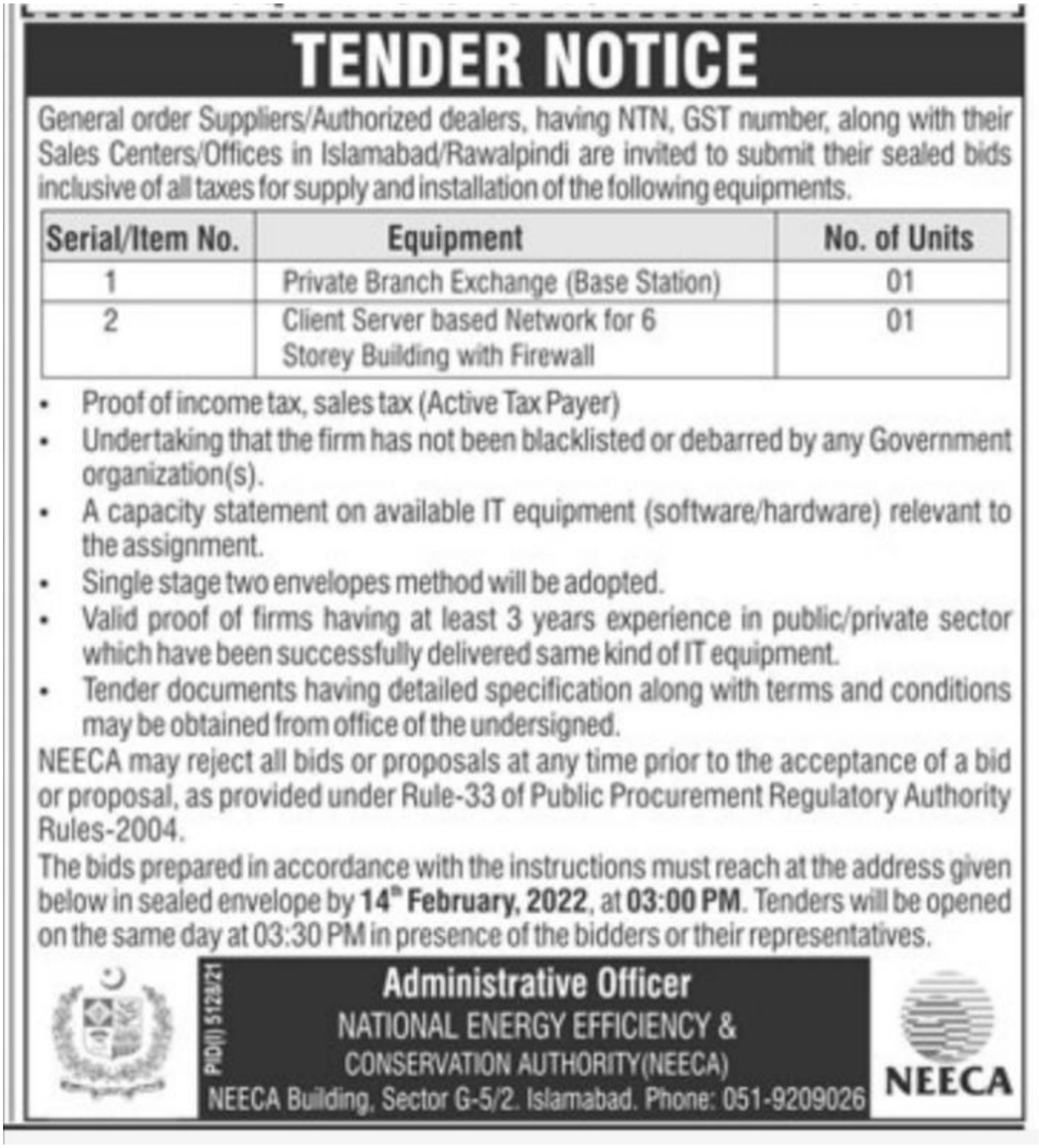

TENDER NOTICE

General order Suppliers/Authorized dealers, having NTN, GST number, along with their Sales Centers/Offices in Islamabad/Rawalpindi are invited to submit their sealed bids inclusive of all taxes for supply and installation of the following equipments.

Serial/Item No.	Equipment	No. of Units
1	Private Branch Exchange (Base Station)	01
2	Client Server based Network for 6 Storey Building with Firewall	01

- Proof of income tax, sales tax (Active Tax Payer)
- Undertaking that the firm has not been blacklisted or debarred by any Government organization(s).
- A capacity statement on available IT equipment (software/hardware) relevant to the assignment.
- Single stage two envelopes method will be adopted.
- Valid proof of firms having at least 3 years experience in public/private sector which have been successfully delivered same kind of IT equipment.
- Tender documents having detailed specification along with terms and conditions may be obtained from office of the undersigned.

NEECA may reject all bids or proposals at any time prior to the acceptance of a bid or proposal, as provided under Rule-33 of Public Procurement Regulatory Authority Rules-2004.

The bids prepared in accordance with the instructions must reach at the address given below in sealed envelope by **14th February, 2022**, at **03:00 PM**. Tenders will be opened on the same day at 03:30 PM in presence of the bidders or their representatives.

PID(I) 5128/21

Administrative Officer
NATIONAL ENERGY EFFICIENCY &
CONSERVATION AUTHORITY(NEECA)
NEECA Building, Sector G-5/2. Islamabad. Phone: 051-9209026

NEECA

Government of Pakistan
Ministry of Energy (Power Division)
National Energy Efficiency and Conservation Authority (NEECA)

TERMS AND CONDITIONS OF TENDER

1. Tender Format

Single stage two envelope bidding procedure under Rule 36 (b) of PPRA Rules 2004 will be adopted. Bids must be accompanied by a bank draft/pay order/call deposit from any schedule bank in favour of National Energy Efficiency and Conservation Authority (NEECA), as earnest money of Rs. 100,000/-. Bids received without earnest money will be rejected. Conditional bids will also be rejected.

2. Date and Time of Receipt of Tender

Bid documents duly completed should reach this office **on or before 14-02-2022, 03:00 P.M. on the tender closing date**. Bids received after the closing date and time will not be entertained. No telegraphic or faxed bid will be accepted. Bids shall be opened on the same date at **03:30 P.M.** in presence of bidders or their authorized representatives in the **Committee Room, NEECA Building, Sector G-5/2, Islamabad.**

3. Earnest Money

The bidder will attach bank draft/pay order/call deposit from any schedule bank of Rs. 100,000/-, in favour of **National Energy Efficiency and Conservation Authority (NEECA),** refundable on satisfactory completion of warranty period of equipment. Cheques will not be acceptable. Bids without valid earnest money shall not be entertained.

4. Prices

i. Bidders will be required to quote on (Standard Bidding Document) all prices ex-Islamabad in Pak Rupees inclusive of government taxes, charges, octroi, GST, transportation etc. and at specified site in Islamabad. Items should be duties and tax paid.

ii. The quotation should remain **valid for at least 90 days** from the date of opening the bid.

5. Technical Documents

i. All information provided in bid should also be adequately supported by relevant documents and technical brochures. Bidder may attach documents that highlight the competitive edge and unique features of their proposal.

ii. Manufacturer’s Authorization Letter is to be submitted along with the tender.

iii. Any specification or condition mentioned in tender document, if not found in bid document, shall give right to National Energy Efficiency and Conservation Authority (NEECA)to consider it as “condition not being met/fulfilled”.

6. Equipment

a. The equipment delivered should be new and in no case used or refurbished. The component of the equipment should be assembled by the manufacturer.

b. The equipment should be arranged through **legal channels** by providing all duties/taxes (if any) levied the government and towards this end, copies of the shipping documents will need to be deposited in NEECA.

c. The successful bidder shall submit original **Bill of Entry** and Packing list at time of delivery of equipment.

7. Office/Service Centre in Islamabad

The bidding firm having valid NTN and duly registered with FBR for Sales Tax must have proper office/service support centre in Islamabad.

8. Delivery Period

The supplier will be required (**DDP)** delivery of equipment at customer’s premises within **One month** from the date of issue of Purchase Order.

9. Warranty

03 Years comprehensive warranty for Private Branch Exchange (Base Station) and Client Server based Network for 6 Storey Building with Firewall from authorized manufacturer/ OEM dealer in Pakistan should be clearly specified.

10. SCOPE OF WORK FOR CLIENT BASED SERVER NETWORK FOR 06 STOREY BUILDING WITH FIREWALL

i) Hardware /software 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) Turnkey solution vendor must offer all items, incase of any discrepancy or less item bid will be rejected.

iv) Product Support Services must be within 24 hours

v) 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.

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

vii) All operating system support, compatibility issues and setup/configuration, services are the responsibility of equipment provider.

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

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

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

xi) 24 x 7 availability of hotline.

xii) 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.

11. Evaluation Criteria

Contract will be awarded on the basis of item-wise lowest cost to the party which meet specifications given in the bidding proforma, instructions mentioned in this tender document and the advertisement.

12. Schedule of Payment

No advance payment shall be made against the purchase of equipment. Bills of payment shall be submitted to NEECA after delivery of equipment on site with necessary installation, configuration and training where required.

13. Disqualifications

Offers are liable to be rejected if, there is any deviation from the instructions as laid down in the bid document i.e.

a. Technical details/brochures and literature pertaining to the offered items are not attached.

b. Tenders are submitted without the required earnest money.

c. Bids/Tenders are received after specified date and time of receipt.

d. Specifications and other requirements are not properly adhered to or manufacturer's brochure shows specifications different from those given in tender.

e. GST/NTN certificate is not attached.

f. Shipping/documents demonstrating that the equipment arranged through legal channels.

g. Service centre is not in Islamabad and service response time exceeds 24 hours.

h. Any other major discrepancy found in the proposal.

14. Clarifications required if any

If further clarification is required regarding this tender, the intended bidder is advised to contact in writing to Director General (HR & SS), National Energy Efficiency and Conservation Authority (NEECA), NEECA Building, Sector G-5/2, Islamabad. The response to clarification will be sent to the bidder.

15. Rights reserved

National Energy Efficiency and Conservation Authority (NEECA) reserves the right to accept or reject any or all the bids under provisions of Rule 33 of PPRA Rules 2004. NEECA also reserves the right to increase/decrease the quantity of equipment or may withdraw the tender without assigning any reason thereof.

STANDARD BIDDING DOCUMENT

Item: Private Branch Exchange (Base Station)

Detailed specification		Conformation to the specification	
		Yes	**No**
IP PBX	06 CO Lines		
	10 Digital Extensions		
	100 Analoge Extensions		
	Expandable up to 500 Lines		
Compatibility	SIP Phone		
	PRI		
	VoIP		
	VPS		
	Voice mail		
	DISA		
Phone Sets	1.Console set with extra Operator keys Addson (**Quantity: 1**)		
	2.Phone Set Digital for executive **(Quantity: 10)**		
	3.Analoge Phone set **(Quantity: 200)**		
Complete Block Wiring, with Termination and Installation	02 pair pvc Cable		
	0. 4mm,		
	UG Cable 50pair		
	UG Cable 100Pair		
	Multi Cables for all floors		
	Duct pipe Face plates I/o box with accessories		
	DPs MDF and IDF		

Note: 03 (three) Years Parts/Labor OEM On Site warranty for all components with supplier on-site support.

Rate quoted per unit (Including taxes)	**Quantity**	**Total Amount** **(In Pak Rupees)**
	01 Private Branch Exchange (Base Station)	

STANDARD BIDDING DOCUMENT

Item: Client Server Based Network for 06 Storey Building with Firewall

Sr.#	Description	Qty.	Delivery/Completion Time	Turn Key LOT
Firewall			**02 Months**	
1	Next Generation Firewall	1		
Core Switch Layer 3				
1.a	24 Port Layer 3 switch with all accessories, Installation and Configuration	2		
Access Switch Layer 2				
1	24 Port 10/100/1000 switch with all accessories, Installation and configuration	16		
2	12 Port 10/100/1000 switch with all accessories, Installation and configuration	3		
SFP				
1	Single Mode 1G SFP	38		
Passive Part				
1	Passive Networking	250Nodes		

Next Generation Firewall

Next Generation Firewalls Requirment	Compliance
1.1 Mandatory System Performance and scaling requirements:	
1.1.1 The Tenderer shall propose 1 Next Generation Firewalls, with three years of below subscription and support services.	
a. Application Visibility	
b. Advanced Intrusion Prevention System	
c. Full/Extended Antivirus Database, Anti-Spyware	
d. URL Filtering	
e. File Blocking and Filtering	
f. Quality of Service	
1.1.2 Quoted Firewall must be in the leaders' quadrant in Gartner's enterprise security firewall report for the last 7 years.	
1.1.3 Quoted Firewall must be rated 95% or above in the latest NSS lab Report.	
1.1.4 The Next Generation Firewall must deliver at least 1.8 Gbps of application firewall throughput with Application Visibility and User Identification enabled utilizing 64K HTTP transactions, using real-world enterprise traffic mix.	
1.1.5 When enabled below threat features, Firewall should deliver at least 850 Mbps throughput utilizing 64K HTTP transaction using real-world enterprise traffic mix:	
a. Advanced/Extended Intrusion Prevention System with all signatures/anomalies and severities	

b. Full/Extended Antivirus Database Scan	
c. Anti-Spyware	
d. Anti-botnet	
e. URL Filtering (including user notification, safe search enforcement etc.)	
f. File-blocking and File-filtering (DLP)	
g. Sandboxing for all supported file types	
h. Application Identification	
i. User Identification (agentless)	
j. Logging enabled	
1.1.6 Proposed solution will be subject to stress testing to validate the technical compliance of the solution if required. Failure to satisfy above parameters will lead to negative impact	
1.1.7 NGFW Performance must not be affected when enabling any of the below features and must still commit to the minimum throughputs	
a. Logging and storing it on local HDD.	
b. All management features like SSH, HTTPS, SNMP, etc	
c. Scheduled threat prevention DB updates up to the level of checking every 1 minute to ensure best security coverage.	
d. Multiple alert systems like Syslog, SNMP and others at the same time.	
e. All applications inspections.	
f. Changing the order of the security rules.	
g. Using all IPS signatures for all supported applications with extended packet captures for critical to high severity alerts.	
h. Virtual Context should not impact the firewall performance	
1.1.8 Administrators must not have to apply any tradeoff between security and performances, choosing to use in any security profile different versions of signature databases, for IPS with reduced numbers of element.	
1.1.9 Administrators must not have to apply any tradeoff between security and performances, choosing to use in any security profile different versions of signature databases, for Antivirus and malware scanning with reduced numbers of element.	
1.1.10 The proposed firewalls shall support at least 128,000 concurrent sessions with all threat prevention enabled features and at least 8,600 new sessions per second.	
1.1.11 The proposed firewalls shall deliver at least 1.4 Gbps IPSEC VPN throughput based on 64K HTTP Transaction Size	
1.1.12 The proposed firewalls shall deliver at least 1000 IPSEC site-to-site tunnels if required.	
1.1.13 Dedicated high availability ports (preferably 1G ports).	
1.1.14 High Availability, Active / Active with Asymmetrical Routing support and Active/Passive	
1.1.15 Proposed Solution must support QoS (marking and/or traffic shaping) for multiple classes at the same time and must be able to make policy as below:	
a. QoS Policy-based traffic shaping (priority, guaranteed, maximum)	
b. QoS Policy-based diffserv marking	

c. QoS Policy-based on application category, users/groups or any combination	
1.1.16 The proposed firewalls must have at least network ports as follow:	
i. (4) 10/100/1000	
ii. (8) 1Gbps SFP	
1.1.17 Reporting: Solution should provide granular reporting (with query builder)	
1.1.18 Reporting: Network Log storage for 45 days	
1.1.19 Reporting: The proposed firewall shall support real time interactive graphical dashboard to highlight high risky applications, suspicious app-centric content and users	
1.1.20 Reporting: The proposed firewall has the ability to schedule PDF report generation and send it over email	
1.1.21 Data Filtering: The firewall should be capable of identifying and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)	
1.1.22 Data filtering: Social Security Numbers, Credit Card Numbers any regex pattern	
1.1.23 Data filtering: Custom Data Patterns	
1.2 Functional Requirements	
1.2.1 Unlimited Concurrent User License for IPSEC, Remote, & SSL Client Based VPNs.	
1.2.2 Proposed Firewalls should be able to decrypt TLS 1.2 Traffic with RSA-AES256-GCM-SHA384 with 2K keys at server response packet size of 1500 bytes	
1.2.3 Possibility to support internally developed applications with application ID customized manually by the customer	
1.2.4 The NGFW platform shall support dual IPv4 and IPv6 stacks application control and threat inspection support in tap mode, transparent mode L1, layer 2 and layer 3	
1.2.5 The NGFW platform shall support multiple virtual routers to run different set of routing protocols (Interfaces can be binded to different virtual routers)	
1.2.6 Anti-Virus should not reduce the IPS inspection throughput and should be able to give full threat prevention capabilities	
1.2.7 Anti-Spyware should not reduce the IPS inspection throughput and should be able to give full threat prevention capabilities	
1.2.8 Advanced malware protection to prevent unknown modern targeted attacks and APTs	
1.2.9 Support IPSec VPN, and dynamic site-to-site VPN support with LSVPN.	
1.2.10 Identify users, not just IP addresses. Leverage information stored in Active Directory for visibility, policy creation, reporting, and forensic investigation.	
1.2.11 Inspect content in real-time. Protect the network against attacks and malware embedded in application traffic at low-latency, high throughput speeds, with all signatures applied at the same time	
1.2.12 Policy-based control by application and/or application category (non-port based) - as a policy matching criteria	

1.2.13 The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before	
1.2.14 The proposed solution should be able decrypt ssh/ssl/tls 1.2 protocols and extend Advance Malware Protection to all file types over HTTP, HTTPS, POP3, IMAP, FTP, SMTP and SMB	
1.2.15 The proposed firewalls shall support Denial of Service (DoS) and fragmented packet Transmission Control Protocol (TCP) reassembly, brute force attack, “SYN cookie”, “IP spoofing” and malformed packet protection.	
1.2.16 The proposed firewalls shall support transparent and tap mode within the appliance.	
1.2.17 The proposed firewalls shall support 802.1Q Virtual Local Area Networks (VLANs) tagging (in tap, transparent, layer 2 and layer 3).	
1.2.18 The proposed firewalls shall support dual IPv4 and IPv6 stacks application control and threat inspection support in tap mode, transparent mode, layer 2 and layer 3.	
1.2.19 The proposed firewalls shall support standards-based link aggregation (IEEE 802.3ad) to achieve higher bandwidth.	
1.2.20 The proposed firewalls shall support policy-based forwarding based on zone, source or destination address, source or destination port, application and users/groups imported from Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial In User Service (RADIUS) user or user groups.	
1.2.21 Should support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic	
1.2.22 The proposed firewalls shall support IPv6 routing for virtual routers.	
1.2.23 Should provide hot swap fans and redundant power supplies	
1.2.24 Should support XML API that would allow the firewall to be integrated with any known NAC, and WLAN controllers for user identification	
1.2.25 Should support Syslog Receiver feature that would allow the firewall to be integrated with any known NAC, and WLAN controllers for user identification	
1.2.26 Firewall should support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)	
1.2.27 The firewall should be capable of identifying and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)	
1.2.28 The firewall should take decision based on different matching parameters not based on layer4 parameters. It should be based on applications, URL categories, device state, IP addresses, security zones, username/group(s)	
1.2.29 Policies based on port-and-protocol And Application as the match criteria (application decision should not be done separately)	
1.2.30 Support Geographical Location policy in a security rule, where connections going to a country or countries can be blocked	
1.3 Threat Prevention: Next Generation IPS	
1.3.1 Block viruses, spyware, malware and network worms and vulnerability exploits within content of application content	

1.3.2 File blocking by type and application	
1.3.3 Anonymous Botnet Detection	
1.3.4 Blocks application vulnerabilities	
1.3.5 Block known network and application-layer vulnerability exploits	
1.3.6 Block buffer overflow attacks	
1.3.7 Block DoS/DDoS attacks; it shall support Denial of Service (DoS) and fragmented packet Transmission Control Protocol (TCP) reassembly, reconnaissance attacks, brute force attack, “SYN cookie”, “IP spoofing” and malformed packet protection.	
1.3.8 Supports attack recognition for IPv6 & IPv4	
1.3.9 Stream-based protection and scanning for Anti-Virus & Antispyware	
1.3.10 Built-in Signature and Anomaly based IPS engine	
1.3.11 Ability to create custom user-defined signatures	
1.3.12 Supports CVE-cross referencing where applicable	
1.3.13 Supports automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)	
1.3.14 All Threats should be part of application context	
1.3.15 The platform should be capable to enforce various threat prevention profiles on different applications running on same L4 session	
1.4 Advanced Malware Prevention	
1.4.1 Identifies unknown malware and zero-day exploits using advanced static and dynamic analysis techniques	
1.4.2 Should support anti-evasion capability which is tested against advance evasion technique.	
1.4.3 Cloud-based detection architecture or self-contained on-premises Sandboxing system	
1.4.4 Malware analysis should support files from Windows, Linux, Mac OS and Android platform	
1.4.5 Drive-by Download Detection & Protection	
1.4.6 Dynamic Analysis should include but not limited to: changes made to hosts, suspicious network traffic, anti-analysis detection plus more potentially malicious behaviors	
1.5 Antivirus/Anti-Spyware:	
1.5.1 Per-application antivirus or anti spyware scanning options	
1.5.2 Per-category scanning options	
1.5.3 Phone-home detection/blocking	
1.5.4 Malware site blocking	
1.5.5 DNS-based botnet signatures	
1.5.6 DNS Sink holing for Malicious and fast-flux domains	
1.6 URL Filtering:	
1.6.1 Multi-category filtering	
1.6.2 Customizable allow and block lists	
1.6.3 Customizable block page & coaching pages	
1.6.4 Custom categories	

1.6.5 Database located locally on the device	
1.6.6 Supports block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time)	
1.7 DNS Security:	
1.7.1 Neutralize DNS tunneling	
1.7.2 Predict and stop DGA-leveraging malware with real-time domain query analysis	
1.7.3 DNS threat detection methods using the modular and infinitely extensible DNS Security cloud-based service	
1.8 Data Filtering:	
1.8.1 Files should be identified by file types or by signature	
1.8.2 The firewall should be capable of identifying and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)	
1.8.3 Compressed information stored in zipped files should be able to be unpacked and filtered per policy	
1.8.4 The firewall should be capable of identifying and optionally preventing the transfer of files containing sensitive information (i.e. credit card numbers) via regular expression	
1.8.5 Should not have any file size limitation in checking content for keywords	
1.8.6 The platform should be capable to enforce file blocking on different applications running on same L4 session	
1.8.7 Control Drive-By Download (Files which are downloaded/transferred via web applications without knowledge of the user - it might have an exploit that can attack end-user’s workstation)	
1.9 User Identification:	
1.9.1 Should support the following authentication services for user-identification: -	
a) Active Directory	
b) Exchange	
c) LDAP	
d) eDirectory	
e) Radius	
f) Kerberos	
g) Client Certificate	
h) Captive Portal	
i) Terminal Server	
j) Supports the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP	
k) Users from Citrix and terminal services environments should be supported in policy and logs	
l) Populate all logs with user identity (traffic, IPS, URL, data, etc.)	
m) Logged user-identification correlated in real-time	
n) Should support REST XML API that would allow the firewall to be integrated with any known NAC, and WLAN controllers for user identification	

o) Should support built in syslog server for collecting user identification logs from unix, and any network controller (WLAN, NAC) for user identification	
1.10 Networking	
1.10.1 Tap Mode, Layer 2, and Layer3 (should be supported in the same virtual system at the same time)	
1.10.2 Can be deployed as virtual wire (Layer 1 with no change to MAC nor Ip addresses). Bump in the wire technology	
1.10.3 RIPv2, OSPFv2 and BGP	
1.10.4 Policy based routing	
1.10.5 Policy based routing with application as matching criteria	

Layer 3 Switch

Sr.No	Requirement	Compliance
1	The switch must be equipped with 24 x SFP ports	
2	The switch must be equipped with 4 x 10/100/1000BaseT Combo ports	
3	The switch must be equipped with 4 x SFP+ ports	
4	The switch should work using a modular operating system with the ability to restart an individual process without a full reset switch.	
5	The switch bandwidth must be not less than 128 Gbps	
6	The maximum number of stored MAC addresses in the switching table the switch shall be not less than 16000	
7	The routing table of the switch must store not less 480 IPv4 routes	
8	The switch must support 256 or more Multicast groups	
9	The switch must support stacking with other families of switches from the same manufacturer and stack bandwidth must be not less than 40Gbps in ring topology through 10 Gigabit Ethernet ports.	
10	The failure of any switch in the stack should not cause stack outage more than 50ms.	
11	The switch must support the joint failover configuration with another identical switch to connected devices can use the mechanism for combining multiple physical channels (LAG) to two switches with active simultaneous use of all channels; the recovery Time in case of any link failure between switches should not exceed 50ms.	
12	The failover configuration must be supported for two separate switches and two separate stacks of switches.	
13	The switch must support the IEEE family protocols: 802.3: 802.3, 802.3ae, 802.3ab, 802.3z.	
14	The switch must support 802.1ad (Q-in-Q) and Selective Q-in-Q protocols	
15	The switch mush support High Availability Network Protocols with 50ms recovery time in ring topology with RFC 3619 Ethernet Automatic Protection Switching.	

16	The switch must support ITU-T G.8032 Ethernet Ring Protocol Switching	
17	The switch must support 802.1w, 802.1s, PVST+ protocols	
18	The switch must support 802.1AS, 802.1Qav, 802.1Qat, 802.1BA	
19	The switch must support Policy-based Routing	
20	The switch must support the IEEE 802.1x protocol.	
21	The switch should support intrusion detection mechanism, prevent the spread of worms and viruses, suppression of attacks such as DoS.	
22	The switch must support sFlow version 5.	
23	The switch must support the scripting language (scripting) that run directly on the switch. The scripting language should support common command language Python.	
24	The switch must support the XML language for a simple embedding procedures for the management switch into external systems	
25	The switch must support the change of configuration parameters upon the occurrence of events such as authentication devices, authenticating users, the offensive certain time, the establishment and breakage of connection on a port and all other events, which detects by the operating system of the switch.	
26	The switch must support ITU-T Y.1731 protocol	
27	The switch must support Cloud Management System	
28	Then switch must support following routing protocols:	
28.a	OSPF	
28.b	RIP v1/v2, PIM,	
29	The switch must support BFD for static routing and dynamic routing protocols OSPFv2/OSPFv3	
30	VMAN Customer Edge Port CVID Egress Filtering / CVID Translation	
31	LAG (802.3ad LACP) core, between switches	
32	VLAN aggregation	
33	Ethernet Audio Video Bridging (AVB) support	

Access Switch 24 Port

Sr.No	Requirement	Compliance
1	The switch must be equipped with 24 x 10/100/1000BaseT ports	
2	The switch must be equipped with SFP ports, not less than 8 (4+4 combo)	
3	The switch must be equipped with SFP+ ports, not less than 4	
4	The switch should work using a modular operating system with the ability to restart an individual process without a full reset switch.	
5	The switch bandwidth must be not less than 128 Gbps	
6	The maximum number of stored MAC addresses in the switching table the switch shall be not less than 16000	
7	The routing table of the switch must store not less 480 IPv4 routes	
8	The switch must support 256 or more Multicast groups	
9	The switch must support stacking with other families of switches from the same manufacturer and stack bandwidth must be not less than 40Gbps in ring topology through 10 Gigabit Ethernet ports.	
10	The failure of any switch in the stack should not cause stack outage more than 50ms.	
11	The switch must support the joint failover configuration with another identical switch to connected devices can use the mechanism for combining multiple physical channels (LAG) to two switches with active simultaneous use of all channels; the recovery Time in case of any link failure between switches should not exceed 50ms.	
12	The failover configuration must be supported for two separate switches and two separate stacks of switches.	
13	The switch must support the IEEE family protocols: 802.3: 802.3, 802.3ae, 802.3ab, 802.3z.	
14	The switch must support 802.1ad (Q-in-Q) and Selective Q-in-Q protocols	
15	The switch mush support High Availability Network Protocols with 50ms recovery time in ring topology with RFC 3619 Ethernet Automatic Protection Switching.	
16	The switch must support ITU-T G.8032 Ethernet Ring Protocol Switching	
17	The switch must support 802.1w, 802.1s, PVST+ protocols	
18	The switch must support 802.1AS, 802.1Qav, 802.1Qat, 802.1BA	
19	The switch must support Policy-based Routing	
20	The switch must support the IEEE 802.1x protocol.	
21	The switch should support intrusion detection mechanism, prevent the spread of worms and viruses, suppression of attacks such as DoS.	
22	The switch must support sFlow version 5.	
23	The switch must support the scripting language (scripting) that run directly on the switch. The scripting language should support common command language Python.	

24	The switch must support the XML language for a simple embedding procedures for the management switch into external systems	
25	The switch must support the change of configuration parameters upon the occurrence of events such as authentication devices, authenticating users, the offensive certain time, the establishment and breakage of connection on a port and all other events, which detects by the operating system of the switch.	
26	The switch must support ITU-T Y.1731 protocol	
27	The switch must support Cloud Management System.	
28	Ethernet Audio Video Bridging (AVB) support	

Access Switch 12 Port

Sr.No	Requirement	Compliance
1	The switch must be equipped with 10/100/1000BaseT ports, not less than 12	
2	The switch must be equipped with SFP+ ports, not less than 4	
3	The switch should work using a modular operating system with the ability to restart an individual process without a full reset switch.	
4	The switch bandwidth must be not less than 104 Gbps	
5	The maximum number of stored MAC addresses in the switching table the switch shall be not less than 16000	
6	The routing table of the switch must store not less 480 IPv4 routes	
7	The switch must support 256 or more Multicast groups	
8	The switch must support stacking with other families of switches from the same manufacturer and stack bandwidth must be not less than 40Gbps in ring topology through 10 Gigabit Ethernet ports.	
9	The failure of any switch in the stack should not cause stack outage more than 50ms.	
10	The switch must support the joint failover configuration with another identical switch to connected devices can use the mechanism for combining multiple physical channels (LAG) to two switches with active simultaneous use of all channels; the recovery Time in case of any link failure between switches should not exceed 50ms.	
11	The failover configuration must be supported for two separate switches and two separate stacks of switches.	

12	The switch must support the IEEE family protocols: 802.3: 802.3, 802.3ae, 802.3ab, 802.3z.	
13	The switch must support 802.1ad (Q-in-Q) and Selective Q-in-Q protocols	
14	The switch mush support High Availability Network Protocols with 50ms recovery time in ring topology with RFC 3619 Ethernet Automatic Protection Switching.	
15	The switch must support ITU-T G.8032 Ethernet Ring Protocol Switching	
16	The switch must support 802.1w, 802.1s, PVST+ protocols	
17	The switch must support 802.1AS, 802.1Qav, 802.1Qat, 802.1BA	
18	The switch must support Policy-based Routing	
19	The switch must support the IEEE 802.1x protocol.	
20	The switch should support intrusion detection mechanism, prevent the spread of worms and viruses, suppression of attacks such as DoS.	
21	The switch must support sFlow version 5.	
22	The switch must support the scripting language (scripting) that run directly on the switch. The scripting language should support common command language Python.	

STANDARD BIDDING DOCUMENT

Passive Networking

Passive work including ducting, copper/ fiber laying, termination and fluke testing.

i. Giga Cable UTP CAT6
ii. CAT 6 Patch Panel
iii. CAT6 I/O
iv. Faceplate Single / dual Shutter
v. Patch Cords CAT 6, (1 & 3 meter)
vi. Fiber Backbone Cable for Uplink the network switches. (Fiber
vii. Optical Distribution Frame.
viii. Dura Duct, Pipe and Accessories

Sr. No	Requirement	Compliance
1	**CAT 6 Cable**	
1.1	Cat 6 Cable, UTP, PVC, 4 pairs, 305 meter /Box Gigabit original copper cable Category 6 U/UTP Cable (with cross-shaped separator) offer the possibility to deploy	
1.2	unshielded Category 6/Class E systems when installed with Cat-6 RJ45 Jacks.	
1.3	• Conductor Diameter: AWG 24 (Ø 0.525 +/- 0.015mm)	
1.4	• Insulation Diameter: PE Ø 0.95 +/- 0.05 mm	
1.5	• Cable assemblies: pairs	
1.6	• Sheath material: PVC	
1.7	**Mechanical Features:**	
1.7a	Maximum cable diameter (mm) 5.40 +/- 0.30	
1.7b	Bending Radius (mm)	
1.7c	Dynamic (installation) / Static (installed) ≥ 8x outer diameter / ≥ 4x outer diameter	
1.7d	Temperature Range In service / Installation, Transport and Storage -20°C +60°C / 0°C +50°C	
1.8	**Electrical Features at 20°C:**	
1.8a	DC Resistance max 9.38 Ω/100m	
1.8b	Resistance Unbalance ≤ 2 %	
1.8c	Insulation Resistance (500 V) ≥ 5000 M Ω/km	
1.8d	Mutual capacitance nom. 5.1 nf / 100 m at 1 kHz	
1.8e	Test Voltage (DC, 1 min) 1 kV / 1m	
1.8f	Capacitance Unbalance (pair to ground) max. 160 pf / 100 m at 1 kHz	
1.8g	VPN (nominal) 67%	
1.9	**Standards Cables**	
1.9a	IEC 61156-5 ed. 2	
1.9b	ANSI/TIA 568-C.2	
1.9c	ISO/IEC11801 ed.2	

1.10	**Fire Rating**	
1.10a	LSZH: IEC 60332-1	
1.10b	PVC: IEC 60332-1	
2	CAT6 I/O	
2.1	RJ45 K6 Jack, Cat 6, UTP, Shuttered (tool-less termination),	
2.2	Category 6/Class E system, fully compliant with Category 6 ISO/IEC, EN and TIA standards	
2.3	for hardware performance, confirmed by independent laboratory certifications (Delta,GHMT).	
2.4	The jacks have the following features:	
2.4a	• Category 6 UTP	
2.4b	• Keystone fixing;	
2.4c	• Tool less assembly (mandatory)	
2.4d	• Capable of being wired to both 568B and 568A	
2.4e	• three cable entry points	
2.4f	• Integral shutter/shuttered jack	
2.4g	• Jacks must be reusable i.e it must support multiple termination.	
2.5	Applications	
2.5a	- IEEE 802.3 1GBASE-T	
2.5b	- PoE – IEEE 802.3at	
2.6	Standards	
2.6a	- ISO/ IEC 11801 Edition 2, Am 1-2	
2.6b	- ISO/ IEC 60603-7-5	
2.6c	- EN 50173-1	
2.6d	- ANSI/ TIA/ EIA-568-C.2-2009	
2.6e	- IEC 60512-99-001	
3	Faceplate	
3.1	Single non-shuttered	
3.2	U.K. Single Gang Faceplate, 1 port, w/o shutter.	
3.3	86 x 86 faceplate range can be loaded with Cat-6 UTP I/O to provide the following configurations:	
3.3a	• Single gang, 1 port	
3.3b	• Single gang, 2 ports	
3.4	Specifications	
3.4a	Faceplates – size (h x w x d) Single gang – 86 x 86 x 10mm	
3.4b	Material V0 – ABS	
4	Optical Distribution Frame	
4.1	along with supporting accessories	
5	Rack mount with sliding tray pre-loaded with SC Duplex couplers	
6	Fluke Testing of Copper Nodes & OTDR testing of fiber links.	
7	Dura Duct	

7.1	Duct, Pipe and accessories 16x25mm, 16x38mm, 40x40mm, 60x60 ,1inch pipe etc.- with Adamjee or equivalent ducting and flexible PVC pipe fiber termination unit/ODF	
8	UPS For centralized power for networks switches firewall and server machine 10KVA	
9	Imported 42 u rack with PDU	
10	Aps(Routers) for wifi Qty: 18/-	

Note: 03 (three) Years Parts/Labor OEM On Site warranty for all components with supplier on-site support.

Rate quoted per unit (Including taxes)	**Quantity**	**Total Amount** **(In Pak Rupees)**
	01 Client Server based Network for 6 Storey Building with Firewall	