference are to supply the proposed goods to the Ministry of Environment, Climate Change and Technology (MECCT) accordingly.

3. TECHNICAL SPECIFICATIONS

3.1. Hardware and Interface

3.1.1. The platform must be supplied with at least 10 x 10/100/1000Mbps ports and 4 x 10GBase-F SFP+ ports (with 1 x SFP+ converter)

3.1.2. The proposed solution must support minimum 10 virtual context and should be upgradable to 20 with further memory upgrade

3.1.3. The proposed solution should have in-built storage of minimum 240GB SSD

3.2. Performance

3.2.1. Firewall throughput must be more than 17 Gbps (in ideal testing conditions)

3.2.2. The VPN AES 128 throughput should be more than 2.5 Gbps

3.2.3. The IPS throughput must be atleast 4.6 Gbps

3.2.4. The proposed solution must support 2 million concurrent connections minimum and should be able to handle upto 8 million with memory upgrade.

3.2.5. The proposed solution should be able to process more than 65,000 new connections per second.

3.2.6. Solution must provide with minimum of 50 remote access VPN client license

3.2.7. Minimum of 16GB memory should be provided and should be upgradeable to 32GB

3.3. General Requirements

3.3.1. The proposed solution should support “Stateful” policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols such as; telnet, ftp etc.

3.3.2. The proposed solution should not use a proprietary ASIC/FPGA hardware for FW and VPN performance only. Either all security controls must be catered by specialised hardware or OEM must mention the performance numbers disabling the specialised hardware.

3.3.3. The solution and integrated IPSEC VPN applications should be ICSA labs certified for ICSA 4.0, FIPS 140-2 certified and NSS Recommended (NGFW - latest report)

3.3.4. The hardware platform and NGFW with integrated SSL VPN application has to be from the same OEM.

3.3.5. The proposed solution (FW , IPS, Application Control, URL Filtering, Anti-Virus & Anti-Bot, SandBoxing) should support for Active – Active connections (without virtual context). It should not depend upon any 3rd party product or appliance for the same.

3.3.6. Licensing should be a per device and not user/IP based (should support unlimited users)

3.3.7. The proposed solution should support the multicast protocols as a multicast host, by participating in DVMRP, IGMP and PIM-DM / PIM-SM

3.3.8. The proposed solution vendor must be a leader in Gartner® Magic Quadrant™ for Enterprise Network NGFWs in last 10 years.
3.3.9. The proposed solution should have a provision to handle the bandwidth management at different levels
3.3.10. It should support the VOIP traffic filtering
3.3.11. Appliance should have Identity Awareness Capabilities
3.3.12. Solution must failover without dropping any connection in active - active mode.
3.3.13. The proposed solution should have Hardware Sensor Monitoring capabilities.
3.3.14. The platform should support VLAN tagging (IEEE 802.1q)
3.3.15. The proposed solution should support ISP link load balancing upto 7 WAN connections
3.3.16. The proposed solution should support Link Aggregation functionality to group multiple ports as single port.
3.3.17. The Proposed Solution should support Ethernet Bonding functionality for Full Mesh deployment architecture.
3.3.18. The Proposed Solution must support atleast 4096 Vlans in virtual mode.
3.3.19. Solution must have search optoin in GUI to search configuration options like NTP, arp, Proxy etc. and should directly take administrator to configuration window of search result by just clicking at search results.
3.3.20. Appliance must support automatic search, downloading and install software hotfixes without any administrator efforts and must notify Administrator through mails on the status and progress of each step. System should automatically roll back upon failure.
3.3.21. Solution must support atleast two clustering protocols.
3.3.22. Solution must support VRRP clustering protocol.
3.3.23. The Proposed Solution must allow to configure password policy for local users to login to NGFW and must support following: disallow palindromes, disallow password reuse from last 10 passwords, set password expiry in number of days, must have option to warn user 7 days before password expiry, block access for certain period of time after certain number of failed login attempts.
3.3.24. Solution must support multiple administrators to work on policies on session based, All the policies and objects on which Administrator 1 is working should be locked for all other administrator, however other administrator can work on other policy rules and objects in their respective sessions. Changes done by Administrator-1 should not be visible to other administrators till the time Administrator-1 publish changes.
3.3.25. Solution must allow administrator to choose to login in readonly or readwrite mode
3.3.26. Solution must allow to open support tickets directly from NGFW GUI.
3.3.27. Solution must support multiple role based administration, (Ex).Routing Administrator must have read write access to all routing protocols, interface configuration, DNS configurations, etc.

3.4. Architecture Features

3.4.1. It should support the IPSec VPN for both Site-Site & Remote Access VPN
3.4.2. Virtual Context must support virtualization of all the feature set which are offered by the vendor
3.4.3. The Gateway system should support virtual tunnel interfaces to provision Route-Based IPSec VPN
3.4.4. It should support the system authentication with RADIUS and local authentication. Both should work simultaneously.

3.4.5. NGFW Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades

3.5. Standards Support Requirements

3.5.1. The Proposed Solution must support unlimited policy option.
3.5.2. The Proposed Solution should be able to handle more than 10,000 routes (HQ Firewall Only)
3.5.3. The Address/host object limit must be above 50,000
3.5.4. The Proposed Solution Modules should support the deployment in Routed as well as Transparent Mode (HQ Firewall Only)
3.5.5. The Proposed Solution must provide state engine support for all common protocols of the TCP/IP stack
3.5.6. The Proposed Solution must provide NAT functionality, including dynamic and static NAT translations
3.5.7. All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, Ms-Exchange etc
3.5.8. Local access to the proposed Solution modules should support authentication protocols – RADIUS & TACACS+
3.5.9. IPSec VPN should support the Authentication Header Protocols – MD5 & SHA
3.5.10. IPSec ISAKMP methods should support Diffie-Hellman Group 1 & 2, MD5 & SHA Hash, RSA & Manual Key Exchange Authentication, 3DES/AES-256 Encryption of the Key Exchange Material and algorithms like RSA-1024 / 1536
3.5.11. IPSec encryption should be supported with 3DES, AES-128 & AES-256 standards
3.5.12. IPSEc should have the functionality of PFS and NAT-T
3.5.13. The Proposed Solution should support authentication proxy for Remote VPN, HTTP/HTTPS Applications Access, and various other applications
3.5.14. The Proposed Solution should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods
3.5.15. The Proposed Solution should support PKI Authentication with PCKS#7 & PCKS#10 standards
3.5.16. It should support BGP, OSPF, RIPv1 &2, Multicast Tunnels, DVMRP protocols
3.5.17. Dynamic policy enforcement on VPN Clients

3.6. **NGFW Filtering Requirements**

3.6.1. It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports
3.6.2. The NGFW must provide state engine support for all common protocols of the TCP/IP stack
3.6.3. The NGFW should be constantly updated with new defenses against emerging threats.
3.6.4. NGFW updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time
3.6.5. NGFW should support over 8400+ applications
3.6.6. The IPS should scan all parts of the session in both directions
3.6.7. It should be able to block Instant Messaging such as; Yahoo, MSN, ICQ, Skype (SSL and HTTP tunneled)
3.6.8. It should enable blocking of Peer-Peer applications such as; Kazaa, Gnutella, Bit Torrent, IRC (over HTTP)

3.6.9. The NGFW should support authentication protocols like LDAP, RADIUS and have support for NGFW passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.

3.6.10. IPS should have the functionality of Geo Protection to Block the traffic country wise in incoming direction, outgoing direction or both. IPS also should alert through Mail if any IPS traffic/event detected from Specific Country.

3.6.11. The NGFW should support advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications

3.6.12. Should support CLI & GUI based access to the NGFW modules

3.6.13. Local access to NGFW modules should support role based access

3.6.14. QoS Support [Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantees, QOS limits and QOS VPN]

3.6.15. NGFW Should support Identity Access for Granular user, group and machine based visibility and policy enforcement

3.6.16. IPS should be able to detect and prevent embeded threats with in SSL traffic.

3.6.17. The solution should allow for third party signiture import such as Snort

3.6.18. NGFW should have Identity based logging option

3.7. **Web Security Solution**

3.7.1. The solution should provide in line proxy, on box malware inspection, content filtering, SSL inspection, protocol filtering functionalities

3.7.2. The solution should protect users from downloading virus / malwares embedded files by stopping viruses / malwares at the gateway itself. Should at least provide Real-Time security scanning.

3.7.3. Should stop incoming malicious files with updated signatures & prevent access to malware infected websites & unblocks the sites when the threats have been removed.

3.7.4. Solution must have a URL categorization that exceeds 100+ million URLs filtering database. Should have pre defined URL categories. The solution should have the capabilities to block, permit, allow & log, protocols other than HTTP, HTTPs, FTP. Also list the protocols that supports.

3.7.5. The solution should have more than millions + malware signature.

3.7.6. The solution should also have the scalability to scan & secure SSL encrypted traffic passing through gateway. Should perform inspection to detect & block malicious content downloaded through SSL.

3.7.7. Solution must be able to create a filtering rule with multiple categories.

3.7.8. Solution must be able to crate a filtering for single sites being support by multiple categories.

3.7.9. The solution must have an easy to use, searchable interface for applications & URLs.

3.7.10. The solution should be able to explicitly limit bandwidth for bi direction traffic i.e upload & download.

3.8. Antivirus / Antibot Features

3.8.1. Solution should be able to detect & Prevent the Bot communication with C&C

3.8.2. Solution should have an Multi tier engine to ie detect & Prevent Comand and Control IP/URL and DNS

3.8.3. Solution should be able to detect & Prevent Unique communication patterns used by BOTs ie Information about Botnet family

3.8.4. Solution should be able to detect & Prevent attack types ie, such as spam sending click fraud or self-distribution, that are associated with Bots
3.8.5. Solution should be able to block traffic between infected Host and Remote Operator and not to legitimate destination
3.8.6. Solution should be able to provide with Forensic tools which give details like Infected Users/Device,Malware type,Malware action etc
3.8.7. Solution should give information related to Perfomance impact and confidence level of protections while creating profiles
3.8.8. Antivirus protection protocols for HTTP,HTTPS etc
3.8.9. Solution should have an option of packet capture for further analysis of the incident
3.8.10. Solution Should Uncover threats hidden in SSL links and communications
3.8.11. The AV should Scan files that are passing on CIFS protocol
3.8.12. The vendor malware update mechanism should include reputation, network signatures and suspicious email activity detection
3.8.13. IPS shall be able to provide complete user visibility in the logs.

3.9. Anti-APT Solution

3.9.1. The hardware and software based solution should provide protection for all incoming and outgoing traffic from /to Internet.
3.9.2. The proposed solution should be able to address both APT attacks and Advanced Malware across Network.
3.9.3. The solution must employ an on cloud analysis engine to detect zero day and unknown threats and must not be signature based. The solution however should have an option to send the samples to on premise based emulation system as well.
3.9.4. The solution should support static as well as dynamic analysis.
3.9.5. The Hypervisor used by sandboxing solution must not be an OEM solution such as from VMWare ,HyperV, VirtualBox, RHEV etc however it should be a custom Hypervisor purpose built for sandboxing requirement
3.9.6. The solution must be able to detect and report malware by using multiple images of Windows XP/7/8/10/11
3.9.7. The solution must support prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft. There should be no requirement for the customer to buy additional Microsoft licences for sandboxing solution
3.9.8. The engine should detect API calls, file system changes, system registry, network connections, system processes, kernel code injection, system calls and direct CPU interaction.
3.9.9. Anti-APT solution should be able to work independently of signature updates from OEM website.
3.9.10. The solution should detect the attack at the exploitation stage – i.e. before the shell-code is executed and before the malware is downloaded/executed.
3.9.11. The solution should be able to detect ROP and other exploitation techniques (e.g. privilege escalation, directory traversal) by monitoring the CPU flow
3.9.12. The solution must be able to support scanning links inside emails for zero days & unknown malware
3.9.13. The solution should be able to perform pre-emulation static filtering
3.9.14. The solution should support sandboxing of file sizes upto 100MB
3.9.15. The proposed solution must be able to run multiple micro tasks in a single VM.

3.9.16. The solution should analyze malware (VM based execution) coming over protocols like HTTP/HTTPS, SMTP, SMTP-TLS, CIFS etc. All the components of the solution must be managed from a centralized management console from the same OEM. However management and logging appliances may be different from the sandboxing appliance.

3.9.17. The Sandboxing solution should allow for 'Geo Restriction' which enables emulations to be restricted to a specific country

3.9.18. The solution must provide the ability to Increase security with automatic sharing of new attack information with other gateways in means of signature updates etc.

3.9.19. The solution must utilize a Global Threat Intelligence feed from OEM regrading new malware profiles, vulnerability exploits, C&C call-back destinations and obfuscation tactics etc.

3.9.20. The virtual execution environment must have anti-evasion capabilities to prevent the malwares to evade detection of the sandboxing environment. Anti VM detection activities like Time delays, Shut down, Restart, VM detection, User interaction etc. must be prevented by the solution.

3.9.21. The solution should have the inherent ability to detect multi-stage attacks. For the purpose of detecting multi stage attacks the solution should include static analysis technologies like IPS, antivirus, anti malware/anti bot however in an integrate mode with the solution. The bidder or SI may use additional appliances(at max 2) for the solution but should be provided by the same OEM in the solution.

3.9.22. The solution should inspect the web sessions(HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate applaince for SSL offloading will not be accepted

3.9.23. The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution should also assign a unique identification number to each identified/detected threat for future reference.

3.9.24. The solution shall detect the entire attack lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration.

3.9.25. The solution shall provide event-based alerts/logs.

3.9.26. The solution should have ability to stop web based attacks and block all outbound call-back communication initiated by the infected internal clients.

3.9.27. The solution should have no limitations in terms of number of users. However for sizing purpose the bidder shall refer to the Section 3.1, 3.2 and 3.3.

3.9.28. The solution should be able to work in tandem with other network device (e.g. firewall, IDS/IPS, Antispam, Web proxy, Endpoint Antivirus etc.) for its functioning. Additional devices required if any should be provided by the bidder. But the upper limit of such devices should not be more than 2

3.9.29. The solution should have the ability to be deployed in the following modes:

- Inline blocking
- Inline monitoring
- TAP/SPAN mode

3.9.30. The solution shall support to identify the IP address (Internal LAN IP address) of a host in a proxy environment.

3.9.31. The solution should provide a Dashboard that offers real time threat visibility and attack characteristics.

3.9.32. The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports daily/weekly/monthly/annually/specific range (day and time), etc.

3.9.33. The solution should provide reports in (not limited to) HTML/CSV/PDF Formats.

3.9.34. Upon malicious files detection, a detailed report should be generated for each one of the malicious files. The detailed report must include:

- Screen shots
- Timelines
- Registry key creation/modifications
- File and processes creation
- Network activity detected

3.9.35. The solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions

3.9.36. The solution should provide for offline updating of threat intelligence

3.9.37. The solution should support:

- LDAP or RADIUS and Local Password authentication schemes (not limited to)
- Remote administration using SSH/HTTPS
- CLI, GUI/Web based Administration Console

3.9.38. The solution should examine the email traffic in real-time for emails having malware and potential spear-phishing and targeted attacks. Such infected email attachments should be remediated in real time and should be retrievable by administrator, if required.

3.9.39. The proposed solution should dynamically generate real-time malware intelligence for immediate local protection via integration with the separate Automated Management and Event Correlation System. This Automated Management and Event Correlation solution must be from the same OEM.

3.9.40. Solution should have an ability to remove all the active content and macros sending only a clean document to the end user

3.9.41. The solution should hold the attachment on the inbound email traffic till the attachment has been dynamically analyzed by the virtual environment.

3.9.42. All necessary additional devices, software & licenses required for achieving functionalities of web and email traffic should be quoted as part of the solution.

3.9.43. The solution should support SNMP, syslog for integration with a SIEM Solution and should support integration of privately generated intelligence on the sandbox to be shared with other security devices through open standards based protocols like STIX/TAXII, Open IOC etc

3.9.44. The core product troubleshooting documents like admin guides, installation guides, manuals should be made available to the customer directly through publically accessible OEM website. The OEM must share the admin guides during technical evaluation

3.9.45. The Proposed Solution must suport multiple Sandboxing appliance to provide load balancing and allow equal distribution of files for Sandboxing without any third party load balancing Appliance/Solution

3.10. Support

3.10.1. Installation and configuration should be done by vendor certified engineers.

3.10.2. One (1) year comprehensive manufacture warranty and subscription for the all the security services should be offered.

3.10.3. On-Site Admin Training should be provided for technical staff. In addition, Certified Administration Training for atleast one technical staff should be provided.

4. DELIVERABLES

The selected party under this Terms of Reference are to supply the below listed goods to the Ministry of Environment, Climate Change and Technology (MECCT) accordingly.

#	Item	Quantity
1	Supply of a Next Generation Firewall as per the requirements (Section 3)	1
2	Configuration and installation of the proposed solution	1
3	Training and support	1

5. PAYMENT SCHEDULE

Applicants must submit their financial proposal which must indicate the rate per item in scope (Section 3) and price for the total assignment. However, the payments will be made upon completion of the full scope of work under deliverables of this TOR.

6. EVALUATION CRITERIA

1. Pre-Evaluation
    a. Pre-Evaluation is a preliminary evaluation done based on the documentation requirement before moving on to the Technical Evaluation. Pre-Evaluation determines if bidder is substantially responsive to the terms of this ToR as specified below;
        i. Bidder confirms to all requirements identified under Section 6. Mandatory Documents and requirements.
        ii. Financial situation:
            1. To be eligible the financial statements of the bidding party must show, minimum annual turnover of MVR 300,000.00, for the year 2020.
            (or)
            2. To be eligible the financial statements of the bidding party must show, Minimum value of MVR 300,000.00, for liquid asset, for the year 2020.
            (or)
            3. For business mentioned in the Section b no. 5, to be eligible the business's bank statement must show a credit balance of minimum MVR MVR 300,000.00
            (or)
            4. If bidding party is unable to meet any of the above requirement they shall submit "Line of Credit Letter" as per the template in FIN Form 3. (credit limit shall be no less than MVR 300,000.00

    b. Substantially non-responsive bids at this pre-evaluation stage will be rejected from further stages of evaluation.
    c. Substantially responsive bids at this pre-evaluation stage shall be qualified for technical evaluation.

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

2. Technical Evaluation
    a. Technical evaluation is to confirm if the proposed product does comply with all the requirements listed under the technical requirements. Ministry of Environment, Climate Change and Technology holds the authority to qualify any proposal technically based on their proposed features, only if the evaluation committee finds it acceptable and would achieve the objective fully. Technically non-responsive bids from this stage would not be qualified to the final evaluation.

3. Final Evaluation
    a. The proposal would be qualified to this stage after being assessed in pre-evaluation and technical evaluation. In this evaluation, the proposals would be compared to their proposed price, duration and experience to complete the project. Point system set for the final evaluation is:

#	Description	Points (percentage)
1	Price $\frac{Lowest\ price\ proposed}{Proposed\ price} \times 80$	80%
2	Duration $\frac{Shortest\ duration\ proposed}{Proposed\ duration} \times 10$	10%
3	Experience $\frac{Total\ experience\ points}{100} \times 10$	10%

Experience would be considered to all submitted letters which is addressed to relevant works (supply and configuration of firewalls) of value higher than MVR 35,000, completed within the past 5 years. Each valid reference letter would carry 1 point (up to 5 reference letters).

ANNEX 1

STANDARD FORMS

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

TECH FORM 1 – Proposal Submission Form

[Location, Date]

To: [Name and address of Client]

Dear Madam/Sir:

I, the undersigned, would like to express my interest for the **''SUPPLY, INSTALLATION AND CONFIGURATION OF A NEXT GENERATION FIREWALL'** in accordance with your Request for Proposal Ref: (IUL)438-ICTU/438/2022/156 dated 21st April 2022, I am hereby submitting my Proposal, which includes all required documents as per Request for Proposal.

I hereby declare that all the information and statements made in this Proposal are true and accept that any misinterpretation contained in it may lead to our disqualification.

If negotiations are held during the period of validity of the Proposal, I undertake to negotiate on the basis of the proposed fees. The Proposal is binding upon myself and subject to the modifications resulting from Contract negotiations.

I undertake, if my Proposal is accepted, to initiate the services and fulfil the terms and conditions related this contract.

I understand you are not bound to accept any Proposal you receive.

I remain,

Yours sincerely,

Signature [In full and initials]:

Name and Title of Signatory:

Name of Individual:

Address:

TECH FORM 2 – Compliance Checklist

Feature	Compliance (Yes / No)	Remarks
Hardware and Interface		
The platform must be supplied with at least 10 x 10/100/1000Mbps ports and 4 x 10GBase-F SFP+		
ports (with 1 x SFP+ converter)		
The proposed solution must support minimum 10 virtual context and should be upgradable to 20 with further memory upgrade		
The proposed solution should have in-built storage of minimum 240GB SSD		
Performance		
Firewall throughput must be more than 17 Gbps (in ideal testing conditions)		
The VPN AES 128 throughput should be more than 2.5 Gbps		
The IPS throughput must be atleast 4.6 Gbps		
The proposed solution must support 2 million concurrent connections minimum and should be able to handle upto 8 million with memory upgrade.		
The proposed solution should be able to process more than 65,000 new connections per second.		
Solution must provide with minimum of 50 remote access VPN client license		
Minimum of 16GB memory should be provided and should be upgradeable to 32GB		
General Requirements		
The proposed solution should support “Stateful” policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols such as; telnet, ftp etc		
The proposed solution should not use a proprietary ASIC/FPGA hardware for FW and VPN performance only. Either all security controls must be catered by specialised hardware or OEM must mention the performance numbers disabling the specialised hardware		
The solution and integrated IPSEC VPN applications should be ICSA labs certified for ICSA 4.0, FIPS 140-2 certified and NSS Recommended (NGFW - latest report)		
The hardware platform and NGFW with integrated SSL VPN application has to be from the same OEM.		
The proposed solution (FW , IPS, Application Control, URL Filtering, Anti-Virus & Anti-Bot, SandBoxing) should support for Active – Active connections (without virtual context). It should not depend upon any 3rd party product or appliance for the same.		
Licensing should be a per device and not user/IP based (should support unlimited users)		

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

	The proposed solution should support the multicast protocols as a multicast host, by participating in DVMRP, IGMP and PIM-DM / PIM-SM		
	The proposed solution vendor must be a leader in Gartner® Magic Quadrant™ for Enterprise Network NGFWs in last 10 years.		
	The proposed solution should have a provision to handle the bandwidth management at different levels		
	It should support the VOIP traffic filtering		
	Appliance should have Identity Awareness Capabilities		
	Solution must failover without dropping any connection in active - active mode.		
	The proposed solution should have Hardware Sensor Monitoring capabilities		
	The platform should support VLAN tagging (IEEE 802.1q)		
	The proposed solution should support ISP link load balancing upto 7 WAN connections		
	The proposed solution should support Link Aggregation functionality to group multiple ports as single port.		
	The Proposed Solution should support Ethernet Bonding functionality for Full Mesh deployment architecture.		
	The Proposed Solution must support atleast 4096 Vlans in virtual mode		
	Solution must have search optoin in GUI to search configuration options like NTP, arp, Proxy etc. and should directly take administrator to configuration window of search result by just clicking at search results.		
	Appliance must support automatic search, downloading and install software hotfixes without any administrator efforts and must notify Administrator through mails on the status and progress of each step. System should automatically roll back upon failure.		
	Solution must support at least two clustering protocols.		
	Solution must support VRRP clustering protocol.		
	The Proposed Solution must allow to configure password policy for local users to login to NGFW and must support following: disallow palindromes, disallow password reuse from last 10 passwords, set password expiry in number of days, must have option to warn user 7 days before password expiry, block access for certain period of time after certain number of failed login attempts.		
	Solution must support multiple administrators to work on policies on session based, All the policies and objects on which Administrator 1 is working should be locked for all other administrator, however other administrator can work on other policy rules and objects in their respective sessions. Changes done by Administrator-1 should not be visible to other administrators till the time Administrator-1 publish changes.		
	Solution must allow administrator to choose to login in read-only or read write mode		
	Solution must allow to open support tickets directly from NGFW GUI.		

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

Solution must support multiple role based administration, (Ex).Routing Administrator must have read write access to all routing protocols, interface configuration, DNS configurations, etc.		
Architecture Features		
It should support the IPSec VPN for both Site-Site & Remote Access VPN		
Virtual Context must support virtualization of all the feature set which are offered by the vendor		
The Gateway system should support virtual tunnel interfaces to provision Route-Based IPSec VPN		
It should support the system authentication with RADIUS and local authentication. Both should work simultaneously.		
NGFW Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades		
Standards Support Requirements		
The Proposed Solution must support unlimited policy option.		
The Proposed Solution should be able to handle more than 10,000 routes (HQ Firewall Only)		
The Address/host object limit must be above 50,000		
The Proposed Solution Modules should support the deployment in Routed as well as Transparent Mode (HQ Firewall Only)		
The Proposed Solution must provide state engine support for all common protocols of the TCP/IP stack		
The Proposed Solution must provide NAT functionality, including dynamic and static NAT translations		
All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, Ms-Exchange etc		
Local access to the proposed Solution modules should support authentication protocols – RADIUS & TACACS+		
IPSec VPN should support the Authentication Header Protocols – MD5 & SHA		
IPSec ISAKMP methods should support Diffie-Hellman Group 1 & 2, MD5 & SHA Hash, RSA & Manual Key Exchange Authentication, 3DES/AES-256 Encryption of the Key Exchange Material and algorithms like RSA-1024 / 1536		
IPSec encryption should be supported with 3DES, AES-128 & AES-256 standards		
IPSEc should have the functionality of PFS and NAT-T		
The Proposed Solution should support authentication proxy for Remote VPN, HTTP/HTTPS Applications Access, and various other applications		
The Proposed Solution should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods		
The Proposed Solution should support PKI Authentication with PCKS#7 & PCKS#10 standards		

It should support BGP, OSPF, RIPv1 &2, Multicast Tunnels, DVMRP protocols		
Dynamic policy enforcement on VPN Clients		
NGFW Filtering Requirements		
It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports.		
The NGFW must provide state engine support for all common protocols of the TCP/IP stack		
The NGFW should be constantly updated with new defences against emerging threats.		
NGFW updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time		
NGFW should support over 8400+ applications		
The IPS should scan all parts of the session in both directions		
It should be able to block Instant Messaging such as; Yahoo, MSN, ICQ, Skype (SSL and HTTP tunneled)		
It should enable blocking of Peer-Peer applications such as; Kazaa, Gnutella, Bit Torrent, IRC (over HTTP)		
The NGFW should support authentication protocols like LDAP, RADIUS and have support for NGFW passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.		
IPS should have the functionality of Geo Protection to Block the traffic country wise in incoming direction, outgoing direction or both. IPS also should alert through Mail if any IPS traffic/event detected from Specific Country.		
The NGFW should support advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications Should support CLI & GUI based access to the NGFW modules		
Local access to NGFW modules should support role-based access		
QoS Support [Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantees, QOS limits and QOS VPN]		
NGFW Should support Identity Access for Granular user, group and machine-based visibility and policy enforcement		
IPS should be able to detect and prevent embedded threats with in SSL traffic.		
The solution should allow for third party signature import such as Snort		
NGFW should have Identity based logging option		
Web Security Solution		
Solution should be able to detect & Prevent the Bot communication with C&C		
Solution should have an multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		

Solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family		
Solution should be able to detect & Prevent attack types ie, such as spam sending click fraud or self-distribution, that are associated with Bots		
Solution should be able to block traffic between infected Host and Remote Operator and not to legitimate destination		
Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc.		
Solution should give information related to performance impact and confidence level of protections while creating profiles		
Antivirus protection protocols for HTTP,HTTPS etc.		
Solution should have an option of packet capture for further analysis of the incident		
Solution Should Uncover threats hidden in SSL links and communications		
The AV should Scan files that are passing on CIFS protocol		
The vendor malware update mechanism should include reputation, network signatures and suspicious email activity detection		
IPS shall be able to provide complete user visibility in the logs.		
Anti-APT Solution		
The hardware and software-based solution should provide protection for all incoming and outgoing traffic from /to Internet.		
The proposed solution should be able to address both APT attacks and Advanced Malware across Network.		
The solution must employ an on-cloud analysis engine to detect zero day and unknown threats and must not be signature based. The solution however should have an option to send the samples to on premise-based emulation system as well.		
The solution should support static as well as dynamic analysis.		
The Hypervisor used by sandboxing solution must not be an OEM solution such as from VMWare, Hyper-V, VirtualBox, RHEV etc. However, it should be a custom Hypervisor purpose built for sandboxing requirement		
The solution must be able to detect and report malware by using multiple images of Windows XP/7/8/10/11		
The solution must support prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft. There should be no requirement for the customer to buy additional Microsoft licenses for sandboxing solution		

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

	The engine should detect API calls, file system changes, system registry, network connections, system processes, kernel code injection, system calls and direct CPU interaction.		
	Anti-APT solution should be able to work independently of signature updates from OEM website.		
	The solution should detect the attack at the exploitation stage – i.e. before the shell-code is executed and before the malware is downloaded/executed.		
	The solution should be able to detect ROP and other exploitation techniques (e.g. privilege escalation, directory traversal) by monitoring the CPU flow		
	The solution must be able to support scanning links inside emails for zero days & unknown malware		
	The solution should be able to perform pre-emulation static filtering		
	The solution should support sandboxing of file sizes upto 100MB		
	The proposed solution must be able to run multiple micro tasks in a single VM.		
	The solution should analyze malware (VM based execution) coming over protocols like HTTP/HTTPS, SMTP, SMTP-TLS, CIFS etc. All the components of the solution must be managed from a centralized management console from the same OEM. However, management and logging appliances may be different from the sandboxing appliance.		
	The Sandboxing solution should allow for 'Geo Restriction' which enables emulations to be restricted to a specific country		
	The solution must provide the ability to Increase security with automatic sharing of new attack information with other gateways in means of signature updates etc.		
	The solution must utilize a Global Threat Intelligence feed from OEM regrading new malware profiles, vulnerability exploits, C&C call-back destinations and obfuscation tactics etc.		
	The virtual execution environment must have anti-evasion capabilities to prevent the malwares to evade detection of the sandboxing environment. Anti VM detection activities like Time delays, shutdown, restart, VM detection, user interaction etc. must be prevented by the solution.		
	The solution should have the inherent ability to detect multi-stage attacks. For the purpose of detecting multi stage attacks the solution should include static analysis technologies like IPS, antivirus, anti-malware/anti bot however in an integrate mode with the solution. The bidder or SI may use additional appliances (at max 2) for the solution but should be provided by the same OEM in the solution.		
	The solution should inspect the web sessions (HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the		

	internet. Third Party/Separate appliance for SSL offloading will not be accepted		
	The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution should also assign a unique identification number to each identified/detected threat for future reference.		
	The solution shall detect the entire attack lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration.		
	The solution shall provide event-based alerts/logs.		
	The solution should have ability to stop web-based attacks and block all outbound call-back communication initiated by the infected internal clients.		
	The solution should have no limitations in terms of number of users. However, for sizing purpose the bidder shall refer to the Section 3.1, 3.2 and 3.3.		
	The solution should be able to work in tandem with other network device (e.g. firewall, IDS/IPS, Antispam, Web proxy, Endpoint Antivirus etc.) for its functioning. Additional devices required if any should be provided by the bidder. But the upper limit of such devices should not be more than 2		
	The solution should have the ability to be deployed in the following modes: • Inline blocking • Inline monitoring • TAP/SPAN mode		
	The solution shall support to identify the IP address (Internal LAN IP address) of a host in a proxy environment.		
	The solution should provide a Dashboard that offers real time threat visibility and attack characteristics		
	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports daily/weekly/monthly/annually/specific range (day and time), etc.		
	The solution should provide reports in (not limited to) HTML/CSV/PDF Formats.		
	3.9.34. Upon malicious files detection, a detailed report should be generated for each one of the malicious files. The detailed report must include: • Screen shots • Timelines • Registry key creation/modifications • File and processes creation • Network activity detected		
	The solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions		
	The solution should provide for offline updating of threat intelligence		
	The solution should support: • LDAP or RADIUS and Local Password authentication schemes (not limited to)		

• Remote administration using SSH/HTTPS • CLI, GUI/Web based Administration Console		
The solution should examine the email traffic in real-time for emails having malware and potential spear-phishing and targeted attacks. Such infected email attachments should be remediated in real time and should be retrievable by administrator, if required.		
The proposed solution should dynamically generate real-time malware intelligence for immediate local protection via integration with the separate Automated Management and Event Correlation System. This Automated Management and Event Correlation solution must be from the same OEM.		
Solution should have an ability to remove all the active content and macros sending only a clean document to the end user		
The solution should hold the attachment on the inbound email traffic till the attachment has been dynamically analyzed by the virtual environment.		
All necessary additional devices, software & licenses required for achieving functionalities of web and email traffic should be quoted as part of the solution.		
The solution should support SNMP, syslog for integration with a SIEM Solution and should support integration of privately generated intelligence on the sandbox to be shared with other security devices through open standards-based protocols like STIX/TAXII, Open IOC etc.		
The core product troubleshooting documents like admin guides, installation guides, manuals should be made available to the customer directly through publicly accessible OEM website. The OEM must share the admin guides during technical evaluation		
The Proposed Solution must support multiple Sandboxing appliance to provide load balancing and allow equal distribution of files for Sandboxing without any third-party load balancing Appliance/Solution		
Support		
Installation and configuration should be done by vendor certified engineers.		
One (1) year comprehensive manufacture warranty and subscription for the all the security services should be offered.		
On-Site Admin Training should be provided for technical staff. In addition, Certified Administration Training for atleast one technical staff should be provided.		

FIN FORM 1 – Financial Proposal Submission Form

[Location, Date]

To: [Name and address of Client]

Dear Madam/Sir:

I, the undersigned, offer the express my interest for the **''SUPPLY, INSTALLATION AND CONFIGURATION OF A NEXT GENERATION FIREWALL'** in accordance with your Request for Proposal Ref: (IUL)438-ICTU/438/2022/156 dated 21st April 2022 in accordance with your Request for Proposal dated [xxx] and Technical Proposal. The attached Financial Proposal is for the sum of [Insert amount(s) in words and figures in MVR]. This amount is inclusive of the all local taxes.

The Financial Proposal shall be binding upon myself subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal.

I undertake, if my Proposal is accepted, to initiate the services and fulfil the terms and conditions related this contract.

I understand you are not bound to accept any Proposal you receive.

Yours sincerely,

Signature:

Name and Title of Signatory:

Address:

FIN FORM 2 - Financial Breakdown Form

Date:

Reference No: (generated by the proponent)

Delivery Period: (in days)

Warranty: (in months)

No.	Quantity	Description	Price/Unit (MVR	Total
1	1	Supply of a Next Generation Firewall		
2	1	Configuration and installation of the proposed solution		
3	1	Training and support		
		Total:		
		GST		
		Total with GST		

The quotation is valid for 120 days from the date of Application.

Indicate the total cost with detail cost to be paid in Maldivian Rufiyaa (MVR).

Note: The total contract price should be quoted inclusive of Goods and Services Tax (GST) or any applicable axes as per the Tax Legislation and must be shown in the breakdown.

Authorized Name, Signature and Stamp

FIN FORM 3 - Financial Situation
Each Applicant must fill in this form

Financial Data for Previous 3 Years [MVR Equivalent]			
	Year 2021:	Year 2020:	Year 2019:

Information from Balance Sheet

Total Assets			
Total Liabilities			
Net Worth			
Current Assets			
Current Liabilities			
Working Capital			

Information from Income Statement

Total Revenues			
Profits Before Taxes			
Profits After Taxes			

❑ Attached are copies of financial statements (balance sheets including all related notes, and income statements) for the last three years, as indicated above, complying with the following conditions.

- All such documents reflect the financial situation of the Bidder.
- Historic financial statements must be complete, including all notes to the financial statements.

- Historic financial statements must correspond to accounting periods

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

FIN FORM 4 – Average Annual Turnover

Each Bidder must fill in this form

Annual Turnover Data for the Last 3 Years		
Year	Amount Currency	MVR Equivalent
2021		
2020		
2019		
Average Annual Turnover		

The information supplied should be the Annual Turnover of the Bidder in terms of the amounts billed to clients for each year for contracts in progress or completed at the end of the period reported.

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

FIN FORM 5 – Financial Resources

Specify proposed sources of financing, such as liquid assets, unencumbered real assets, lines of credit, and other financial means, net of current commitments, available to meet the total construction cash flow demands of the subject contract or contracts as indicated in Section 3 (Evaluation and Qualification Criteria)

Financial Resources		
No.	**Source of financing**	**Amount (MVR equivalent)**
1		
2		
3		
4		

FIN FORM 6 – Line of Credit Letter

[letterhead of the Bank/Financing Institution/Supplier]

[date]

To:*[Name and address of the Contractor]*

Dear,

You have requested {name of the bank/financing institution) to establish a line of credit for the purpose of executing {insert Name and identification of Project}.

We hereby undertake to establish a line of credit for the aforementioned purpose, in the amount of {insert amount}, effective upon receipt of evidence that you have been selected as successful bidder.

This line of credit will be valid through the duration of the contract awarded to you.

Authorized Signature: _____

Name and Title of Signatory: _____

Name of Agency: _____

FIN FORM 7 – Current Contract Commitments / Work in Progress
Current Contract Commitments/Works in Progress

Tenderers and each partner to a JV should provide information on their current commitments on all contracts that have been awarded, or for which a letter of intent or acceptance has been received, or for contracts approaching completion, but for which an unqualified, full completion certificate has yet to be issued.

No	Name of contract	Employer, contact address/tel/fax	Value of outstanding work (current MVR equiv)	Estimated completion date	Average monthly invoicing over last six months (MVR/month)
1.					
2.					
3.					
4.					
5.					

+960 3018300 secretariat@environment.gov.mv MoEnvmv www.environment.gov.mv

GENERAL INFORMATION

1	**Bid Awarding**	
	1.1	Bidder will be informed of the decision to award a bid via an official intent to award the bid.
	1.2	If the value of the bid exceeds **MVR 500,000** the bidder will be required to submit a performance guarantee of **(…. %)** of the total contract value prior to signing the contract. The performance guarantee must be issued by a Bank or a Financial Institution located in any eligible country. If the institution issuing the gurantee is located outside the Republic of Maldives, it shall have a correspondent financial institution located in the Republic of Maldives to make it enforceable. **(Excluding Consultancy Service)**
	1.3	Failure of the successful bidding party to submit the aforementioned performance guarantee, or sign the Contract, shall constitute sufficient grounds for the annulment of the award and forfeiture of the Bid Security. In that event the Ministry may award the contract to the next lowest evaluated bidder, provided the bidder is capable of performing the contract satisfactorily.
	1.4	Standstill period
		The Contract shall be awarded not earlier than the expiry of the Standstill Period. The duration of the Standstill Period is 5 days. The Standstill Period commences the day after the date the Employer has transmitted to each Bidder (that has not already been notified that it has been unsuccessful) the Notification of Intention to Award the Contract. Where only one Bid is submitted, the Standstill Period shall not apply.
2	**Liquidated Damages (Excluding Consultancy Service)**	
	2.1	The Contractor shall pay liquidated damages to the Employer at the rate per day **stated in the Public Procurement Regulation** for each day that the Completion Date is later than the Intended Completion Date. The total amount of liquidated damages shall not exceed the amount **defined in the Public Procurement Regulation.** The Employer may deduct liquidated damages from payments due to the Contractor. Payment of liquidated damages shall not affect the Contractor's liabilities.
3	**Securities (Excluding Consultancy Service)**	
	3.1	If the price quoted by a bidding party exceeds MVR 500,000 in value, the bidding party will be required to submit a bid security of MVR……, with validity of no less than 90 days. Bid Security must be a bank guarantee letter or security issued by a Bank or a Financial Institution located in any eligible country. Bank Cheques, Bonds and Cash will not be accepted as bid security.
4	**Advance Payment (Excluding Consultancy Service)**	
	4.1	Vendor has to request for Advance payment within 45 days from the contract date start.
	4.2	Vendor has to submit Advance payment guarantee with the Invoice (15% of Contract price Maximum)

5	**Arithmetic**	
	5.1	Provided that the Tender is substantially responsive, the *Employer* shall correct arithmetical errors on the following basis:
	5.1.1	only for unit price contracts, if there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected, unless in the opinion of the Employer there is an obvious misplacement of the decimal point in the unit price, in which case the total price as quoted shall govern and the unit price shall be corrected;
	5.1.2	if there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected; and
	5.1.3	if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to (a) and (b) above.
	5.2	If the Tenderer that submitted the lowest evaluated Tender does not accept the correction of errors, its Tender shall be declared non-responsive.