Annex-1

MINIMUM SPECIFICATIONS	
Bid Announcement No:	(IUL)223/1/2022/25 (23·06·2022)
Bid Submission Deadline Date:	05th July 2022
Bid Submission Deadline Time:	10:00 am
Bid Submission Venue:	Tax Appeal Tribunal (G. Maagaha – 2nd Floor, Meeting Room)
Contact Number and email for Information:	procurement@tat·gov·mv Phone: 3015555

LOT 01 (FIREWALL & NAS STORAGE)

1. FIREWALL (QTY 1)

Specification for Next Generation and Cloud End point Security

		Yes/no
For networks in the range	10-50 users/devices	
CPU (Core/Threads)	x86 AMD CPU	
CPU (Memory)	6 GB DDR4	
NPU (Core/Threads)	Marvell NPU	
NPU (Memory):	4 GB DDR4	
Firewall throughput:	4,000 Mbps	
IPS throughput:	2,600 Mbps	
Threat Protection Throughput	900 Mbps	
Concurrent connections:	5000000	
New connections/sec:	69900	
Email Protection	126	
Webserver Protection	126	
Xstream SSL/ TLS (Mbps):	800 Mbps	
Xstream SSL/TLS Concurrent connections:	12288	
Storage (local quarantine/logs):	Integrated min 64 GB SSD	
Ethernet interfaces (fixed)	12 GbE copper, 2 x SFP fiber	
Power over Ethernet:	2 x GbE (max· 30 W pro Port)	
Management ports	1 x COM (RJ45), 1 x Micro-USB (cable incl·)	
Other I/O ports:	1 x USB 2·0 (front) 1 x USB 3·0 (rear)	
No· of expansion slots:	1	

ދިވެހިރާއްޖެ ޓެކްސް ޕީލް ޓްރައިބިއުނަލް، ހ.ޖ.ގ، ދ.ގާގަހ ވަނަ ފަންގިފުނި، ފ.ގުޅީ، 20152، ގ.ދ، ދިވެހިރާއްޖެ
info@tat·gov·mv www·tat·gov·mv 301 5555

Mounting:	Rackmount kit available (to be ordered separately)	
Power supply:	External auto-ranging AC-DC 100-240 VAC, 2,5 A@50-60 Hz 12 VDC, 12,5 A, 150 W Optional second redundant power supply UK power cord	
Including	1 year Standard Protection	
Warranty and Others	1 Year Product warranty and Service warranty Delivery and Setup with Installation and Configurations	
Professional Services	Installation & Configuration should be provided by vendor accredited engineers	

Base Firewall Features	
Performance	**Comply / Non-Comply**
Minimum 10 Gbps firewall throughput, 5,000,000 Concurrent connection and 69,000 New connection per second support from day one	
Minimum IPS throughput of 2.5 Gbps & IMIX throughput of 4 Gbps from day one	
Appliance should have minimum 900 Mbps of Threat Protection throughput & 800 Mbps SSL/TLS Inspection throughput	
Physical interfaces & power supply	
Appliance should have Integrated min. 64 GB SSD	
12 x GbE copper Ethernet Interfaces from day one	
Minimum 2 x SFP fiber Interface Ports	
Minimum one expansion slots and Multi-function LCD Display	
Appliance should have Connector for external redundant power supply	
General Management	
Manufacturer Authorization Letter is must to provide for both Solutions	
If both solutions are the same brand will be an advantage	
Both products Should be able to manage from same console	
Antivirus Solution should be cloud base and should be Cloude base and QTY 4 servers and 21 end points please make the changes	
The proposed system should have a purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators	
Should support two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN	
Should support features like advanced trouble-shooting tools in GUI (e.g. Packet Capture) &Full command-line-interface (CLI) accessible from GUI	

ޓެކްސް އަޕީލް ޓްރައިބިއުނަލް، ގ.މާގަނޑު، ދިލްބަރު ވަށަ ފަސްގަނޑުވަށަ، ބޮޑުތަކުރުފާނުމަގު 20152، މާލެ، ދިވެހިރާއްޖެ
info@tat.gov.mv www.tat.gov.mv 301 5555

Solution should support High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup	
Solution should support automated firmware update notification with easy automated update process and roll-back features	
Solution should support reusable system object definitions for networks, services, hosts, time periods, users and groups, clients, and servers	
Solution should have self-service user portal & role-based administration	
Solution should have configuration change tracking & Flexible device access control for services by zones	
Solution should support email or SNMPv3 trap notification options and Netflow support	
Solution should have Centralized management support via Cloud-based Unified Console	
Solution should support Automatic Email Notifications for any important event	
Solution Should support Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly, or monthly	
Solution should support API for 3rd party integration	
Solution should support Interface renaming	
Solution should have Remote access option for vendor Support	
Solution should have Cloud-based license management via Licensing Portal	
Solution should support Real-Time Flow Monitoring & Syslog support	
Solution Should have Instant Insights at a Glance with traffic light style indicators	
Solution should support Quick Drill-down Interaction with Any Control Center Widget	
Solution should support SNMP with a Custom MIB and support for IPSec VPN Tunnels	
Solution should Support for cloud formation templates	
Solution should Support Virtual WAN zone support on custom gateways for post deployment single arm usage	
Solution should have Stronger password hash algorithm (requires a password change)	
Centralized Firewall Management	
The proposed solution should support Cloud-based management and reporting for multiple firewalls provides group policy management	
Solution should have Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group	
Solution should support full historical audit trial and status monitoring of group policy changes	
Solution should support Backup firmware management which stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access	
Solution should support Firmware updates which offer one-click firmware updates to be applied to any device	

info@tat.gov.mv www.tat.gov.mv 301 5555

Solution should support Zero-touch deployment enables the initial configuration to be performed in Cloud-based management and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to Centralized cloud management portal	
Should support Firmware update scheduling	
Should support multi-firewall reporting across firewall groups	
Should support Save, schedule and export reports from Centralized cloud portal	
Firewall, Networking & Routing	
The proposed system should have Packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing	
Solution should have TLS inspection with high performance, support for TLS 1·3 with no downgrading, port agnostic, enterprise-grade polices, unique dashboard visibility, and compatibility troubleshooting	
Solution should have DPI Engine that provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single high-performance engine	
Accelerates SaaS, SD-WAN, and cloud traffic such as VoIP, video, and other trusted applications via Fast Path through the new Xstream Flow Processors·	
Solution should have Pre-packaged exception list & covers all ports/protocols	
Solution should Supports all modern cypher suites	
Solution should have User, group, time, or network-based policies and access time policies per user/group	
The Proposed solution should have Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to create complex NAT rules quickly and easily in just a few clicks	
Solution should support Flood protection: DoS, DDoS and port scan blocking	
Solution should have IPv6 Ready Logo Program Approval Certification and IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec	
Base Traffic Shaping & Quotas	
Solution should have Flexible network or user-based traffic shaping (QoS)	
Solution Should have et user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical	
Solution should have Real-time VoIP optimization and DSCP marking	
Secure Wireless	
Solution should have Simple plug-and-play deployment of wireless access points (APs) — automatically appear on the firewall control center	
Shouls support High performance with the latest 802·11ac, Wave 2 wireless standard, and powerful radios	

ﷺ ﷺ ﷺ ﷺ، ﷺ.ﷺ.، ﷺ ﷺ ﷺ، ﷺ 20152، ﷺ: ﷺ
info@tat·gov·mv www·tat·gov·mv 301 5555

Should support Centralized monitoring and management of APs and wireless clients through the built-in wireless controller	
Should support separate zones with client isolation options and Multiple SSID support per radio including hidden SSIDs	
Should support Channel width selection option	
Should Support for 802·11r (fast transition)	
Should support Hotspot support for (custom) vouchers, password of the day, or T&C acceptance	
Should support Wireless guest Internet access with walled garden options and Time-based wireless network access	
Authentication	
Solution should support Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+	
Should support Server authentication agents for Active Directory SSO, STAS, SATC	
Should support Single sign-on: Active directory, eDirectory, RADIUS Accounting	
Should support Radius Timeout with Two-Factor Authentication (2FA)	
Should support Client authentication agents for Windows, Mac OS X, Linux 32/64	
Should support Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos	
Should support Browser Captive Portal	
Should support Authentication certificates for iOS and Android	
Should support Authentication services for IPSec, SSL, L2TP, PPTP	
Should support Google Chromebook authentication support for environments with Active Directory and Google G Suite	
Should support API-based authentication	
Should support Azure AD integration	
Should support for creating users with UPN format for RADIUS authentication	
User Self-Serve Portal	
Should support Download SSL remote access client (Windows) and configuration files (other OS) or another authentication client	
Should support to Change username and password	
Should support to View personal internet usage	
VPN Client	
Should support IPSec and SSL support	
Should support Easy provisioning and deployment	
Should support Free (unlimited SSL remote access licenses included at no extra charge)	
Should support Authentication: Pre-Shared Key (PSK), PKI (X·509), Token and XAUTH	
Should support Intelligent split-tunneling for optimum traffic routing	
Should support NAT-traversal support	

ދިވެހިރާއްޖެ ޓެލެކޮމިއުނިކޭޝަންސް ކޯޕަރޭޝަން، ފ.ގާދިއްޔާ، ދަތުރުދާރު ގަސް ގާތް، ތ.ގ 20152، ގާދި، ދިވެހިރާއްޖެ
info@tat·gov·mv www·tat·gov·mv 301 5555

Should support Client-monitor for graphical overview of connection status	
Should support Mac and Windows Support	
Network Protection	
Intrusion Prevention (IPS)	
The proposed solution should have High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection	
Should support Zero-day threat protection and Perimeter Defenses	
Should support Granular category selection and Custom IPS signatures	
Should support IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added	
ATP	
Should support Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)	
Solution should have Intelligent firewall policies (block any compromised device accessing network resources)	
Clientless VPN	
Should have encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC	
Web Protection and Control	
Solution should have Fully transparent proxy for anti-malware and web-filtering	
Should have URL Filter database with categories backed by OEMLabs	
Should support Surfing quota time policies per user/group and Access time policies per user/group	
Should support Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email	
Should have Advanced web malware protection with JavaScript emulation and Pharming Protection	
Should support Live Protection real-time in-the-cloud lookups for the latest threat intelligence	
Should have Second independent malware detection engine for dual scanning	
Should support HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions	
Should have SSL protocol tunnelling detection and enforcement and Certificate validation	
Should support YouTube for Schools enforcement per policy (user/group)	
Should support Safe Search enforcement (DNS-based) for major search engines per policy (user/group)	
Should have Web keyword monitoring and enforcement to log, report, or block web content matching keyword lists with the option to upload customs lists	

info@tat.gov.mv www.tat.gov.mv 301 5555

Should Block Potentially Unwanted Applications (PUAs)	
Should ave Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users	
Cloud Application Visibility	
Solution should have Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated	
Should have Discover Shadow IT at a glance	
Should support Drill down to obtain details on users, traffic, and data	
Should support One-click access to traffic shaping policies	
Should support Filter cloud application usage by category or volume	
Should have Detailed customizable cloud application usage report for full historical reporting	
Application Protection and Control	
Should have Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level	
Should support Per-user or network rule application control policy enforcement	
Web & App Traffic Shaping	
Should support Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared	
Reporting	
Centralized Cloud Firewall Reporting	
Should have pre-defined reports with flexible customization options and create custom reports with powerful visualization tools	
Should support Intuitive user interface provides graphical representation of data	
Should have Report dashboard provides an at-a-glance view of events over the past 24 hours	
Should support Easily identify network activities, trends, and potential attacks	
Should support Easy backup of logs with quick retrieval for audit needs	
Should support Syslog data storage in Cloud portal, Syslog search and view	
Should have On-demand reporting in cloud portal	
Should support New Cloud Application (CASB) report	
On-Box Reporting	
Should support on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Search Engines, Web Servers, Web Keyword Match, FTP), Network and Threats (IPS, ATP, Wireless), VPN, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)	
Should support Built-in storage for log data storage for historical reporting	

20152 ، މާލެ
info@tat.gov.mv www.tat.gov.mv 301 5555

Should support Current Activity Monitoring: system health, live users, IPSec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks	
Should support Report anonymization	
Should support Report scheduling to multiple recipients by report group with flexible frequency options	
Should support to Export reports as HTML, PDF, Excel (XLS) and Report bookmarks	
Should support Syslog and Log retention customization by category	
Should support Full-featured Live Log Viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization	
Warranty and Support	
Should support Hardware warranty I year & RMA with Advanced Exchange	
Should have 24x7 Support via Telephone & Email	
Should support FREE Security Updates, Patches & Software Features Updates, Upgrades	
Subscriptions	
Should include licensing for Networking, Wireless, Unlimited Remote Access VPN, Site-to-Site VPN, & reporting	
Should include licensing for TLS and DPI engine, IPS, ATP,	
Should include licensing for Web Security and Control, Application Control	
Should include licensing for centralized management on a cloud console: Group firewall management, backup management, firmware update scheduling	
Should include cloud reporting for minimum 7days history for unlimited events	

ދިވެހިރާއްޖެ ޓެރެސްޓްރިއަލް ސަރވިސް ކޮމިޝަން، ގ.ފ.ގ.ބ، ފުވައްމުލަ ކައިރި، ފުވައްމުލަ، ދިވެހިރާއްޖެ، 20152
info@tat.gov.mv www.tat.gov.mv 301 5555

2. NAS Storage (QTY 1)

NAS Storage - Specifications

Item	Details	Yes/No
Product Authorization	Manufacturer Authorization should be provided	
Qty	One (01) Hardware Appliance with necessary Software	
CPU	Intel 4-core 2·1 GHz or above	
System Memory	4 GB RAM (Upgradable to 32GB or more)	
Ports	4 x RJ-45 1GbE LAN Port	
	2 x USB 3·0 Port	
	1 x eSATA Port	
PCIe	1 x Gen3 x8 slot (black, x4 link)	
RAID Types Support	Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10	
File Systems	Btrfs, EXT4, EXT3, FAT, NTFS, HFS+, exFAT	
Drive Bays	8 Bay	
Drive Bay Expansion	Should support up to 16 Bays in Total	
Hard Drives	3x12TB 7200RPM RAID5 HDD 5 Years warranty	
Compatible Drives	3·5" SATA HDD	
	2·5" SATA HDD	
	2·5" SATA SSD	
Hot Swappable Drive	All drives Should be Hot Swappable Drive	
General	Chat - Messaging service that runs locally, ensuring sensitive corporate information remains safely stored on company premises while providing users usability equivalent of public cloud services· Built to work with Office and Calendar seamlessly	
Management	Provides mail services with SMTP, IMAP, POP3 protocols,	
	SMTP authorization	
	SSL secured connection	
	SMTP relay with optional TLS secured connection	
	Multiple domain support	
	Supports LDAP/AD account	
	Create aliases for local users, groups, existing aliases and external mailboxes	
	Customization of auto BCC rules, SMTP/SMTPS port number, and the maximum size of a single email	
	Customize user and group policies on login methods, daily email traffic, and mail delivery	
	Delegate server management to normal users by function	

ޓެލެކޮމް ތަރައްޤީ ކޯޕަރޭޝަން، ގ.ދ.ދަރަ، ފަތުރަ ގަދަ ގަލޮޅު، ތ.ފ 20152، ދިވެހިރާއްޖެ
info@tat·gov·mv www·tat·gov·mv 301 5555

	Migrates emails from external mail servers: o Microsoft Exchange (no need for password collection) o Gmail o G Suite (no need for password collection) o Outlook o Office 365 o Yahoo Mail o General IMAP servers,	
Security	Spam filter: ransomware filter engine and DNS-based blackhole list	
	Spam reporting allows the system to learn for better spam identification	
	Spam engine supports Chinese segmented to effectively detect Chinese spam mail	
	Use the antivirus engine ClamAV or paid service McAfee to detect viruses in mail attachments	
	Google Safe Browsing database for detecting malicious URLs in the mail threads	
	Leverage third-party databases to enhance detection for malware, phishing contents and spam	
	Post-auditing and action policies for virus-infected mails	
	Threat Monitor provides security-related information: o General threat statistics in clear and interactive graphs o Real-time status of anti-spam and antivirus engines o DNSBL self-check result o Threat sources displayed in a world map o Statistics of blocked Inbound and outbound mail	
	Sender validation mechanism with SPF/DKIM and DMARC	
	Content Scan filters messages containing potentially dangerous content	
	Attachment filter to block specific file types	
	Message Content Protection (MCP) to prevent sensitive data leakage	
	Global black and whitelists to allow through or reject messages based on customized criteria	
Other Features		
Backup Features	Support local backup, network backup, and backup data to public clouds, Snapshot Replication - Maximum of shared folder snapshots: 1,024, Maximum of Replication: 64· RS1221-SYN	

ދިވެހިރާއްޖެ ޓެލެކޮމިއުނިކޭޝަންސް ކޯޕަރޭޝަން، ގ.ފ.ދ.ބ، ދިވެހިރާއްޖެ، ކޮމާޝަލް ކޮމްޕްލެކްސް، 20152، ފ.ކ، ދިވެހިރާއްޖެ
info@tat.gov.mv www.tat.gov.mv 301 5555

Cloud Sync	One or two-way synchronization with public cloud storage providers including Amazon Drive, Amazon S3-compatible storage, Baidu cloud, Box, Dropbox, Google Cloud Storage, Google Drive, hubiC, MegaDisk, Microsoft OneDrive, OpenStack Swift-compatible storage, WebDAV servers, Yandex Disk	
Form Factor (RU)	2 U	
Warranty	3 Years	
Professional Services	Installation & Configuration should be provided by vendor accredited engineers	

ޓެލެކޮމް ޑިވެލޮޕްމަންޓް ކޯޕަރޭޝަން، ގ.ދ.ގަދޫ، ދިވެހި ރާއްޖެ، ފޯސްކޮޅު 20152، ދ.ގދ، ދިވެހިރާއްޖެ
info@tat.gov.mv www.tat.gov.mv 301 5555