The Bank of Khyber

Information Technology Division

TENDER

The Bank of Khyber invites two separate sealed envelopes, One for Technical Proposal and One for Financial proposal of the following branded items as per the following specifications:

Lot: 1 - Routers

Specifications **Details**

QUANTITY : 40

S.NO	Requirement	Yes	No
	The proposed product should support :		
1	At-least 8 x 1G Copper RJ45 Interfaces		
2	High Availability in Active/ Active, Active/Passive and Cluster		
3	Any port of any type to be used as High Availability monitoring port		
4	Firewall throughput of at-least 2.7Gbps		
5	IPSEC VPN Throughput of at-least 1.8Gbps		
6	Minimum concurrent sessions of 1.2 Millions		
7	Minimum New Sessions/Second TCP of 28,000		
8	SSL Inspection Throughout of at-least 160 Mbps		
9	Application Aware controlling of at-least 600 Mbps		
10	Threat Protection Throughput of 180 Mbps		
11	Working as a Wireless Controller		
12	2-Factor authentication (on-device) for administrator login		
13	To be managed from On-Premises Management solution		
14	To be managed from Cloud Management Solution without additional cost & license		
15	The proposed product should support SSH/TELNET/HTTP/HTTPS for remote management of the device		
16	Stateful session maintenance for traffic including VPN traffic in the event of a fail-over to a standby unit.		
17	High Availability feature must be supported for either NAT/Route, Transparent or hybrid mode while running both NAT/Route and Transparent configurations simultaneously		
18	More than two heartbeat links, any of the interfaces must be configurable as a heartbeat interface.		
19	VLAN & PPPoE based interfaces along with Interface based Zoning		
20	IPv4 and IPv6		
21	Link Load Balancer without any addition of hardware or license		
22	Inbuilt 2 factor authentication services without the need of a third-party server and database using tokens (Either Hardware or Software)		
23	SSL Encryption, Decryption and Re-Encryption on the same device itself without any additional hardware.		
24	RESTFul API		
25	Security inspection inside dedicated processor.		
26	Integration with Microsoft Active Directory/Radius Server/TACACS+		

	Server		
27	Single-Sign-On through Active Directory Polling Mechanism		
28	Single-Sign-On through Single Sign On agent providing a buffer zone between the Firewall and Authentication Database		
29	User and device based Security policies		
30	Data Leak Prevention & Internal Server Load Balancer without any addition of external hardware		
31	Traffic shapping based on Username, IP address, Applications, Source Addresses, Destination addresses, URL Category in Inbound and Outbound Direction		
32	Remote logging		
33	SYSLOG logging to at-least 3 syslog servers with Log Format in Default Syslog, CSV (Comma Separated Values), CEF (Common Event Format)		
34	Dynamic Routing protocol (RIP-V1, RIP-V2, OSPF, BGP, ISIS, RIPng, OSPFv3), Static Routing and Policy Based Routing		
35	The proposed product latency should not exceed from 3 µs		
36	The Vendor of proposed product should be in MQ Leader Quadrant of UTM Firewalls		
37	Flow mode & Proxy Mode based traffic flow & Inspection		
38	ICAP protocol		
39	The Vendor of proposed product should be in MQ Leader Quadrant of Enterprise Firewalls		
40	Remote access VPN Client with functionality of IPSEC and SSL VPN simultaneously		
41	Remote Access Client VPN for IPSEC/SSL VPN should not add any cost or additional license for VPN Connectivity		
42	logical isolation of device with at-least 10 Logical devices		
43	Not be more the 2-Rack-Unit		
44	Hardware accelerated IPSEC (DES, 3DES, AES128, AES192, AES256) encryption/decryption		
45	The proposed product should support DH Groups 1,2,5,14,15-21		
46	The proposed product should support IPSEC (SHA1, SHA256, SHA384, SHA512) hashing algorithms		
47	Of accommodating multiple Proxy-IDs in an IPSEC VPN Site to Site VPN		
48	NAT traversal		
49	Hub and Spoke Site to Site IPSEC VPN architecture		
50	DDNS & Split DNS support		
51	The system shall provide IPv6 IPsec feature to support for secure IPv6 traffic in an IPsec VPN.		
52	Proxy Based AV Inspection as well as Flow Based AV Inspection		
53	Tprotection to communication with Malicious IP/Domain/Botnets		
54	Integrated Web Content Filtering solution without external solution, devices or hardware modules.		
55	To enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.		
56	NetFlow and Sflow		
57	SNMP v1/v2c and SNMP v3		

58	Network Time Protocol		
59	Explicit Forward Web Proxy		
60	For 8x5 Return to Factory Support for 1 Year (**Mandatory**)		

Note:-
The successful bidder will provide **Onsite**, 05 days professional training for administration of proposed product.

Trainer's travelling, boarding, lodging and any other relevant expanses should be covered by the successful bidder.

LOT: 2 - WEB APPLICATION FIREWALL

Technical Specifications for the Web Application Firewall device (Bidder's proposal should strictly conform to the following technical specifications)
Note: Bidders should carry out their own investigation to capture any additional information required for licensing and sizing for the proposed solution.

No.	Requirements	Compliance (Yes/No/Partial)	Remarks
1.	**Web Application Firewall Specs**		
1.1.	The proposed solution MUST be Hardware based		
1.2.	Support both a positive security model and a negative security model, or similar terminology *Refer to Note # (1)*		
1.3.	MUST inspect HTTP, HTTPs, & FTP to prevent attacks		
1.4.	Provide Protection against OWASP Top Ten		
1.5.	MUST be PCI\DSS compliant		
1.6.	Support flexible deployment options (please mention)		
1.7.	MUST support SSL offloading		
1.8.	MUST prevent access by unauthorized IP(s) and subnets		
1.9.	Out of the box, The WAF should have a database of signatures, designed to detect known problems and attacks		
1.10.	Support automatic updates to the signature database, ensuring complete protection against the latest application threats.		
1.11.	Ability to correlate multiple security events together to accurately distinguish between good and bad traffic		
1.12.	Supports custom security rules, Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria		

1.13.	MUST address most of the Open Web Application Security Project (OWASP) Top Ten		
1.14.	Should have Reputational Base Service which can provides a near- real time live feed of the following known attack sources:-		
1.15.	▪ Malicious IPs		
1.16.	▪ Phishing URLs		
1.17.	▪ Anonymous Proxies		
1.18.	▪ Tor IPs		
1.19.	Should have "anti-automation" protection, which can block the automated attacks using hacking tools, scripts, framework etc		
2.	**Management and Reporting**		
2.1.	MUST Inspect and monitor all HTTP data and the application level including HTTP headers, form fields, and the HTTP body		
2.2.	Support proper reporting and logging facilities		
2.3.	Report events via standard mechanisms, for example, to a sys log or SNMP server or a SIEM solution		
2.4.	Customized logging levels and filters		
2.5.	Generates custom or pre-defined graphical reports		
2.6.	High-level dashboard of system status and Web activity		
2.7.	Ability to integrate with proposed DB Security		
2.8.	Ability to share threat logs with proposed DB to provide end-end threat visibility		
2.9.	Ability to integrate with standard Security Event Management tools and system		
2.10.	1. The solution should be able to locally store event (audit) information. 2. The solution should be able to locally store alert information. 3. The solution should be able to locally store traffic information. 4. The solution should be able to send all log types above to an external sys log server. 5. The alert information should contain at least the following information: 6. Source to Destination connection information 7.. Extensive packet header information 8. Raw and Hex body presentation for POST parameters 9. Full Parameter view 10. Highlighting the attack in the attack log 11. With cookie alerts show the alerted cookie and changed values 12. The solution should aggregate logging per day and per attack type 13. The log should show both original encoding		

	and decoded values for analysis 14. Log should be able to provide top attacks, top source and countries of attacks in GUI 15. Should be able to create customized reports 16. Should be able to provide PCI DSS compliance and reporting 17. Should be able to group incidents with violation correlation 18. The solution should have a dashboard for data analytics in which you can see: 19. Attacks per Country 20. Hits per Country 21. Data per Country 22. Exportable to PDF 23. Clickable view of the various attacks per website 24. Zoom-able world map with color coding of attacks 25. The solution should have a view of all blocked IP addresses and the blocked time period. 26. From the above view it should be possible to release the blocked IP addresses.		
2.11.	Solution must support on-board Anti-Virus without any additional software/hardware/third-party Anti-Virus		
2.12.	The Device must support Following deployment modes • Reverse Proxy • Offline Protection • Transparent Proxy/Inspection • WCCP		
2.13.	The device must support Policy-Based Routing		
2.14.	The device should support protection from DDoS.		
2.15.	The device should support Anti-Defacement.		
2.16.	The device should support load balancing based on Round-Robin, Weighted Round-Robin and Least Connection.		
2.17.	The solution should be capable of supporting persistency features like, Persistent IP, Persistent Cookies, Insert Cookies.		
3.	**Administration & Authentication**		
3.1.	Support web-based and CLI-based access methods		
3.2.	The solution should support role-based access control		
3.3.	The Solution MUST support SNMP V2c V3		
3.4.	The solution MUST support policy based authentication and authorization		
3.5.	Out-of- band management port		

3.6.	Out-of- band management port		
4.	**Vulnerability Assessment and Management**		
4.1.	WAF should provide a Vulnerability Assessment and provide a detailed Assessment Report for the monitored WEB Application(s)		
4.2.	Ability to measure compliance with industry standards and regulations		
5.	**Hardware Requirement**		
5.1.	System Throughput – 1Gbps HTTP & 500Mbps HTTPS		
	SSL/TLS Processing must be performed in Hardware/ASIC		
5.2	HTTP transactions per second : 40,000 minimum HTTPS transaction per second : 20,000 minimum		
5.3	HTTP Concurrent Connections: 125000 HTTPS Concurrent Connections: 85000		
5.3	Storage: 3TB Minimum		
5.4	RAM Minimum 8 Gb		
5.4	Application Licenses: Unlimited		
5.5	High Availability: Active/Passive, Active/Active, Clustering		
5.6	Support of 10/100/1000 Interface 6 x 1G Copper RJ-45.		
5.7	Support of SFP GE (Optical) x 2		
5.8	Power Supply: DUAL + HOT SWAPPABLE		

Web Application Firewall (WAF) Notes:

(1) WAF Security Models

a. Negative Security Model:

i. Explicitly defines known attack signatures, transactions with content matching known attack signatures are blocked, everything else is allowed

ii. Includes a pre- configured comprehensive and accurate list of attack signatures.

iii. Ability to modify or add Signatures by the administrator

iv. Ability to detect known attacks at multiple levels, including operating system, Web server software and application-level attacks.

1. Cross site scripting (XSS)
2. Layer 4 & Layer 7 DoS and DDoS
3. SQL Injection
4. SQL LDAP and XPath Injections
5. Generic Attacks
6. Brute Force
7. Trojans
8. Known Exploits

9. Information Disclosure
10. Form Field Parameter Tampering and HPP tampering
11. Session high jacking
12. Cookie manipulation and poisoning
13. Buffer Overflows
14. Bad Robot
15. Credit Card Detection
16. Protection against known database and Web server vulnerabilities
17. Forceful browsing
18. Broken access control
19. Request smuggling

v. Ability to detect known malicious users who are often responsible for automated and botnet attacks. Malicious users may include malicious IP addresses, anonymous proxy addresses, and TOR networks.

b. **Positive Security Model:**

i. Explicitly states what input is allowed; everything else is blocked
ii. Includes URLs, directories, cookies, form fields and parameters, and HTTP methods.
iii. Ability to learn the Web Application structure and elements.
iv. In learning mode: WAF should be able to be used for a period with a trusted set of users, and user input to various fields of the Web application is recorded, and should be able to recognize application changes while simultaneously protecting Web applications.
v. Based on the recording of this input, the acceptable values for input fields are learned.
vi. The learned values are used as the configuration for input checking in the positive security model.
vii. Ability to learn the structure and elements of the application (directories, URLs, parameters, cookies) Ability to learn expected the behavior from the user (i.e. expected value length, acceptable characters, whether the parameter value is read only or editable by the client and whether the parameter is required or optional).
viii. Ability to access and modify the learned configurations by an administrator.
ix. Quantity 01

Note:-

The successful bidder will provide 02 x OEM & 05 Days International professional classroom training for administration of proposed product.

BOK IT Personnel's travelling, boarding, lodging, commute and any other relevant expenses should be covered by the successful bidder.

LOT 3 NEXT GENERATION FIREWALL (Core)

Technical Specifications for the Next Generation Firewall devices (Bidder's proposal should strictly confirm to the following technical specifications)

Note: Bidders should carry out their own investigation to capture any additional information required for licensing and sizing for the proposed solution.

No.	Requirements	Compliance (Yes/No/Partial)	Remarks
5.	**Next Generation Firewall Specs**		
5.1.	IPv4 Firewall throughput 30 Gbps or higher		
5.2.	Firewall throughput (Packet per second 45Mbps or Higher)		
5.3.	Concurrent Sessions (TCP) 10 Million or above		
5.4.	New Sessions per second (TCP) 250,000 to 280,000		
5.5.	IPsec VPN throughput 22 Gbps or Higher		
5.6.	SSL-VPN Throughput 3.5 Gbps or Higher		
5.7.	Must Have Explicit Proxy feature having Web Filter, Application Control, Port Blocking, and Antivirus Scanning.		
5.8.	IPS Throughput Minimum 4 Gbps		
5.9.	Application Control Throughput 8 Gbps or Higher		
5.10.	NGFW Throughput Minimum 5 Gbps		
5.11.	Support automatic updates to the signature database, ensuring complete protection against the latest application threats.		

Hardware Requirement

GE RJ45 Interfaces	16
GE SFP Slots	Minimum 10
Console Port	1
Internal Storage	250 GB

1 Year Software license and operational support for the following:-

1. Antivirus.
2. Application Control.
3. Web filtering.
4. Data Leak Prevention.
5. Anti spam.
6. Intrusion Prevention System.
7. **Quantity** **01**

Note:-

The successful bidder will provide 02 x OEM & 05 Days International professional classroom training for administration of proposed product.

BOK IT Personnel's travelling, boarding, lodging, commute and any other relevant expenses should be covered by the successful bidder.

Lot: 4 – Video Conferencing			
Specifications		Details	
SR.	ITEM	DISCRIPTION	Compliance YES/NO
1	Video Resolution	Full HD (1080p 30fps) VC solution slide/desktop sharing	
2	Product Type Approval	Mandatory - Pakistan Telecommunication Authority	
3	Communication	H.323 and SIP Standards	
		Connect with Skype, Google Hangout, Skype for business, and Microsoft Lync.	
		Connectivity with existing system	
		64kbps-4mbps	
		RJ45 Network LAN (10/100/1000)	
		Manual bandwidth setting	
4	Camera	9X Optical zoom or better	
5	Multipoint	Multipoint – 03 sites	
6	PSTN Call	Any Mobile or Landline user.	
7	Meeting Recording	One touch recording.	
8	Video Resolutions	HD1080P (1920 x 1080) at 30fps	
9	Video Standards	H.264 HP, H.264 SVC, H.264, H.263+, H.263, H.261	
		H.239 dual video streams	
10	Video Inputs	Camera or equivalent	
		VGA/HDMI	
11	Video Output	HDMI X 2	
12	Audio Standards	G.711, G.722, G.722.1, G.728, G.722.1C	
13	Audio Features	Automatic gain control (AGC)	
		Advance noise reduction	
		Acoustic echo cancellation (AEC)	
14	Audio Input and Output	Audio Input	
		Audio Output	
		HDMI	
15	User Interface	Multiple layout styles	
		User-friendly OSD	
		Display / edit site name	
16	Networks	10/100/1000Mbps	
		NAT/firewall traversal	
		High Efficiency Lost Packet Recovery	
		API support via Telnet	
17	Security	AES (Advanced Encryption Standard) function (128-bit) and Password protection for system settings and for remote system management	
18	Web management tool	Remote management through the web	
		Live monitoring via the web	
		Firmware update via Ethernet/Internet	
		Phonebook download/upload/edit	
		Restore system settings	

19	Value-added features	Meeting recording	
		In meeting and offline recording	
		Save directly to USB flash drive	
		Supports screen re-layout during playback	
20	Warranty	One Year Comprehensive Warranty	
21	Document	Import documentation Letter from Manufacture/ Principle	

Installation and Provision of Video Conferencing Equipment

S #	Equipment	Qty.
A	Conference Room VC solution (Head Office) Full HD Video conferencing solution with Slide/ Desktop Sharing.	02
B	Cabling and Installation Complete cabling Installation and configuration of Video Conferencing equipment.	02

Lot 5 : Renewal of Licenses of IDS/IPS		
Specifications	**Details**	**Qty**
Annual renewal and maintenance support of IDS/IPS Licenses (Intrusion Detection System / Intrusion Prevention System).	IBM Security Network Protection XGS3100 - Primary Appliance	1
	IBM Security Network Protection XGS3100 - I.P Reputation Primary Appliance	1
	IBM Security Network Protection XGS3100 - Application / Web Control Updates –	1
	IBM Security Network Protection XGS3100 - SSL Inspection –	1

Lot 6 : Renewal of Licenses of Network Monitoring Software

Specifications	Details	Qty
Annual renewal and maintenance support of Solarwind Network Monitoring Software Licenses.	Net -Work Performance Monitor SL500	1
	Network Configuration ManagerDL500	1
	Net Flow Traffic Analyzer SL500	1
	Log & Event ManagerLEM30	1
	Web Performance Monitor	1
	Server & Application Monitor	1
	Patch Manager PM250	1
	Secure Managed File Transfer Server	5
	Secure FTP Server	2
	Device Tracker U2500	

TERMS & CONDITIONS

1. The Procurement shall be conducted in accordance with the Khyber Pakhtunkhwa Procurement Rules 2014 on **Single Stage Two Envelope Procedure**.
2. The Bank of Khyber invites two separate sealed envelopes, One for Technical Proposal and One for Financial proposal from TR1 partner for the supply and delivery of the Routers, Web Application Firewall, Next Generation Firewall, Video Conferencing System, Renewal of Licenses for IDS\IPS and Renewal of Licenses for Network Monitoring Software.
3. The bidder can apply for the whole Tender or for any one specific **LOT** as per his expertise.
4. The Technical bid should clearly mention Make, Model and Brand, (Specification of bid) without quoting the price and must mention the warranty period.
5. Company seal / stamp must be fixed on Technical Specification and Financial Proposal.
6. **If any firm fails to qualify the Technical Evaluation Criteria based upon Mandatory Requirements, then financial bid of the same will not be opened.**
7. **Mandatory Requirements are as follows:-**
    a. The bidder should provide the item manufacture's **TR1** authorization certificate.
    b. The bidder should provide **KPPRA/PPRA/SPPRA** registration Certificate with Technical Proposal.
    c. The bidder should provide **FBR** registration certificate with Technical Proposal.
    d. The bidder should provide an **undertaking** on stamp paper that it is not blacklisted by any of the Provincial / Federal Government or organization of the state / Federal Government in Pakistan.
    e. The bidder must submit **Annual Audited Report** for the last three years.
    f. The firm preferably has office in Peshawar and must submit a **List of Offices** across Pakistan.
    g. The bidder shall give at least **Five Relevant References** (Purchase Order) of similar equipment delivery / installation by their firm.
    h. The bidder shall have at least **Five Year Relevant Experience** for the supply of similar equipment.
    i. **Call Deposit** of Two percent (2%) of the total bid amount must be attached with financial proposal in separate sealed envelope in favor of Head IT Division, The Bank of Khyber **on or before 10:00 AM, 12-12-2017.**
8. **Tender bid opening will be held on Tuesday, 12-12-2017 at 11:00AM at BOK I.T Division**.
9. **Any bid submitted after due date and time will not be entertained.**
10. The Bank of Khyber will not be responsible for any costs or expenses incurred by bidders in connection with the preparation or delivery of bids.
11. The prices quoted shall remain valid for **120 days**, after the date of opening the tender.
12. Delivery of all items must be made within **(6 – 8)** weeks of issuance of purchase order.
13. All prices quoted must be inclusive of all Taxes applicable, such as GST, Income Tax, etc.
14. Rate should be quoted in words and figures.
15. **In case of failure to supply the item under specified time. The work order should be awarded to second lowest.**
16. Failure to supply items within **(6 - 8)** weeks' time period will invoke. In addition to that, two percent (2%) Call Deposit (CDR) amount will be forfeited**.**
17. Bidders must submit at least one bid that matches or is better than the required specifications and are free to quote more options each clearly marked as option 1, option 2 in separate envelops.
18. **No negotiations and revised bids will be allowed.**

I T Division, Head Office
The Bank of Khyber
4th Floor,
State Life Building, Peshawar.
Phone: 091-5279690, 091-5274399

The Bank of Khyber

Tender

The Bank of Khyber invites two separate sealed envelopes, One for Technical Proposal and One for Financial proposal from TR1 partner for the supply and delivery of the following items:-

1) **Router**
2) **Web Application Firewall**
3) **Next Generation Firewall**
4) **Video Conferencing System**
5) **Renewal of Licenses for IDS\IPS**
6) **Renewal of Licenses for Network Monitoring Software**

The Procurement shall be conducted in accordance with the Khyber Pakhtunkhwa Procurement Rules 2014 on **Single Stage Two Envelope Procedure**.

Terms and conditions for the above purchase equipment can be seen on website http://www.bok.com.pk/downloads/

All bids must be accompanied by a call deposit of two percent (2%) of the total bid amount in favor of The Bank and must be delivered to the HEAD IT DIVISION, THE BANK of KHYBER **on 12-12-2017 Tuesday at 10:00AM and the opening timings is 11:00AM on same day at BOK I.T Division**.

IT Division, Head office

The Bank of Khyber

4th Floor,

State Life Building, Peshawar.

Phone: 091-5279690, 5274399.

UAN: 091-111-95-95-95

Fax: 091-5286769