भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Notification pertaining to Request for Proposal for supply, installation, Commissioning and Maintenance of Firewall & DDNS Solution

About NPCI

National Payments Corporation of India (NPCI) is a registered company under Section 25 of the Companies Act, 1956 with its Registered Office in Mumbai, India. NPCI is promoted by 10 banks in India under the aegis of the Indian Banks Association with majority shareholding by Public Sector Banks.

The 10 promoter banks are State Bank of India, Punjab National Bank, Canara Bank, Bank of Baroda, Bank of India, Union Bank of India, ICICI Bank Ltd, HDFC Bank Ltd, Citibank N.A, and HSBC. The core objective was to consolidate and integrate the multiple systems with varying service levels into a Nation-wide uniform and standard business process in the retail electronic payments system segment. The vision, mission and objectives of NPCI are to operate for the benefit of all the Member Banks and the common man at large.

Objective of RFP

NPCI has various business verticals to process variety of retail payments prevailing in India today. NPCI intends to improve the current retail payment systems and add new lines of business in future. NPCI will be processing all the Electronic retail payments in a centralized mode of operation for which it is needed to setup new systems and communication lines to support the business verticals.
In order to expand the current infrastructure for various projects, NPCI intends to procure Firewall & DDNS Solution mentioned in Section 3.

Cost of the RFP

The Bidder shall bear all costs associated with the preparation and submission of its bid including any travel cost and NPCI shall, in no case, be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

The Bidders can procure the RFP document from NPCI's office at 13th Floor, South Side in R-Tech (Building 2), Pahadi, Goregaon (East), Mumbai – 400063, on payment of non-refundable amount of Rs.11,236.00 (Inclusive service tax@12.36%) (INR Eleven Thousand Two Hundred Thirty Six only), payable in the form of Demand Draft/Pay order from any scheduled commercial bank in India favoring "**NATIONAL PAYMENTS CORPORATION OF INDIA**" payable at Mumbai. This RFP document is non-transferable and cost of RFP document is non-refundable.

RFP document containing detailed specifications and requirements with terms and conditions can be obtained by eligible Bidders on any working day during office hours

from 10:30 hrs to 18:30 hrs on payment of RFP cost in the form of Demand Draft / Pay Order.

Due Diligence

The Bidders are expected to carefully examine all instructions, the RFP document, the terms and specifications stated in this RFP, and if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document, the Bidders are requested to seek necessary clarifications by e-mail as mentioned in Section-1.

The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders' risk and may result in rejection of the bid. Also the grounds for rejection of Bid should not be questioned after the final declaration of the successful Bidder.

Ownership of this RFP

The content of this RFP is a copy right material of National Payments Corporation of India. No part or material of this RFP document should be published on paper or electronic media without prior written permission from NPCI.

Scope of Work

Broad Scope of Work

The scope of work will include

a) Supply, installation & maintenance of comprehensive network security solution which includes upgrade or replacement of existing firewall.

b) Monitoring and Management will be done from any of existing NOC setup at Mumbai & Chennai at below mentioned address:

Mumbai:
National Payments Corporation of India,
TATA Communications Ltd, Tower A-IDC 4th Floor,
Bandra Kurla Complex,
Near MTNL Office,
Bandra (E)

Chennai Datacenter:
National Payments Corporation of India,
Reliance Communication Infrastructure Limited,
Floor IDC Sha 1-A, Reliance House No-6,
Haddows Road, Nungambakkam,
Chennai -600006.

➢ The bidder should study the existing perimeter security environment for providing the upgrade/replacement (buyback) solution before submitting the bids.

➢ NPCI intends to procure the following devices:

- Perimeter Firewall – 2 nos.
- Dynamic Domain Name Server - 2 nos.
- Web Application Firewall (WAF) – 2 nos.

- The devices should have onsite comprehensive support for a period of 5 years from the date of acceptance from the OEM.

- Requirement of one L2 resource at existing NOC setup at Mumbai/Chennai for management. The L2 engineer will provide on-site services during the Business Hours i.e. 9.30 AM to 5 PM and on call support during Holidays and non- business hours. The L2 resource should have the necessary skillset/expertise with minimum 2 years for managing the devices being supplied through this RFP.

- The equipment quoted by bidder should not be declared as EOL or EOS by the OEM before the last date of RFP.

- The bidder should provide a non cisco solution for perimeter firewall.

- The bidder should migrate to new setup with no/minimum downtime as possible.

- The bidder should provide OEM product training at NPCI location (minimum 1 week for 10 persons)

- The bidder shall submit the project details in MS project (MPP based).

Single point of Contact

The short listed L1 Bidder shall appoint a single point of contact with whom NPCI will deal for any activity pertaining to the requirements of this RFP.

Eligibility Criteria

Pre-requisite

The Bidder should possess the requisite experience, resources and capabilities in providing the services necessary to meet the requirements, as described in the tender document. The Bidder should also possess the technical know-how and the financial wherewithal that would be required to successfully implement, integrate, and support the Network devices sought by NPCI for the entire period of the contract. The bid must be complete in all respects and should cover the entire scope of work as stipulated in the document. Bidders not meeting the Eligibility Criteria will not be considered for further evaluation.

Eligibility Criteria

The invitation to bid is open to all Bidders who qualify the Eligibility Criteria as given below:

1. The bidder should be a Company registered under the Companies Act, 1956 since the last three years.
2. The bidder should have minimum annual turnover of Rs. 30 crores during the last three financial years (2009-10, 2010-11, 2011-12 or Calendar year 2009, 2010,2011 or the Bidder's financial year).
3. The bidder should be a profit (profit after tax) making company in the last financial year i.e. 2011-12 (or Calendar year 2011 or the Bidder's financial year).
4. The bidder should not be currently blacklisted by any bank / institution in India or abroad.
5. The bidder should have the facility for local support to NPCI at NPCI Operation/Data Centre locations.
6. The bidder should have expertise in deploying/configuring all devices mentioned in the RFP with atleast 2 live installations and support.

Hardware Requirement:

Type	Equipment	Qty
Data Center - Mumbai and Chennai		
1	Perimeter Firewall (Active-Passive appliance needed at both locations)	2
2	DDNS Solution	2
3	Web Application firewall	2
4	Patch panel, Cat 6 patch cables & accessories	*

Technical Specifications:

		TECHNICAL SPECIFICATIONS
		EQUIPMENT SPECIFICATIONS
9.1		**Perimeter Firewall**
	A	**General**
		The Perimeter Firewalls must support the following specifications-
	9.1.1	The Firewall should be Hardware based, purpose-built security appliance with hardened operating system
	9.1.2	The proposed firewall must allow policy rule creation for application identification, user identification, threat prevention, URL filtering, QOS and scheduling in a single rule and not in multiple locations in the management console.
	9.1.3	The Firewall should support IPSec and SSL VPN technologies
	9.1.4	The firewall should support minimum 15 Gbps Firewall Throughput
	9.1.5	The firewall should support minimum 2 Gbps VPN Throughput
	9.1.6	The proposed IPS should support minimum throughput of 3 Gbps

	9.1.7	The firewall should support site to site as well as client based VPN's.
	9.1.8	The firewall should support 20,00,000 Concurrent Connections (2 million)
	9.1.9	The firewall should support 1,20,000 New Connections/ Second - Session setup and Teardown rate
	9.1.10	The proposed firewall should have atleast 12x10/100/1000 interfaces and minimum of 8x1 Gig SFP interfaces and 4x10 Gig SFP with option to expand number of Ethernet ports.
	9.1.11	The proposed firewall should have dedicated management interface
	9.1.12	The proposed firewall should support atleast 500 security zones
	9.1.13	The proposed firewall should support atleast 25 Virtual Systems
	9.1.14	The firewall should have an Ethernet interface for out-of-band device management
	9.1.15	The firewall should support 802.1q VLAN interfaces 802.1q VLAN interfaces
	9.1.16	The firewall should support 100 Virtual Interfaces (VLANs)
	9.1.17	The firewall should support Active/Active and Active/ Standby High Availability feature. Appliance failover should be complete Stateful in nature without any manual intervention.
	9.1.18	Solution should not require any downtime/reboot for failover.
	9.1.19	Authentication for adding new HA members is required.
	9.1.20	Solution should provide stateful failover for IPS and AntiBot functionalities.
	9.1.21	The firewall should support the following functionality: -Application Detection -IPS -Anti-Virus -Anti-Spyware -Botnet detection -URL-Filtering -Data Content Filtering -IPSec VPN -SSL-VPN

		-High Availability -Virtual Systems -QoS (marking and/or traffic shaping)
	9.1.22	The firewall should have Redundant Power Supply
	B	**Operation Mode**
	9.1.23	The proposed firewall must be able to operate in L2 & L3 mode.
	9.1.24	The proposed firewall must be able to support Network Address Translation (NAT)
	9.1.25	The proposed firewall must be able to support Port Address Translation (PAT)
	9.1.26	The proposed firewall must be able to support Policy-based NAT
	9.1.27	The proposed firewall must be able to support Traffic Management QoS per policy
	9.1.28	The proposed firewall must be able to support Network attack detection
	9.1.29	The proposed firewall must be able to support Brute force attack mitigation
	9.1.30	The proposed firewall must be able to support SYN cookie protection
	9.1.31	The proposed firewall must be able to support IP spoofing protection
	9.1.32	The proposed firewall must be able to support Malformed packet protection
	9.1.33	The proposed firewall must support tap mode (via mirrored, taped, or SPAN port)
	9.1.34	The proposed firewall must support transparent mode (layer 1, or bump on the wire)
	9.1.35	The proposed firewall must be able to support DoS and DDoS protection
	9.1.36	The Firewall should support L3 (Routed) mode
	9.1.37	The Firewall should support L2 (Stealth/Transparent) mode
	9.1.38	The Firewall should support Layer 2-7 firewall security services in L2 mode
	9.1.39	The Firewall should support NetFlow or equivalent flow-based technologies
	9.1.40	The Firewall should support dynamic, static and policy-based NAT and PAT services

	9.1.41	The proposed firewall must be able to support TCP reassembly for fragmented packet protection
	9.1.42	The Firewall should support full reassembly of all ICMP error messages
	9.1.43	The Firewall should be capable of limiting TCP and UDP connections and embryonic connections
	9.1.44	The Firewall should allow administrators to test and fine-tune ACLs without the need to remove and replace ACL entries
	9.1.45	The Firewall should support reporting of detailed statistics on which ACL entries are triggered by network traffic
	9.1.46	The Firewall should support filtering based on time-of-day
	9.1.47	The Firewall should support to build ACLs for multicast traffic
	9.1.48	The proposed firewall must have IPv6 Routing Support even for virtual routers.
	9.1.49	The Firewall should support enhanced application inspection capabilities
	9.1.50	The Firewall should support Inspection engines for protocols that embed IP addressing information in the user data packet
	9.1.51	The Firewall should support Inspection engines for protocols that open secondary channels on dynamically assigned ports
	9.1.52	The Firewall should support inspection engines, anomaly detection, state tracking for FTP
	9.1.53	The Firewall should support Network Address Translation (NAT), Port Address Translation (PAT), and dynamic port opening and closing for FTP
	9.1.54	The Firewall should support server obfuscation techniques and additional attack signatures to protect FTP servers from attack
	9.1.55	The Firewall should support IPv6-enabled inspection services for HTTP, FTP, SMTP, ICMP, TCP and UDP
	9.1.56	The Firewall should support per-flow, policy-based QoS services

	9.1.57	The Firewall should support Low Latency Queuing and Traffic Policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications
	9.1.58	The Firewall should support RFC 3377 - Lightweight Directory Access Protocol (v3)
	9.1.59	The Firewall should support RFC 4347 - Datagram Transport Layer Security (DTLS)
	9.1.60	The proposed firewall shall support DNS proxy
	9.1.61	The proposed firewall shall support DHCPv6 relay
	9.1.62	The Firewall should support SSL and IPsec encryption performed by dedicated hardware processors
	C	**Network Integration**
	9.1.63	The Firewall should support Open Shortest Path First (OSPF) with MD5-based OSPF authentication, plain-text OSPF authentication
	9.1.64	The Firewall should support route redistribution between different routing protocols (OSPF, BGP etc.)
	9.1.65	The Firewall should support load balancing across equal-cost multipath routes
	9.1.66	The Firewall should support RIP version 1 & 2 protocol with authentication
	9.1.67	The Firewall should support dual-stack support of IPv4 and IPv6
	9.1.68	The Firewall should support Protocol Independent Multicast (PIM) Sparse Mode v2
	9.1.69	The Firewall should support for Internet Group Management Protocol (IGMPv2)
	9.1.70	The Firewall should support for stub multicast routing
	D	**High Availability**
	9.1.71	The proposed firewall solution must be able to support Active/Active HA configuration (transparent & L3 mode)
	9.1.72	The proposed firewall solution must be able to support Active/Passive HA configuration
	9.1.73	The proposed firewall solution must be capable to detect device failure

	9.1.74	The proposed firewall solution must be capable to detect link and path failure
	9.1.75	Authentication for new HA members
	9.1.76	The proposed firewall solution must be able to support encryption of HA heartbeat & control traffic.
	9.1.77	The proposed firewall shall synchronize the following for HA:
	9.1.78	- All sessions
	9.1.79	- Decryption Certificates
	9.1.80	- All VPN security associations
	9.1.81	- All threat and application signatures
	9.1.82	- All configuration changes
	9.1.83	- FIB tables
	E	**Management**
	9.1.84	The Firewall should syslog with real time monitoring through external syslog servers and accurate time stamping and numbering of syslog messages
	9.1.85	A centralized monitoring and management system with multiple administrators who have administrative rights based on their roles. Should provide Audit Trail of the Changes
	9.1.86	The Firewall should support for dynamically addressed appliances via a central Management Server
	9.1.87	The Firewall should support management over IPv6
	9.1.88	The Firewall should support authentication through a enterprise databases using a AAA server as well as local authentication
	9.1.89	The Firewall should support multiple levels of customizable administrative roles-please specify number
	9.1.90	The Firewall should support ability to generate AAA records for tracking administrative access and configuration changes
	9.1.91	The Firewall should support sending accounting information to multiple AAA servers simultaneously
	9.1.92	The Firewall should support ability to dynamically fall back to the local user database in case of external AAA server outages

	9.1.93	The Firewall should enable administrators to perform configuration rollback, store multiple configurations and software images in compact flash memory
	9.1.94	The Firewall should support automatic wiping flash memory contents if an asset recovery or password reset procedure occurs
	9.1.95	The Firewall should support robust packet-capturing facilities on each interface
	9.1.96	The Firewall should support accessing captured packets through the consoles, secure web access, TFTP file exports
	9.1.97	The Firewall should support administrator alerts when critical events are encountered, by sending e-mail
	9.1.98	Communication between the IPS Management System and the IPS Sensor should be encrypted.
	9.1.99	Vendor must provide signature updates and must have a facility for automatically distributing these updates to all intrusion detection servers in the organization
	9.1.100	Should support latest SNMP version
	9.1.101	In the event of an attack the following activities should be possible
	9.1.102	Send an SNMP Trap to a management console
	9.1.103	Send e-mail to an administrator to notify of the intrusion
	9.1.104	Save the attack information (timestamp, intruder IP address, victim IP address/port, and protocol information).
	9.1.105	Save a trace file of the raw packets for later analysis.
	9.1.106	Forge a TCP FIN packet to force a connection to terminate
	9.1.107	Device should have the capability of backing up the configuration details and the transmission should be encrypted also it should have feature of auto updating of signature files
	9.1.108	The Management System should be able to automatically download the latest signature files off the vendor's web/ftp site.

	9.1.109	Vendor should provide updated signature files at least on weekly basis by making them available on its web/ftp site.
	9.1.110	Solution should have hardened OS for both appliance and management platform
	F	**IPS Features**
	9.1.111	The IPS should support at least Six 10/100/1000BASE-TX.
	9.1.112	Must perform stateful pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.
	9.1.113	Must perform protocol decoding and validation for network traffic including: IP, TCP, UDP, and ICMP.
	9.1.114	Must provide anomaly identification for attacks that may cover multiple sessions and connections, using techniques based on identifying changes in normal network traffic patterns.
	9.1.115	The device should have full virtualization support. Each virtual sensor must be configurable with unique signatures, rules and anomaly detection.
	9.1.116	Virtualized sensor can be managed through CLI and GUI security management tool
	9.1.117	Support creation of baseline of normal network traffic and then uses baseline to detect worm-infected hosts
	9.1.118	The Firewall should offer a “default blocking policy”
	9.1.119	Must identify attacks based on observed deviations in the normal RFC behaviour of a protocol or service.
	9.1.120	Must be able to identify Layer 2 Address Resolution Protocol (ARP) attacks and man-in-the-middle attacks.
	9.1.121	Must have an embedded GUI Based Management interface.
	9.1.122	Must support automated software fail-open.

	9.1.123	User-specified signatures can be created based upon content; i.e. string matching
	9.1.124	Device should have features to prioritize alerts after an alert action is taken place e.g. - if a high priority attack is dropped, the alert should be logged, however if an high priority attack is allowed, the alert should be an email.
	9.1.125	The ability to define a default operating system that will be used in the attack relevance calculation - e.g. if a Linux based attack is targeted towards a windows server, the alert severity of the attack should be lowered.
	9.1.126	Device should have the ability to dynamically understand the risk posed by an attack to the network so as to best adjust the rating of the alert. This risk should be assessed via various parameters like - relevancy of an attack (Linux vs. windows) and value of target (printer vs. server)
	9.1.127	The sensors should be able to detect attacks running inside of these tunnelling protocols - GRE, IP-in-IP, MPLS, and IPv6
	9.1.128	Ability to identify attacks in IPv6 environments through the inspection of IPv4 traffic being tunnelled in IPv6
	9.1.129	The IPS should be able to inspect SSL/https traffic
	9.1.130	Can exceptions be setup to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis
	9.1.131	The product should be resistant to IPS evasion and protection from anti-NIPS (Network Intrusion Prevention System) techniques.
	9.1.132	Proposed solution should have automatic bypass for IPS in case of performance suffer beyond defined administrative threshold or IPS function/engine fails
	G	**Reporting**

	9.1.133	Should provide a comprehensive system for capturing information and making it available for analysis. Should provide the ability to filter, sort, and view the archived information, and to create detailed customised reports.
	9.1.134	Must give detailed statistical reports on numbers of policy violations and where they came from, web usage, protocol distribution etc.
	9.1.135	Product should have a comprehensive “drill-down” querying and reporting facility of intrusion events that took place off the database
	9.1.136	Product should provide real-time statistics of the intrusion events detected, which could be represented in a graphical form.
	H	**Policy based controls**
	9.1.137	The proposed firewall shall control parameters by security Zone, Users, IP, Application, Schedule, QOS etc.
		The proposed firewall shall support the following policy types/capabilities:
	9.1.138	Policy-based control by port and protocol
	9.1.139	Policy-based control by application and/or application category (non-port based)
	9.1.140	Policy-based control by user, group or IP address
	9.1.141	Block files by type: bat, cab, dll, exe, pif, and reg
	9.1.142	Data filtering: Credit Card Numbers etc.
	9.1.143	Data filtering: Custom Data Patterns
	9.1.144	QoS Policy-based traffic shaping (priority, guaranteed, maximum)
	9.1.145	QoS Policy-based diffserv marking
	9.1.146	Policy support of IPv6 rules/objects
	9.1.147	Policy support of multicast rules/objects
	9.1.148	Policy support for scheduled time of day enablement
	9.1.149	The proposed firewall shall control parameters by security Zone, Users, IP, Application, Schedule, QOS etc.
	I	**Application Security**

	9.1.150	The proposed firewall shall support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic
	9.1.151	The proposed firewall shall have multiple mechanisms for classifying applications
	9.1.152	The proposed firewall shall have application identification technology based upon IPS or deep packet inspection
	9.1.153	The proposed firewall shall be able to handle unknown/unidentified applications e.g. alert, block or allow
	9.1.154	The proposed firewall shall be able to create custom application signatures and categories
	9.1.155	The proposed firewall shall include a searchable list of currently identified applications with explanation and links to external sites for further clarification
	9.1.156	The proposed firewall shall warn the end-user with a customizable page when the application is blocked
	9.1.157	The proposed firewall shall allow port-based controls to be implemented for all applications
	9.1.158	The proposed firewall shall delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.)
	9.1.159	The proposed firewall shall delineate specific instances of instant messaging (AIM, YIM, Facebook Chat, etc.)
	9.1.160	The proposed firewall shall delineate different parts of the application such as allowing chat capability but blocking its file-transfer capability
	9.1.161	The proposed firewall shall delineate specific instances of Proxies (ultrasurf, ghostsurf, freegate, etc.)
	9.1.162	The proposed firewall shall support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)
	9.1.163	The proposed firewall shall be able to create filters to control groups of application based on category, sub category, technology , risk or characteristics etc.

	9.1.164	The proposed firewall shall support user-identification allowing Active Directory, LDAP, RADIUS groups, or users to access a particular application, while denying others
	J	**Data Filtering**
	9.1.165	The proposed firewall shall support file identification by signature and not only file extensions.
	9.1.166	The proposed firewall shall support identification and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)
	9.1.167	The proposed firewall shall support compressed information stored in zipped format and be able to unpack and filter per policy
	9.1.168	The firewall shall be capable of identifying and optionally preventing the transfer of files containing sensitive information (i.e. credit card numbers) via regular expression
	9.1.169	List applications supported for data-filtering
	9.1.170	List file-types supported for data-filtering
	K	**User Identification**
		The proposed firewall shall support authentication services for user-identification:
	9.1.171	- Active Directory
	9.1.172	- LDAP
	9.1.173	- eDirectory
	9.1.174	- RADIUS
	9.1.175	- Kerberos
	9.1.176	- Client Certificate
	9.1.177	The proposed firewall shall support user-identification in policy
	9.1.178	The proposed firewall shall support user-identification from terminal services environments in policy and logs
	L	**QoS**
		The proposed firewall should support the ability to create QoS policy on a per rule basis:
	9.1.179	- by source address

	9.1.180	- by destination address
	9.1.181	- by user/user group as defined by AD
	9.1.182	- by application (such as Skype, Bit torrent, YouTube, azureus)
	9.1.183	- by static or dynamic application groups (such as Instant Messaging or P2P groups)
	9.1.184	- by port
		The proposed firewall shall define QoS traffic classes with:
	9.1.185	- guaranteed bandwidth
	9.1.186	- maximum bandwidth
	9.1.187	- priority queuing
	M	**VPN**
	9.1.189	The proposed firewall shall support IPSec/SSL VPN
	9.1.190	The proposed firewall shall support NAT T
	9.1.191	IPSec VPN should be integrated with the proposed firewall and support full encryption standards suites:
	9.1.192	- DES, 3DES, AES
	9.1.193	- MD5 and SHA-1 authentication
	9.1.194	- Diffie-Hellman Group 1 , Group 2 and Group 5
	9.1.195	- Internet Key Exchange (IKE) algorithm
	9.1.196	-Should support redundant VPN gateway
	9.1.197	- AES 128, 192 & 256 (Advanced Encryption Standard)
	N	**Authentication**
		The proposed firewall administrative module shall support the following authentication protocols:
	9.1.201	- LDAP
	9.1.202	- Radius (vendor specific attributes)
	9.1.203	- Token-based solutions (i.e. Secure-ID)
	9.1.204	- Kerberos
		The proposed firewall's SSL VPN shall support the following authentication protocols
	9.1.205	- LDAP
	9.1.206	- Radius
	9.1.207	- Token-based solutions (i.e. Secure-ID)
	9.1.208	- Kerberos
	9.1.209	- Any combination of the above
	O	**TCP Dump/PCAP**

		The proposed firewall shall support packet captures based on:
	9.1.210	- Source Address
	9.1.211	- Destination Address
	9.1.212	- Applications
	9.1.213	- Unknown Applications
	9.1.214	- Port
	9.1.215	- any threat
	9.1.216	- data-filters
	9.1.217	- any combination of the above
	9.1.218	The proposed firewall shall support PCAP downloads of specific traffic sessions from the GUI from the logging screen
	P	**Malware Prevention**
	9.1.219	The proposed firewall shall support automated signature generation for discovered malware
	9.1.220	should be able to identify suspicious activities such as participating in DDoS attacks, self distribution attempts
	9.1.221	should have reputation based database on malicious Bot network along with the white listing/black listing for the Sites (URL/DNS/IP)
	9.1.222	should provide automatic updates to the Anti- latest IP/URL/DNS reputation data and botnet communication patterns.
	9.1.223	The proposed firewall shall support inline control of malware infection and command/control traffic
	Q	**Threat Prevention**
	9.1.224	The proposed firewall shall support IPS features on the proposed firewall hardware
	9.1.225	The proposed firewall shall support Anti-Virus and Anti-Spyware on the proposed firewall.
	9.1.226	The proposed firewall shall block application vulnerabilities.
	9.1.227	The proposed firewall shall block spyware and malware.
	9.1.228	The proposed firewall shall block known network and application-layer vulnerability exploits

	9.1.229	The proposed firewall shall block buffer overflow attacks
	9.1.230	The proposed firewall shall block DoS/DDoS attacks
	9.1.231	The proposed firewall shall be able to perform Anti-virus scans for SMB traffic
	9.1.232	The proposed firewall shall support attack recognition for IPv6 traffic the same way it does for IPv4
	9.1.233	The proposed firewall shall support Built-in Signature and Anomaly based IPS engine on the proposed firewall
	9.1.234	The proposed firewall shall support the ability to create custom user-defined signatures
	9.1.235	The proposed firewall shall support be able to exclude certain hosts from scanning of particular signatures
	9.1.236	The proposed firewall shall support CVE-cross referencing where applicable
	9.1.237	The proposed firewall shall support granular tuning with option to configure overrides for individual signatures
	9.1.238	The proposed firewall shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)
	9.1.239	The proposed firewall Threat/Anti-Virus/Anti-Spyware updates shall not require reboot of the unit.
	9.1.240	The proposed firewall shall support the same signature packages across all platforms and models
	9.1.241	The proposed firewall shall support several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc.
	9.1.242	The proposed firewall shall support response adjustment on a per signature basis.

		TECHNICAL SPECIFICATIONS
		EQUIPMENT SPECIFICATIONS
		DDNS Solution
	A	**General**
	9.2.1	Augments and optimizes the DNS infrastructure by taking over the domain resolution process for content requests and delivery for all types of static and dynamic Web content, and processes the request-responses at thousands of requests per second.
	9.2.2	Ensure application availability across different sites
	9.2.3	Scale DNS performance up to 10x in throughput
	9.2.4	Ensure global load balancing across data centres and should be scalable too.
	9.2.5	Geographic load balancing.
	9.2.6	Infrastructure and application health monitoring.
	9.2.7	DR / BCP planning
	9.2.8	DNS persistency and resolving
	9.2.9	Ensure application security against dDOS (DNS Denial of Service), cache poisoning and DNS hijacking.
	9.2.10	Should support DNSSEC completely
	9.2.11	Ensure the device should be hardened OS and there is no open vulerability
	B	**Technical Specifications**
	9.2.12	Should be able to process > 20,000 maximum sustained DNS for moderately complex, 1000+ VIPs configuration
	9.2.13	Should be able to forward > 1000 name server forwarding requests per second
	9.2.14	Should support 150 + load balancers and 1000 DNS rules
	9.2.15	Should have a keep alive time of 60 seconds or less
	9.2.16	Should work on power of 100 – 240 V AC
		Should have at least :
	9.2.17	• 8 x 1000/100/10 BASE-T Ethernet ports

	9.2.18	• Console serial port (for out of band management)
	9.2.19	Should have redundant power supply.
	9.2.20	Should be single U
	9.2.21	High MTBF of more than 1,85,000 Hours, validated by third party
	9.2.22	Should support 1 Gbps Throughput and upgradable to 4 Gbps in future without additional hardware
	C	**DNS Load Balancing**
	9.2.23	Should support load balance traffic based on DNS names
	9.2.24	Should support load balance traffic based on DNS query types
	9.2.25	Should support load balance traffic based on DNS versus DNSSEC queries.
	9.2.26	Should support load balance traffic based on character of DNS name in query
	9.2.27	Should support redirect traffic based on query for single domain but of different type like A, AAAA, MX and DNSKEY for all hostnames / subdomains.
	D	**Management**
	9.2.28	Device should have web based user interface in order for management purposes
	9.2.29	Device should be easy to setup and synchronize.
	9.2.30	Device configuration should be stored and it should be possible to retrieve the last configuration.
	9.2.31	Device should monitor the DNS server health on TCP and UDP both
	9.2.32	Device should support latest SNMP version.
	9.2.33	Device should be able to integrate with multiple application network equipment (L4-7) like servers, routers, load balancers etc
	9.2.34	Device should be able to support IP v4 and IP v6
	9.2.35	Supports role-based access control (RBAC) and operation to limit access to the device

Sl. No.	Sub. Serial No.	TECHNICAL SPECIFICATIONS
		EQUIPMENT SPECIFICATIONS
9.3		**WAF Equipment**
	A	**General**
	9.3.1	Should support minimum 1 Gbps throughput
	9.3.2	Must have minimum 5 interfaces and one dedicated management port.
	9.3.3	Should be able to run on virtualized infrastructure.
	9.3.4	Should support both IPv4 and IPv6 addresses
	B	**Threat Prevention**
	9.3.5	Should support HTTP, XML, AJAX and JASON Protocols
	9.3.6	Should support positive and negative deployment model
	9.3.7	Should support traffic learning on the same appliance without increased latency.
	9.3.8	Should support IP Reputation
	9.3.9	Should support online & manual attack signature database
	9.3.10	should mitigate zero day attack with script engine
	C	**Deployment**
		WAF should have the flexibility to be deployed in the following modes:
	9.3.11	Bridge Mode
	9.3.12	Transparent Proxy Mode
	9.3.13	Reverse Proxy Mode
		Should support following failover mechanisms during hardware failure:
	9.3.14	Fail - open
	9.3.15	Fail - Close
	9.3.16	The WAF should decrypt the encrypted traffic to get access to the HTTP data.
	9.3.17	Client Authentication based on client (SSL) certificated should be available
	9.3.18	WAF should support different policies for different web applications
	9.3.19	WAF should support web application level role-based management
	9.3.20	WAF should support adding exceptions to policy from the security events

	9.3.21	WAF should support defining exceptions on policy per page or parameter
		WAF should support configuration of web application defined by:
	9.3.22	virtual hosts (host name)
	9.3.23	physical hosts (web server ip/port)
	9.3.24	a web server folder
	9.3.25	WAF should support different policies for different application section (different security zones within the app)
	9.3.26	WAF should support different enforcement modes (active, passive) on different sections of the application
	9.3.27	WAF should not just depend on manual configuration but should support auto learning of application paths and associated vulnerabilities by itself without depending on external vulnerability scanners.
	9.3.28	WAF should protect while learning
	9.3.29	WAF should restrict file upload by file type and upload destination
	9.3.30	WAF should support negative (out-of-the-box) and positive (application tailored) security models
	9.3.31	WAF should support dynamic source IP blocking based on the attack scores.
	9.3.32	WAF should support masking sensitive content in response - Data Leakage Prevention
	9.3.33	WAF should support custom defined (regular expression) sensitive content for masking in response
	9.3.34	WAF should support response replacement in case of error messages in web server response
	9.3.35	WAF should support Layer 7 Whitelisting and Blacklisting
	9.3.36	WAF should support Parameter signing.
	9.3.37	WAF should support Parameter Encryption.
	9.3.38	WAF should support hidden form fields signing and encryption.
	9.3.39	should support integration with Third Party Vulnerabilities Scanners like Whitehat , Cenzic etc
	9.3.40	Should support importing XML File from Vulnerabilities Scanners to mitigate application bugs
	9.3.41	Should support configuration and reporting on same appliance
	9.3.42	Should support integration with third party SIEM Solution
	9.3.43	WAF should support cookie encryption and signing.
	D	**Attack Prevention**
		WAF should protect against the following (but not limited to)
	9.3.44	brute force
	9.3.45	Cookie Poisoning
	9.3.46	session hijacking

	9.3.47	parameter tampering
	9.3.48	XML injection
	9.3.49	SQL Injection
	9.3.50	LDAP and XPath injections
	9.3.51	OS commanding
	9.3.52	cross site scripting (XSS)
	9.3.53	Cross-site Request Forgery (CSRF)
	9.3.54	HTTP response splitting
	9.3.55	header injection
	9.3.56	path traversal
	9.3.57	remote file inclusion
	9.3.58	buffer overflow
	9.3.59	null byte injection
	9.3.60	dictionary attacks
	9.3.61	automation and excessive data access
	9.3.62	uploading of executable files
	9.3.63	known web server vulnerability
	9.3.64	Geo Location and Client Source IP address based Security Policy
	9.3.65	ICAP integration with DLP server
	9.3.66	Base64 Encoded attacks blocking
	9.3.67	WAF should support LDAP integration for user authentication
	9.3.68	WAF should support user tracking and authentication to provide accurate policies to prevent fraud.
	9.3.69	WAF should support geo-location based policies.
	9.3.70	blocking JSON-injection and NO-SQL database attacks
	E	**Auto Policy Generation**
	9.3.71	WAF should support learning all web application pages for Layer 7 access control
	9.3.72	WAF should support learning the application structure, resources, and legitimate value ranges
	9.3.73	WAF should support automatically identify application traffic attributes & build dynamic traffic profile
	9.3.74	WAF should support automatically analyze the security threats residing in the application
	9.3.75	WAF should support auto activate security modules to block attacks which exploit identified vulnerabilities
	9.3.76	WAF should support automatically switch from learning to active mode once policy is optimized
	9.3.77	WAF should support automatically creates the application tailored rules for the different security modules
	F	**Logging, Reporting and Alerting**

	9.3.78	WAF should support logging all blocking, reset, and other protection/prevention actions
	9.3.79	WAF should support configurable request and response logging
	9.3.80	Should mask sensitive content in logs
	9.3.81	report filtering for audit and remediation review
	9.3.82	automatic report generation and distribution
	9.3.83	sending reports to a predefined list of email addresses
	9.3.84	hierarchical attack logs with drill-down capabilities for attack analysis
	9.3.85	Selectable report formats: HTML, PDF & XML.
	9.3.86	real-time dashboards such as top attacks view, traffic monitoring view, etc.
	9.3.87	detailed reports for all web application attacks
	9.3.88	detailed PCI compliance report with action plan to achieve compliance
	9.3.89	report distribution using email
	9.3.90	Should Alerting via SNMP, Syslog and email
	F	**System Management**
	9.3.91	WAF should support security policy backup
	9.3.92	WAF should support policy distribution from one device to another
	9.3.93	WAF should support system configuration via HTTPS and SSH
	9.3.94	LDAP based management user authentication
	9.3.95	Radius based management user authentication
	9.3.96	NTP clock synchronization

Bid Schedule and Address

Sr.No.	Description	Detailed Information
1	Name of Project	RFP for Supply, Installation, Commissioning and Maintenance of Firewall & DDNS Solution
2	Tender Reference Number	NPCI:RFP:2012-13/0035 dated 26.02.2013
3	Date of sale of Bidding Document	26.02.2013
4	Last date and time for receiving Bidders Pre-Bid clarifications in writing	13.03.2013 6.30PM
5	Date and Time for Pre Bid Meeting	20.03.2013
6	Address of Pre Bid meeting location	National Payments Corporation of India 13th Floor, R Tech Park, off western express highway, Nirlon Complex, Near HUB mall , Goregaon-East, Mumbai – 400063
7	Last date and time for Bid Submission	01.04.2013 3.00PM
8	a) Date and Time for Opening of Envelope A i.e. Eligibility criteria b) Date and Time for Opening of Envelope B-Technical Bid c) Date and time for Opening of Envelope C i.e. Commercial Bid	01.04.2013 Will inform to the Eligible qualified Bidders Will inform to the Technical qualified Bidders
9	Place for Bid Submission & Eligibility Bid Opening.	National Payments Corporation of India 13th Floor, R Tech Park, off western express highway, Nirlon Complex, Near HUB mall , Goregaon-East, Mumbai – 400063
10	Name and Address for Communication	Head - IT Procurement National Payments Corporation of India 13th Floor, R Tech Park, off western express highway, Nirlon Complex, Near HUB mall , Goregaon-East, Mumbai – 400063
11	Bid Related Queries	**Mr. Rajesh Nadkarni : 91 8108186541** Email: Rajesh.Nadkarni@npci.org.in **Mr. Vinay Tiwari: +91 8108122828** Email:Vinay.Tiwari@npci.org.in **Mr. Prashant Awale: +91 8108108650** Email: prashant.awale@npci.org.in
12	Bid Cost	Rs. 11,236.00 (Rs.10,000.00 plus Service Tax@12.36%))
13	EMD/Bid Security	Rs.5,00,000/-