ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
Type	Next Generation Enterprise Firewall in HA	Fortigate/PaloAlto	
3rd Party Test Certification	The proposed vendor must be in the Leader's quadrant of the Enterprise/OT Firewalls Gartner Magic Quadrant for consecutive 5 years		
Form factor	The NGFW appliance should be of max 1 RU rack space		
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 16GB or above memory with Minimum 8 Core or above processors from day 1.There should not be any proprietary ASIC based solution		
Storage RAID1	The NGFW should have at least 200GB solid-state drive for System storage		
Interface Requirement	Minimum 12 Ports required along with dedicated of HA ports/ interfaces from day 1 - BRPL will create 08 Zones for network seggrgation and 04 Interfaces are required for Future usage		
	One each Console Management, Micro USB and USB Port		
	Dedicated HSCI 10G high availability port with active optical cable of minimum 5 meter length		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
Performance Capacity	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 4.5Gbps throughput considering 64KB HTTP transaction size . The bidder shall submit the performance test report for the same		
	Also proposed appliance must support SCADA protocols like IEC-104 ,DNP3 & Modbus for OT security.		
	IPsec VPN throughput – minimum 5Gbps or more with 64KB HTTP transaction and logging enabled		
	VLAN on single Gateway-1000		
	New sessions per second – Min 140K considering 1 byte HTTP transaction size with AVC ON/application override enabled		
	Concurrent sessions – Min 1.4 Million		
SSL Decryption Sessions	NGFW appliance should support 100K Concurrent SSL decryption sessions		
High Availability	Active/Active , Active/Passive and HA clustering support . Should also ability to configure interface/Zone based HA		
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		
	which identifies applications across all ports irrespective of port/protocol/evasive tactics.		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
Next Generation Firewall Features	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.		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
	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.		

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
Threat Protection	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		
	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		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
	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. If the cloud based sandbox solution is not available then on-premise hardware based sandobx solution should be deployed for 26 VMs in HA		
	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		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
	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.		
OT Security	The Proposed NGFW shall Protect control systems and SCADA environments from threats emanating enterprise systems.		
	The Proposed NGFW shall provide visibility over OT, IIOT, and IT traffic. Provide protection against known Exploits, Malware, Block commands, and Control traffic.		
	The Proposed NGFW shall support deployment in Layer 3, TAP Mode, virtual wire mode and capable to Segment between the different levels in ICS using IEC 62443 standards.		
	The Proposed NGFW to have capabilities to support ICS/SCADA-specific protocols including BACNet, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), MMS, Modbus, OPC, Profinet, S7 (Siemens), Cygnet. It shall be able to detect and prevent exploits of ICS vulnerabilities with SCADA IPS signatures, closing the window of exposure between vulnerable and patched systems.		
	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)		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
SSL/SSH Decryption	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		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
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		
Routing and Multicast support	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		
	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		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
	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		
	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 order to prevent rogue administrators from misusing keys.		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
Monitoring, Management and Reporting	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		
	Firewall Policy management and deployment should be GUI and dedicated		
	Should support creation of report based on custom query for any logging attributes		

Bidder's Seal Singnature

ANNEXURE-XIII

Corrigendum - II

REVISED BOQ

Hardware BoQ for BRPL-SCADA-MCC-BCC Core Firewall Solution (NGFW , Lag Manager , Policy deployment) Qto 04

Features	Specification	Make (OEM Cisco not required)	Compliance (Yes/No)
Authorization	Original Manufacturer Authorization Certificate to be submitted along with the bid. We reserves the right to reject in case deviation on the basis of technical compliance as submitted in the tender document.		
Log Manangement	Device/Solution Should support storage of 6 Months Logs or enable integration withNAs or NMS application / hardware		
Installtion,Configuration ,Support & Warranty	Bidder Ensure 5 Year Warranty term with 30 min Response and 4 Hours resolution of tickets through ticketing tool(For P1 complaints where Physical Hardware needs to replace NBD support should be available) The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, Anti Virus , Anti Spyware, Threat Protection, APT Protection (Zero Day Protection), from day 1. Also must have license to provide security for OT which includes IEC-101-104,DNP3 & Modbus protocols.		

Bidder's Seal Singnature