



# SUPPLY, DELIVERY AND INSTALLATION OF FIREWALL & ENDPOINT SECURITY SOLUTION

WAMCO-PRO/IUL/2022/097



Issued on: 13<sup>th</sup> September 2022

Issued by:

**WASTE MANAGEMENT CORPORATION LIMITED**  
**MALE', REPPUBLIC OF MALDIVES**

[www.wamco.com.mv](http://www.wamco.com.mv)

**SUPPLY, DELIVERY AND INSTALLATION OF FIREWALL  
& ENDPOINT SECURITY SOLUTION.**

WAMCO-PRO/IUL/2022/097

## Project Brief

Waste management Corporation limited invites interested parties to submit proposals for the supply, delivery and installation of firewall and endpoint security solution for Waste Management Corporation Limited.

1. Description of Works:		
1.1.Details of the Equipment		
2. Firewall	Type:	Enterprise
	Quantity:	2 (Clustered)
	Licensing & Support:	3 years
	Warranty:	3 years
1. Branch Firewall	Quantity:	15
	Licensing & Support:	3 years
2. Wireless AP	Quantity:	15
	Licensing & Support:	3 years
3. Integrated Endpoint Security	Licensing & Support:	Should include 3 Year license subscription for a minimum 400 endpoints, 85 mobile devices, and 15 servers.
	Supported Operating Systems:	- Windows 10 and later - Windows Server 2012 and later - macOS 10.14, 10.15, 11+ - iOS 9.0 and later - Android 5.0 and later - Linux Ubuntu, Red Hat 7.4 and later
4. Centralized Management and Security Analytics	Centralized management for core firewall and all branch firewalls Centralized management for Integrated Endpoint Security	

## 1.2. Installation, Configuration and Training

## Hardware installation

- Certified specialist onsite for the duration of the configuration and migration execution
- Design appropriate LAN, WAN, and DMZ security.
- Configure application control policies
- Configure AV and Web filtering policies
- Configure antispam filtering
- Configure traffic shaping and ISP WAN load balancing
- Network segmentation and configure appropriate security policy per segment
- Configure branch firewalls and remote access connectivity policies
- Configure wireless network and relevant policies
- Configure endpoint security, centralized reporting and management
- Configure centralized management
- Configure centralized log analytics and standard security reporting
- Manufacturer certified training for 3 technical staff
- On the job training on basic management, operation and maintenance.
- Comprehensive testing and a detailed documentation on the configuration and settings of the delivered solution should be provided.

**2. Bid language:**

English

### 3. Bid Currency:

All prices are to be quoted in Maldivian Rufiyaa (MVR)

**4. Period of bid validity.**

120 Calendar days from the date of bid submission

## 5. Bid Security

Bids Should be accompanied with a bid security of MVR 50,000.00 (Fifty Thousand). The Bid Security should be valid for 45 (forty-five) days beyond the validity of the bid. Bid Security Should be an original bank guarantee letter (or) Bank Guaranteed and stamped Cheque (or) An Insurance Policy from MMA registered insurance company.





## 9. Documents to be Submitted

1. Proposal/Quotation (inclusive of the delivery period)
2. Bid Security
3. Form 1 – Bid Form
4. Form 2 – Bidder's Information Form
5. Company profile prepared by company/firm (Bidder)
6. Copy of Business Registration Certificate
7. Copy of Goods and Service Tax (GST) Registration certificates if applicable.
8. National identity card of all share holders / individual
9. Copy of Company Shareholder's Certificate (Ministry of Economic Development).
10. Proof of financial capability: last 3 (three) months (May, June and July) Bank Statement (with stamp from bank in the letterhead of respective Bank) or other financial proof of capability from a relevant authority.
11. Form 3 – Experience Information Form
12. Proof of experience documents / reference letters (Documents signed by previous clients indicating the project value, duration and completion date corresponding to and supporting the above).
13. Form 4- Technical Compliance Form

Failure to submit above mentioned documents will be considered as a failure to submit and late submissions of any such documents will not be entertained.

## 10. Liquidated Damages

If the successful bidder fails to deliver any or all of the Goods by the Date(s) of delivery or perform the related services within the period specified in the Contract, 0.5% of the total price as awarded will be deducted per day as a delay damage up to a total of 15% of the total price. Once the maximum is reached, WAMCO may terminate the Contract.

## 11. Payments terms

### 11.1. Advance payment:

If the successful Bidder wishes, an advance payment less than or equal to 15% of the total bid price could be awarded.

Any required advance payment should be clearly mentioned in the Proposal.



Fifteen (15) percent of the Bid Price shall be paid within Fourteen (14) days of signing of the Contract against a proforma invoice and an advance payment guarantee for the equivalent amount and in the form provided in the bidding documents or another form acceptable to WAMCO.

The Advance payment guarantee shall be valid for 30 days beyond the date of delivery and shall be returned following the completion of delivery upon request.

**11.2. Payment Period:**

WAMCO shall pay to the consultant within 30 Calendar days after the date of delivery and acceptance by WAMCO and upon completion of the work in accordance with the agreement. Invoice must be submitted by the consultant along with signed Acceptance certificates.

## 12. Delivery

- Delivery of Hardware's and licenses to WAMCO within 60 days.
- Installation, configuration and training of the solution within 30 days after delivery.

### 13. Bid Evaluation Criteria

Criteria	Points
<b>1. Price</b> $\text{Price} = \frac{\text{Lowest Amount}}{\text{Proposed Amount}} \times 80$	<b>80</b>
<b>2. Experience in similar Works</b> No of similar projects in last five years (each project: value not less than MVR 250,000) $\text{Experience} = \frac{\text{no experience letters by the bidder}}{\text{maximum no of exp letters by a bidder}} \times 20$	<b>20</b>
<b>Total</b>	<b>100</b>

### Experience in Similar Work:

- A valid reference letter with the company letterhead on completion of similar project/works should be provided. In case if a reference letter is not available, purchase order with a delivery note, agreement with delivery note or invoice with delivery note will be accepted. Two (2) points will be awarded to each valid experience letter upto a maximum of 20 points.

\* The works performed should be within the last 5 years.

**Similar works:** Supply, delivery and installation of firewall, endpoint security solutions and server-side hardware.



2.

## Technical Compliance & Technical Evaluation

Item	Specifications	Bidder can provide items as per specification (YES/NO)	If NO, please mention the specification provided
<b>FIREWALL</b>			
<b>Brand / Model</b>			
<b>Quantity</b>	- 2 (must support active-active / active-passive cluster)		
<b>Minimum Throughput</b>	- Firewall Throughput: 25Gbps - SSL VPN Throughput: 2 Gbps - SSL Inspection Throughput: 3 Gbps - Threat Protection Throughput: 2.5 Gbps - IPS Throughput: 5 Gbps		
<b>Minimum Supported APs</b>	- 50		
<b>Licensing / Support</b>	- Should be supplied with <b>3 Year Security Subscription</b> - Web Filtering, Malware Protection, IPS, Antispam, Antivirus, Botnet, Virus Outbreak Protection, Application Control, zero-day malware threat protection, Sandbox - Should be supplied with <b>3-Year Support Subscription: 24x7</b> Support, Hardware Replacement & Firmware Upgrades		

<b>Minimum Hardware Requirement</b>	- Six (6) Gigabit Ethernet RJ45 Ports		
	- Two (2) Gigabit Ethernet SFP Ports		
	- Two (2) 10Gigabit Ethernet SFP+ Ports		
<b>Management</b>	Should include a Centralized Management console for all features of the firewall including integrated endpoint security, branch firewall, Wireless AP and analytics.		
<b>BRANCH FIREWALL</b>			
<b>Brand / Model</b>			
<b>Quantity</b>	15		
<b>Licensing / Support</b>	- Should be supplied with <b>3-Year Support Subscription: 24x7</b> Support, Hardware Replacement, Firmware Upgrades		
	- Should provide <b>3-Year Technical Support:</b> By OEM or Local technical support by certified engineers		
<b>Minimum Firewall throughput</b>	850 Mbps		
<b>Minimum Hardware Requirement</b>	- One (1) Gigabit Ethernet RJ45 WAN Port		
	- Three (3) Gigabit Ethernet RJ5 LAN Ports - One (1) USB Port - 3G/4G Support		





Page 9 of 27

	- Real-time Endpoint Status always provides current information on endpoint activity and security events		
<b>Supported Operating Systems</b>	<ul style="list-style-type: none"> <li>- Windows 10 and later</li> <li>- Windows Server 2012 and later</li> <li>- macOS 10.14, 10.15, 11+</li> <li>- iOS 9.0 and later</li> <li>- Android 5.0 and later</li> <li>- Linux Ubuntu, Red Hat 7.4 and later</li> </ul>		
<b>Licensing / Support</b>	<ul style="list-style-type: none"> <li>- Should include 3-Year license subscription for a minimum 400 endpoints, 80 mobile devices, and 15 servers.</li> <li>- Subscription license should include Telemetry, Remote Access (SSL and IPSec VPN), Vulnerability Scan, Malware, Web Security, Application Firewall, Application Control, Zero-day threat protection and Sandbox</li> <li>- 24x7 support by OEM or Certified local technical engineers</li> </ul>		
<b>CENTRALIZED MANAGEMENT AND SECURITY ANALYTICS</b>			
<b>Brand / Model / Product Name</b>			
<b>Centralized Management</b>	<ul style="list-style-type: none"> <li>- Central management for core firewall and all branch firewalls</li> <li>- Provide signature updates to managed devices</li> </ul>		



	<ul style="list-style-type: none"> <li>- Use templates for firmware upgrades and zero-touch provisioning for Secure SDWAN, setting up VPN, and static route</li> <li>- Automate workflows and configurations for firewalls, switches, and wireless infrastructure</li> <li>- Scalable to manage to all devices</li> <li>- Automated device configuration backups and revision control make daily administrative tasks easy</li> <li>- 3-Year cloud-based management subscription license for all devices</li> </ul>		
<b>Security Analytics</b>	<ul style="list-style-type: none"> <li>- Security Analytics with event correlation and real-time detection across all logs, with</li> <li>- Indicators of Compromise (IOC) service and detection of advanced threats</li> <li>- Integration with Firewall and endpoint security for deeper visibility and critical network insights</li> <li>- Centralized security operation center visibility for the attack surface with access to real-time log and threat data in the form of actionable views with deep drill-down capabilities, notifications &amp; reports, and predefined or customized dashboards for single-pane visibility and awareness.</li> </ul>		



	<ul style="list-style-type: none"> <li>- Event Manager enables security teams to monitor and manage alerts and events from logs</li> <li>- Out of the box playbook templates allowing organization's security team's abilities to simplify investigation efforts through automated incident response</li> <li>- Correlated log data with threat intelligence for analysis of real-time and historical events, providing context and meaning to network activity, risks, and vulnerabilities, attack attempts, operational anomalies, and continuous monitoring of sanctioned and unsanctioned user activity and investigation of Shadow IT</li> <li>- Predefines report templates, datasets and charts that are ready-to-use with sample reports</li> <li>- Should be a Cloud based platform delivering reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture.</li> </ul>		
<b>License</b>	- 3-Year cloud-based subscription license for Central Logging & Analytics		

## INSTALLATION & CONFIGURATION

- Hardware installation
- Certified specialist onsite for the duration of the configuration and migration execution
- Design appropriate LAN, WAN, and DMZ security.
- Configure application control policies
- Configure AV and Web filtering policies
- Configure antispam filtering
- Configure traffic shaping and ISP WAN load balancing
- Network segmentation and configure appropriate security policy per segment
- Configure branch firewalls and remote access connectivity policies
- Configure wireless network and relevant policies
- Configure endpoint security, centralized reporting and management
- Configure centralized management
- Configure centralized log analytics and standard security reporting
- Manufacturer certified training for 3 technical staff
- On the job training on basic management, operation and maintenance.
- Comprehensive testing and a detailed documentation on the configuration and settings of the delivered solution should be provided.





## FORM 2 – BIDDER'S INFORMATION FORM

1. Bidder's Name:		
2. Company Registration Number:		
3. Registered Address:		
4. GST Number:		
5. Contact Number:		
6. Email Address:		
7. Tenderer's Authorized Representative Information:		
Name:		
ID Card Number:		
Address:		
Contact Number:		
Email Address:		
8. Managing Director / CEO information:		
Name:		
ID Card Number:		
Address:		
Contact Number:		
Email Address:		
9. Name of shareholders:		
#	Name	ID Card No.
1.		
2.		
3.		
4		

Attached are copies of original documents of *[check the box(es) of the attached original documents]*

- ☐ Company Registration Copy
- ☐ GST Registration Copy
- ☐ National Identification Card (if Individual) Copy
- ☐ Shareholder's Certificate provided by Ministry of Economic Development.

#	Document	✓
1	Proposal/Quotation (inclusive of the delivery period)	
2	Bid Security	
3	Form 1 - Bid Form	
4	Form 2 - Bidder's Information Form	
5	Company Profile prepared by the company/firm (Bidder)	
6	Copy of Business Registration Certificate	
7	Copy of Goods and Service Tax (GST) Registration certificates if applicable.	
8	National Identity Card of all shareholders/ individual	
9	Copy of Company Profile Information Sheet / Shareholder's Certificate (From Ministry of Economic Development)	
10	Proof of financial capability: last 3 (three) months (May, June and July) Bank statement (with stamp from bank in letter head of the respective Bank) or other financial proof of capability from a relevant authority.	
11	Form 3 - Experience Information Form	
12	Proof of experience documents / reference letters (Documents signed by previous clients indicating the project value, duration and completion date corresponding to and supporting).	
13	Form 04- Technical Compliance Form	



## FORM 3 – EXPERIENCE INFORMATION FORM

## 1. Experience

### 1.1. Works of similar nature performed over the last 5 years.

(Reference Letters/Proof of experience of the works completed, shall be submitted along with the bid).

*(if the bidder fails to submit reference letters/proof of experience for a particular project that the bidder has listed in the form, it will not be considered during the evaluation stage of the bid and marks will not be given for that particular project.*

[illegible]

I/We Hereby confirm that the said documents/relevant paperwork/supporting documents have been attached with the Forms. We agree that failure to submit above mentioned documents will be considered as a failure to submit. Late submissions of any such documents will not be entertained by Waste Management Corporation Limited and this will affect the evaluation of our bid.

Name:	
ID Card Number:	
Company Name and Seal/Stamp:	
Date:	
Signature:	

# FORM 4 – TECHNICAL COMPLIANCE FORM

Item	Specifications	Bidder can provide items as per specification (YES/NO)	If NO, please mention the specification provided
<b>FIREWALL</b>			
<b>Brand / Model</b>			
<b>Quantity</b>	- 2 (must support active-active / active-passive cluster)		
<b>Minimum Throughput</b>	- Firewall Throughput: 25Gbps - SSL VPN Throughput: 2 Gbps - SSL Inspection Throughput:3 Gbps - Threat Protection Throughput: 2.5 Gbps - IPS Throughput: 5 Gbps		
<b>Minimum Supported APs</b>	- 50		
<b>Licensing / Support</b>	- Should be supplied with <b>3 Year Security Subscription</b> - Web Filtering, Malware Protection, IPS, Antispam, Antivirus, Botnet, Virus		

Page 19 of 27



<b>Minimum Firewall throughput</b>	850 Mbps		
<b>Minimum Hardware Requirement</b>	- One (1) Gigabit Ethernet RJ45 WAN Port - Three (3) Gigabit Ethernet RJ5 LAN Ports - One (1) USB Port - 3G/4G Support		
<b>WIRELESS AP</b>			
<b>Brand / Model</b>			
<b>Quantity</b>	15		
<b>Class</b>	Enterprise Class Wi-Fi 5 or higher (Indoor)		
<b>Radio</b>	Dual Radio (2x2 MU-MIMO)		
<b>User/Device Authentication</b>	WPA2, and WPA3 with 802.1x or pre-shared key, WEP, Web Captive Portal		
<b>Accessories</b>	The Access point Should be provided with all necessary accessories (POE Injector, power cables, etc.)		

<p><b>Licensing / Support</b></p>	<p>Should be supplied with 3-Year Support Subscription: 24x7 Support by OEM or certified local technical engineers, Hardware Replacement, Firmware Upgrades</p>		
<p><b>INTEGRATED ENDPOINT SECURITY</b></p>			
<p><b>Brand / Model</b></p>			
<p><b>Central Management Features</b></p>	<ul style="list-style-type: none"> <li>- Simple and user-friendly UI</li> <li>- Remote deployment</li> <li>- Real-time dashboard</li> <li>- Software inventory management</li> <li>- Active Directory integration</li> <li>- Automatic group assignment</li> <li>- Dynamic access control</li> <li>- Automatic email alerts</li> <li>- Remote triggers</li> <li>- On-premise and cloud-based management</li> <li>- Allows administrators to remotely deploy endpoint software and perform controlled upgrades</li> </ul>		

<p><b>Security</b></p>	<ul style="list-style-type: none"> <li>- Native endpoint visibility, compliance control, vulnerability management, and automation</li> <li>- Remote web filtering, delivering web security and content filtering.</li> <li>- Provides botnet protection and granular application traffic control</li> <li>- Administrators can investigate in real time and set policies to automate responses, including quarantining suspicious or compromised endpoints to contain incidents and stem outbreaks</li> <li>- Ransomware protection, with the ability to roll back changes made by malicious programs, putting the endpoint back to a preinfectious state</li> <li>- Software Inventory Management provides visibility into installed software applications and license management to improve security hygiene</li> <li>- Real-time Endpoint Status always provides current information on endpoint activity and security events</li> </ul>		
<p><b>Supported Operating Systems</b></p>	<ul style="list-style-type: none"> <li>- Windows 10 and later</li> <li>- Windows Server 2012 and later</li> <li>- macOS 10.14, 10.15, 11+</li> <li>- iOS 9.0 and later</li> <li>- Android 5.0 and later</li> <li>- Linux Ubuntu, Red Hat 7.4 and later</li> </ul>		



<p><b>Licensing / Support</b></p>	<ul style="list-style-type: none"> <li>- Should include 3-Year license subscription for a minimum 400 endpoints, 80 mobile devices, and 15 servers.</li> <li>- Subscription license should include Telemetry, Remote Access (SSL and IPSec VPN), Vulnerability Scan, Malware, Web Security, Application Firewall, Application Control, Zero-day threat protection and Sandbox</li> <li>- 24x7 support by OEM or Certified local technical engineers</li> </ul>	
<p><b>CENTRALIZED MANAGEMENT AND SECURITY ANALYTICS</b></p>		
<p><b>Brand / Model / Product Name</b></p>		
<p><b>Centralized Management</b></p>	<ul style="list-style-type: none"> <li>- Central management for core firewall and all branch firewalls</li> <li>- Provide signature updates to managed devices</li> <li>- Use templates for firmware upgrades and zero-touch provisioning for Secure SDWAN, setting up VPN, and static route</li> <li>- Automate workflows and configurations for firewalls, switches, and wireless infrastructure</li> <li>- Scalable to manage to all devices</li> </ul>	

	<ul style="list-style-type: none"> <li>- Automated device configuration backups and revision control make daily administrative tasks easy</li> <li>- 3-Year cloud-based management subscription license for all devices</li> </ul>		
Security Analytics	<ul style="list-style-type: none"> <li>- Security Analytics with event correlation and real-time detection across all logs, with</li> <li>- Indicators of Compromise (IOC) service and detection of advanced threats</li> <li>- Integration with Firewall and endpoint security for deeper visibility and critical network insights</li> <li>- Centralized security operation center visibility for the attack surface with access to real-time log and threat data in the form of actionable views with deep drill-down capabilities, notifications &amp; reports, and predefined or customized dashboards for single-pane visibility and awareness.</li> <li>- Event Manager enables security teams to monitor and manage alerts and events from logs</li> <li>- Out of the box playbook templates allowing organization's security team's abilities to simplify investigation efforts through automated incident response</li> </ul>		

	<ul style="list-style-type: none"> <li>- Correlated log data with threat intelligence for analysis of real-time and historical events, providing context and meaning to network activity, risks, and vulnerabilities, attack attempts, operational anomalies, and continuous monitoring of sanctioned and unsanctioned user activity and investigation of Shadow IT</li> <li>- Predefines report templates, datasets and charts that are ready-to-use with sample reports</li> <li>- Should be a Cloud based platform delivering reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture.</li> </ul>		
<b>License</b>	- 3-Year cloud-based subscription license for Central Logging & Analytics		
<b>INSTALLATION &amp; CONFIGURATION</b>			
	<ul style="list-style-type: none"> <li>- Hardware installation</li> <li>- Certified specialist onsite for the duration of the configuration and migration execution</li> <li>- Design appropriate LAN, WAN, and DMZ security.</li> </ul>		



- Configure application control policies
- Configure AV and Web filtering policies
- Configure antispyware filtering
- Configure traffic shaping and ISP WAN load balancing
- Network segmentation and configure appropriate security policy per segment
- Configure branch firewalls and remote access connectivity policies
- Configure wireless network and relevant policies
- Configure endpoint security, centralized reporting and management
- Configure centralized management
- Configure centralized log analytics and standard security reporting
- Manufacturer certified training for 3 technical staff
- On the job training on basic management, operation and maintenance.
- Comprehensive testing and a detailed documentation on the configuration and settings of the delivered solution should be provided.

