Request for Proposal for Supply and Installation of Firewalls

Tender No.: [PNBGILTS/ RFP/ Firewall/ 2024-25/ 01]

Date: 17.02.2025

PNB GILTS LIMITED

5, Sansad Marg,

New Delhi, 110001

Schedule of Events

Bid Details:

Date of commencement of Bidding Process.	17/02/2025
Last date and time for bids submission	03/03/2025 till on or before 1600 Hrs.
Date and Time of Bids Opening	03/03/2025 on or before 1700 Hrs.
Place of opening of Bids & Address for communication	PNB GILTS LTD , HO, 5 Sansad Marg, New Delhi – 110001
Contact to Bidders	Interested Bidders may send their query to it@pnbgilts.com so that in case of any clarification, same may be addressed to them.

Note: - Bids will be opened in the presence of bidders in the form of physical or VC on the specified date as mentioned above. The above schedule is subject to change, if required. Notice of any changes will be communicated via Email. PNB Gilts (referred to hereinafter as the Company)

Company is in process for procurement of 4 Firewalls in DC (2) and 'DR (2). The details of annexures are as below:

Annexure	Annexure Details	Page no.
A	Scope of work	5-6
B	Terms and conditions	7
C	Technical proposal covering letters (Format I, II and III)	8-10
D	Minimum Eligibility Criteria Covering Letter	11-13
E	Commercial Proposal Covering letter and Bid Format (Format I and II)	14-15
F	Firewall specifications	16-18

2. Interested bidder is required to submit their Techno-Commercial proposals along with required annexures as mentioned above.
3. Bids have to be submitted separately in a separate envelope along with sign of authorized signatory on all pages of the bids.
4. In case of soft copy (Bids), a separate password protected techno-commercial proposals over email should be shared at IT@pnbgilts.com . Passwords not to be shared with the proposals or separate email, until requested.
5. Contact Persons: - Mr. Ashutosh Sharma Contact no. : 8178823688, Mr. Ajit Kumar Contact No: - 9868886380.

1. Introduction

PNB Gilts Limited ("PNBG") is a company incorporated and registered under Companies Act, 1956 and authorized by Reserve Company of India to act as Standalone Primary Dealer. "PNBG" is engaged in conducting Government Securities business 'PNBG" has its Registered Office at 5 Sansad Marg, New Delhi – 110001.

Company intends for procurement of firewalls (4) including supply, installation for DC, Delhi (2) and DR, Mumbai (2) and invites technically competent and commercially competitive proposals from reputed Solution providers for this purpose.

2. Requisite Standard of Services

a. Being a financial institution, security of its internal business, systems, and data/ information is a prime concern of the Company while availing the services as mentioned in this document. To ensure this, the bidders are required to submit the implementation plan based on Information Technology Services management (ITSM) and Information Technology Infrastructure Library (ITIL) framework as part of their technical proposal. This plan should be comprehensive enough and should include the milestones, description, timelines etc. so as to ascertain that the Services delivered to the Company by the bidder are:

    i. As per the agreed Service levels
    ii. Professionally managed with domain expertise

b. To ensure this, the bidders are required to submit the well documented plan to address the RFP Requirements as part of their technical proposal.

3. Instruction to Bidders

a. Technical and commercial bids are invited from Vendors for providing deliveries as per the terms and conditions mentioned hereunder.
b. The above mentioned envelopes should be separately sealed and super-scribing "Supply, Installation of Firewalls" sealed and submitted on or before at specified date and time as mentioned under bid details at PNB Gilts Ltd., 5 Sansad Marg, New Delhi -110001.
c. Bidder will submit the financial bid with 3 years of warranty and OEM premium support in their proposal.
d. Any bid received by the Company after the deadline for submission of bids prescribed by the Company will not be entertained.
e. Only technically qualified bidder will be eligible for commercial bids.
f. Company reserves the right to reject any proposal in case it is found incomplete.
g. Company reserves the right to accept or reject any or all tenders without assigning any reasons thereof.
h. The objective of evaluation methodology is to facilitate the selection of the technically superior solution at optimal cost.
i.
j. **Minimum Eligibility Criteria**:

Sr. No.	Financial and other Requirements
1	Bidder should have minimum turnover of INR 100 Cr. per annum in the last three financial years ending March 2024 in Indian operations only, out of which Rs.25 Cr. Per annum from Cyber security product.
2	Bidder Should have positive net worth for the last 3 years.
3	Bidder should have experience of implementation of proposed OEM for at least 3 projects in RBI/BFSI Sector etc.
4	The bidder should be a registered company incorporated in India, registered under Company act 1956 / 2013
5	Consortium/JV bidding is not allowed.

ANNEXURE - A

Scope Of Work for Supply of firewall and implementation

1) The Vendor will supply and do the installation of the Firewalls as per technical specifications as enclosed in separate documents.
2) The Vendor has to provide all necessary hardware, software & licenses for appliance, etc. required to make the solution work strictly as per RFP based on the requirement of PNB Gilts.
3) The Vendor shall procure all required licenses in the name of PNB Gilts.
4) The Vendor should be responsible for de-commissioning of existing devices in co-ordination with existing Network System Integrator i.e. replacing the existing Firewalls with the new Firewalls in such a way that there is no impact on business continuity.
5) Vendor should ensure that installation/operation/commissioning of the proposed solution and should not have significant impact on existing infrastructure.
6) The Vendor will be responsible for transit insurance up to delivery at the PNB Gilts side.
7) During the delivery & installation of devices at PNB Gilts location, the Vendor shall physically check the items as per the packing list. If any of the items which are not delivered or not as per the specification or damaged etc., the Vendor's resources at the sites shall take immediate steps and ensure all the items are delivered so that the installation is not hampered. The Vendor shall have to arrange for all testing equipment and tools if required for installation and implementation and also arrange the vehicle for transport at no additional cost to the PNB Gilts.
8) The Vendor shall ensure compatibility of the hardware, software and other equipment that they supply, with the hardware and software systems being used in the PNB Gilts.
9) Vendor shall also provide evidence to prove all the features as advised in technical requirements as per technical specification or suggest model in RFP.
10) The installation/implementation activity should be carried out during non- session/Non-Peak, engineer support should be provided according to the requirement. All the Firewall equipment should be covered under the contract period of 3 years warranty. Delivery of all hardware, licenses, and warranty documentation to be submitted at designated location.
11) Configuration of firewall rules, policies, and access controls based on the company's IT policy requirements, including but not limited to:

    - Securing internal and external network traffic.
    - Role-based access control for users and devices.
    - Setting up Virtual Private Networks (VPNs) for secure remote access.
    - Implementation of intrusion detection and prevention systems (IDS/IPS)

12) The Vendor shall be responsible to carry out all the required changes/configuration during the implementation phase in co-ordination with the Network System Integrator as per requirement of the PNB Gilts.
13) Firewall features along with detailed specification are enclosed at Annexure F.

14) Delivery, Commissioning and Implementation Schedule

Sl. No	Description	Timelines
1	Supply of Firewall at DC & DR Location	4 Weeks from issuance of PO
2	Commissioning & Implementation of Devices	6 Weeks from issuance of PO

Payment Terms

Sl. No	Description	Payment Terms
1	Supply of Firewall and Software License with Three Years Support	100% on Delivery and implementation of the complete hardware /appliance software at PNB Gilts.
2	One time installation charges	After successful installation

Note:

For Hardware /Appliances – Payment process shall be initiated only after the delivery and implementation of all the Hardware /Appliances and Software.

ANNEXURE – B

TERMS AND CONDITIONS

1) The offered Firewalls must be IPV4 and IPV6 compliant from Day1.
2) Vendors shall work in coordination with existing Firewall vendor of the Company for getting the necessary configuration, for assigning IP address to firewalls for seamless migration. In case, if any firewall goes faulty due to reasons non attributable to Company, Vendor is required to replace the firewall of same or higher version at no additional cost to the Company.
3) The firewalls should operate within a heterogeneous environment of network devices from multiple OEMs (e.g. Firewalls, Firewalls, and Security Solutions etc.) In case the supplied firewalls are unable to operate in heterogeneous environment of Company, Vendor will take back all the equipment's and supply new equipment's compatible with heterogeneous environment. In such case Company will not bear any additional cost other.
4) If any firewall is damaged in transit or during installation by the Vendor, it will be responsibility of the Vendor to replace the same free of cost.
5) It is Vendor's responsibility to check the contract parameters (like earthling, power, UPS backup, Rack space etc.) before installation of firewalls at the various locations. If any parameter is not as per standard requirement, then Vendor in writing should approach Company to provide/rectify the same and after confirmation from Company, installation should be done. In any case supplied equipment goes faulty due to the negligence of checking necessary parameters, then it will be sole responsibility of the Vendor to replace the same free of cost. Further, in these cases where revisit is required then Vendor will send the engineer again for the installation without any additional cost to Company.
6) Purchase order should be accepted within 3 days from the issue date of purchase order.

ANNEXURE - C

FORMAT - I

Technical Proposal Covering Letter (On Company Letter Head)

To,

Ashutosh Sharma/Ajit Kumar,
PNB Gilts Limited,
4th Floor, 5, Sansad Marg,
New Delhi-110001

Dear Sir/ Madam(s),

Sub: Technical Proposal for RFP for Supply and Installation of Firewalls

Having examined the Request For Proposal (RFP) ____ Documents dated __ the receipt of which is hereby duly acknowledged, we, the undersigned, offer to Supply and Installation of Firewalls required capabilities in terms of functional and technical expertise for Firewalls including all licenses required (other than mentioned in complete RFP document) and implement for in conformity with the said RFP Documents and hereby undertake that we accept all the conditions of the RFP and will provide the complete services as per the Scope of Work. We undertake to state that we have submitted all the necessary documents / responses as per the technical proposal of this RFP.

Date:
Name of the Authorized Signatory:
Signature of the Authorized Person:
Place:
Designation:
Name of the Organization:
Seal:

ANNEXURE - C

FORMAT - II

Conformity Letter (On Company Letter Head)

To,

Ashutosh Sharma/Ajit Kumar,
PNB Gilts Limited,
4th Floor, 5, Sansad Marg,
New Delhi-110001

Sir/Madam,

Sub: Conformity for RFP for Supply and Installation of Firewalls

Further to our proposal dated _____, in response to the Request for Proposal (RFP No. hereinafter referred to as "RFP") issued by PNB Gilts Limited we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms, conditions and stipulations as contained in the aforesaid RFP and the related annexures, addendums, corrigendum and other documents including the changes made to the original tender/RFP documents, issued by the PNB Gilts Limited, however that, only the list of deviations furnished by us along with technical bid which are expressly accepted by the PNB Gilts Limited and communicated to us in writing, shall form a valid and binding part of the aforesaid RFP document. The PNB Gilts Limited is not bound by or bound to accept any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal / document or any subsequent deviations sought by us, whether orally or in writing, and the PNB Gilts Limited's decision not to accept any such extraneous conditions and deviations, will be final and binding on us.

We also confirm that the soft-copies of the proposal submitted by us in response to the RFP and the related addendums and other documents issued by PNB Gilts Limited conform to and are identical with the hard-copies of aforesaid proposal submitted by us, in all respects.

Yours faithfully,
Date:
Name of the Authorized Signatory:
Signature of the Authorized Person:
Place:
Designation:
Name of the Organization:
Seal:

ANNEXURE - C

FORMAT - III

Confirmation of Genuineness of hardware (On Company Letter Head)

To,

Ashutosh Sharma/ Ajit Kumar,
PNB Gilts Limited,
4th Floor, 5, Sansad Marg,
New Delhi-110001

Dear Sir/ Madam(s),

Sub: Confirmation of Supply Genuineness of hardware for RFP for Supply and Installation of Firewalls

Further to our proposal dated _, in response to the Request for Proposal (RFP) _____ dated . issued by PNB Gilts Limited, we hereby confirm that all the components / parts / assembly / software used in the said project to be supplied shall be original new components / parts / assembly / software(s) from Original Equipment Manufacturer and that no refurbished / duplicate / second hand components / parts / assembly / software(s) shall be supplied or shall be used. We shall also produce a certificate from the Original Equipment Manufacturers in support of the above statement.

We also confirm that in respect of licensed operating systems and other software utilities to be supplied; the same will be procured from authorized sources and supplied with Authorized License Certificate such as Paper Licenses, Product Keys etc.

Yours faithfully,

Date:
Name of the Authorized Signatory:
Signature of the Authorized Person:
Place:
Designation:
Name of the Organization:
Seal:

ANNEXURE - D

Minimum Eligibility Criteria Covering Letter (On Company Letter Head)

To,

Ashutosh Sharma/ Ajit Kumar,
PNB Gilts Limited,
4th Floor, 5, Sansad Marg,
New Delhi-110001

Dear Sir/ Madam(s),

Sub: Minimum Eligibility for RFP for Supply, Installation of Firewalls

Having examined the Request for Proposal (RFP) Documents____dated __the receipt of which is hereby duly acknowledged, we, the undersigned, undertake that we fulfill the Minimum Eligibility Criteria requirements.

We further undertake to state that we have enclosed / submitted all the necessary documents and details as per the “Minimum Eligibility Criteria” requirements of the said RFP.

Yours faithfully,

Date:
Name of the Authorized Signatory:
Signature of the Authorized Person:
Place:
Designation:
Name of the Organization:
Seal:

ANNEXURE – D

QUALIFICATION CRITERIA (On Company Letter Head)

Note/Ref:

1. Bidders are requested to strictly adhere to the format given in this document.
2. Bidders are required to sign & stamp on Eligibility Criteria.

Criteria	Bidders Comments	Documents required
The bidder must be an Indian firm/ Company / Organization registered under Companies Act/Partnership Act/LLP Act etc. or a foreign company, registered under applicable laws & regulations, with Sales and Support arrangement in India.	YES/NO	Copy of the Certificate of Incorporation issued by Registrar of Companies and full address of the registered office. Proof of Partnership / LLP. Foreign companies also to provide declaration with details of sales and support arrangement in India.
The Bidder should not be blacklisted / debarred / negative list by any Statutory or BFSI or Regulatory Authorities	YES/NO	Self-Declaration by authorized signatory.
The Bidder should have engaged in minimum 3 similar project services (as mentioned in RFP)	YES/NO	Project Completion Certificate from Client / Relevant document showing proof and Client contact details / self-declaration.
The Bidder should be minimum authorized partner with OEM for the proposed make/model.	YES/NO	Valid OEM partnership certificate / Authorization Letter from OEM
The bidder should be ISO-27001 Certified Company, and the certificate should be valid as on date of bid submission and should also cover the proposed product/solution. Note: this point is applicable to critical products/ applications / support services.	YES/NO	Certificate required
Bidder should have minimum turnover of INR 100 Cr. per annum in the last three financial years ending March 2024 in Indian Operations only, out of which Rs.25 Cr. Per annum from Cyber security Product.	YES/NO	Certificate required
Bidder Should have positive net worth for the last 3 years.	YES/NO	Certificate required
Consortium/JV bidding is not allowed.	YES/NO	Certificate required

Date:

Name of the Authorized Signatory:
Signature of the Authorized Person:
Place:
Designation:
Name of the Organization:
Seal:

Annexure - E

Commercial Proposal Covering Letter Format -I (On Company Letter Head)

To,

Ashutosh Sharma/ Ajit Kumar,
PNB Gilts Limited,
4th Floor, 5, Sansad Marg,
New Delhi-110001

Dear Sir/ Madam(s),

Sub: Commercial Proposal for RFP for Supply and Installation of Firewalls

Having examined the Request For Proposal (RFP) Documents ___dated _____the receipt of which is hereby duly acknowledged, we, the undersigned, offer our services, as mentioned, conformance with the scope of work of said RFP documents and as per the attached Commercial Proposal and hereby undertake that we accept all the terms and conditions of the RFP.

We further undertake, if our bid is accepted, to deliver the services in accordance with the delivery schedule finalized.

Our commercial proposal shall be binding upon us, subject to the modifications resulting from contract negotiations, up to expiration for the validity period of the Proposal.

We understand that you are not bound to accept the lowest or any bid you may receive. Enclosure-

1. Commercial Bid

Yours faithfully,

Date: Signature of the Authorized Person
Name of the Authorized Signatory:
Place: Designation:
Name of the Organization:
Seal:

ANNEXURE-E

Commercial Proposal bid Format – II (On Company Letter Head)

Commercial Proposal for RFP for Supply and Installation of Firewalls

Commercial Bid Format (On Company Letter Head)

ITEM	Make/PART No./Model no.	No of units	TOTAL PRICE (Excl. of Taxes)
Firewalls with three years comprehensive warranty Locations: Delhi (Qty:2) & Mumbai (Qty:2) (as per scope of work and specifications mentioned in Annexure A)		4	
One Time Installation and Configuration Charges		1	
	GRAND TOTAL		

Date:

Price Valid Till: -

Signature of the Authorized Person:

Name of the Authorized Signatory:

Designation:

Name of the Organization:

Seal:

Annexure F Firewall Specifications

Features	Specification
Type	Next Generation Enterprise Firewall in HA
3rd Party Test Certification	The proposed vendor must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive 5 years. The proposed NGFW appliance vendor product must be Common Criteria (CC) Certified Product. The proposed NGFW firmware/operating system shall confirm to ICSA and FIPS-140-level-II security standard. The device should be FCC Class A, CE Class A, VCCI Class A, cTUVus and CB Certified
Size	The NGFW appliance should be with dimensions 1.74" H x 8.83" D x 8.07" W
Fans and Power Supply	The offered firewall must be a single appliance and not a cluster and should be provided with redundant hot swappable power supplies and redundant fans within the NGFW appliance
Architecture	The proposed NGFW solution should be a single appliance architecture that has Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).
	The proposed firewall must have min 8 CPU cores with x86 processor and minimum 16 GB RAM from day 1.There should not be any proprietary ASIC based solution
	The device or any of its family should not have any feature of wireless within its hardware or software.
Storage	The NGFW should have at least 128 GB of local storage
Interface Requirement	Min 8 Copper, 10/100/1000 Ports interfaces from day 1
	10/100/1000 out-of-band management (1), RJ-45 console (1),USB (2), MicroUSB console (1)
Power Supply	Dual redundant 50 W. The device should support Redundant power supply.
Performance Capacity	A Minimum NG Firewall application control throughput in real world/production environment/Application Mix – minimum 4.5 Gbps with 64KB HTTP transactions including Application-Identification/AVC/Application control and Logging enabled. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.
	Minimum NG Threat prevention throughput in real world/production environment (by enabling and measured with Application-ID/AVC, User-ID/Agent-ID, NGIPS, Anti-Virus, Anti-Spyware, Anti Malware, File Blocking, Sandboxing, advanced DNS Security and logging security threat prevention features enabled – minimum 3 Gbps Throughput considering 64KB HTTP transaction size . The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.
	IPsec VPN throughput – Minimum 2.3 Gbps or more with 64KB HTTP transaction and logging enabled
	Remote Access VPN – 1,500 Concurrent SSL VPN License from Day-1
	New sessions per second – Min 65K considering 1 byte HTTP transaction size with AVC ON/application override enabled
	Concurrent sessions – Min 400 K
High Availability	Active/Active , Active/Passive and HA clustering support
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in:
	- Tap Mode
	- Transparent mode (IPS Mode)
	- Layer 2
	- Layer 3
	- Should be able operate mix of multiple modes
Next Generation Firewall Features	port/protocol/evasive tactics.
	The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP
	The proposed firewall should have the ability to create custom application signatures and categories directly on frewall without the need of any third-party tool or technical support. Also the device should have capability to provide detailed information about dependent applications to securely enable an application
	The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration
	The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.
	The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.
	The firewall must have the ability to manage firewall policy even if management server is unavailable
	The firewall must disallow root access to firewall system all users(including super users) at all times.
	The Firewall should support virtual System and should be scalabile upto 5 within the same appliance with additional licenses whenever required. The virtual system should have all the features as of physical device.
	Should support insertion of customer 2 factor authentication into any application before permitting the connection
	Solution should be have machine learning capabilities on the dataplane to analyze web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Inline ML should prevent web page threats from infiltrating network by providing real-time analysis capabilities.
	The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood(Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc
	All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc should work in isolated airgapped environment without any need to connect with Internet.
	Should have protocol decoder-based analysis which can statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits
	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.
	Should block known network and application-layer vulnerability exploits
	The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures
	The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour
	All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS or AV engines.
	Should be able to perform Anti-virus scans for HTTP, smtp, imap, pop3, ftp, SMB traffic with configurable AV action such as allow, deny, reset, alert etc

Threat Protection	Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs
	Shoud suppot inspection of headers with 802.1Q for specific Layer 2 security group tag (SGT) values and drop the packet based on Zone Protection profile
	The device should support zero day prevention by submitting the executable files and getting the verdict back in five minutes post detection.
	The device should have protection for at least 20000 IPS signatures
	Should have. threat prevention capabilities to easily import IPS signatures from the most common definition languages Snort and Suricata
	The solution must be able to define AV scanning on per application basis such that certain applications may be excluded from AV scan while some applications to be always scanned
	The solutiopn must have data loss prevention by defining the categories of sensitive information that is required to filter.
	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data
	Vendor should automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service
	The NGFW should have native protection against credential theft attacks(without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the folowing :
	· Automatically identify and block phishing sites
	· Prevent users from submitting credentials to phising sites
	· Prevent the use of stolen credential
Advanced Persistent Threat (APT) Protection	There should be provision to enable the APT solution with following features. This could be a on premise or cloud base unknown malware analysis service with guaranteed protection signature delivery time not more than 5 minutes.The cloud based ATP solution should leverage only India based threat data lake.
	Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment
	Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis
	The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required using hybrid setup.
	The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload.
DNS Security	The Solution should support DNS security in line mode and not proxy mode from day 1
	Solution should support database maintenance containing a list of known botnet command and control (C&C) addresses which should be updated dynamically
	The DNS Security solution should be able to detect and categorize hijacked and misconfigured domains in real-time by operating cloud based detection engines, which provide DNS health support by analyzing DNS responses using ML-based analytics to detect malicious activity.
	DNS Security should support predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control
	DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains if needed for any future considerations
	It should support prevention against new malicious domains and enforce consistent protections for millions of emerging domains.
	The solution should support integration and correlation to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links. Integrate.with URL Filtering to continuously crawl newfound or uncategorised sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots. Should take inputs from at least 25 third-party sources of threat intelligence.
	Should support simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.
	Solution should support prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection
	The solution should support capabilities to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers.
	The solution should have support for dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sink-holing malicious domains to cut off Command and control and quickly identify infected users.
SSL/SSH Decryption	The proposed firewall should have SSL decryprion in Hardware and shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
	The firewall must have the capability to be configured and deployed as SSL connection broker and port mirroring for SSL traffic
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic
	The device should be capable of SSL automatic exclusions for pinned applications.
	The firewall supports TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection, Broker and SSL Decryption Port Mirroring.
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well
Network Address Translation	The proposed firewall must be able to operate in routing/NAT mode
	The proposed firewall must be able to support Network Address Translation (NAT)
	The proposed firewall must be able to support Port Address Translation (PAT)
	The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6 or equivalent)
	Should support Dynamic IP reservation, tunable dynamic IP and port oversubscription
IPv6 Support	L2, L3, Tap and Transparent mode
	Should support on firewall policy with User and Applications
	Should support SSL decryption on IPv6
	Should support SLAAC Stateless Address Auto configuration
	Should be IPv6 Logo or USGv6 certified
	The proposed firewall must support the following routing protocols:
	- Static
	- RIP v2
	- OSPFv2/v3 with graceful restart
	- BGP v4 with graceful restart
	The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address

Routing and Multicast support	The firewall must support VXLAN Tunnel content inspection
	The firewall must support DDN sprovides such as DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org, and No-IP.
	The proposed firewall must have support for mobile protocols like GTP, SCTP and support for termination of GRE Tunnels
	The device should support load balancing of traffic on mnultiple WAN links based on application, latency, cost and type.
	The proposed solution must support Policy Based forwarding based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports
	The proposed solution should support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, Bittorrent, YouTube, azureus) -by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3
	Bidirectional Forwarding Detection (BFD)
Authentication	should support the following authentication protocols:
	- LDAP
	- Radius (vendor specific attributes)
	- Token-based solutions (i.e. Secure-ID)
	- Kerberos
	The proposed firewall's SSL VPN shall support the following authentication protocols
	- LDAP
	- Radius
	- Token-based solutions (i.e. Secure-ID)
	- Kerberos
	- SAML
	- Any combination of the above
Monitoring, Management and Reporting	Should support on device and centralized management with complete feature parity on firewall administration
	There should be provision to permanently block the export of private keys for certificates that have been generated or imported to harden the security posture in orfer to prevents rogue administrators from misusing keys.
	The management solution must have the native capability to optimize the security rulebase and offer steps to create application based rules
	The proposed solution should support a single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.
	Should support separate real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunnelled Traffic and correlated log view base on other logging activities
	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
	Should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.
	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs
	Should support creation of report based on SaaS application usage
	Should support creation of report based on user activity
	Should support creation of report based on custom query for any logging attributes
Support & Warranty	OEM should be present in India from at least 5 years and should be proposed with 3 Years OEM support bundle with 24x7x365 days TAC support, RMA (There should be at least 4 RMA dept and one TAC for support in India), software updates and subscription update support. The NGFW should be proposed with 3 years subscription licenses for NGFW, NGIPS, Anti Virus , Anti Spyware, Advanced URL Filtering , Threat Protection, APT Protection (Zero Day Protection) and DNS Security from day 1.