Pakistan Tobacco Board
Ministry of National Food Security & Research
Government of Pakistan

Terms of Reference (TORs)
&
Instructions to the firms / Organizations/Suppliers

Assignment Title:	**Up gradation of IT Infrastructure & Procurement of Next Generation Firewall**
Duration:	**3 months**
Location:	**Peshawar**
Reports to:	**Procurement Evaluation Committee OF PTB.**

Background:

Pakistan Tobacco Board (PTB) has been established under Pakistan Tobacco Board Ordinance, 1968 (I of 1968) mainly to regulate, control and promote cultivation and export of tobacco and tobacco products and to undertake research in tobacco and develop new tobacco growing areas. PTB intends to hire firms / Organizations/Suppliers for ‘‘Up gradation of IT Infrastructure & Procurement of Next Generation Firewall’’ in order to implement the E-office system through virtual private network at its regional offices.

Scope of Work:

i) Hardware /software etc installation, configuration and support services will be solely responsibility of the vendor.

ii) Software bidder will be responsible for the installation, configuration and support services.

iii) In case of any discrepancy or less item bid will be rejected. Compliance/ Checklist sheet with the Technical specification must be attached with the Technical proposal.

iv) In case of failure or malfunctioning of hardware equipment/component, a free replacement and installation of the device/part will be the responsibility of the vendor and on exchange bases as Free of Cost (FOC) under warranty.

v) Technical Support services should include resolution of complaints related to equipment.

vi) The drivers/applications support CD/media must be provided for hardware equipment compatible with the OS respectively (if any)

vii) Hardware devices having end of life must be communicated, moreover, nearly end of life hardware devices will not be acceptable.

viii) Vender will responsible for all types of IT equipment being delivered.

ix) 24 x 7 availability of hotline.

2. **Note**: *Vendor is solely responsible to provide the support services for the offered product even the support for the same product would have been discontinued by the OEM*

Details of the Task:

Next Generation Firewall

Technical Specifications **Qty 1**

General Requirements

i) The proposed NGFW should be the leader in the latest Gartner Magic Quadrant for Enterprise Network Firewalls for more than 10 years.

ii) The proposed NGFW should be ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Germany C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA and NEBS certified

iii) The proposed NGFW should require no reboot for checking and installing security updates

iv) The proposed NGFW should have integrated reporting capabilities requiring no additional hardware to generate reports

v) The proposed NGFW should identify applications regardless of port, SSL/SSH encryption, or evasive techniques employed

vi) The proposed NGFW should categorize unidentified applications for policy control, threat forensics, or application identification technology development

vii) The proposed NGFW should be a natively engineered security solution (Not an application control blade with underlying stateful inspection firewall)

viii) The proposed NGFW should be a natively engineered appliance with a single-pass parallel processing architecture for traffic processing

ix) The proposed NGFW should have integrated traffic shaping functionality (QoS) based on source/destination IP, port, protocol, and application

x) The proposed NGFW must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability

xi) The proposed NGFW should control access and enforce policies for websites and applications, including SaaS applications

xii) The proposed NGFW should have a single OS across all form factors

xiii) The proposed NGFW should support creating security policies to prevent credential theft

xiv) The proposed NGFW should support enforcing multi-factor authentication to internal applications

xv) The proposed NGFW should support an unfettered open API without a paywall (subscription) to access Dev toolkit, Tools and Scripts and samples

xvi) The proposed NGFW should support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed

xvii) The proposed NGFW must provide visibility and the ability to restrict applications using non-standard ports in a single security policy rule

xviii) The proposed NGFW must be able to tag objects to enable dynamic enforcement of policy no matter any changes to IP, area, or direction traffic originates from with no need to recommit policy

xix) The proposed NGFW must be able to provide Machine Learning algorithms for advanced protections directly from the NGFW with no external connections needed

xx) The proposed NGFW should grant easy OS updates without the need of certain combinations for hotfixes or patches to be in place

xxi) The proposed NGFW should have a feature of holding multiple OS images to support resilience and easy roll-backs during the version upgrades

xxii) The proposed NGFW should support enabling any new security offering without impacting the performance of the traffic flowing through it

xxiii) The proposed NGFW should have a feature of identifying what applications are hitting the security policies and migrating these policies into application based policies

Architecture, Physical & Performance Specifications

i) The proposed NGFW should deliver 1.4 Gbps of documented firewall throughput (Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions).

ii) The proposed NGFW should deliver 0.8 Gbps of documented threat prevention throughput (Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions)

iii) The proposed NGFW should deliver 0.6 Gbps or above of IPsec VPN throughput
(IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled)

iv) The proposed NGFW should support 64,000 Max sessions

v) The proposed NGFW should support 11,000 new connections per second (measured with application-override utilizing 1byte HTTP transactions)

vi) The proposed NGFW should support the addition of virtual systems for future expansion

vii) The proposed NGFW must support minimum of 7 x 1G RJ45

viii) The proposed NGFW should support 1 x 10/100/1000 out-of-band management port ,1 x RJ45 console port , 2 x USB port

ix) The proposed NGFW should support Active/Active, Active/ Passive & Clustering deployments

x) The proposed NGFW should support state full session maintenance in the event of a fail-over to a standby unit

xi) The proposed NGFW should support the High Availability feature for either NAT/Route or transparent mode

xii) The proposed NGFW should support multiple heartbeat links

xiii) The proposed NGFW should support L3, L2, transparent and tap mode deployments

Security Policy Control features

i) The proposed NGFW should support creating security policies based on Layer 7 applications irrelevant to the TCP/UDP port number (non-profile-based application control)

ii) The proposed NGFW should support the management of unknown traffic (unidentified applications) through security policies

iii) The proposed NGFW should have a built-in security policies optimization tool which facilitates converting legacy Layer 4 port-based security policies to Layer 7 application-based ones

iv) The proposed NGFW should support enforcing security policies based on a schedule

v) The proposed NGFW should simplify rule use tracking via a timestamp for the most recent rule match, a timestamp for the first rule match, and a rule hit counter

Advanced Threat Prevention Features

i) The proposed NGFW should protects networks by providing multiple layers of prevention, confronting threats at each phase of an attack

ii) The proposed NGFW should detect and block threats on any and all ports instead of invoking signatures based on a limited set of predefined ports

iii) The proposed NGFW should benefit from other cloud-delivered security subscriptions for daily updates that stops exploits, malware, malicious URLs, command and control (C2), and spyware

iv) The proposed NGFW should provide protections against unknown threats instantly by embedding ML in the core of the firewall to provide inline signature-less attack prevention

v) The proposed NGFW should utilize Inline malware protection—through signatures based on payload, not hash

vi) The proposed NGFW should continuously collect telemetry to enable data-intensive ML processes to automatically compute and recommend policy changes

vii) The proposed NGFW should use cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW

viii) The proposed NGFW should leverage heuristic-based analysis detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks

ix) The proposed NGFW should support creating custom signatures, which allows tailoring intrusion prevention capabilities to a network’s unique needs

x) The proposed NGFW should support other attack protection capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against evasion and obfuscation techniques

xi) The proposed NGFW should employ natively integrated defensive technologies to ensure that, when a threat evades one technology, another catches it

xii) The proposed NGFW should inspect and classify traffic as well as detect and block both malware and vulnerability exploits in a single pass

xiii) The proposed NGFW should comb each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload

xiv) The proposed NGFW should analyze the context provided by the arrival order and sequence of multiple packets to catch and prevent evasion techniques

xv) The proposed NGFW should support protocol decoder-based analysis

xvi) The proposed NGFW should provide protocol anomaly-based protection

xvii) The proposed NGFW should leverage inline, stream-based detection and prevention of malware hidden within compressed files and web content

xviii) The proposed NGFW should provide protections against payloads hidden within common file types, such as Office/Microsoft 365 documents and PDFs#

xix) The proposed NGFW should enable the correlation of a series of related threat events (e.g., from Threat Prevention logs) that, when combined, indicate a likely attack

xx) The proposed NGFW should have an option of configuring exception

xxi) The proposed NGFW should be able to detect & prevent the malware by scanning different file types

xxii) The proposed NGFW should be able to identify malwares coming from incoming files and malwares downloaded from Internet

xxiii) The proposed NGFW should provide an option to create custom signature for applications

xxiv) The proposed NGFW should have all major applications signatures and it should able to understand well known application like P2P and voice without any dependency on the port

xxv) The proposed NGFW should enforce inline deep learning for real-time enforcement for new and unknown command and control

xxvi) The proposed NGFW machine learning and deep learning models should be aligned to key protocols, such as SSL, HTTP, unknown UDP, and unknown TCP

xxvii) The proposed NGFW should use ML-based analysis to identify advanced DNS-based threats

xxviii) The proposed NGFW should utilize a cloud-based database which contains tens of millions of known malicious domains, enabling the blocking of phishing, malware, and other high-risk categories

xxix) The proposed NGFW should provide threat reporting capabilities that allow full visibility into DNS traffic, along with the full DNS context around security events and traffic trends over time

xxx) The proposed NGFW should enable forging a response to a DNS query for a known malicious domain and cause that malicious domain name to resolve to a definable IP address given to the client to identify infected hosts

xxxi) The proposed NGFW should allow defining separate policy actions as well as a log severity level for a specific signature type

xxxii) The proposed NGFW should identify the use of DGAs, which generates random domains on the fly for malware to use as a way to call back to a C2 server

xxxiii) The proposed NGFW should identify DGA (Domain Generation Algorithms) domains based on dictionary words

xxxiv) The proposed NGFW should prevent the use of DNS tunneling, which exploits the DNS protocol to tunnel malware and other data through a client-server model

xxxv) The proposed NGFW should disrupt ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network

xxxvi) The proposed NGFW should leverage predictive analytics that protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors

xxxvii) The proposed NGFW should prevent fast flux domains

xxxviii) The proposed NGFW should protect against domains surreptitiously added to hacked DNS zones of reputable domains

xxxix) The proposed NGFW should prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet

xl) The proposed NGFW should prevent dangling DNS attacks

xli) The proposed NGFW should prevent attackers from directing users to malicious domains with the use of a wildcard DNS record

xlii) The proposed NGFW should prevent techniques that exploit DNS protocol to tunnel malicious payloads into networks

xliii) The proposed NGFW should protect users from connecting to domains that can be used to launch DDoS attacks

xliv) The proposed NGFW should support traffic static analysis

xlv) The proposed NGFW should support traffic dynamic analysis

xlvi) The proposed NGFW should support advanced file analysis with URL crawling to prevent multistage, multi hop attacks

xlvii) The proposed NGFW analysis environment should replicate macOS, Android, Windows XP/7/10, and Linux

xlviii) The proposed NGFW file analysis should support PE files (EXE, DLL, and others), all Microsoft Office file types, Mac OS X files, Linux (ELF) files, Android Package Kit (APK) files, Adobe Flash and PDF files, archive (RAR and 7-Zip) files, script (BAT, JS, VBS, PS1, Shell script, and HTA) files, analysis of links within email messages, and encrypted (TLS/SSL) files

xlix) The proposed NGFW support protocols should be SMTP, POP3, SMB, FTP, IMAP, HTTP, and HTTPS

l) The proposed NGFW should generate signatures based on the malware payload of the sample and tested for accuracy and safety

li) The proposed NGFW should provide protection updates for unknown malware within seconds

Advanced URL Filtering

i. The proposed NGFW should possess a patented inline real-time web threat prevention capability which uses cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time

ii. The proposed NGFW machine-learning models should get retrained frequently, ensuring protection against new and evolving never before-seen threats (e.g., phishing, exploits, fraud, C2)

iii. The proposed NGFW should protects against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding

iv. The proposed NGFW URL database should maintain hundreds of millions of known malicious and benign URLs categorized through a combination of static, dynamic, machine learning, and human analysis

v. The proposed NGFW should be allow classifying websites based on site content, features, and safety, and includes more than 70 benign and malicious content categories

vi. The proposed NGFW should support risk rating which scores URLs on a variety of factors to determine risk

vii. The proposed NGFW should have multi-category support, which categorizes a URL with up to four categories, allowing for flexible policy and the creation of custom categories

viii. The proposed NGFW should detect and prevent credential theft by controlling sites to which users can submit corporate credentials based on the site’s URL category

ix. The proposed NGFW should se ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts

x. The proposed NGFW allow designating multiple policy action types based on URL categories or criteria

xi. The proposed NGFW should apply URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies

xii. The proposed NGFW should apply URL filtering policies when end users attempt to view the cached results of web searches and internet archives

xiii. The proposed NGFW should prevent inappropriate content from appearing in users’ search results

xiv. The proposed NGFW should enable administrators to notify users of a violation using a custom block page

xv. The proposed NGFW should support crawling and analysis in 41 languages

User Identification & Authentication Features

i. The proposed NGFW should support identifying user-id by integrating with Active Directory through WinRM and WMI

ii. The proposed NGFW should support identifying user-id by integrating with Exchange through WinRM and WMI

iii. The proposed NGFW should support identifying user-id by running as syslog receiver

iv. The proposed NGFW should support identifying user-id by Integrating through XML APIs with Third Party solutions

v. The proposed NGFW should support identifying user-id through captive portal

vi. The proposed NGFW should support Identifying user-id in terminal servers

vii. The proposed NGFW should support identifying user-id by running an agent at user machines

viii. The proposed NGFW should have direct Multi-Factor Authentication integration with RSA, Okta, PingID and Duo

ix. The proposed NGFW should support SSO authentication

x. The proposed NGFW should support multiple server profiles like SAML 2.0, Radius, LDAP, Tacacs+, and Kerberos.

Advanced Mobility & Host Information Profiling Features

i. The proposed NGFW should offer a remote user VPN agent for Windows, MAC, Linux, Chrome, iOS, and Android

ii. The proposed NGFW should support app-Level VPN for iOS and Android devices

iii. The proposed NGFW should have support portal based and clientless SSL VPN

iv. The proposed NGFW should support MFA

v. The proposed NGFW should offer a host information check feature by collecting & reporting device information & attributes. Host Information Profiling attributes based on Managed/Unmanaged certificates status, OS type, Client version, Host name, Host ID, Serial number, Mobile model, Phone number, Root/Jailbroken status, Passcode presence, Installed Applications, Patch presence & status, Firewall agent presence & status, Antimalware agent presence & status, Disk backup agent presence & status, Disk encryption agent presence & status, DLP agent presence & status, process list presence & status, registry key presence & status and Plist presence & status

vi. The proposed NGFW should support enforcing security policies based on device/host information profiles

vii. The proposed NGFW should support the integration with Third Party MDM solutions like AirWatch or MobileIron

viii. The proposed NGFW should support split tunneling based on IP addresses, domains and applications

ix. The proposed NGFW should support VPN authentication override using cookies

x. The proposed NGFW should support the exclusion of video traffic from main remote user VPN tunnel

xi. The proposed NGFW should support trusted root certificates push to remote VPN user devices to help enable features like SSL offload

xii. The proposed NGFW should support VPN gateway selection criteria based on source user-id, region, OS and IP address

Management, Logging & Reporting Features

i. The proposed NGFW should offer a Command Line Interface (CLI)

ii. The proposed NGFW should offer a built-in web interface, non Java base (GUI)

iii. The proposed NGFW should support XML Rest API based management

iv. The proposed NGFW should have a commit-based configuration management

v. he proposed NGFW should support config-audit by comparing running config against candidate config

vi. The proposed NGFW should offer an interactive graphical summary around the applications, users, URLs, threats, and content traversing the network

vii. The proposed NGFW should offer a customized graph-based network activity for applications using non-standard ports

viii. The proposed NGFW should offer a customized graph-based blocked activities which includes blocked applications activity, blocked users activity, blocked content activity, blocked threats activity, and security policies blocking activity

ix. The proposed NGFW should offer a customized graph-based tunnel activities including tunnel ID/Tag, tunnel application usage, tunnel user activity, and tunnel ip source/destination activity

x. The proposed NGFW should support custom reporting with the ability to generate a report per user, user group and application

xi. The proposed NGFW should support exporting reports to PDF and sending reports by email

xii. The proposed NGFW should have a dedicated SaaS applications usage report

xiii. The proposed NGFW should have dedicated log sets for traffic, threats, URL filtering, data filtering, file control, user id mapping, authentication, configuration, system and alarms

xiv. The proposed NGFW should support custom admin roles

xv. The proposed NGFW should allow administrators to work directly on the appliance, and make configuration changes as needed, without having to log in to a central manager

xvi. The proposed NGFW should allow central administrators to monitor and view the changes made by local administrators

xvii. The proposed NGFW management should be done directly through the appliance without the need of installing any clients or virtual machines

xviii. The proposed NGFW should offer the ability to choose which firewall administrator’s configuration changes to be committed on the firewalls

xix. The proposed NGFW should offer the ability to quickly roll back changes from specific users and restore configurations

Three (03) years license:

xx. Advance Threat prevention subscription.

xxi. Sandboxing subscription.

xxii. Advanced URL Filtering Subscription.

xxiii. DNS Security subscription.

xxiv. SD-WAN

Qualification and Experience:

The project/Assignment is open for national firms / Organizations/Suppliers having sound experience in the relevant field, specifically;

i. At least 10 years of experience in supplying similar nature of the software to any Public and Private Sector Organization.

ii. The firms / Organizations/Suppliers must provide an affidavit on the Stamp Paper attested by Notary Public which certifies to provide One -years warranty/guarantee after installation for IT equipment's/software.

iii. The firms / Organizations/Suppliers must provide an affidavit on the Stamp Paper duly attested by Notary Public that the bidder is not blacklisted by any government / semi government / public Department.

iv. The firms / Organizations/Suppliers shall be authorized distributor/partner/reseller of OEM.

v. The firms / Organizations/Suppliers Certified Resource of the quoted brand

vi. Proven track record of working on similar assignments, particularly on Firewall supply

vii. The firms / Organizations/Suppliers have a valid Registration Certificate for Income Tax, Sales Tax and/or other allied agencies / organizations / regulatory authorities

viii. The firms / Organizations/Suppliers must have multiple offices in different cities in Pakistan.

ix. The firms / Organizations/Suppliers must be registered in Pakistan and must adhere to all legal requirements to operate in Pakistan.

x. The firms / Organizations/Suppliers should have very good understanding of government functioning and processes as evidenced in the past experience.

xi. The firms / Organizations/Suppliers should have strong skills and knowledge of international standards and control frameworks.

xii. The firms / Organizations/Suppliers are an Active Taxpayers as per Federal Board of Revenue (FBR)'s database i.e. Active Taxpayers List (ATL)

Timeline of the project:

i. Delivery Time of hard ware within 4 weeks after the selection of the firm / Organization/Supplier.

ii. Installation / configuration within 2 week after delivery of hardware

iii. Testing of the system within 01 week after the Installation / configuration

Time Schedule for Deliverables:

Table 1

Deliverable	Date/Time schedule
Delivery of hard ware	Within 04 Weeks of signing of contract
Installation / configuration	Within 06 Weeks of signing of contract
Testing of the system	Within 07 Weeks of signing of contract

Terms of Payment

The firm/organization/supplier shall be paid as per the following payment schedule:

Table 2

No. of Installments	Percentage of contract price	Milestones	Timelines
Installment 1	40%	Delivery of hard ware	Within thirty days on receipt and approval of Invoice
Installment 2	30%	Installation / configuration	-do-
Installment 3	30%	Testing of the system	-do-

Review procedure to Monitor Pace of Work

Review meetings would be held as per schedule given below at Conference Room, Pakistan Tobacco Board office Peshawar, to review the progress of work and provide guidance to the firm/ Organization/Supplier for ensuring consistency of review work:

Table 3

Sr. No	Description	Timelines
1	Progress Review Meetings	On Fortnightly basis

*****