Directorate General, ITBP Force
MHA, Government of India,
Block No.-02, CGO Complex,
Lodhi Road, New Delhi-110003

No.I-45024/11/ICT/DataCentre/2025- 195 Date :- 28.04.2025

Subject : Invitation for comments of Vendors/ OEM/System Integrators(SI)/ Industry players on Draft QRs of **"ITBP Data Centre"**

The Draft QRs of various products of Data Centre are attached as Appendix 'A'. The OEM/Vendors are requested to forward their comments on draft QRs with full justifications. If possible and required please enclose supporting documents. The firms are also requested to furnish the following details:-

- Whether you are OEM/ Vendor?
- If Vendor, then details of OEM.
- Authorization certificate from OEM.
- Contact details with name, email and mobile no.

2. The required information/ details may please be forwarded at the following address within 15 days from the date of publication on MHA/ITBP website.

Communication Directorate, ITBP
Block-2 , CGO Complex
Lodhi Road, New Delhi - 110003
Email:- itproc@itbp.gov.in
(For any query please contact on mobile - 7000719523)

3. An early response is requested.

Digitally signed by
ROSHAN LAL THAKUR
Date: 25-04-2025
16:17:10

DIG(Communication)
Comn Dte, ITBP
Director General, ITBP

HCI Hyper Convergent Infrastructure (6 Node)

S.N	Specifications	Requirement	Compliance (Yes/No)	References (Document/Page No)
1	Type of HCI	Generic node HCI (consisting both Compute and Storage)		
2	Total usable Cores available (after installation of HCI software resources).	Min 320		
3	Total usable Storage in TB available without using De-duplication, Compression (after installation of HCI software resources).	Min 50 TB NVMe SSD		
4	Total usable RAM in GB available (after installation of HCI software resources).	Min 6 TB		
5	Types of data copies across Cluster available in the offered solution.	2		
6	Number of Sockets offered per Node	2		
7	Number of Cores per Sockets	Min 32		
8	Number of populated Processor per Node	2		
9	Type of Processor offered in the system	5th Generation Intel® Xeon Gold/2.4GHz/DDR5 or equivalent AMD Zen 4 EPYC™ or better		
10	Indicate Processor Model number with Make	Intel/AMD		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

11	Type of storage media offered with the solution	NVMe SSD		
12	RAM Capacity (Raw) offered per node in GB.	Min 1200 GB		
13	Number of Network ports per node	4		
14	Throughput Per Network port	Min 10 Gbps		
15	Type of Network port	Optical (SFP+)		
16	IOPS delivered at 70:30 Read: Write Ratio on 8K block size with latency of 5ms maximum for each node	Min 70000		
17	Scalability: Any additional node/ storage/ RAM added to the cluster to augment compute/storage/memory capacities, the same performance per node on upgraded node / Storage / RAM	YES		
18	HCI Features 1	1. HCI have all the features of offered industry standard hypervisor. 2. HCI have independently scale storage and compute as and when needed without any downtime. 3. HCI have mechanism for Metadata protection for all offered nodes within the cluster so as to provide high availability and no single point of failure. 4. HCI is configuration of SSD/SAS/NVMe then the caching must		

		be on appropriate capacity of SSD/ NVME drives to meet the IOPS/performance requirements. 5. HCI supports thin provisioning of both storage entities and virtual machine hard disks. 6. HCI provides automatic failover in case of hardware failure.		
19	HCI Features 2	1. HCI provides management through a remote/On premise GUI console. Also provides storage, compute & hypervisor metrics on aper VM /Node level as well as health and monitoring of entire platform. 2. Platform support LDAP Active Directory integration. The clients installed on any major Operating System. 3. Platform supports monitoring via SNMPv3, email alerting via SMTP. 4. Capable of creating instant snapshots of virtual machines and maintaining multiple copies of snapshots & clones. 5. Capability to support native VM/HCI level replication for installed Hypervisor.		

20	HCI Features 3	1. Redundant components with no single point of failure in the system. 2. Intelligent Optimum data distribution across all nodes. 3. HCI support container-based application. 4. Single management tool supports multiple clusters. 5. Management tool is built into the solution, scales with the cluster. 6. HCI capable to sustain single power supply failure.		
21	Encryption	Yes (At Rest Encryption)		
22	Supports	Anti-Spyware, Antivirus and Anti malware		
23	Supported industry protocols by HCI	NFS, SMB and Iscsi		
24	HCI capability to support File/Block Services and file/block replication across clusters for	NFS, CIFS, SMB, ISCSI and S3, NFS & CIFS		
25	Inline data Compression & Deduplication function licenses requirement.	Unlimited		
26	Number of nodes HCI supports in same cluster/deployment, such that any node out of the offered be able to use the storage of all other nodes	Min 32		

27	Hypervisor to be integrated with SDS	Within/Outside kernel		
28	HCI support	AHV (Acropolis Hypervisor), Hyper-V, V-Sphere		
29	Bare-metal / non-bare metal type of virtualization hypervisor	Bare-Metal		
	Additional mandatory specifications			
30	Physical structure	All the components of HCI, i.e. CPU, RAM, Disks should be physically inside the HCI node and no component should be provisioned from outside the node.		
31	Disk Retention	In case of faulty hard disk replacement during the warranty period or out of warranty, the Faulty Hard Disk Storage will be retained.		
32	Control of East-West Traffic	Solution must have Micro segmentation/Distributed Firewall for east & west traffic security natively through HCI.		
33	Security certifications	At least FIPS-140, CCC and EAL2 certifications required.		
34	Cluster scalability	The cluster should be scalable upto at least 32 nodes and all these 32 nodes should be generic, i.e. consisting of both compute & storage.		
35	Replication Factor	The HCI solution should be capable of configuring storage in both RF2 and RF3 depending on the need at the time of implementation.		
36	GPU support	The supplied HCI solution should be capable of hosting at least 1 GPU card per node in case of future requirement.		
37	Integration ability with public cloud	Capable of integrating with public cloud and able to provide unified management.		

38	Replication and DR Automation	Offered platform shall support Stretch cluster across locations while ensuring that dual write is being maintained at each location. Replication across locations shall be able to natively manage or monitor inside the platform. Replicated from DC To DR should be in encrypted form or vise-versa. Offered Platform shall have ability to replicate only incremental changes between two sites (Primary and Secondary). Offered platform shall support asynchronous replication from primary location to at-least two secondary locations for a given volume / Data store. It shall provide the flexibility to define the separate schedule for each replication relationship. The solution should be able to replicate and DR automation for 100VMs (scalable up to 200) natively form HCI.		
39	Past experience	The OEM directly or through its resellers must have successfully supplied and configured the proposed HCI solution of more than 5 nodes at any central/PSU/state govt. At least one such projects in each of the last 5 years should be cited along with their satisfactory installation report.		
40	Compute & Processing Power	Trusted Platform Module (TPM) 2.0 support, which is critical for hardware security. Evaluavated Solutions are very well certified the nVidia Based GPUs to run any AI/ML application. GPU can be added at initial stage or at any stage as & when requirement arise.		

41	Network & Connectivity	Should have 25G/40G SFP ports or better network port expandability for future scalability and Specify Layer 3 networking support to improve inter-node communication. Evaluated Solution is certified to work with 10/25/40/100Gbps Network, looking at the requirement and backend infra, department is going ahead with 10Gbps interfaces.		
42	Security & Encryption	Should have hardware-based root-of-trust security (e.g., Intel SGX, AMD SEV) and define monthly security patching requirements. Solution will have capabilities to control East & West traffic to minimize the lateral spread of any new age threats and data would be in encrypted stage all the time.		
43	Virtualization & Management	Should have native support for containerized workloads (Docker, Kubernetes).		
44	Memory & Storage	Evaluated solution support Hybrid (SSD+HDD), All Flash (NVMe or SSD or combination) based on the customer requirement. Offered solution has built-in intelligence to tier the data automatically and frequently accessed data always will be on fastest tier.		
45	Fault Tolerance	Should have complete replication and DR automation services built-in.		

HCI (Hyper Convergent Infrastructure) (4 Node)

S.N	Specifications	Requirement	Compliance (Yes/No)	References (Document/Page No.)
1	Type of HCI	Generic node HCI (consisting both Compute and Storage)		
2	Total usable Cores (after installation of HCI software resources required for solution)	Min 160 Physical Cores		
3	Total usable Storage in TB available without using De-duplication, Compression (after installation of HCI software resources required for solution).	Min 50 TB NVMe SSD		
4	Total usable RAM in GB available (after installation of HCI software resources required for solution).	Min 6 TB		
5	Types of data copies across Cluster available in the offered solution.	2		
6	Number of Sockets offered per Node	2		
7	Number of Cores per Sockets	Min 32		
8	Number of populated Processor per Node	2		
9	Type of Processor offered in the system	5th Generation Intel® Xeon Gold/2.4GHz/DDR5 or equivalent AMD Zen 4 EPYC™ or better		
10	Indicate Processor Model number with Make	Intel/AMD		
11	Type of storage media offered with the solution	NVMe SSD		

12	RAM Capacity (Raw) offered per node in GB	Min 1200 GB		
13	Number of Network ports per node	4		
14	Throughput Per Network port	Min 10 Gbps		
15	Type of Network port	Optical (SFP+)		
16	IOPS delivered at 70:30 Read: Write Ratio on 8K block size with latency of 5ms maximum for each node	Min 70000		
17	Scalability: Any additional node/ storage/ RAM added to the cluster to augment compute/storage/memory capacities, the same performance per node on upgraded node / Storage / RAM	YES		

18	HCI Features 1	1. HCI have all the features of offered industry standard hypervisor. 2. HCI have independently scale storage and compute as and when needed without any downtime. 3. HCI have mechanism for Metadata protection for all offered nodes within the cluster so as to provide high availability and no single point of failure. 4. HCI is configuration of SSD/SAS/NVMe then the caching must be on appropriate capacity of SSD/NVME drives to meet the IOPS/performance requirements. 5. HCI supports thin provisioning of both storage entities and virtual machine hard disks. 6. HCI provides automatic failover in case of hardware failure.		
19	HCI Features 2	1. HCI provides management through a remote/On premise GUI console. Also provides storage, compute & hypervisor metrics on as per VM /Node level as well as health and monitoring of entire platform. 2. Platform support LDAP Active Directory integration. The clients installed on any major Operating System.		

		3. Platform supports monitoring via SNMPv3, email alerting via SMTP. 4. Capable of creating instant snapshots of virtual machines and maintaining multiple copies of snapshots & clones. 5. Capability to support native VM/HCI level replication for installed Hypervisor.		
20	HCI Features 3	1. Redundant components with no single point of failure in the system. 2. Intelligent Optimum data distribution across all nodes. 3. HCI support container-based application. 4. Single management tool supports multiple clusters. 5. Management tool is built into the solution, scales with the cluster. 6. HCI capable to sustain single power supply failure.		
21	Encryption at	Yes (At Rest Encryption)		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

22	Supports	Anti Spyware, Antivirus and Anti malware.		
23	Supported industry protocols by HCI	NFS, SMB and Iscsi.		
24	HCI capability to support File/Block Services and file/block replication across clusters for	NFS, CIFS, SMB, ISCSI, S3, NFS and CIFS.		
25	Inline data Compression &Deduplication function licenses	Unlimited		
26	Number of nodes HCI supports in same cluster/deployment, such that any node out of the offered be able to use the storage of all other nodes	32		
27	Hypervisor to be integrated with SDS	Within/Outside kernel		
28	HCI support	AHV (Acropolis Hypervisor), Hyper-V and V-Sphere		
29	Bare-metal / non-bare metal type of virtualization hypervisor	Bare-Metal		
	Additional mandatory specifications			
30	Physical structure	All the components of HCI, i.e. CPU, RAM, Disks should be physically inside the HCI node and no component should be provisioned from outside the node.		
31	Disk Retention	In case of faulty hard disk replacement during the warranty period the Faulty Hard Disk Storage will be retained.		

32	Control of East-West Traffic	Solution must have Micro segmentation/Distributed Firewall for east & west traffic security natively through HCI.		
33	Security certifications	At least FIPS-140, CCC and EAL2 certifications required.		
34	Cluster scalability	The cluster should be scalable upto at least 32 nodes and all these 32 nodes should be generic, i.e. consisting of both compute & storage.		
35	Replication Factor	The HCI solution should be capable of configuring storage in both RF2 and RF3 depending on the need at the time of installation.		
36	GPU support	The supplied HCI solution should be capable of hosting at least 1 GPU card in case of future requirement.		
37	Integration ability with public cloud	Capable of integrating with public cloud and able to provide unified management.		
38	Replication and DR Automation	Offered platform shall support Stretch cluster across locations while ensuring that dual write is being maintained at each location. Replication across locations shall be able to natively manage or monitor inside the platform. Offered Platform shall have ability to replicate only incremental changes between two sites (Primary and Secondary).		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

		Offered platform shall support asynchronous replication from primary location to at-least two secondary locations for a given volume / Datastore. It shall provide the flexibility to define the separate schedule for each replication relationship. The solution should be able to replicate and DR automation for 100VMs (scalable up to 200) natively form HCI.		
39	Past experience	The OEM directly or through its resellers must have successfully supplied and configured the proposed HCI solution of more than 5 nodes at any central/PSU/state govt. At least one such projects in each of the last 5 years should be cited along with their satisfactory installation report.		
40	Compute & Processing Power	Should have Trusted Platform Module (TPM) 2.0 support, which is critical for hardware security. Evaluavated Solutions are very well certified the nVidia Based GPUs to run any AI/ML application. GPU can be added at initial stage or at any stage as & when requirement arise.		
41	Network & Connectivity	Should have 25G/40G SFP ports or better network port expandability for future scalability and Specify Layer 3 networking support to improve inter-node communication. Evaluated Solution is certified to work with 10/25/40/100Gbps Network, looking at the requirement and backend infra, department is going ahead with 10Gbps interfaces.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

42	Security & Encryption	Should have hardware-based root-of-trust security (e.g., Intel SGX, AMD SEV) and define monthly security patching requirements. Solution will have capabilities to control East & West traffic to minimize the lateral spread of any new age threats and data would be in encrypted stage all the time.		
43	Virtualization & Management	Should have native support for containerized workloads (Docker, Kubernetes).		
44	Memory & Storage	Evaluated solution support Hybrid (SSD+HDD), All Flash (NVMe or SSD or combination) based on the customer requirement. Offered solution has built-in intelligence to tier the data automatically and frequently accessed data always will be on fastest tier.		
45	Fault Tolerance	Should have complete replication and DR automation services built-in.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

NGFW (External)

S.N	Specifications	Compliance Yes/No	References (Document/Page No.)
A	**Eligibility Criteria**		
1	Solution should be purpose build hardware appliance.		
2	The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials to raise the technical issues in the name of customer, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful Bidder must provide the login credentials.		
3	The provided hardware should not be end of support during the contractual period. It should continue to provide		
	a) Upgrades and latest OS version in market		
	b) Updates at least 07 years		
	c) Patches and Fixes		
4	All the components of the solution shall be from the same OEM.		
B	**Specification**		
1	The proposed firewall solution shall run on a hardened OS and delivered on purposeful built hardware and security appliance.		
2	Firewall Appliances shall be rack mountable/rack mount kit shall be supplied along.		
3	Solution shall provide features and licenses for contractual period for Firewall, IPS, Web/Url Filtering, AntiBot, Antivirus, Antispam, DNS Security, Site to Site VPN, Granular Application control on same appliance managed through a separate centralized management.		

4	Solution shall support Application level and "Stateful" policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.		
5	The proposed security platform shall be supplied, installed and configured in High Availability.		
6	Firewall Appliance shall provide high availability in Active-Active and Active-Passive mode. Appliance failover shall be completely stateful in nature without any manual intervention and should be completely transparent to end-user without any session drops.		
7	Appliance shall not require any downtime/reboot for failover & backup purpose.		
8	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public websites.		
9	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/services over secure channel.		
10	Solution shall be supplied with the support for static and dynamic routing protocols.		
11	The solution shall support VLAN tagging (IEEE 802.1q).		
12	Solution shall have inbuilt integration with Identity Awareness Capabilities without any external devices. Integration shall work with/without any agent on the remote side.		
13	Solution shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications. Solution must have minimum 10,000+ application signature on day1.		
14	Shall provide IPv4 and IPv6 support including NAT64, NAT66/NTPv6 & NAT 46.		
15	Solution shall support Link aggregation functionality (LACP) to group multiple ports as single Channel.		
16	Solution must support the policies to block the credit card, Bank numbers etc.… also must provide flexibility to create the polices to block file types and direction of data passing via firewall (download and upload etc.).		

17	Firewall must support zero day phishing.		
18	The firewall appliance shall support virtual systems/VDOM/virtual contexts. The functionality can be requested in future.		
19	Should have AI-driven threat detection		
20	Should have real-time DDoS mitigation		
21	Should have DPI for internal lateral movement detection		
22	Should have MFA & role-based access control (RBAC)		
C	**Performance Requirements**		
1	Shall have Firewall throughput of minimum 60Gbps from day one.		
2	Shall have Next Generation Firewall throughput of minimum 27Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix/Application Mix traffic testing conditions.		
3	Shall have Threat protection throughput of min **10Gbps and more (FW+AVC+Web Filtering/URL Filtering+AntiMalware/Antivirus+ Sandboxing)** with Logging enabled in Enterprise Mix/Application Mix traffic testing conditions.		
4	Shall have threat preventions throughput with SSL(Secure Socket Layer) certificate/HTTPS inspection of Min 5Gbps		
5	Shall have Next Generation IPS throughput of at least 32Gbps with logging enabled in Enterprise Mix / Application Mix traffic.		
6	Shall support at least 7 million concurrent sessions/connection from day one and scalable to 14 Million in near future and minimum 350K Million new connection per second from day one.		
7	Solution shall have minimum following ports from day one and expansion slot/fixed ports to support additional ports requirement.		
	- 8x RJ45 and 12x 10G SFP+ Ports from day one.		

	- Separate & Dedicated 1 x 1G port for out of band management.		
	- Separate & dedicated port for HA connectivity.		
	- Short Range Transceiver must be included from day one.		
	Additional Ports required in future.		
	4 x 10/25GBASE-F SFP28 port card		
	2 x 40/100GBASE-F QSFP28 port card		
8	Must have integrated redundant hot swappable power supplies.		
9	Solution hardware should be a multi core CPU architecture with a hardened 64-bit operating system.		
10	Should support minimum of 32 GB of RAM from day one and scalable to 64 GB in future if required without changing the hardware.		
11	Should have onboard 900 GB or higher of storage from day one.		
12sss	Appliance should have unlimited Remote access VPN/SSL VPN from day one license must be included from day one.		
D	**Network Protocols/Standards Support Requirements**		
1	Solution shall support the deployment in Routed or Transparent Mode.		
2	Must support Static, RIP, OSPF, OSPFv3 and BGP.		
3	The proposed firewall shall be able to handle unknown /unidentified applications with actions like allow, block or alert.		
4	The proposed firewall shall have granular application identification technology based upon deep packet inspection.		
5	The proposed firewall shall warn the end user with a customizable page when the application is blocked.		
6	The proposed firewall shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).		

7	The Firewall shall provide stateful engine support for all common protocols of the TCP/IP stack.		
8	The Firewall shall provide NAT functionality, including dynamic and static NAT translations.		
9	Firewall should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, application wise geolocation control, URL wise, zone wise, vlan wise, etc.		
10	The solution should have at least 114 application categories and 200 Million URL from Day one.		
11	Should have more than 10,000+ pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency.		
12	Solution modules shall support authentication protocols like RADIUS/ TACACS+ etc.		
13	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		
	b) Network Address Translation (NAT) shall be configurable as 1:1, 1:many, many:1 and many: many.		
	c) Reverse NAT shall be supported.		
	d) Port address translation /Masquerading shall be supported.		
14	Dynamic Host Configuration Protocol (DHCP) & Virtual Private Network (VPN) shall be supported		
15	The firewall shall support Internet Protocol Security (IPsec).		
	support Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509)		
	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.		
	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.		
	IPsec NAT traversal shall be supported		
E	**Firewall Policy Requirements**		

1	Firewall shall be able to configure rules based on the following parameter -		
	a) Source/Destination IP/Port/Geo locations		
	b) Time and date access		
	c) User/group role (After Integration with AD)		
	d) Customizable services		
	e) Combination of one or multiple of above-mentioned parameters		
2	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.		
3	Firewall shall support Access for Granular user, group & machine based visibility and policy enforcement. It shall have following features:		
	a) The firewall shall mask/NAT the internal network from the external world.		
	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.		
	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
	d) Ingress/egress filtering capability shall be provided.		
	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
	f) Basic attack protection features listed below but not limited to :		
	• It shall enable rapid detection of network attacks		
	• SYN cookie protection/SYN Flood		
	• Protection against IP spoofing		
	• Out of state TCP packets protection"		
4	The proposed solution must support Policy Based forwarding based on:		
	- Zone		
	- Source or Destination Address		
	- Source or destination port/service		

	- AD/LDAP user or User Group		
	- Application, sub applications groups		
5	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks must be supported.		
Firewall Management and Reporting Device			
F	**Administration, Management , Logging & Reporting**		
1	Dedicated Firewall Management, log server and reporting server must be hardware appliance at On-prem only. External Firewall and NGFW (For patch downloading) must be managed from the same management appliance. Must be rack mountable.		
2	Appliance must have minimum 6x RJ45 port, 2 TB storage , 50 GB per day of Logs,2000 (Sustained log per sec), minimum 32GB of memory and minimum 10 device license management from day one.		
3	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
4	The Solution shall receive logs for the overall proposed solution in a single system, and shall not be separate for each module of proposed firewalls.		
5	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
6	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance.		
7	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other.		
8	Solution must be able to install threat related protections and access related rules separately or in a single policy.		
9	Log viewer must have a free text search capability.		
10	Appliance must support minimum 10 appliance update from day one.		

NGFW (Internal)

S.N	Specifications	Compliance Yes/No	References (Document/Page No.)
A	**Eligibility Criteria**		
1	Solution should be purpose build hardware appliance.		
2	The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials to raise the technical issues in the name of customer, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful Bidder must provide the login credentials.		
3	The provided hardware should not be end of support during the contractual period. It should continue to provide		
	a) Upgrades and latest OS version in market		
	b) Updates at least 07 years		
	c) Patches and Fixes		
4	All the components of the solution shall be from the same OEM.		
B	**Specification**		
1	The proposed firewall solution shall run on a hardened OS and delivered on purposeful built hardware and security appliance.		
2	Firewall Appliances shall be rack mountable/rack mount kit shall be supplied along.		

3	Solution shall provide features and licenses for contractual period for Firewall, IPS, Web/Url Filtering, AntiBot, Antivirus, Antispam, DNS Security, Site to Site VPN, Granular Application control on same appliance managed through a separate centralized management.		
4	Solution shall support Application level and "Stateful" policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.		
5	The proposed security platform shall be supplied, installed and configured in High Availability.		
6	Firewall Appliance shall provide high availability in Active-Active and Active-Passive mode. Appliance failover shall be completely stateful in nature without any manual intervention and should be completely transparent to end-user without any session drops.		
7	Appliance shall not require any downtime/reboot for failover & backup purpose.		
8	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public websites.		
9	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/services over secure channel.		
10	Solution shall be supplied with the support for static and dynamic routing protocols.		
11	The solution shall support VLAN tagging (IEEE 802.1q).		
12	Solution shall have inbuilt integration with Identity Awareness Capabilities without any external devices. Integration shall work with/without any agent on the remote side.		
13	Solution shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications. Solution must have minimum 10,000+ application signature on day1.		
14	Shall provide IPv4 and IPv6 support including NAT64, NAT66/NTPv6 & NAT 46.		

15	Solution shall support Link aggregation functionality (LACP) to group multiple ports as single Channel.		
16	Solution must support the policies to block the credit card, Bank numbers etc.… also must provide flexibility to create thepolices to block file types and direction of data passing via firewall (download and upload etc.).		
17	Firewall must support zero day phishing.		
18	The firewall appliance shall support virtual systems/VDOM/virtual contexts. The functionality can be requested in future; however, all virtual domains must work as dedicated firewall with all features.		
19	Should have behaviour-based anomaly detection and Integrate AI/ML-based security analytics		
20	Should have deep packet inspection (DPI)		
21	Should have AD/LDAP integration and also have MFA & role-based access control (RBAC)		
C	**Performance Requirements**		
1	Shall have Firewall throughput of minimum 60 Gbps from day one.		
2	Shall have Next Generation Firewall throughput of minimum 27 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic testing conditions.		
3	Shall have Threat protection throughput of min **10 Gbps and more (FW+AVC+Web Filtering/URL Filtering+AntiMalware/Antivirus+ Sandboxing)** with Logging enabled in Enterprise Mix/Application Mix traffic testing conditions.		
4	Shall have Next Generation IPS throughput of at least 32Gbps with logging enabled in Enterprise Mix / Application Mix traffic.		

5	Shall support at least 7 million concurrent sessions/connection from day one and scalable to 14 Million in near future and minimum 350K Million new connection per second from day one.		
6	Solution shall have minimum following ports from day one and expansion slot/fixed ports to support additional ports requirement.		
	- 8x RJ45 and 12x 10G SFP+ Ports from day one.		
	- Separate & Dedicated 1 x 1G port for out of band management.		
	- Separate & dedicated port for HA connectivity.		
	- Short Range Transceiver must be included from day one.		
	Additional Ports required in future.		
	4 x 10/25GBASE-F SFP28 port card		
	2 x 40/100GBASE-F QSFP28 port card		
7	Must have integrated redundant hot swappable power supplies.		
8	Solution hardware should be a multi core CPU architecture with a hardened 64-bit operating system.		
9	Should support minimum of 32 GB of RAM from day one and scalable to 64 GB in future if required without changing the hardware.		
10	Should have onboard 900 GB or higher of storage from day one.		
11	Appliance should have unlimited Remote access VPN/SSL VPN from day one license must be included from day one.		
D	**Network Protocols/Standards Support Requirements**		
1	Solution shall support the deployment in Routed or Transparent Mode.		
2	Must support Static, RIP, OSPF, OSPFv3 and BGP.		

3	The proposed firewall shall be able to handle unknown /unidentified applications with actions like allow, block or alert.		
4	The proposed firewall shall have granular application identification technology based upon deep packet inspection.		
5	The proposed firewall shall warn the end user with a customizable page when the application is blocked.		
6	The proposed firewall shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).		
7	The Firewall shall provide stateful engine support for all common protocols of the TCP/IP stack.		
8	The Firewall shall provide NAT functionality, including dynamic and static NAT translations.		
9	Firewall should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, application wise geolocation control, URL wise, zone wise, vlan wise, etc.		
10	The solution should have at least 114 application categories and 200 Million URL from Day one.		
11	Should have more than 10,000+ pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency.		
12	Solution modules shall support authentication protocols like RADIUS/ TACACS+ etc.		
13	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		
	b) Network Address Translation (NAT) shall be configurable as 1:1, 1:many, many:1 and many: many.		
	c) Reverse NAT shall be supported.		

	d) Port address translation /Masquerading shall be supported.		
14	Dynamic Host Configuration Protocol (DHCP) & Virtual Private Network (VPN) shall be supported		
15	The firewall shall support Internet Protocol Security (IPsec).		
	support Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509)		
	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.		
	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.		
	IPsec NAT traversal shall be supported		
E	**Firewall Policy Requirements**		
1	Firewall shall be able to configure rules based on the following parameter -		
	a) Source/Destination IP/Port/Geo locations		
	b) Time and date access		
	c) User/group role (After Integration with AD)		
	d) Customizable services		
	e) Combination of one or multiple of above-mentioned parameters		
2	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.		
3	Firewall shall support Access for Granular user, group & machine-based visibility and policy enforcement. It shall have following features:		
	a) The firewall shall mask/NAT the internal network from the external world.		
	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.		

	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
	d) Ingress/egress filtering capability shall be provided.		
	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
	f) Basic attack protection features listed below but not limited to :		
	• It shall enable rapid detection of network attacks		
	• SYN cookie protection/SYN Flood		
	• Protection against IP spoofing		
	• Out of state TCP packets protection"		
4	The proposed solution must support Policy Based forwarding based on:		
	- Zone		
	- Source or Destination Address		
	- Source or destination port/service		
	- AD/LDAP user or User Group		
	- Application, sub applications groups		
5	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks must be supported.		
Firewall Management and Reporting Device			
F	**Administration, Management , Logging & Reporting**		
1	Dedicated Firewall Management, log server and reporting server must be hardware appliance at On-prem only. Perimeter Firewall and NGFW (For patch pushing in WAN facing DC) must be managed from the same management appliance. Must be rack mountable.		

2	Appliance must have minimum 6x RJ45 port, 2 TB storage , 50 GB per day of Logs,2000 (Sustained log per sec), minimum 32GB of memory and minimum 10 device license management from day one.		
3	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
4	The Solution shall receive logs for the overall proposed solution in a single system, and shall not be separate for each module of proposed firewalls.		
5	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
6	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance.		
7	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other.		
8	Solution must be able to install threat related protections and access related rules separately or in a single policy.		
9	Log viewer must have a free text search capability.		
10	Appliance must support minimum 10 appliances update from day one.		

NGFW (For WAN Facing DC) with Central console

S.N	Specifications	Compliance Yes/No	References (Document/Page No.)
A	**Eligibility Criteria**		
1	Solution should be purpose build hardware appliance.		
2	The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials to raise the technical issues in the name of customer, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful Bidder must provide the login credentials.		
3	The provided hardware should not be end of support during the contractual period. It should continue to provide		
	a) Upgrades and latest OS version in market		
	b) Updates at least 07 years		
	c) Patches and Fixes		
4	All the components of the solution shall be from the same OEM.		
B	**Specification**		

1	The proposed firewall solution shall run on a hardened OS and delivered on purposeful built hardware and security appliance.		
2	Firewall Appliances shall be rack mountable/rack mount kit shall be supplied along.		
3	Solution shall provide features and licenses for contractual period for Firewall, IPS, Web/Url Filtering, AntiBot, Antivirus, Antispam, DNS Security, Site to Site VPN, Granular Application control on same appliance managed through a separate centralized management.		
4	Solution shall support Application level and "Stateful" policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.		
5	The proposed security platform shall be supplied, installed and configured in High Availability.		
6	Firewall Appliance shall provide high availability in Active-Active and Active-Passive mode. Appliance failover shall be completely stateful in nature without any manual intervention and should be completely transparent to end-user without any session drops.		
7	Appliance shall not require any downtime/reboot for failover & backup purpose.		
8	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public websites.		
9	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/services over secure channel.		
10	Solution shall be supplied with the support for static and dynamic routing protocols.		
11	The solution shall support VLAN tagging (IEEE 802.1q).		

12	Solution shall have inbuilt integration with Identity Awareness Capabilities without any external devices. Integration shall work with/without any agent on the remote side.		
13	Solution shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications. Solution must have minimum 10,000+ application signature on day1.		
14	Shall provide IPv4 and IPv6 support including NAT64, NAT66/NTPv6 & NAT 46.		
15	Solution shall support Link aggregation functionality (LACP) to group multiple ports as single Channel.		
16	Solution must support the policies to block the credit card, Bank numbers etc.... also must provide flexibility to create the polices to block file types and direction of data passing via firewall (download and upload etc.).		
17	The firewall appliance shall support virtual systems/VDOM/virtual contexts. The functionality can be requested in future.		
C	**Performance Requirements**		
1	Shall have Firewall throughput of minimum 70 Gbps from day one.		
2	Shall have Next Generation Firewall throughput of minimum 30 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic testing conditions.		
3	Shall have Threat protection throughput of min **10 Gbps (FW+AVC+Web Filtering/URL Filtering+AntiMalware/Antivirus+ Sandboxing)** with Logging enabled in Enterprise Mix/Application Mix traffic testing conditions.		

4	Shall have Next Generation IPS throughput of at least 40 Gbps with logging enabled in Enterprise Mix / Application Mix traffic.		
5	Shall support at least 7 million concurrent sessions/connection from day one and scalable to 14 Million in near future and minimum 350K Million new connection per second from day one.		
6	Solution shall have minimum following ports from day one and expansion slot/fixed ports to support additional ports requirement.		
	- 8x RJ45 and 12x 10G SFP+ Ports from day one.		
	- Separate & Dedicated 1 x 1G port for out of band management.		
	- Separate & dedicated port for HA connectivity.		
	- Short Range Transceiver must be included from day one.		
	Additional Ports required in future.		
	4 x 10/25GBASE-F SFP28 port card		
	2 x 40/100GBASE-F QSFP28 port card		
7	Must have integrated redundant hot swappable power supplies.		
8	Solution hardware should be a multi core CPU architecture with a hardened 64-bit operating system.		
9	Should support minimum of 32 GB of RAM from day one and scalable to 64 GB in future if required without changing the hardware.		
10	Should have onboard 900 GB or higher of storage from day one.		
11	Appliance should have unlimited Remote access VPN/SSL VPN from day one license must be included from day one.		
D	**Network Protocols/Standards Support Requirements**		
1	Solution shall support the deployment in Routed or Transparent Mode.		

2	Must support Static, RIP, OSPF, OSPFv3 and BGP.		
3	The proposed firewall shall be able to handle unknown /unidentified applications with actions like allow, block or alert.		
4	The proposed firewall shall have granular application identification technology based upon deep packet inspection.		
5	The proposed firewall shall warn the end user with a customizable page when the application is blocked.		
6	The proposed firewall shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).		
7	The Firewall shall provide stateful engine support for all common protocols of the TCP/IP stack.		
8	The Firewall shall provide NAT functionality, including dynamic and static NAT translations.		
9	Firewall should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, application wise geolocation control, URL wise, zone wise, vlan wise, etc.		
10	The solution should have at least 114 application categories and 200 Million URL from Day one.		
11	Should have more than 10,000+ pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency.		
12	Solution modules shall support authentication protocols like RADIUS/ TACACS+ etc.		
13	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		

	b) Network Address Translation (NAT) shall be configurable as 1:1, 1:many, many:1 and many: many.		
	c) Reverse NAT shall be supported.		
	d) Port address translation /Masquerading shall be supported.		
14	Dynamic Host Configuration Protocol (DHCP) & Virtual Private Network (VPN) shall be supported		
15	The firewall shall support Internet Protocol Security (IPsec).		
	support Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509)		
	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.		
	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.		
	IPsec NAT traversal shall be supported		
E	**Firewall Policy Requirements**		
1	Firewall shall be able to configure rules based on the following parameter -		
	a) Source/Destination IP/Port/Geo locations		
	b) Time and date access		
	c) User/group role (After Integration with AD)		
	d) Customizable services		
	e) Combination of one or multiple of above-mentioned parameters		
2	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.		

3	Firewall shall support Access for Granular user, group & machine based visibility and policy enforcement. It shall have following features:		
	a) The firewall shall mask/NAT the internal network from the external world.		
	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.		
	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
	d) Ingress/egress filtering capability shall be provided.		
	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
	f) Basic attack protection features listed below but not limited to :		
	• It shall enable rapid detection of network attacks		
	• SYN cookie protection/SYN Flood		
	• Protection against IP spoofing		
	• Out of state TCP packets protection"		
4	The proposed solution must support Policy Based forwarding based on:		
	- Zone		
	- Source or Destination Address		
	- Source or destination port/service		
	- AD/LDAP user or User Group		
	- Application, sub applications groups		
5	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks must be supported.		
Firewall Management and Reporting Device			
F	**Administration, Management , Logging & Reporting**		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M - V	M - IV	M - III	M - II	M - I	PO

1	Dedicated Firewall Management, log server and reporting server must be hardware appliance at On-prem only.		
2	Appliance must have minimum 4x RJ45 port, 24TB storage in raid, 100GB/day of Logs, 20000 (Sustained log per sec), minimum 190GB of memory or and minimum 100 device management license from day one and scalable to 150 devices without changing the hardware.		
3	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
4	The Solution shall receive logs for the overall proposed solution in a single system, and shall not be separate for each module of proposed firewalls.		
5	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
6	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance.		
7	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other.		
8	Solution must be able to install threat related protections and access related rules separately or in a single policy.		
9	Log viewer must have a free text search capability.		
10	Appliance must support minimum 150 appliances update from day one.		

NGFW (For patch downloading)

S.N	Specifications	Compliance Yes/No	References (Document/Page No.)
A	**Eligibility Criteria**		
1	Solution should be purpose build hardware appliance.		
2	The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials to raise the technical issues in the name of customer, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful Bidder must provide the login credentials.		
3	The provided hardware should not be end of support during the contractual period. It should continue to provide		
	a) Upgrades and latest OS version in market		
	b) Updates at least 07 years		
	c) Patches and Fixes		
4	All the components of the solution shall be from the same OEM.		
B	**Specification**		
1	The proposed firewall solution shall run on a hardened OS and delivered on purposeful built hardware and security appliance.		
2	Firewall Appliances shall be rack mountable/rack mount kit shall be supplied along.		

3	Solution shall provide features and licenses for contractual period for Firewall, IPS, Web/Url Filtering, AntiBot, Antivirus, Antispam, DNS Security, Site to Site VPN, Granular Application control on same appliance managed through a separate centralized management.		
4	Solution shall support Application level and "Stateful" policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.		
5	The proposed security platform shall be supplied, installed and configured in High Availability.		
6	Firewall Appliance shall provide high availability in Active- Active and Active-Passive mode. Appliance failover shall be completely stateful in nature without any manual intervention and should be completely transparent to end-user without any session drops.		
7	Appliance shall not require any downtime/ reboot for failover & backup purpose.		
8	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites		
9	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/ services over secure channel.		
10	Solution shall be supplied with the support for static and dynamic routing protocols.		
11	The solution shall support VLAN tagging (IEEE 802.1q).		
12	Solution shall have inbuilt integration with Identity Awareness Capabilities without any external devices. Integration shall work with/without any agent on the remote side.		

13	Solution shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications. Solution must have minimum 10,000+ application signature on day1.		
14	Shall provide IPv4 and IPv6 support including NAT64, NAT66/NTPv6 & NAT 46.		
15	Solution shall support Link aggregation functionality (LACP) to group multiple ports as single Channel.		
16	Solution must support the policies to block the credit card, Bank numbers etc.... also must provide flexibility to create the polices to block file types and direction of data passing via firewall (download and upload etc).		
17	Firewall must support zero-day phishing.		
18	The firewall appliance shall support virtual systems/VDOM/virtual contexts. The functionality can be requested in future however all virtual domains must work as dedicated firewall with all features.		
19	Should have integrated AI-driven security analytics and threat detection		
20	Should have TLS/SSL deep packet inspection and SSL decryption for advanced security		
<u>**C**</u>	<u>**Performance Requirements**</u>		
1	Shall have Firewall throughput of minimum 50 Gbps from day one.		
2	Shall have Next Generation Firewall throughput of minimum 10 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic testing conditions. Should submit public document.		

3	Shall have Threat protection throughput of minimum **4 Gbps (FW+AVC+Web Filtering/URL Filtering+AntiMalware/Antivirus+ Sandboxing)** with Logging enabled in Enterprise Mix / Application Mix traffic testing conditions. Should submit public document.		
4	Shall have Next Generation IPS throughput of at least 15 Gbps with logging enabled in Enterprise Mix / Application Mix traffic.		
5	Shall support at least 7 million concurrent sessions/connection from day one and scalable to 14 Million in near future and minimum 180K Million new connection per second from day one.		
6	Solution shall have minimum following ports from day one and expansion slot/fixed ports to support additional ports requirement.		
	- 8x RJ45 and 8x 10G SFP+ Ports from day one.		
	- Separate & Dedicated 1 x 1G port for out of band management.		
	- Separate & dedicated port for HA connectivity.		
	- Short Range Transceiver must be included from day one.		
7	Must have integrated redundant power supplies.		
8	Solution hardware should be a multi core CPU architecture with a hardened 64-bit operating system.		
9	Should support minimum of 32 GB of RAM from day 1 and scalable to 64 GB in future if required without changing the hardware.		
10	Should have onboard 400 GB or higher of storage from day 1.		
D	**Network Protocols/Standards Support Requirements**		
1	Solution shall support the deployment in Routed or Transparent Mode.		

2	Must support Static, RIP, OSPF, OSPFv3 and BGP.		
3	The proposed firewall shall be able to handle unknown /unidentified applications with actions like allow, block or alert.		
4	The proposed firewall shall have granular application identification technology based upon deep packet inspection.		
5	The proposed firewall shall warn the end user with a customizable page when the application is blocked.		
6	The proposed firewall shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).		
7	The Firewall shall provide stateful engine support for all common protocols of the TCP/IP stack.		
8	The Firewall shall provide NAT functionality, including dynamic and static NAT translations.		
9	Firewall should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, application wise geolocation control, url wise, zone wise, vlan wise, etc.		
10	The solution should have at least 114 application categories and 200 Million URL from Day 1.		
11	Should have more than 10,000+ pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency.		
12	Solution modules shall support authentication protocols like RADIUS/ TACACS+ etc.		

13	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		
	b) Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many.		
	c) Reverse NAT shall be supported.		
	d) Port address translation /Masquerading shall be supported.		
14	Dynamic Host Configuration Protocol (DHCP) & Virtual Private Network (VPN) shall be supported		
15	The firewall shall support Internet Protocol Security (IPsec).		
	support Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509)		
	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.		
	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.		
	IPsec NAT traversal shall be supported		
E	**Firewall Policy Requirements**		
1	Firewall/shall be able to configure rules based on the following parameter --		
	a) Source/Destination IP/Port/Geo locations		
	b) Time and date access		
	c) User/group role (After Integration with AD)		
	d) Customizable services		

	e) Combination of one or multiple of above mentioned parameters		
2	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.		
3	Firewall shall support Access for Granular user, group & machine based visibility and policy enforcement. It shall have following features:		
	a) The firewall shall mask/NAT the internal network from the external world.		
	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.		
	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
	d) Ingress/egress filtering capability shall be provided.		
	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
	f) Basic attack protection features listed below but not limited to :		
	• It shall enable rapid detection of network attacks		
	• SYN cookie protection/SYN Flood		
	• Protection against IP spoofing		
	• Out of state TCP packets protection"		
4	The proposed solution must support Policy Based forwarding based on:		
	- Zone		
	- Source or Destination Address		
	- Source or destination port/service		
	- AD/LDAP user or User Group		

	- Application, sub applications groups		
5	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks must be supported.		
Firewall Management and Reporting Device			
F	**Administration, Management , Logging & Reporting**		
1	Dedicated Firewall Management, log server and reporting server must be hardware appliance at On-prem only. External Firewall and NGFW (For patch downloading) must be managed from the same management appliance. Must be rack mountable.		
2	Appliance must have minimum 6x RJ45 port, 2 TB storage, 50GB per day of Logs,2000 Sustained Rate (logs/sec), 32GB of memory and minimum 10 device license management from day one.		
3	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
4	The Solution shall receive logs for the overall proposed solution in a single system and shall not be separate for each module of proposed firewalls.		
5	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
6	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance.		
7	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other.		

8	Solution must be able to install threat related protections and access related rules separately or in a single policy.		
9	Log viewer must have a free text search capability.		
10	Appliance must support minimum 10 appliance update from day one.		

NGFW (For patch pushing in WAN facing DC)

S.N	Specifications	Compliance Yes/No	References (Document/Page No.)
A	**Eligibility Criteria**		
1	Solution should be purpose build hardware appliance.		
2	The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials to raise the technical issues in the name of customer, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful Bidder must provide the login credentials.		
3	The provided hardware should not be end of support during the contractual period. It should continue to provide		
	a) Upgrades and latest OS version in market		
	b) Updates at least 07 years		
	c) Patches and Fixes		
4	All the components of the solution shall be from the same OEM.		
B	**Specification**		
1	The proposed firewall solution shall run on a hardened OS and delivered on purposeful built hardware and security appliance.		
2	Firewall Appliances shall be rack mountable/rack mount kit shall be supplied along.		
3	Solution shall provide features and licenses for contractual period for Firewall, IPS, Web/Url Filtering, AntiBot, Antivirus, Antispam, DNS Security, Site to Site VPN, Granular Application control on same appliance managed through a separate centralized management.		

4	Solution shall support Application level and "Stateful" policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.		
5	The proposed security platform shall be supplied, installed and configured in High Availability.		
6	Firewall Appliance shall provide high availability in Active- Active and Active-Passive mode. Appliance failover shall be completely stateful in nature without any manual intervention and should be completely transparent to end-user without any session drops.		
7	Appliance shall not require any downtime/ reboot for failover & backup purpose.		
8	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites		
9	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/ services over secure channel.		
10	Solution shall be supplied with the support for static and dynamic routing protocols.		
11	The solution shall support VLAN tagging (IEEE 802.1q).		
12	Solution shall have inbuilt integration with Identity Awareness Capabilities without any external devices. Integration shall work with/without any agent on the remote side.		
13	Solution shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications. Solution must have minimum 10,000+ application signature on day1.		
14	Shall provide IPv4 and IPv6 support including NAT64, NAT66/NTPv6 & NAT 46.		
15	Solution shall support Link aggregation functionality (LACP) to group multiple ports as single Channel.		
16	Solution must support the policies to block the credit card, Bank numbers etc.… also must provide flexibility to create the polices to block file types and direction of data passing via firewall (download and upload etc..).		
17	Firewall must support zero day phishing.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

18	The firewall appliance shall support virtual systems/VDOM/virtual contexts. The functionality can be requested in future however all virtual domains must work as dedicated firewall with all features.		
19	Should have sandboxing for patch validation and automated malware scanning.		
20	Should have cryptographic patch integrity verification and also have SHA-256 validation and digital signatures.		
C	**Performance Requirements**		
1	Shall have Firewall throughput of minimum 50 Gbps from day one.		
2	Shall have Next Generation Firewall throughput of minimum 10 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic testing conditions. Should submit public document.		
3	Shall have Threat protection throughput of minimum 4 Gbps and more (FW+AVC+Web Filtering/URL Filtering+AntiMalware/Antivirus+ Sandboxing) with Logging enabled in Enterprise Mix / Application Mix traffic testing conditions. Should submit public document.		
4	Shall have Next Generation IPS throughput of at least 15 Gbps with logging enabled in Enterprise Mix / Application Mix traffic.		
5	Shall support at least 7 million concurrent sessions/connection from day one and scalable to 14 Million in near future and minimum 180K Million new connection per second from day one.		
6	Solution shall have minimum following ports from day one and expansion slot/fixed ports to support additional ports requirement.		
	- 8x RJ45 and 8x 10G SFP+ Ports from day one.		
	- Separate & Dedicated 1 x 1G port for out of band management.		
	- Separate & dedicated port for HA connectivity.		

	- Short Range Transceiver must be included from day one.		
7	Must have integrated redundant power supplies.		
8	Solution hardware should be a multi core CPU architecture with a hardened 64-bit operating system.		
9	Should support minimum of 32 GB of RAM from day 1 and scalable to 64 GB in future if required without changing the hardware.		
10	Should have onboard 400 GB or higher of storage from day 1.		
D	**Network Protocols/Standards Support Requirements**		
1	Solution shall support the deployment in Routed or Transparent Mode.		
2	Must support Static, RIP, OSPF, OSPFv3 and BGP.		
3	The proposed firewall shall be able to handle unknown /unidentified applications with actions like allow, block or alert.		
4	The proposed firewall shall have granular application identification technology based upon deep packet inspection.		
5	The proposed firewall shall warn the end user with a customizable page when the application is blocked.		
6	The proposed firewall shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).		
7	The Firewall shall provide stateful engine support for all common protocols of the TCP/IP stack.		
8	The Firewall shall provide NAT functionality, including dynamic and static NAT translations.		
9	Firewall should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, application wise geolocation control, url wise, zone wise, vlan wise, etc.		
10	The solution should have at least 114 application categories and 200 Million URL from Day 1.		

11	Should have more than 10,000+ pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency.		
12	Solution modules shall support authentication protocols like RADIUS/ TACACS+ etc.		
13	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		
	b) Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many.		
	c) Reverse NAT shall be supported.		
	d) Port address translation /Masquerading shall be supported.		
14	Dynamic Host Configuration Protocol (DHCP) & Virtual Private Network (VPN) shall be supported		
15	The firewall shall support Internet Protocol Security (IPsec).		
	support Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509)		
	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.		
	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.		
	IPsec NAT traversal shall be supported		
E	**Firewall Policy Requirements**		
1	Firewall/shall be able to configure rules based on the following parameter --		
	a) Source/Destination IP/Port/Geo locations		
	b) Time and date access		
	c) User/group role (After Integration with AD)		
	d) Customizable services		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-	PO

	e) Combination of one or multiple of above mentioned parameters		
2	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.		
3	Firewall shall support Access for Granular user, group & machine based visibility and policy enforcement. It shall have following features:		
	a) The firewall shall mask/NAT the internal network from the external world.		
	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.		
	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
	d) Ingress/egress filtering capability shall be provided.		
	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
	f) Basic attack protection features listed below but not limited to :		
	• It shall enable rapid detection of network attacks		
	• SYN cookie protection/SYN Flood		
	• Protection against IP spoofing		
	• Out of state TCP packets protection"		
4	The proposed solution must support Policy Based forwarding based on:		
	- Zone		
	- Source or Destination Address		
	- Source or destination port/service		
	- AD/LDAP user or User Group		
	- Application, sub applications groups		

5	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks must be supported.		
Firewall Management and Reporting Device			
F	**Administration, Management , Logging & Reporting**		
1	Dedicated Firewall Management, log server and reporting server must be hardware appliance at On-prem only. Perimeter Firewall and NGFW (For patch pushing in WAN facing DC) must be managed from the same management appliance. Must be rack mountable.		
2	Appliance must have minimum 6x RJ45 port, 2 TB storage, 50GB per day of Logs, 2000 Sustained Rate (logs/sec), 32GB of memory and minimum 10 device license management from day one.		
3	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
4	The Solution shall receive logs for the overall proposed solution in a single system, and shall not be separate for each module of proposed firewalls.		
5	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
6	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance.		
7	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other.		
8	Solution must be able to install threat related protections and access related rules separately or in a single policy.		
9	Log viewer must have a free text search capability.		
10	Appliance must support minimum 10 appliance update from day one.		

Core Switch

S. N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
A	**General Features**		
1	The switch should be Gigabit Layer 2 and Layer 3 switch with console, OOBM ports, USB ports along with all accessories.		
2	Switch should have hot swappable redundant Power Supply and fan tray from day one.		
3	Switch should have non-blocking throughput from day one.		
4	Software upgrades, updates shall be included as part of the warranty		
5	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software to optimize performance and capacity		
6	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source. Network Access Control (NAC) mechanisms are supported for enhanced security. The ability to prevent unauthorized access using dynamic ARP inspection (DAI) and IP source guard should be explicitly mentioned.		
7	Operating temperature of 0°C to 45°C		
8	All mentioned features (above & below) should be available from day 1. Any license required to be factored from day 1		
B	**Performance**		
1	Should have 16GB DRAM and 32GB Flash.		
2	The switch will have at up to 2.4 Tbps switching capacity		
3	Forwarding rates: The switch should have min 1000Mpps forwarding rates.		
4	IPv4 Routing entry support: 600K or more.		
5	IPv6 Routing entry support: 600K or more.		

6	IPv4 and IPv6 Multicast Routes: 7K or more.		
7	MAC addresses support: 32K or more.		
8	VLANs ID: 4K or more and 4K or more VLANs simultaneously.		
9	ACL /QOS entry support: 5K or more.		
10	Packet buffer : 32 MB or more		
11	The device should be IPv6 logo certified from day one.		
12	Should support the ability to configure backup of the previous configuration automatically.		
C	**Functionality:**		
1	The proposed switch should support distributed and redundant architecture by deploying two switches with each switch maintaining independent control and synchronized during upgrades or failover and should support upgrades during live operation and a hot patching feature for zero-downtime updates should be considered.		
2	The Switch should support long distance across the Rack and Floor Switch Stacking.		
3	**Must support RIPv2, RIPng, EVPN, BGP, BGP4, VRF, VXLAN, EVPN, OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR), PIM SM, PIM-DM, PIM-SSM, DCBX, PFC, ETS and Virtual Router Redundancy Protocol (VRRP) from Day one.**		
4	The switch should support IEEE 802.3ad link-aggregation control protocol (LACP) and port trunking		
5	The switch should support IEEE 802.1s Multiple Spanning Tree		
6	The switch should support STP, Trunking, Private VLAN (PVLAN), Q-in-Q, Deficit Weighted Round-Robin (DWRR) or equivalent scheduling, Committed Information Rate (CIR)/Equivalent and eight egress queues per port		
7	Switch shall support rolled back to the previous successful configuration		
8	**The switch should support SNMPv1, v2, and v3, SSL, SSHv2, Telnet, ping, trace route.**		
9	The switch should support Zero-Touch Provisioning (ZTP). The switch shall support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests		
10	The switch should be able to manage from cloud NMS and On-premises NMS solution.		
11	The switch should support IEEE802.1X		

12	The switch should support Port-based authentication		
13	The switch should support MAC-based authentication		
14	The switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number		
15	The switch should support Source-port filtering		
16	**The switch should support RADIUS/TACACS+, Dynamic ARP protection, Port Security, STP route guard, BPDU guard.**		
17	OS Should support for Management automation via Netconf/Yang/REST-API, Python or equivalent technology		
18	Should support Netflow/Sflow/Jflow, Port mirroring or equivalent technology		
D	**Interface Requirement**		
1	**Min 24 Nos. of 10G/25G SFP ports**		
2	**Min 4 Nos. of 40G/100G SFP uplink ports.**		
E	**Regulatory Compliance**		
1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.		
2	Switch shall conform to EN 55022/55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.		
F	**OEM qualification criteria, Warranty and Support**		
1	The switch shall be offered with minimum five years hardware warranty with NBD Shipment and software updates/upgrades from OEM directly. OEM support should be provided Min 07 years.		
2	Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification.		

Access Switch

S. N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
A	**General Features**		
1	Access switch should be Gigabit Layer 2 switch with 1 x RJ-45 Console Port, 1x USB Type-A Host port, 1x USB-C Console Port, 1x OOBM RJ-45 along with all accessories.		
2	Switch should have non-blocking throughput from day 1.		
3	Software upgrades, updates shall be included as part of the warranty		
4	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software to optimize performance and capacity		
5	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source		
6	Operating temperature of 0°C to 45°C		
7	All mentioned features (above & below) should be available from day 1. Any license required to be factored from day 1		
B	**Performance**		
1	Should have min 4 GB DRAM and 8GB Flash.		
2	The switch will have at upto 128Gbps switching capacity.		
3	The switch should have min 95Mpps forwarding rates.		
4	IPv4 Routing entry support: 2K or more.		
5	IPv6 Routing entry support: 1K or more.		
6	IGMP Groups and MLD Group: 1K or more.		

7	MAC addresses support: 32K or more.		
8	VLANs ID: 4K or more and 2K VLANs simultaneously.		
9	ACL /QOS entry support: 1K or more.		
10	Packet buffer: 8 MB or more		
11	The device should be IPv6 logo certified from day one.		
12	Should support the ability to configure backup of the previous configuration automatically.		
C	**Functionality:**		
1	The switch should support front plane stacking on uplink port or Backplane stacking and should have Stacking Performance of minimum 40 Gbps. The switch should support minimum 8 switch in stack		
2	The Switch should support long distance across the Rack and Floor Switch Stacking.		
3	**Must support RIPv2, RIPng, VXLAN, OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR), PIM SM, PIM-DM and Virtual Router Redundancy Protocol (VRRP) from Day one.**		
4	The switch should support IEEE 802.3ad link-aggregation control protocol (LACP) and port trunking		
5	The switch should support IEEE 802.1s Multiple Spanning Tree		
6	The switch should support STP, Trunking, Private VLAN (PVLAN), Q-in-Q, Deficit Weighted Round-Robin (DWRR) or equivalent scheduling, Committed Information Rate (CIR)/Equivalent and eight egress queues per port		
7	Switch shall support rolled back to the previous successful configuration		
8	**The switch should support SNMPv1, v2, and v3, SSL, SSHv2, Telnet, ping, trace route.**		
9	The switch should support Zero-Touch Provisioning (ZTP). The switch shall support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests		
10	The switch should be manageable from cloud NMS or On-premises NMS solution offered		
11	The switch should support IEEE 802.1X		
12	The switch should support Port-based authentication		
13	The switch should support MAC-based authentication		

14	The switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number		
15	The switch should support Source-port filtering		
16	**The switch should support RADIUS/TACACS+, Dynamic ARP protection, Port Security, STP route guard, BPDU guard.**		
17	OS Should support for Management automation via REST-API, Python or equivalent technology		
18	Should support Netflow/Sflow/Jflow, Port mirroring or equivalent technology		
D	**Interface Requirement**		
1	**Min 24 Nos. 10G/25G SFP to connect end devices.**		
2	**Min 4 Nos. of 25G/40G SFP uplink ports to connect distribution switch and 2 Nos. of 25G/40G SFP port for stacking from day one.**		
E	**Regulatory Compliance**		
1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.		
2	Switch shall conform to EN 55022/55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.		

Distribution Switch

S. N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
A	**General Features**		
1	Switch should be Gigabit Layer 2/Layer 3 switch with console, OOBM ports, USB ports along with all accessories.		
2	Switch should support dual redundant Power Supply and fan tray.		
3	Switch should have non-blocking throughput from day one.		
4	Software upgrades, updates shall be included as part of the warranty.		
5	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software to optimize performance and capacity		
6	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source		
7	Operating temperature of 0°C to 45°C		
8	All mentioned features (above & below) should be available from day one. Any license required to be factored from day one.		
B	**Performance**		
1	Should have min 8 GB DRAM and 32GB Flash.		
2	The switch will have at up to 880Gbps switching capacity.		
3	The switch should have min 650Mpps forwarding rates.		
4	IPv4 Routing entry support: 60K or more.		
5	IPv6 Routing entry support: 60K or more.		
6	IPv4 and IPv6 Multicast Routes: 8K or more.		
7	MAC addresses support: 32K or more.		
8	VLANs ID: 4K or more and 4K VLANs simultaneously.		

9	ACL /QOS entry support : 5K or more ACL entries (ingress)		
10	Packet buffer: 8 MB or more		
11	The device should be IPv6 logo certified from day one.		
12	Should support the ability to configure backup of the previous configuration automatically.		
C	**Functionality:**		
1	The switch should support front plane stacking on uplink port or Backplane stacking and should have **Stacking Performance of minimum 200Gbps**. The switch should support minimum 10 switches in stack.		
2	The Switch should support long distance across the Rack and Floor Switch Stacking.		
3	**Must support RIPv2, RIPng, BGP, BGP4, MP-BGP, VXLAN, OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR), PIM SM, PIM-DM and Virtual Router Redundancy Protocol (VRRP) from Day 1**		
4	The switch should support IEEE 802.3ad link-aggregation control protocol (LACP) and port Trunking.		
5	The switch should support IEEE 802.1s Multiple Spanning Tree		
6	The switch should support STP, Trunking, Private VLAN (PVLAN), Q-in-Q, Deficit Weighted Round-Robin (DWRR) or equivalent scheduling, Committed Information Rate (CIR)/Equivalent and eight egress queues per port		
7	Switch shall support rolled back to the previous successful configuration		
8	**The switch should support SNMPv1, v2, and v3, SSL, SSHv2, Telnet, ping, trace route.**		
9	The switch should support Zero-Touch Provisioning (ZTP). The switch shall support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests		
10	The switch should be manageable from cloud NMS and On-premises NMS solution		
11	The switch should support IEEE 802.1X		
12	The switch should support Port-based authentication		
13	The switch should support MAC-based authentication		

14	The switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number		
15	The switch should support Source-port filtering		
16	**The switch should support RADIUS/TACACS+, Dynamic ARP protection, Port Security, STP route guard, BPDU guard.**		
17	OS Should support for Management automation via REST-API, Python or equivalent technology		
18	Should support Netflow/Sflow/Jflow, Port mirroring or equivalent technology		
D	**Interface Requirement**		
1	i) **24 Nos. of 1G/10G SFP+/Ethernet ports**		
2	ii) **4 Nos. of 1G/10G/25G SFP uplink ports or 4 nos of 40G/100G SFP28 uplink ports**		
E	**Regulatory Compliance**		
1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.		
2	Switch shall conform to EN 55022/55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.		

Switch (For pushing patches in WAN facing DC)

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1	Type of Switch should be Managed.		
2	Technology & Number of Ports are Non PoE, 24 x 1G Copper Ports, 2 x 10G Copper Ports, 0 x 1G SFP Port (Uplink), 2 x 10G SFP+ Ports.		
3	Redundant Power Supply will be Supported from day one.		
4	Console Port should be Available.		
5	Switching Capacity-Non-Blocking is Min 128Gbps.		
6	Throughput should be Min 95Mpps.		
7	Operating System should be Available.		
8	Dedicated Stacking Port/Slot should be Supported from day one.		
9	Stacking Bandwidth should be Minimum 80Gbps.		
10	Basic Layer-3 Protocol supported Static RIPv1 /v2, RIPng, OSPF, Routed Access, VRRP v2/v3, ECMP, IGMP v1/v2/v3, MLD v1/v2.		
11	Security Features are should be uRPF, Port Security, 16K MAC, SSL, SSH, broadcast, unicast/ multicast storm control, ARP, 802.1x, ARP Spoofing Prevention, IPv6 DHCPv6 Guard, ARP Spoofing Prevention		
12	Management Protocol supported CLI, SNMP v1/v2/v3, TFTP, Syslog, SMON, DHCP Server, RMON v1/v2, WebUI, LLDP/LLDP-MED		
13	QoS WRR, 802.1Qbb Priority-based Flow, 802.lp CoS DSCP, SRR scheduling		
14	Operating Temperature Range are -5°C to +45°C		
15	Operating Humidity (RH)(%) Min 80%		
16	IPv6 Ready from day one and duly certified		
17	On Site OEM Warranty is Min5 years		

IGW Router (Public Facing)

S.N	Specifications	Compliance (Yes/No)	References (Document /Page No.)
A	**Hardware and Performance**		
1	Should be fixed lRU to SU based configuration to support at least 241/10GbESFP+Ports populated with1210GLR SFP, 41GLX & 41G RJ45 and should have minimum 4 40/l00G uplink ports populated with 2l00G LR & 2lO0G SR 4 SFP's		
2	Must have hot-swappable redundant power supplies(N+l) and fans(N+l)		
3	Should support min throughput of 40Gbps or min 500000 sessions		
4	Shall support modern modular operating system designed for scalability and reliability and should support auto process recovery from failures		
5	Device should have virtual output-based architecture to avoid head offline blocking issues with deep packet buffers Memory minimum 2GB		
6	Should support Ethernet standards like IEEE802.lp, IEEE802.lQ, Flow control, Jumbo frame, 802.lD,802.1w, 802.ls, Jumboframes,802.3ad, private vlan		
7	Shouldsupport4096 Vlans, MLAG,64STPinstances		
8	Should support LLDP		
9	Must have routing protocols like BGP, MP-BGP, RIPv2, OSPFv3, ISISv4, BFD, PIM, SSM, Policy based routing, Selective route download, VXLAN EVPN, VRF. Should have BGP route filtering and traffic engineering capabilities (such as BGP-LU).		
10	Should support minimum 60K IPv4/IPv6 routes and separate tables for IPv4 and IPv6		
11	Should support VRRP, should support active-active port channeling mechanism.		
B	**Security**		
1	Should support IP ddosSource guard, ARP inspection, DHC Prelay		

2	Should support IPv4/IPv6 and MAC based ACL		
3	Should support Ingress ACL Scale of 10k or better.		
4	Should support real time data collection with sflow/net flow.		
C	**QoS features**		
1	Should support 8 queues per port		
2	Should support QoS classification and policing		
3	Should support priority queuing, DSCP, traffic shaping		
4	Should support control plane policing to protect switch CPU from DoS attack		
5	Should support IEEE 1588		
6	Management and Troubleshooting		
7	Should support telnet, ssh, https, SNMPv3, configuration rollback feature for ease of management		
8	Device Should support RSVP-TE, BGP-LU, BGP-LS, auto-bandwidth, split-tunneling, SR-TE, TI-LFA, BGP-SR, BGP-LU		
9	Should support port mirroring based on Inbound & outbound, mirroring based on ports.		
10	Should provide with all software license from day-1 as per RFP specification		
11	Should support real time telemetry from Day 1		
12	Should comply to following certifications: EN61000-3-2/EN61000-3-3, EN 55035, IEC/EN62368-l, RoHS		
13	All licences should be provided with the devices for the mentioned features. The licenses should be perpetual in nature of should be provided or 7yr on day-1 in case of subscription-based licensing. Hardware warranty 60 months.		
14	Router Should support for LDP, MP-BGP, L3VPN, EVPN and L2-EVPN		
15	EVPN should be supported with MPLS and VXLAN for layer-2 and layer-3 VPN services.		
16	Should support symmetric and asymmetric Integrated Routed and Bridging with MPLS and VXLAN		
17	Should support TI-LFA with ISIS		

18	Should support for SR-TE and BGP-LU		
19	Router shall support 6PE and 6VPE mode for IPV6 transport over IPV4		
20	Should support VRFs over MPLS and VXLAN transport.		
21	All the licenses for mentioned protocol support and scale to be provided as per the specification.		
22	Should have ability to collect real-time telemetry data is a strong feature, but it should be specified whether it integrates with SIEM solutions for broader security visibility		
D	**QoS and Security Features**		
1	The Device should have 8 egress queues per port and support for strict priority queuing for differentiated QoS treatment for voice, video and other type of traffic.		
2	The Device should support 802.lp CoS and DSCP classification, ACL based classification, VLAN based classification.		
3	Weighted round robin (WRR)/Weighted fair queuing (WFQ) or equivalent		
4	should support traffic Policing/Shaping		
5	Should support 802.lQbb Per-Priority Flow Control (PFC)		
6	should support Ingress and Egress ACLs using L2, L3, L4 fields		
7	Should support l0K or more ACLs in hardware		
8	Should support Service ACLs to restrict traffic for management telnet, SNMP, etc.		
9	Should have 2 GB of deep packet buffer backed with VOQ based architecture.		
10	Should have configurable control plane (CPU) protection mechanism as a safeguard from DoS attacks.		
E	**Management Features**		
1	Configuration through the CLI, console, Telnet, SSH.		
2	SNMP vl/2/3 support, NTP, Syslog		
3	AAA support for Router management with RBAC and privileged login		
4	TACACS+ and RADIUS for AAA		
5	Flow or similar open standard to support traffic analysis		

6	Device should support IEEE 1588 PTP for advance timing/clock support.		
7	Management over IPv6 should be supported		
8	Device should have modular operating system with ability to contain faults and repair/restart process state fully. Should support for ISSU/fast upgrade or live patching.		
9	Device should support real time streaming telemetry.		
10	Should support SCP, SFTP, NTP		
11	Should support TWAMP or equivalent open IETF standard for link/host monitoring.		
12	Device should support API for configuration and monitoring for custom requirements		
13	Router Operating System should support SDK for writing custom programs for automation		
14	Should support Open Config over Netconf, RESTCONF and gRPC and IPv6 logo certification includes compliance with RFC 8200 for enhanced IPv6 features.		
15	Should support configuration checkpoint and rollback.		
16	Device should have inbuilt support for python and bash.		
17	Device should support docker container for custom application deployment for custom monitoring and management use cases. Should support for dev Op tools like ansible/ChePuppet.		
18	Device should support local and encapsulated remote port mirroring with support for ACL filtering for targeted capture analysis/reporting and simplified troubleshooting.		
19	Should support 12 or more monitoring sessions		
20	Should have integrated packet capture tool like tcp dump for control plane troubleshooting.		
21	Detection of microburst congestions and its reporting.		
22	Device should have zero touch provisioning support.		
23	Should support to view historical route and mac table changes for troubleshooting purpose.		
F	**Other**		
1	Hardware and TAC support should be quoted directly from the OEM. OEM should have 24x7TAC support.		
2	Should be NDcPP/EAL common criteria certified.		

3	Compliance: EN61000-3-2/EN61000-3-3, EN 55035, IEC/EN62368-l, RoHS		
4	Operating temperature of0°C to 40°C		
5	Manufacturer Authorization is Required		
6	All licenses should be provided with the devices for the mentioned features.		
7	Device should be IPv6 Certified/IPv6 logo ready		

IGW Router (WAN Facing)

S.N	Specifications	Compliance (Yes/No)	References (Document /Page No.)
A	**Hardware and Performance**		
1	Should be fixed l RU to SU based configuration to support at least 241/10GbESFP+Ports populated with1210GLR SFP, 41GLX & 41G RJ45 and should have minimum 4 40/l00G uplink ports populated with 2l00G LR & 2lO0G SR 4 SFP's		
2	Must have hot-swappable redundant power supplies(N+l) and fans(N+l)		
3	Should support min throughput of 40 Gbps or min 500000 Session		
4	Shall support modern modular operating system designed for scalability and reliability and should support auto process recovery from failures		
5	Deviceshouldhavevirtualoutput-basedarchitecturetoavoidheadofflineblocking issues with deep packet buffers Memory minimum 2GB		
6	Should support Ethernet standards like IEEE802.lp, IEEE802.lQ, Flow control, Jumbo frame, 802.lD,802.1w, 802.ls, Jumboframes,802.3ad, private vlan		
7	Shouldsupport4096 Vlans, MLAG, 64STP instances		
8	Should support LLDP		
9	Must have routing protocols like BGP, MP-BGP, RIPv2, OSPFv3, ISISv4, BFD, PIM, SSM, Policy based routing, Selective route download, VXLAN EVPN, VRF		
10	Shouldsupportminimum60KIPv4/IPv6routes		
11	Should support VRRP, should support active-active port channeling mechanism.		
B	**Security**		
1	Should support IP Source guard, ARP inspection, DHC Prelay		
2	Should support IPv4/IPv6 and MAC based ACL		

3	Should support Ingress ACL Scale of 10k or better.		
4	Should support real time data collection with sflow/net flow.		
C	**QoS features**		
1	Should support 8 queues per port		
2	Should support QoS classification and policing		
3	Should support priority queuing, DSCP, traffic shaping		
4	Should support control plane policing to protect switch CPU from DoS attack		
5	Should support IEEE 1588		
6	Management and Troubleshooting		
7	Should support telnet, SSH, https, SNMPv3, configuration rollback feature for ease of management		
8	Device Should support RSVP-TE, BGP-LU, BGP-LS, auto-bandwidth, split-tunneling, SR-TE, TI-LFA, BGP-SR, BGP-LU		
9	Should support port mirroring based on Inbound & outbound, mirroring based on ports.		
10	Should provide with all software license from day-1 as per RFP specification		
11	Should support real time telemetry from Day 1		
12	Should comply to following certifications: EN61000-3-2/EN61000-3-3, EN 55035, IEC/EN62368-1, RoHS		
13	All licenses should be provided with the devices for the mentioned features. The licenses should be perpetual in nature of should be provided or 7yr on day-1 in case of subscription-based licensing. Hardware warranty 60 months.		
14	Router Should support for LDP, MP-BGP, L3VPN, EVPN and L2-EVPN		
15	EVPN should be supported with MPLS and VXLAN for layer-2 and layer-3 VPN services.		
16	Should support symmetric and asymmetric Integrated Routed and Bridging with MPLS and VXLAN		
17	Should support TI-LFA with ISIS		
18	Should support for SR-TE and BGP-LU		

19	Router shall support 6PE and 6VPE mode for IPV6 transport over IPV4		
20	Should support VRFs over MPLS and VXLAN transport.		
21	All the licenses for mentioned protocol support and scale to be provided as per the specification.		
D	**QoS and Security Features**		
1	The Device should have 8 egress queues per port and support for strict priority queuing for differentiated QoS treatment for voice, video and other type of traffic.		
2	The Device should support 802.lp CoS and DSCP classification, ACL based classification, VLAN based classification.		
3	Weighted round robin (WRR)/Weighted fair queuing (WFQ) or equivalent		
4	should support traffic Policing/Shaping		
5	Should support 802.lQbb Per-Priority Flow Control (PFC)		
6	should support Ingress and Egress ACLs using L2, L3, L4 fields		
7	Should support l0K or more ACLs in hardware		
8	Should support Service ACLs to restrict traffic for management telnet, SNMP, etc.		
9	Should have 2 GB of deep packet buffer backed with VOQ based architecture.		
10	Should have configurable control plane (CPU) protection mechanism as a safeguard from DoS attacks.		
E	**Management Features**		
1	Configuration through the CLI, console, Telnet, SSH.		
2	SNMP vl/2/3 support, NTP, Syslog		
3	AAA support for Router management with RBAC and privileged login		
4	TACACS+ and RADIUS for AAA		
5	Flow or similar open standard to support traffic analysis		
6	Device should support IEEE 1588 PTP for advance timing/clock support.		
7	Management over IPv6 should be supported		

8	Device should have modular operating system with ability to contain faults and repair/restart process state fully. Should support for ISSU/fast upgrade or live patching.		
9	Device should support real time streaming telemetry.		
10	Should support SCP, SFTP, NTP		
11	Should support TWAMP or equivalent open IETF standard for link/host monitoring.		
12	Device should support API for configuration and monitoring for custom requirements		
13	Router Operating System should support SDK for writing custom programs for automation		
14	Should support Open Config over Netconf, RESTCONF and gRPC.		
15	Should support configuration checkpoint and rollback.		
16	Device should have inbuilt support for python and bash.		
17	Device should support docker container for custom application deployment for custom monitoring and management use cases. Should support for dev Op tools like ansible/ChePuppet.		
18	Device should support local and encapsulated remote port mirroring with support for ACL filtering for targeted capture analysis/reporting and simplified troubleshooting.		
19	Should support 12 or more monitoring sessions		
20	Should have integrated packet capture tool like tcp dump for control plane troubleshooting.		
21	Detection of microburst congestions and its reporting.		
22	Device should have zero touch provisioning support.		
23	Should support to view historical route and mac table changes for troubleshooting purpose.		
F	**Other**		
1	Hardware and TAC support should be quoted directly from the OEM. OEM should have 24x7TAC support.		
2	Should be NDcPP/EAL common criteria certified.		
3	Compliance: EN61000-3-2/EN61000-3-3, EN 55035, IEC/EN62368-l, RoHS		
4	Operating temperature of0°C to 40°C		
5	Manufacturer Authorization is Required		

6	All licenses should be provided with the devices for the mentioned features.		
7	Device should be IPv6 Certified/IPv6 logo ready		

Server Load Balancer (SLB) (with Physical Appliance)

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
A	**Server Load Balancer**		
1	The proposed OEM should be Parent Technology OEM (Should NOT be White labeled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement). Allow equivalent certified solutions from reputed vendors to prevent vendor lock-in.		
2	Appliance should be dedicated hardware; it should not be part of Firewall or UTM. Consider allowing integrated NGFW/WAF solutions that meet the same performance metrics.		
3	**Traffic Ports:** 4 x 10G SFP+, 8 x 1G SFP and 8 x 1G RJ45. Additionally should have 8 x 1G SFP for future use **Device L4 Throughput**: 20Gbps and scalable upto 40Gbps **Layer 4 connections per second:** 500,000 **Layer 7 requests per second:** 900,000 Perform real-world workload validation before procurement. **Concurrent Connections:** 40 Million **RSA CPS(2K Key):** 20,000 **ECC CPS (EC-P256):** 12,000 with TLS1.3 Support Ensure cryptographic readiness for future threats by adopting NIST PQC recommendations. **SSL Throughput:** 10Gbps The appliance should have dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45 Console Port		

4	Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day one.		
5	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend and also have HTTP/3 readiness to improve future compatibility and performance.		
6	**The proposed appliance should support the below metrics:** — Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc		
7	**Following Server Load Balancing Topologies should be supported:** • Client Network Address Translation (Proxy IP) • Virtual Matrix Architecture • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delay Binding		
8	The solution Should support for multiple VLANs with tagging capability.		
9	The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure.		

10	A framework for customizing application delivery should be provided using user-written scripts, that provides the flexibility to control application flows and fully meet business requirements in a fast and agile manner. **The proposed framework should enables to:** • Extend Server Load Balancer Fabric services with delivery of new applications • Quickly deploy new services • Mitigate application problems without changing the application • Preserve infrastructure investment by adding new capabilities without additional equipment investment		
11	The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (No Multi-Tenancy) that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. The Hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and NOT a commercially available hypervisor (like XEN, VMware, KVM etc). **Each Virtual Instance contains a complete and separated environment of the Following:** a) Resources, b) Configurations, c) Management, d) Operating System The proposed device should support 5 Virtual Instance from Day 1 and scalable upto 10 Virtual Instances. Increase scalability to at least 15 Virtual Instances to accommodate future growth.		
12	Appliance should support Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Content-based Load Balancing, Persistency, HTTP Content Modifications.		
13	The Proposed Appliance should support Standalone as well as Virtualized Mode. The proposed Hardware must have Bandwidth Management feature from Day one.		
14	DNSSEC based Global Load Balancing should be supported in the proposed device from Day one.		
15	The proposed device should support standard VRRP (RFC - 2338) or equivalent for High Availability purpose.		
16	**Centralized Management**		

	Should propose Separate Centralized Management & Reporting Solution from Day one.		
17	Device should be accessed through the below: • Using the CLI • Using SNMP • REST API • Using the Web Based Management		
18	Should have built-in SIEM integration or compatibility with major platforms like Splunk, ELK.		
19	Define logging formats in compliance with ISO 27001 Annex A and NIST 800-53.		
20	Should have PCI DSS compliance requirements in the RFP for bidder adherence.		
21	Should have adaptive rate-limiting and 77ehavior analytics for bot and volumetric DdoS attacks.		
22	Should have support for real-time threat intelligence feeds using STIX/TAXII.		
23	Should have logs are stored in tamper-proof immutable storage (e.g., SHA-256 hashing).		

Archival Storage

S.N	Specifications	Compliance (Yes/No)	References (Document /Page No.)
1	Proposed object storage should be offered with min 250 TB of usable storage capacity. Proposed Object storage should be able to scale to Petabytes of unstructured data storage and to store it over longer periods of time.		
2	Storage appliance should be supplied with minimum 3 nodes (Appliance Based) consisting of NL-SAS Drives. Each storage appliance should be configured with min 2x25Gbps LAN ports, Redundant Load Balancer must be offered. Object Storage appliance, Load Balancer HW and Software solution must be owned and supported by single OEM.		
3	The proposed object storage solution should support mirroring and geo erasure coding across sites for data high availability.		
4	The proposed solution should support Dynamic Data information lifecycle Management Policies which can be applied manually or automatically at ingest or any later time. The policies must support defining the type of protection, tiering of data across available nodes/sites basis the age of the data and geography of storage locations and set retention period.		
5	The object storage cluster shall be scalable to min 1 PB in a single namespace by adding drives and nodes. The expansion of object storage should support intermixing of node types (hybrid and all flash) & disk sizes supporting asymmetric upgrades across sites.		
6	Proposed solution should support both geographically distributed erasure coding and node-level erasure coding to optimize performance, storage efficiency, and WAN bandwidth usage. Even if geographic erasure coding is being leveraged, recovery/rebuild from drive failures should not have dependency on WAN Network and Remote sites		
7	Proposed object storage should be fully distributed, asymmetrical, and scale-out architecture allowing multi-site Active/Active architecture.		

8	For enhanced data security requirement, the solution must support data at rest encryption along with data in transit encryption capabilities based on AES-128-SHA and AES-256-SHA or better.		
9	Offered Config must offer min of 1GB/sec read throughput, OEM Sizer report must be submitted duly signed and stamped by OEM on their letterhead, Architecture must support policy-based tiering of data from NL-SAS and Flash Tiers within the cluster.		
10	The proposed solution should also support tiering of data to third-party public cloud storage.		
11	Object storage must provide balancing of the stored capacity across all nodes in a cluster, ensuring, load get evenly distributed across all nodes. Load Balancer should be included as part of the solution as per throughput asked.		
12	Object storage should return the unique identity information for the stored object, which is a digital cryptographic hash algorithm along with unique version ID, storage location, date & time stamp etc		
13	Object storage nodes/controllers must have inbuilt support for S3 API should not require any third-party software or hardware or gateway to perform ingest & retrieval.		
14	Proposed object storage solution should support "indexing" and should have time base retention at the object level. Furthermore, the solution should also provide integration capabilities with external search engines.		
15	The proposed object storage solution should support object sizes from few kilobytes to 5TB. If space reclaim after deletion is impacted with small size object deletion (less than 1MB) then addon 30% Capacity must be supplied.		
16	Object should be tampering proof from outside access/intrusion and there should not be root level permission. Only remote monitoring should be available, if required.		
17	Proposed Object Storage should not allow users to access data via system-console login to the cluster's nodes and it should be used only for management.		
18	Object storage should perform online storage migration to newer system generations to handle end of life support without application downtime.		

19	Object storage should maintain the authenticity and integrity of objects using hash keys such as MDS/SHA-1/SHA-2 with self-healing and auto-configuration feature as well.		
20	Object storage should have metadata-driven policies to automate placement, protection, availability at object, tenant, custom intent either manually or from application or system levels and set retention and expiration.		
21	Object storage should be able to scale seamlessly and asymmetrically across geographically dispersed data centers without any reconfiguration of system.		
22	Object storage should be able to scale up seamlessly with zero impact to existing data availability.		
23	Offered HW and SW must be engineered for single lifecycle and supported by one OEM for end-to-end environment. Respective must be providing firmware and hardware upgrades for end-to-end environment including storage hardware, Object Storage code and OS components		
24	Should have compliance with DPDP Act, CERT-IN, and ISO 27001 standards. Verify encryption strength (AES-256) and key management for regulatory alignment.		
25	Should have seamless scalability without downtime or major architecture changes. Assess real-world throughput under mixed workloads and geo-erasure coding impact		
26	Should have hash-based verification (SHA/MD5) is efficient without performance overhead. Review metadata-driven policies for retention, tiering, and data lifecycle automation.		
27	Should have zero-impact scaling and online migration for future upgrades.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

TAPE Library

S.N	Parameter	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1	Capacity	Shall be offered with Minimum of LTO-10 tape drives. Tape Drive shall support encryption. Shall be offered with 130 Cartridge slots all activated and ready to use.		
2	Tape Drive Architecture	Offered LTO-10 drive in the library shall conform to the Data rate matching technique for higher reliability. Tape Drive Architecture in the Library shall conform to the INCITS T10 standard ADI Protocols or newer standards.		
3	Speed	Offered LTO-10 drive shall support 300MB/sec in Native mode and 750MB/sec in 2.5:1Compressed mode and should have NVMe-based cache or buffer to improve read/write speeds.		
4	Scalability	Tape Library shall be scalable to more than 500 slots and 40 number of LTO-10 Drives within the same Library.		
5	**Connectivity**	**Tape Library shall provide minimum 8Gbps Connectivity.**		
6	Partitioning	Offered Tape Library shall have partitioning support so that each drive can be configured in a separate partition. Offered Tape Library shall have support for at-least 20 partitions.		
7	Management	Tape Library shall provide AI-driven predictive.		
8	Encryption device	Offered Library shall be provided with a hardware device like USB key, separate appliance etc. to keep all the Encrypted keys in a redundant fashion.		

9	Barcode Reader	Out of 130 slots, Tape library shall support Barcode reader and at-least 5 mail slots and shall be scalable to 30 And Mail slots when fully populated.		
10	Other Features	Tape Library shall have GUI Panel Shall be rack mountable. 2. Shall have redundant power supply. 3. Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action. 4. Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved Integrated color touch control panel for installation and configuration shall barrack mountable and shall be offered with mounting kit.		
11	Reliability	MSBF (Mean swaps before failure)min 2,000,000. The tape library shall support a MTBF (Mean time between failures) of 100,000 hours. Should have dual control path redundancy for improved failover.		
12	Cartridge	130 Numbers of bar coded LTO-10 Data Cartridge and 10 Numbers of cleaning Cartridge or better.		
13	Removable Cartridge Magazines	The Offered Tape Library must be provided with Removable cartridge magazines facilitate the loading, unloading and offline storage of data cartridges, reducing media handling costs.		
14	Warranty	Five Years Comprehensive warranty with Six Hours Call to Resolution (CTR)		
15	Support	The product/appliance should not be in any road map for End of Support in next seven years as on date of RFP submission.		

16	Software	All required software's and licenses to run the full functionality of product should be provided by bidder with best level of warranty/support.		
17	Preventive Action and Integrity	Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action. Tape library shall support automated data verification while backing up the data and subsequently on media to ensure availability of data for successful restores should be supported. Tape library should support data integrity check of the backups.		
18	Backup Software Compatibility	Physical Tape Library should be compatible with Network backup software and must support existing 19.9 version of Networker Software along with support for other major industry leading backup software solution providers.		
19	SAN Switch support	The proposed appliance should be hardware compatible with various storage arrays of OEMs like HPE, IBM etc. and SAN switches of various industry leading OEMs like Brocade, Cisco etc. FC cables for connectivity to SAN switch should be provided as part of solution. Should have full API-based integration with cloud backup providers for hybrid storage.		
20	Robotic Arm Redundancy	The tape library shall be supplied with dual path for robotics to maintain high availability, Control Path Failover, Data Path Failover, LUNM aping and Library Partitioning which should support at least 4 partitions.		
21	Remote Monitoring and redundant Power supplies	Tape Library shall provide remote monitoring capability, hot replaceable tape drives and redundant hot swap power supplies. Should have automation with self-healing and automated media management.		
22	Rack	Standard rack to be provided		
23	certified	FIPS 140-2 certified encryption to meet regulatory compliance.		

RACK SERVER (For Backup solutions and Patch management)

S. N	Specifications		Compliance (Yes/NO)	References (Document /Page No.)
1	Processor Make	Intel/AMD		
2	Number of Cores	16 Cores		
3	Processor Base Frequency (GHz)	2.1 or better		
4	Processor Turbo Frequency (GHz)	4.0 or better		
5	Total Cache(L1+L2+L3) (MB)	Min 60 MB L2+160 MB L3		
6	Processor Description	5th Generation Intel® Xeon Gold/ AMD Zen 4 EPYC or better		
7	Form Factor	Rack		
8	Size (RU)	2		
9	Expansion Slots	Min 2 PCIe Gen5 slots		
10	Maximum number of Sockets available on Server	2		
11	RAM	Min 32 GB DDR5		
12	Total Number of DIMM Slots available	Min 16		
13	Number of DIMM Slots populated with DDR SDRAM	01/02		
14	Type of Interface for Hard Disk Drive	NVMe		
15	Total number of Slots available for Hard Drive	Min 8		
16	Capacity offered per Drive	Min 1TB		

17	ATA drive speed (hot plug or better) (RPM)	Min 10000		
18	Total Storage Capacity offered with SATA Drive	Min 4 TB		
19	Network Card Supported	1G, 10G, or better		
20	Number of Networking Interface Cards (LAN)	2 onboard, expandable		
21	Total Number of Ethernet Ports required in Server	Min 4x1G		
22	Networking Interface Card Features	Asset Feature Tracking, Security Management, Remote Wakeup, Each Adapter should support vNICs		
23	Video Controller (support VGA or above resolution)	Integrated GPU with VGA resolution support		
24	Certifications/Compliance (OS)	Windows Server, Linux (RHEL, Ubuntu), VMware ESXi		
25	Certification/Compliance (Virtualization/Cloud Platform)	VMware, Hyper-V, Oracle Virtualization, Red Hat Virtualization, Power VM, Open Stack		
	Features			
26	Management Features	Remoter power on/ Shutdown of server, Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port. Should have virtual Media support with all required licenses. Remote KVM, Server Health Logging, Out of Band		

		Management		
27	Security Features-1	Intel Total Memory Encryption (TME)/ AMD Secure Memory Encryption (SME)		
28	Security Features-2	Platform Firmware Resilience (PFR), Secure Boot/ Secure Encrypted Virtualization (SEV), Secure Boot		
29	Redundant Power Supply	Yes		
30	Hot Swappable (Redundant Power Supply)	Yes		
31	Power Supply Efficiency	80 PLUS Platinum or Titanium		
32	Installation and Commissioning shall be included in the scope of Supply	Yes		

Proxy Server (For patch downloading)

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1	The solution should have complete license for Web Security, URL Filtering, Antivirus, SSL and content inspection built in solution for user base from the first day in same appliance. The Solution should intercept user requests for web destinations (HTTP, HTTPs and FTP) for web security, Critical & Sensitive data upload, Data Exfiltration and in-line AV scanning. Same hardware Appliance with the visibility to provide the sanctioned and unsanctioned application visibility and control along with AI Based Category controls.		
2	The proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively and Data exfiltration control should natively be applied on same hardware or via ICAP protocol and also information protection over web channel in form of partial and exact match fingerprints, keywords, dictionaries, machine learning, destination URL category wise via natively on the same box or ICAP with Data Protection solution. Should have TLS 1.3 support.		
3	The Solution should be designed for user base request to server in active-active mode with the appliance, managed through centralized management console on server platform. Bidder to factor multiple appliances to cater the load in the DC and DR location.		
4	The solution should be capable of dynamically blocking a legitimate website which has become infected and unblock the site in real time when the threat has been removed for below mentioned security categories and vulnerabilities, block anonymizer sites or proxy avoidance tools. For example - Ghost surf, Google web accelerator		

5	The solution should have an application program interface (API) is provided to create categories and populate them with URLs and IP addresses for use in policy enforcement. The solution also supports all decrypted HTTPS traffic to a physical network interface to allows a trusted service device to inspect and analyze the decrypted data for its own purpose, without adding extra decryption products		
6	Solution should provide the details and reports for the data exfiltration happening in the password and encrypted files uploads over the web natively/ Via Integration with ICAP, protect the sensitive data exfiltration based on geo-location natively or Data Protection integration.		
7	Solution vendor should ensure to provide below mentioned security categories from day1 with automatic database updates for security categories- Advanced malware command and control, Advanced malware payloads, Bot networks, compromised websites, key loggers, Phishing and other frauds, Spywares		
8	The solution should have at least 40+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that 95+ predefined categories & 100+ pre-defined protocols should be available on product from day-1. Also, in-addition solution should have ability to configure custom categories for organization.		
9	Solution should provide separate Management server which can push policies for centralized management and reporting in case of multiple site solution deployment. Management console should provide automatic policy sync to all the remote boxes when the change is made to central console.		

10	Solution should provide the detection and protection for the transaction - based information leaks in slow and low volume and also should have cloud application usage and associated risk visibility and blocking the malicious cloud app.		
11	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM FIRST DAY: 1) Advanced Malware Command and Control category 2) Advanced Malware payload detection category 3) Malicious embedded links and iframe detection category 4) Mobile malware category 5) Key logger and Spyware category 6) P2P software database 7) AI ML Applications from day 1 to control/block 8)Generative AI – Multimedia, Conversation and Text & Code.		
12	The solution should support Shadow IT feature to identify application with their Risk level like High, Medium and Low based on various criteria from day one and the solution should have various inbuilt templates to identify Data Theft by rogue users.		
13	The solution should have authentication options for administration, the specific permissions available depend on the type of administrator and Administrator activity is logged and available for auditing or troubleshooting.		
14	The Bidder to ensure that OEM should provide Customer SPOC for better case management & should serve as the primary point of contact during escalation and SPOC should do annual review to understand the progress in achieving goals of the organization and to bring out the value of solution for the overall Information security.		
15	OEM or Authorized distributor/Partner of OEM must have a registered office in India to provide sales and Support. OEM SPOC should maintain the success plan over the contract period minimum every quarter for review.		

16	The web isolation service system shall support the ability to configure the user session inactivity timeout to save resources used by the remote browser and shall also provide the ability to stream video while isolating the rest of the traffic, shall Perform AV Scan on downloaded file(s)		
17	Isolation solution should be provided for 100 users for sending the uncategorized and phishing URL traffic though the isolation service provided by the same OEM		
18	Sandboxing service solution must support Manual Upload of files for Ad Hoc File Analysis directly to the Sandboxing Manager. Also, solution must carry out static analysis on Files submitted including YARA engine File analysis and signature lookup.		

UPS (25 KVA)

S. N	Specifications	Description	Compliance (Yes/No)	References (Document/Page No.)
1	Capacity	Min 25 kVA		
2	Output Power Factor	0.8 to 1.0 (20 to 25 kW)		
3	Input Voltage	380/400/415 V AC (3-phase)		
4	Output Voltage	380/400/415 V AC (3-phase)		
5	Input Frequency	50/60 Hz (auto-sensing)		
6	Output Frequency	Synchronized with input or 50/60 Hz		
7	Operating Efficiency	90-95% in online mode		
8	Eco Mode Efficiency	Up to 98%		
9	Battery Type	Lead-acid (VRLA) or Lithium-ion		
10	Backup Time	60 Minutes		
11	Battery Configuration	Separate battery cabinet		
12	Topology	Online double conversion		

13	Transfer Time	0 ms (no transfer time)		
14	Bypass Mode	Automatic and manual bypass options		
15	Display	LCD or LED interface		
16	Communication Interfaces	USB, RS-232, SNMP, or Ethernet		
17	Management Software	Compatible with UPS management software		
18	Overload Protection	Automatic shutdown or alarm		
19	Short Circuit Protection	Built-in protection mechanisms		
20	Surge Protection	For input and output		
21	Form Factor	Tower or rack-mountable		
22	Dimensions	Varies by manufacturer		
23	Weight	Typically, 200-300 kg		
24	Operating Temperature	0 to 40°C		
25	Humidity	0 to 95% non-condensing		
26	Cooling	Internal fans with airflow design		
27	Warranty	05 Years		

Smart Rack (42U)

S.N	Specifications	Description	Compliance Yes/No	References (Document/Page No.)
1	Rack Size	42U		
2	Width	600mm/800mm		
3	Depth	1000mm/1200mm		
4	Load Capacity	Min 1400 Kg		
5	Cooling	3.5 Tons X 2 AC Units Passive/Active cooling Modes		
6	Power Distribution	Integrated PDU (Power Distribution Unit)		
7	Cable Management	Vertical/horizontal management options		
8	Material	Steel, aluminum, or other durable materials		
9	Security Features	Fire Extinguishers, Lockable doors, side panels, cameras and biometrics access control system should be available.		
10	Monitoring	Temperature, humidity, and power monitoring		
11	Accessibility	Front and rear access for maintenance		
12	Compatibility	Compatible with standard 19" equipment		

13	Weight	Typically, around 100-200 kg (empty)		
14	Finish	Powder-coated or anodized finish		
15	Mobility	Optional caster wheels for mobility		
16	Environmental Rating	IP rating (IP20 or Higher)		
17	Warranty	5 years standard		

Laptop

S.N	Specifications	Description	Compliance (Yes/No)	References (Document/Page No)
1	Chassis Material and screen size	Metallic/15–16-inch with Backlit keyboard		
2	Hinges/keyboard	Metallic/Backlit		
3	Processor Make	Intel/AMD/Qualcomm		
4	Processor Type	Intel Core i7-1355U Processor 13th Generation or higher (while quoting a higher version CPU it shall be ensured that the no. of cores/threads, processor base frequency and Cache should be equivalent or higher than the specified CPU) or AMD 7730U Processor or higher (while quoting a higher version CPU it shall be ensured that the no. of cores/threads, processor base frequency and Cache should be equal to or higher than the specified CPU)		
5	Clock Speed	4GHz or higher		
6	Memory	Min 16 GB DDR5 4800 MHz, expandable up-to 32 GB or higher without discarding of any existing modules		
7	HDD	Min 1TB SSD		
8	Graphics	Integrated UHD Graphics/Integrated AMD Radeon Graphics or higher		

9	Bluetooth	Bluetooth 5.2 or higher		
10	WiFi	WiFi 802.11n, WiFi 802.11ac, WiFi 802.11ax		
11	Network Port	Min 1x 10/100/1000 Mbps		
12	I/O Ports	a) Min 2x USB 3.2 Gen 1 port or higher		
		b) Min 1x USB-C Type/Thunderbolt 3 or higher		
		c) Min 1x HDMI 2.0 or higher		
		d) Min 1x Universal audio port		
13	Security Feature	a) Finger Print reader		
		b) TPM 2.0		
		c) Lock Slot (cable to be provided)		
14	Operating System (Supported)	Microsoft Windows 11 Pro or later– 64 bit, Ubuntu Latest version, Dual boot OS		
15	Operating System (Factory pre-loaded)	Pre-loaded with only Microsoft Windows 11 Pro or later– 64 bits.		
16	Keyboard	Standard backlit keyboard		
17	Mouse	External USB Wired Optical Mouse		
18	Battery Backup	3 Cell 50 W/Hr or higher battery to provide battery backup of more than 8 hours		

19	Weight	Max 1.5 Kg		
20	Webcam	Integrated HD Webcam or higher		
21	Audio	Integrated microphone and stereo speakers		
22	Power Adaptor	USB Type-C power input/65 W External AC power adapter		
23	Accessories	Premium Backpack		
24	Warranty	Comprehensive onsite warranty of 5 years or higher.		
25	Support	a) Support should be either from OEM/Vendor participating in this quote.		
		b) Service response time should be NBD.		
		c) Downtime should not exceed 3 working days.		
		d) Vendor should either service the system or provide standby system with- in the specified time frame else warranty shall be extended by 15 days for every one day of delay		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

Web Application Firewall (WAF) (with Physical Appliance)

S.N	Specifications	Compliance (Yes/No)	References (Documents/ Page No.)
	General Requirements:		
1	Should be an appliance with hardened OS and available for the VMware vSphere, Microsoft Hyper-V, Nutanix AHV and KVM or OpenStack.		
2	Web application firewall should provide specialized application threat protection.		
3	Should protect against application layer attacks targeted at web applications.		
4	Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting and support OWASP application security Methodology.		
5	Should provide controls to prevent identity theft, financial fraud and corporate espionage.		
6	Solution should have provision to add application licenses as per the raised/scalable requirement.		
7	Automatic signature updates and install		
8	Should monitor and enforce government regulations, industry best practices, and internal policies.		
	Performance requirements		
9	Should deliver minimum 2Gbps of throughput scalable to 3Gbps. (As discussed this would be a H/W appliance of 2GB)		
	Interface and connectivity requirements		
10	Should support 4 no's of virtual Network interfaces.		
	Feature specifications.		
11	The Solution should be able to perform in multiple modes such as Active/ Passive mode, Transparent mode, proxy mode.		

12	Should have Data Leak Prevention module to analyze all outbound traffic alerting/blocking any credit card/Aadhar No leakage and information disclosure		
13	Provide controls to meet PCI DSS compliance requirements for web application servers.		
14	Should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.		
15	Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.		
16	Should support automatic signature updates to protect against known and potential application security threats.		
17	Ability to define different policies for different applications		
18	Ability to create custom attack signatures or events		
19	Ability to combine detection and prevention		
20	Should protect certain hidden form fields		
21	Must provide ability to allow or deny a specific URL access/IP(s).		
22	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, converting back slash to forward slash character etc..		
23	Must support Website anti defacement		
24	A given user must be enforced to follow a sequence of pages while accessing.		
25	The WAF should support IP Reputation Service and able to provide up to date information about threatening sources.		
26	Support IPv6 for Reverse Proxy deployments and It should also Support IPv4 to IPv6 and IPv6 to IPv4 communication		
27	Device should be able to control BOT traffic and It should be able to block known bad bots and fake search engine requests		
28	WAF should support File Upload Violation & should provide support for scanning of malicious content		

29	The Solution should protect against HTTP parameter pollution attacks.		
30	It shall have features to hide errors from server and redirect to customized page		
31	It should allow IP addresses or IP address range for bypassing applied security policy for one particular hosted application but should not bypass others.		
32	Web Application firewall should facilitate in hiding/masking sensitive parameters in all user logs.		
33	Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address permanently or for a time period.		
34	Should inspect Simple Object Access Protocol (SOAP) and extensible Mark-up Language (XML), in addition to HTTP (HTTP headers, form fields, and the HTTP body).		
35	The negative security model should detect and protect attack based on Signature (Regular expression) and complex logic (logical AND, Logical OR) against incoming URL request and the same may be extended for all parts (i.e., URI, parameters, headers, cookies.)		
36	The positive security model should validate URLs, directories, cookies, headers, form/query parameters, HTTP methods, File upload Extensions, Allowed meta characters etc		
37	The WAF should support profiling to configure fine grained controls for each deployed web application		
38	The solution should support all operating systems/Development frameworks and their versions including but not limited to Windows, AIX, Unix, Linux, Solaris, HP Unix.		
39	The Solution should provide HTML rewriting functionality (e.g., edit, add, delete request and response header, rewrite and redirect the URL in the request, rewrite response body etc).		
40	The Solution should have the ability to generate and issue CAPTCHA or equivalent queries to challenge suspicious clients.		
	Auto Learn		
41	Should have the capability to Auto-Learn Security Profiles required to protect the infrastructure.		
42	Should provide a statistical view on collected application traffic		

43	auto-learn options should be available to tweak and fine tune rules		
44	WAF may continue to provide protection even while in learning mode.		
	Brute Force Attack		
45	Should have controls against Brute force attacks		
46	should Detect brute force attack (repeated requests for the same resource) against any part of the applications		
47	Custom brute force attack detection for applications that do not return 401.		
48	The solution should provide protection from application layer DDoS attacks such as slowloris, RUDY and slow read attacks		
49	Protection against SYN-flood type of attacks (This is L3/L4 DDoS which can be taken care by dedicated DDoS appliance within infra)		
	Cookie Protection		
50	Should be able to protect Cookie Poisoning and Cookie Tampering.		
51	Strict Protocol Validation		
52	Must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1		
53	Should support restricting/Controlling the methods used.		
54	Should validate header length, content length, Body length, Parameter length, body line length etc..		
	SSL		
55	It shall support hosting/terminating of SSL web applications and should allow to upload the certificates and private/public key pairs for the Web servers.		
56	In termination mode, the backend traffic (i.e., the traffic from the WAF to the web server) can be encrypted via SSL		
57	Are all major cipher suites should be supported by the stable upgraded SSL/TLS implementation.		
58	Should provide protection against SSL Based attacks.		

59	Should support for SSL off loading		
	High Availability and load balancing		
60	Should support High Availability in active/passive & active/active mode		
	Vulnerability Scanning.		
61	Shall be integrated with Third Party Vulnerability scanning tools to provide virtual patching with required understanding of WAF policy		
	Authentication and Administrative access.		
62	Should support Secure Administrative Access using HTTPS and SSH		
63	Should support Role Based Access Control for Management		
64	Ability to remotely manage boxes		
65	Management User Interface support for both GUI and CLI access.		
66	Separate network interface for SSH/HTTPS access.		
67	Support for trusted hosts		
68	Role-based management with user authentication		
69	Centralized Management / Reporting of multiple WAF devices for large distributed environment		
70	Should support two Factor Authentication for login into the Management Web GUI		
	Logging, Reporting and Troubleshooting.		
71	Ability to identify and notify system faults and loss of performance		
72	Should support Log Aggregation		
73	Should support multiple log formats such as CSV, Syslog, TXT, etc.. (we support all standard formats such as CEF, LEEF, and W3C for SIEM integration)		
74	Should support inbuilt Reporting and sending the report via E-Mail		
75	Should support report formats in PDF, HTML/WORD/RTF, etc..		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M - V	M - IV	M - III	M - II	M - I	PO

76	Reports should be customizable		
77	Report Distribution Automatically via email		
78	Should generate comprehensive event reports		
79	Should be able to monitor real-time HTTP throughput		
80	ALL Logs must have compliance to separate Log Server/SIEM solutions as per standard norms		
81	Alerts to be raised to SOC team through Email, Syslog, SNMP Trap, Notification etc for blocking the traced malicious IP source causing specific attack		
82	Shall support to generate reports like pie-chart, bar-chart based on user defined security compliance baseline.		
83	Shall allow commands from WAF for Troubleshooting network related issues like Ping, traceroute.		
84	It shall support to generate vulnerability reports based on standard vulnerability database like CVE, NVD etc.		
	Backup Solution		
85	It shall support to take full secure configuration back up on a physical disk/VM disk or SAN/NAS storage.		
86	Should Support automatic failover with geo-distributed clustering for resilience.		
	Service Support		
87	OEM should be able to deploy the Web application firewall and remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.		
88	System should have Open Stack Neutron plugins or API integration should be supported.		

DDoS Protection Appliance

S.N	Specifications	Compliance (Yes/No)	References (Document/ Page No.)
1	The proposed OEM should be Parent Technology. (The OEM should NOT be White labeled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).		
2	The Proposed solution should be a Dedicated appliance (NOT a part of Router, NGFW, Application Delivery Controller, Proxy based architecture or any StateFul Appliance) with 10 Gbps of Mitigation Throughput.		
3	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Legitimate throughput handling: 2Gbps from day one and scalable up to 12Gbps Attack Concurrent Sessions: Unlimited Inspection Ports supported: 12 x 10G SFP+ from day one and option for additional 12 x 10G SFP+ for future use. Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port Change: DDoS Flood Attack Prevention Rate: 45MPPS (In addition to Legitimate throughput) Attack Concurrent Sessions: Unlimited Inspection Ports supported: 12 x 10G SFP+ Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port		
4	System should support horizontal and vertical port scanning behavioral protection.		
5	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms and stateless solution to detect and defend against threats at L3-7.		

6	Behavioral DoS (Behavioral Denial of Service) Protection should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. **Network-flood protection should include:** • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP flood • ICMP flood • IGMP flood		
7	System should have DNS Flood protection for each type of query including, A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV etc.		
8	Positive Security Model should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic		
9	System should support DNS Challenge and DNS Rate Limit.		
10	System should support HTTP Challenge Response authentication without Scripts		
11	System should have SIP Flood Protection, UDP and UDP Fragmented Flood.		
12	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 1.5 million inbuilt IoC's and integration with TIP on STIX / TAXI to support up to 3.5 million IOC's		
13	Solution should be transparent to control protocol like MPLS and 802.1 Q tagged VLAN environment. Also, it should transparent to L2TP, GRE, IP in IP traffic.		
14	Countermeasure should be updated in real time.		

15	The appliance should have below Security Protection Profiles: 1. DDoS Protection. 2. DNS Protection. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Anti-Scanning.		
16	System should protect from DDoS attacks behind a CDN Network.		
17	**The proposed Device should use the following Block Actions:** 1) Drop packet, 2) Reset (source, destination, both), 3) Suspend (source IP address, source port, destination IP address, destination port or any combination), 4) Challenge-Response for TCP, HTTP and DNS suspicious traffic		
18	The solution should support Integration with ISP / OEM Cloud based Scrubbing Centers (IN INDIA) in case of Bandwidth Saturation attacks for future use. Proposed vendor should have reference deployment in atleast 5 T1 ISP's in India.		
19	Bidder should propose Centralized Management & Reporting Solution from Day One.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

SOC Infrastructure

All Displays screens, Computers, Surveillance equipment, fire alarm system with fire extinguishers etc. will be part of SOC. (ITBP will finalize the sizing according to requirements.)

QRs not required.

Authentication, Authorization and Accounting (AAA) Internet Facing

S.N	Specifications	Compliance (Yes/No)	References (Document/ Page No.)
1	The solution must support authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+.		
2	The solution should provide authentication, user or administrator access and policy control for centralized access control. The solution must support an integrated user repository in addition to integration with existing external identity repositories such as Microsoft Active Directory servers, LDAP servers.		
3	Authentication protocols: The solution must support authentication protocols like PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication through Secure Tunneling (FAST), EAP-Transport Layer Security (TLS), and PEAP-TLS. Should have Multi-Factor Authentication (MFA) (e.g., biometric, TOTP, security keys)		
4	The solution must support a rules-based, attribute-guided policy model that provides access control policies, which can include authentication protocol requirements, device restrictions, time-of-day restrictions, and other access requirements. Should have Implement Context-Aware Authentication (Geo-location, device trust score) and Automated Certificate Lifecycle Management. Should have Micro-Segmentation for strict access control.		
5	The solution must support a web-based GUI centralized management for primary and secondary instances.		
6	The centralized management must support management of software upgrades on both primary and secondary instances.		
7	The solution must support AAA features for TACACS+-based device administration on both IPv4 and IPv6 networks.		

8	The solution must support high availability from day one.		
9	The solution must include monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI.		
10	The solution must support central database for all user accounts and centralized control of all user privileges, which can distribute throughout the network-to-network switches and access points.		
11	The solution must be able to provide AAA services for wired and wireless LAN, firewalls, and VPN.		
12	Shall be able to provide for diverse type of network devices like switches, routers, firewalls, VPN using AAA.		
13	Shall be able to provide IEEE802.1x authentication services for network switches and wireless access points.		
14	Shall support Lightweight Directory Access Protocol (LDAP) authentication forwarding for user profiles stored in directories from leading directory vendors.		
15	Shall provide features to define different access levels for each administrator and the ability to group network devices to enforce and change of security policy.		
16	Shall provide for defining sets of ACLs that can be applied per user or per group for layer3 network devices like routers, firewalls and VPNs		
17	Shall provide for certificate revocation using the X.509CRL profile for enhanced security with EAP-TLS.		
18	The solution must be software based and shall be deployable on a Virtual Machine and also have load balancing & redundancy.		
19	Shall be provided separate hardware for public facing and WAN facing data centers.		
20	AAA+ integrates with **network infrastructure using RADIUS/TACACS** (switches, access points, and controllers) and provides flexibility to integrate with third-party network equipment and security tools.		

21	Should have Integrate with SIEM & XDR for real-time security insights		
22	Should have Hybrid/Cloud-Based AAA Integration		
23	Should have Introduce Granular & Adaptive RBAC (Access based on user behavior, risk level) and Just-In-Time (JIT) Access Management.		
21	Standard Warranty up to 05 years and technical support for 5 years.		

NAC (Network Access Control) Specification for Internal Network

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1.2	Customer intends to procure the solution for 5,000 devices covering endpoints, routers, switches, desktops, IP phone, printers, etc. The implementation should be at DC-DR locations and there should be HA between DC-DR.		
1.3	The Solution should offer the flexibility to incorporate additional functionality in future for storage of asset inventory data and device posture history, allowing the Customer to retain asset inventory records for up to 90 days as Customer may need to search and monitor configuration changes and device posture to facilitate forensic investigations as needed.		
1.4	Customer reserve the right to conduct the onsite POC of Solution as a part of technical evaluation in live environment with 2,000 endpints. Customer Team may ask to demonstrate all or specific capabilities as per compliance sheet. Bidder/OEM must demonstrate the same within 7 working days. Bidder/OEM have to arrange POC Hardware & License of Solution. If Bidder/OEM fails to demonstrate such features, Customer may technically disqualify such solution/Bidder		
2	Visibility, Categorization and Assessment		
2.1	The solution should provide comprehensive visibility by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint of each & every device connected with the Customer's network.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

2.2	Agent & Agentless -The proposed solution must support both agent based & Agentless deployment and provide complete posture analysis both with & without agent. Customer will be at its discretion to implement either agent based or Agentless solution at all endpoints(functioning without the need for persistent installation of agents or executable files on the endpoints)		
2.3	Solution should be able to detect, classify and restrict all endpoints dynamically mentioned above as soon as these are introduced to the Customer Generation Corporation's network based on various parameters (including and not limited to) as OS signature, chassis, traffic pattern, OEM information, MAC address, IP address, passive network telemetry, etc. Information may be fetched by querying the actual endpoints, or alternatively from the infrastructure, Domain Name, Hostname using MAC OUIs, using RADIUS, AD, HTTP, DNS, Net Flow, SPAN/Mirrored traffic, network scan, etc.		
2.4	Solution must get complete visibility of all open ports (TCP/UDP) of all connected device in the enterprise & help in categorization of vulnerable port Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk- compromised endpoints within the network.		
2.5	The Solution should support all the features& Functionalities like Profiling, Compliance check, Remediation, Blocking, reporting, alerting the device admin, notifying the end user etc. in both agent and Agentless mode(functioning without the need for persistent installation of agents or executable files on the endpoints)		
2.6	The proposed solution must support central client installation on AD and non-AD endpoints with a zero touch deployment approach to the extent possible		

2.8	The proposed solution must support validation of endpoints through three methods: agentless (functioning without the need for persistent installation of agents or executable files on the endpoints), persistent client-based agents, and dissolvable agents. It should ensure that endpoints comply with the company's posture policies, which include, but are not limited to, checks for: Latest OS patches Antivirus and antispyware software packages with up-to-date definitions Registry keys and values Installed applications Local firewalls Peer-to-peer (P2P) applications Disk encryption USB device checks		
2.9	The solution should support both 802.1X and non-802.1X architecture and integration with Customer's existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployment.For Non-802.1X supported component it should support other Protocol viz. Agent-less, MAC Address based Authentication, SNMP, SSH, etc.		
2.10	The solution must automatically classify detected devices into categories based on their functions, such as Windows (all versions), Apple Mac, Printers, Network Devices, Linux, Unix, and IoT devices. This classification should be achieved without installing any agents (functioning without the need for persistent installation of agents or executable files on the endpoints), particularly in environments where 802.1x is not implemented.		
2.11	Solution should support auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies and must check the end device compliance before permitting access to the network.		

2.12	Solution must support discovery, classification and assessment with multiple IOT devices (e.g. IP Phone , IP Camera, IP Printers , IP Scanners etc.) without doing any changes in network infrastructure. Discovery of the IOT Devices with accurate classification (Based on OS, Vendor Model, MAC OUI, Network function) & assessment (where device are connected , how device is connected , Must be in appropriate segment, vulnerable (TCP/UDP) port assessment, SNMP/ SSH/ Telnet Default/ Weak credentials verification etc.) and help in determining which devices in Customer's network are vulnerable.		
2.13	The Solution must provide complete visibility of every connected devices. Visibility must not only be limited to IP address, MAC address and Operating System but it should also include OS version, service running, process running, application version, application installed etc.		
2.14	The solution must have ability to perform passive discovery of all IP-based devices such as Device type (computers, printers, network equipment), HTTP user agent , HTTP/DNS header infotmation by using SPAN or traffic mirroring functionality and helping Customer to identify, profile, and monitor devices on Customer's network.		
2.15	Solution must support functionality in both managed and un-managed switches. Solution must help in uncovering of unmanaged & unknown Switches through number of hosts detection, etc. and block non-compliant endpoints which are connected to un-managed switches.		
2.16	Solution must be able to detect all users (domain as well as local) including local admin across all endpoints.		
2.17	The solution should provide comprehensive visibility into all installed applications with their exact version details in the network, as well as all processes and services running on the network. Once complete visibility is achieved, the solution must support the creation of custom policies to address vulnerable services and enforce necessary controls on the endpoints. These controls may include notifying administrators, terminating processes or services, and uninstalling applications.		

2.18	Solution must support controlling capabilities of USB devices (with Class level detection of Peripheral Devices like printer, imaging devices, WPD, Bluetooth, etc.) with and without endpoint agents(functioning without the need for persistent installation of agents or executable files on the endpoints)		
2.19	Solution should have option to create posture assessments policies by checking availability of latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), and applications.		
2.20	Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.		
2.21	The solution must support all types of endpoints and devices used by Customer, regardless of vendor, operating system, or connection type (wired, wireless, VPN, etc.).		
2.22	The solution should support Customer‘s existing network infrastructure i.e. managed & unmanaged switches to block or limit the non-complied and rogue devices behind that.		
2.23	Solution should verify access by users to network resources according to an authorization scheme defined in an existing authorization system, such as Active Directory, RADIUS servers, TACACS etc. It shall allow enforcement of identity- based policies after an element is allowed in the network.		
2.24	The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, posture, profiling, and guest management services on a single platform.		
2.25	Solution must be deployable in out-of-band model (with all feature& functionality) to ensure network keeps functioning even if the solution goes down for whatever reason.		
2.26	The proposed solution should be fully functional without requiring the deployment of a client, agent, or any executable file on endpoints(functioning without the need for persistent installation of agents or executable files on the endpoints)		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

2.27	The solution should provide policies to address known ransomware threats by detecting, evaluating, and responding to vulnerabilities and threats used by ransomware. Policies should offer instant visibility, options for a fast and simple response, and the ability to track and segment devices that cannot be patched or mitigated.		
2.28	The solution should check for known vulnerabilities on Windows endpoints and remediate or handle the device as specified within the rule, without relying on any third-party tools.		
2.29	The solution must support at least the following IOC types for scanning: CnC Address (Command and Control URL). Process (Process Name, Process Hash, Process Hash Type). File Exists (File Name, File Path). Mutex (Mutex Name). Registry Key (Path, Value). Service (Service Name)		
2. 30	The solution should be capable of performing IoT posture assessments by identifying all IoT devices, such as routers, switches, printers, IP cameras, and IP printers, that are using factory default credentials. It should also be able to test these devices for factory default and weak credentials across various protocols, including SSH, Telnet, and SNMP.		
2.31	The proposed NAC solution should provide Hardware/Asset Management information, including all TCP/UDP ports open in the network, hardware information of endpoints, all services, processes, and applications installed on the network.		
2.32	The solution should provide out-of-the-box visibility into Virtual Machine properties, including Boot Time, Virtual Machine Hardware, Orphan Status, Peripheral Devices info, Port Group, Power State, CPU Usage (in thousandths), Network I/O (KBps), etc.		

2.33	The proposed solution should support vendor agnostic switch infrastructure and operate in a heterogeneous network with switches and routers from multiple OEMs such as Cisco, Juniper, 3com, Nortel, D-link etc. and legacy switches		
2.34	Solution should integrate seamlessly with Customer's existing IT infrastructure comprising of Routers, switches, firewalls, Antivirus solution, SIEM solution, Active Directory, vulnerability assessment tool, patch management solution etc		
2.35	Solution must be able to provide compliance for Hardware properties on windows like Hardware Computer, Disks, Monitors, Motherboard, Network Adapter, Physical Device, Physical Memory, Plug and Play Device, Processor, etc.		
2.36	The proposed solution must seamlessly integrate with existing SIEM platform to enhance threat detection and response capabilities. Upon a device connecting to the network, it shall automatically transmit comprehensive device status information, including device type, operating system, compliance posture etc, to the SIEM system.Subsequently based on the SIEM's assessment from log collected, instructions, such as quarantine or remediation, will be relayed back to the proposed solution. The solution should then enforce these instructions, dynamically allowing or denying network access based on the device's compliance status and the SIEM's assessment, thereby automating and accelerating threat mitigation.		
2.37	The proposed solution must provide robust integration with existing Patch mangement solution/SCCM infrastructure to automate and streamline endpoint management. This integration should enable the automatic discovery and enrollment of unregistered devices into Patching solution, including those with missing or corrupted SCCM/Patch maangement agents, significantly reducing manual IT workload. The solution should continuously validate endpoint compliance with security and patching policies, ensuring all systems maintain the required software, security patches, and configurations throughout their network. This integration will enhance security operations efficiency, minimize business risk in real-time, and ensure consistent endpoint security posture across the organization		

2.38	The solution must provide seamless integration with our existing Endpoint Protection Platform (EPP) to ensure comprehensive endpoint security and compliance. The solution should Verify EPP client presence and compliance upon network connection and Enforce isolation for non-compliant endpoints with missing/not installed/broken/corrupt EPP agents. If the EPP detects a non-compliant state, it must immediately tag the endpoint and report the non-compliance to the solution, triggering immediate isolation until remediation is completed		
2.39	The solution must integrate with our existing XDR/EDR platform to strengthen device security and compliance. This integration should verify XDR/EDR client presence and compliance upon network connection and Enforce isolation for non-compliant endpoints with missing/not installed/broken/corrupt XDR/EDR. Leverage XDR/EDR-provided malware and Indicator of Attack (IOA) threat intelligence to monitor network-wide endpoint activity and enable dynamic network access limitation for compromised devices based on policy-driven responses to XDR/EDR threat detections		
3	Management:		
3.1	Solution should have a Centralized Management for managing, monitoring & controlling for all the features of the NAC.		
3.2	Centralized Management solution must have executive, detail and customizable dashboard and support role-based users/admins.		
3.3	The solution should able to categorize the alerts on the basis of risk (high, medium and low), type of devices, location etc.		
3.4	The solution should offer a built-in alerting mechanism through email & SMS based on the categorization of alerts.		
3.5	The solution should have a single web-based or client based. GUI console for admin users for managing the full functionalities of NAC solution.		
4	Remediation & Control: Auto-remediation capability		

4.1	Solution must be able to integrate with existing Antivirus for auto- remediation.		
4.2	Solution must validate list of blacklisted applications running on the machine.		
4.3	Solution must help Customer in enforcing security policies by blocking, isolating, and repairing non-compliant machines in a quarantine area without requiring administrator attention.		
4.4	Solution must support auto-remediation on all the non- compliant end point like Update AV automatically, Update Patches automatically, Start Antivirus/ Patch Endpoint agent, Kill/ Uninstall blacklisted application/ Service/ process etc.		
4.5	The solution should be able to provide capability to run custom scripts on Windows endpoints to meet endpoint compliance. (For Example, but not limited to endpoints chassis type, Free Space in C drive or Windows Activation status details etc.) or for auto- remediation (For Example Uninstalling Blacklisted application, Kill Blacklisted process, installing security host-based agent etc.)		
4.6	The solution should be able to provide capability to run custom scripts on Linux endpoints. Running a custom script or command is based on compliance policy or for auto- remediation. For Example, but not limited to: - To fetch the details custom details from Linux endpoint, get the running process related details or uninstalling the malicious software from endpoint etc.		
4.7	The solution should be able to provide capability to run custom scripts on Apple Macintosh. Running a custom script or command is based on compliance policy or for auto- remediation. Example but not limited to:- To fetch the custom details from Apple Macintosh endpoint , get the running process related details or uninstalling the malicious software from endpoint etc.		
4.8	Solution Must support the capabilities to detect and disable unauthorized dual-homed and NAT endpoints.		
4.9	Solution must provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, or Security Group Access (SGA) tagging.		
6	Reporting and administration		

6.1	Solution must have built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.		
6.2	The solution must support the capability to generate reports on: Hardware components (e.g., Memory, RAM, HDD, Peripheral devices) All installed software with version details across the network All TCP/UDP open ports in the network Services running on the network Processes running on the network Application inventory across the managed extended enterprise		
6.3	The solution must include predefined, out-of-the-box reports that can be customized to meet the specific needs of Customer. It should support generating reports on a scheduled basis and on-demand in real-time. Additionally, it should have the capability to send these reports via email from the console to ensure timely access to critical information.		
7	Support requirements		
7.1	OEM of the solution must have its own technical support center in India		
7.2	The OEM should offer 24/7 remote support for the software.		
7.3	Bidder has to maintain the Security solutions and its related components and Customer should have direct access to OEM TAC support on 24x7x365 basis throughout the period of the contract with the Customer i.e. for 5 years. The bidder has to consider related cost for such OEM TAC support for the solutions from concerned OEMs in their commercial bid.		

NMS (NETWORK MANAGEMENT SYSTEM)

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1	Complete end to end fault & Performance monitoring system having: 1. Network Fault & Performance Monitoring 2. Network configuration & Change management 3. Net Flow Traffic analysis 4. Log management 5. ITSM/Ticketing 6. Reporting & Dash boarding with integration		
2	The solution should be capable of running in Linux platform with open-source database as backend and should be 64-bit application to fully utilize the server resources on which it is installed. Also have Cloud-native or hybrid deployment support for better scalability		
3	The OEM should be ISO 9001:2015, ISO 20000-1:2018, ISO/IEC 27001:2013, ISO/IEC 27034-1:2011 & CMMI3 certified.		
4	The solution should have dual-stack IP support (support both IPv4 and IPv6) and Zero Trust principles with identity-based access control for NMS users and should be completely vendor-agnostic in nature also have API-based integration for better interoperability with third-party tools to be able to monitor a multi-vendor environment.		
5	The solution should be a unified system which can monitor networks, servers, apps and any IT or Non-IT Communicable device (IP based).		

	Network Fault and Performance Management		
6	Detect & highlight faults (abnormal situations) in near real-time occurring anywhere within the monitored IT Infrastructure.		
7	Provides Filtering, De-duplication, Holding, Suppression and Correlation capability to let user focus on the critical event that affects the business and business processes. Should have Machine learning for better event correlation and prioritization		
8	Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement. Should have dynamic severity scoring based on real-time risk assessment		
9	System should support separate Rule Engine based alarms apart from the generic threshold. a. Should have capability to configure Device Group based, Node Based, Resources/Interface based, and Aggregation link based. b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information c. Rules should have option to apply configuration on top of performance value or based on configured threshold alarms d. Rules should have option configure the breach based on min, max and average values e. Should have option to configure rules n repeat counters f. Should have options to select custom alarm and clear alarm messages for individual configured rules g. Should have option to send severity levels like error, warning and information h. Notifications support based on configured rules		

10	Sends alert via E-mail, SMS, Execute Batch file, SNMP Trap, XML notification, Pop-up window and Audio alert.		
11	Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group by location, branch, departments etc as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters.		
12	Provision to change the polling interval to any frequency depending on the priority till the individual component/resource level like each interface might have the different polling interval in the same device based of the criticality and importance of service customer		
13	SLA calculation/Isolation report should be made with the consideration of both the Primary and Secondary link together instead of individual link based. The downtime calculation will be measured when both the links are down for internal reporting and link based for ISP reporting. System should provide the flexible configuration in UI itself based on user needs		
14	System should provide many different types of topology representation. To perform the following: 1. Display physical connections of the different devices being monitored in the system 2. Display flat maps of the entire network or networks in a single view 3. Display customer maps based on user configurations 4. Display maps based on geo locations		
	Network Configuration and Change Management		

15	Tool must support CLI-based network device configuration snapshot management including backup of configuration files, traffic logs, messages etc., pushing configuration files to target network devices, with option to perform remote firmware upgrades. Should have Automate configuration backup and change tracking with version control		
16	Tool must provide network device vulnerability detection based and Integrate with vulnerability management solutions to auto-remediate detected risks on their model number and firmware version. It should also provide options to remedy the vulnerabilities by pushing required patch to the device.		
17	Tool must provide option to perform standard compliance checks like PCI-DSS, NIST, DISA etc. across all target CLI-based network devices		
18	The configuration changes to be done on target network devices must follow an approval-based system wherein changes can be performed only after required approvals are passed. Tool must have in-built approval mechanism along with option to integrate with Change Management module of other ITSM tools for the approval process.		
19	Tool must provide network device vulnerability detection based on their model number and firmware version. It should also provide options to remedy the vulnerabilities by pushing required patch to the device.		
20	Tool must provide an option for taking remote access via Telnet/SSH to target CLI-based Network Devices with an option to record all sessions to capture all commands being executed on the remote devices. The tool must allow session relay wherein a higher-privileged user can view the ongoing CLI session of a lower-privileged user in real-time from the tool GUI. The sessions should be saved for historical analysis with flexible filter options like searching for sessions in which a particular command has been executed.		

21	Tool must provide an option for taking remote access via Telnet / SSH to target CLI-based network devices with an option to record all sessions to capture all commands being executed on the remote devices. Should have GUI-based configuration management for ease of use.		
	NetFlow Traffic analysis		
22	The proposed monitoring solution should be capable to monitor network traffic by capturing flow data from network devices, including Cisco Netflow v5 or v9, Juniper J-Flow, IPFIX, sFlow, Expand support for additional telemetry sources (e.g., Deep Packet Inspection), NetStream data and sampled Netflow data. Solution must be able to store ALL flows without any rollups or loss for retention period – for security and audit purposes.		
23	Solution should support advanced SSL/TLS analysis like detecting false certificates, expired, self-signed		
24	Solution should feature threat monitoring by comparing enterprise traffic against known IOC		
25	Solution should also feature signature-based detection techniques and allow drilldown to packets from alerts		
26	Solution should be able to detect DDoS attacks based on volumetric attacks, application attacks, scanning etc		
27	Solution should provide DDoS reports in real time within 1 minute after detection of attack with details of IP, Ports, ASN numbers, Router Interfaces, Customers facing the attacks		
28	Should monitor Class-Based Quality of Service (CBQoS) to find out if traffic prioritization policies are effective and if business-critical applications have network traffic priority. Should also support CBQoS Nested policies		

	Log Monitoring		
29	Tool should have option to collect and store system logs from target devices including firewalls, routers, switches, WLC, servers, applications & databases. Should have Integration with SIEM/XDR solutions for centralized security monitoring		
30	Tool should have multiple filtering options for incoming system logs based on target device, log_ID, severity, level, message, OS type, application / database etc.		
31	Tool should have option to export specific syslog messages to users via email / SMS		
	Ticketing Solution/ITSM		
32	Platform Pink Elefant PINK VERIFY /ITIL V4 certified for minimum 9 ITIL processes		
33	Platform Named User Licensing and concurrent in same instance		
34	Platform Ability to configure different versions of ITSM analyst Licenses in one instance.		
35	Platform True Multi-tenant platform		
36	Platform Configurable Role Templates		
37	Platform Quarterly/Half yearly/ Yearly Surveys on services provided		
38	Incident Management Chat with technician for users within an incident		
39	Incident Management Adding incident into Knowledge Base		
40	Incident Management Creation of relationship with other modules		
41	Incident Management Major Incident Management process		
42	Request Fulfillment		

43	Management Automatic creation of work-orders by Service catalog.		
44	Request Fulfillment		
45	Service Catalog Management Upto 10 Levels of approvals		
46	Service Catalog Management Conditional Approvers configuration		
47	Should have feature for manual and auto ticketing		
48	Ability to define CI in CMDB		
49	Incident mgmt. should have the ability to define priority to tickets. Should have smart auto-assignment based on workload and expertise		
50	Should allow users to attach documents/images to the tickets.		
51	Should also allow to attach RCA documents and text to the resolved tickets.		
52	Email notifications for status of the tickets, escalations & updates related to actions performed on the tickets		
	Reporting & Dash boarding		
53	Provide standard reports and Customizable, role-based dashboards with drill-down capabilities that display current status of nodes and interfaces. Reports could be viewed on daily graph, weekly graph, monthly graph, and yearly graph.		
54	Provide online and offline reports that allow the user to view the present usage of their devices. Reports generates should be exportable in the format of HTML, PDF, Excel and CSV. Allows		

	end-users to browse all reports using any web browser like Internet Explorer, Mozilla Firefox, Google Chrome etc. without the need to install any report specific software.		
55	Automatically generate daily reports that provide a summary of the IT Infrastructure as well as custom Reports and that are automatically sent by email at a pre-defined schedule to any recipient or save into any specific folder or drive and also have Adaptive alert thresholds based on historical trends.		
56	The tool should have Integrated Web based feature to build Network Diagram, No separate client window to configure network Diagram. The builder should be similar to MS Visio with all pre-loaded shapes and icons.		
57	It should be a Drag & Drop based Network Diagram builder, Dynamically Upload Images, Customizable objects to support multiple vendors, capability to export maps in an XML format and upload to any other system.		
58	Should support creation of customized dashboards and reports as per requirement.		
59	Should be able to manage and display events/alerts in the web console/Dashboard.		
60	It should allow the creation of new alerts and customizable threshold limits.		
61	Should Support Assignment of Alerts to System Administrators for processing and completion.		
62	The alerts and events should be stored into the database.		
63	Shall include a tool to generate asset and inventory reports based on the available data.		

64	Shall also provide a tool which analyses collected data with a variety of different reporting functions.		
65	Shall be able to filter report data by transaction, by specific monitored location and user-defined regions.		
66	Shall allow end-users to browse all reports using Internet Explorer without the need to install additional report viewing software.		
67	Shall be able to automatically generate daily reports and email at a pre-defined schedule to the configured recipient.		
68	Shall provide custom report manager for generating custom, personal reports.		
69	RESTful API Support Should be available to integrate with 3rd party applications.		

XDR (Extended Detection & Response)

S. N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1	The Endpoint Security Solution setup must have the capability to manage endpoints at Central Console, with phased implementation.		
2	The proposed solution should support either SaaS-based platform or on-premises deployment. It should have hybrid-cloud architecture with centralized management		
3	If the proposed solution is cloud-based, it must be deployed on a MeitY empaneled data center in India with no endpoint data sharing outside India.		
4	The solution must be scalable to manage up to 10000 End Points and servers.		
5	Solution features must be fully compatible over IPv4/IPv6 network.		
6	Solution should have management infrastructure, operational monitoring, upgrades, reporting, notifications & 24x7 support.		
7	The quoted solution must be part of MITRE ATTACK evaluations or equivalent programs in the last 3 years. It should		

	have Integrate with Threat Intelligence Platforms (TIPs) for enriched data correlation.		
8	The solution should provide a unified web-based console for all functionalities without installing additional software. Should have AI-powered automation for threat detection and response.		
9	The solution should support policy inheritance from Account to Site to Group with break inheritance option.		
10	The solution must have the option to create role-based access/view(s) of the management console.		
11	The solution should provide API access to all management capabilities, well-documented and available without extra cost.		
12	Solution must provide non-reputable centralized auditing and logging of management console activities.		
13	Endpoint Agent must provide EPP and EDR capabilities in a single agent, with features like threat intel, device control, and real-time analysis. EPP and EDR capabilities should be there for future requirement.		
14	The solution should support collecting forensic data using the same EDR agent. Should have Automated Digital Forensics & Incident Response (DFIR) capabilities.		
15	The solution should provide protection against exploits including MacOS, Windows, Linux, and processes.		

16	Solution should monitor and protect from lateral movements & insider threats. It should have User & Entity Behaviour Analytics (UEBA) for anomaly detection		
17	The solution should allow the safe download of malicious or convicted files from the management console.		
18	Solution should provide similar exploit protection across all OS (Windows, Linux, Mac). Should have coverage to containerized workloads and serverless functions		
19	Solution must provide real-time prevention against exploits of application vulnerabilities. Should have Memory Protection & Behavioral Analysis to prevent in-memory attacks.		
20	The solution should provide advanced response capabilities (Kill process, Isolate device, Block process).		
21	Solution must have capability to implement policies for rogue devices, including isolating them or installing agents.		
22	The proposed solution must have the capability to manage live global asset inventory, advanced ML device fingerprinting, and isolating malicious devices. Should have Automated Playbooks for Incident Response		
23	The solution should have native integrations with SIEM solutions. Should have API-Based SIEM integration.		
24	Should have AI/ML-driven Threat Prioritization.		

25	Should have Automated Compliance Reporting for Regulatory Frameworks (ISO 27001, NIST, GDPR, DPDPA 2023).		
26	Introduce Adaptive Risk-Based Scoring for dynamic policy enforcement.		

Vulnerability Scanner

S. N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
A	**Installation, Deployment and Integration**		
1	Solution must be able to support installation on 64-bit Linux and Windows (64-bit) also containerized deployment support for cloud-native environments.		
2	Solution shall have latest updates (e.g. exploit module) as frequent as on a weekly basis and also have real-time vulnerability updates via cloud-based threat intelligence feeds.		
3	Solution shall support offline activation and manual updates.		
4	Solution must be able to perform full backup to prevent data loss and enable to easily migrate data.		
B	**Administration**		
1	Solution shall allow API integration with other systems or be able to automate workflow and also provide out-of-the-box integrations with SOAR and ADR platforms.		
2	Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule and Auto-remediation recommendations linked to CVSS scores.		
C	**Host Scan and Web Scan**		
1	Solution shall support dry runs to show the scan information in task log only. Should be AI-powered risk prioritization for identified vulnerabilities.		
2	Solution must be able to integrate with Enhance auto-discovery of assets and shadow IT through network scans to discover host's OS, running services and		

	vulnerabilities via existing scan results or new scans. Additionally, it should enhance assets auto-discovery and detect shadow IT through network scans.		
3	Solution must support importing of scan result from external solutions including but not limited to Nexpose, Metasploit, Foundstone, Microsoft, nCircle, NetSparker, Nessus, Qualys, Burp, Acunetix, AppScan, Nmap, Retina, Amap, Critical Watch, IP Address List, Libpcap, Spiceworks and Core Impact. It should also support compliance mapping to frameworks like ISO 27001, DPDPA 2023,NIST and GDPR.		
D	**System Exploitation**		
1	Solution shall automatically select and apply exploit modules based on OS, service and vulnerability references.		
2	Solution shall have at least 6 reliability levels of exploit codes for automated exploitation.		
3	Solution shall support running individual exploit module manually from the user interface. It should also enable automated penetration testing based on discovered vulnerabilities.		
4	Solution shall support dry run to show exploit information in task log only.		
5	Solution shall support replay of exploitation tasks. It should also integrate real-time incident response triggers with SIEM solutions.		
6	Solution shall support the reuse of manually added or captured credentials within a project to validate specified credentials on additional hosts in the target network. It should also implement privileged account security monitoring.		
E	**Brute Forcing**		
1	Solution shall support brute force testing on services including but not limited to AFP, SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, SSH		

	PUBKEY, Telnet, FTP, POP3, VNC, SNMP, WinRM. It should also include multi-protocol adaptive brute-force prevention.		
2	Solution shall support customized credentials and dictionary import for brute force. It should also include AI-driven credential mutation and testing.		
3	Solution shall support credential mutation to create multiple permutations of a specified password, which enables building of a larger list based on a defined set of passwords.		
F	**Post Exploitation Action And Evidence Collection**		
1	Solution must support exploitation payload types “Meterpreter”, “Command Shell” and "Powershell".		
2	Solution must support customized macros to run selected operations automatically after exploit.		
3	Solution must support post exploitation actions including but not limited to collect system data (screen capture, password, system information), build a virtual desktop connection, access file system, search the file system, run a command shell, create proxy pivot, create VPN pivot.		
4	Solution must support deploying of persistent listeners to allow exploited hosts to connect back to Metasploit automatically.		
G	**Social Engineering Campaign**		
1	Solution must support web campaign, Email campaign and USB campaign.		
2	Solution must allow web campaign customized with http/https, IP address, port and path (e.g. https://www.abc.com:1234/abcd).		
3	Solution must support web content to be cloned from another web site (e.g. www.google.com).		

4	Solution must support web campaign that browser autopwn (apply all the appropriate exploit modules based on the browser version), specific browser exploit (e.g. MS11-050) and not do anything (just checking the connection from the users).		
5	Solution must support email campaign content customization to include a specific URL or an agent attachment.		
6	Solution must support USB campaign that generates an agent deployment .exe file.		
H	**Report and Data Export**		
1	Solution must provide built-in standard reports and support customized report functionality. It should have risk-based dashboard with graphical insights.		
2	Solution must support reports to be stored locally and sent to recipient by email after created.		
3	Solution must be able to support data export which allows a zip archive of the project suitable for importing into another instance of the solution.		

Data Loss Prevention (DLP) (Storage DLP)

S.N	Specifications	Compliance (Yes/No)	References (Document/ Page No.)
A	**Content Detection & Classification**		
1	The solution should detect on patterns in binary file types		
2	The solution should detect keywords/patterns based on location (beginning/end) and proximity to each other within documents.		
3	The solution should detect on full *Boolean* expression for keywords and key phrases.		
4	The solution should detect on pre-built dictionaries.		
5	The solution should detect and validate a wide range of sensitive data types (e.g., Source Codes, Indian PII documents etc.).		
6	The solution should detect classified Proprietary File types (types that are not predefined) and on file content not on file extensions. (eg. Document owner, authors, title etc.)		
7	The solution should detect fingerprints contents in an automated way where the user does not have to touch the files or import hashes.		
8	The proposed solution should provide the ability to the end user to manually classify the solution on the endpoint.		
9	The Proposed solution should provide Policy enforcement with combined automatic and manual classifications		
11	The solution should support user-initiated scan and remediation allowing users to run endpoint discovery scans and take self-remediation actions.		
12	The proposed solution should have single management console for data classification policies and DLP policy configuration and assignments.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

13	The proposed solution should have application, web and location-based data tagging actions. Eg. DGH developed custom built application output file shoud be automatically tagged with defined classification tag.		
B	**DLP Policy Creation**		
1	The solution should have the ability to define a single set of policies based on content, sender/recipient, file characteristics and communications protocols once and deploy across all products.		
2	The solution should provide Out of the Box Rule Sets.		
3	The solution should create policies that support full Boolean expression for keywords/patterns (not just and/or).		
4	The solution should provide directory-based policies to selectively monitor downloads based on user, business units, or directory groups, specific groups of computers and specific groups of users.		
5	The solution should provide ability to configure policies to detect on fingerprints and files from share/repository/date created etc.		
C	**Host DLP**		
1	The agent should Monitor content traversing across the endpoint by I/O channel (bus, Bluetooth, LPT, etc.) & Application Access.		
2	The solution should notify the end user of a policy violation using a customizable pop-up message and should capture content that violates a policy and store it in an evidence repository.		
3	The solution should be able to enforce policies while the endpoint system is disconnected from the corporate network and the endpoint agent should log all violations and reports into the central database when a connection to the corporate network is established.		
4	The solution should be able to Identify mass storage device by vendor specific identification numbers.		
5	The solution should be able to Identify content using regular expressions, key words, hash functions, Document Fingerprint Signatures and pattern matching.		

6	The solution should be able to Identify content based on location and allow creation of policies based on Users and Groups.		
7	The solution should provide an option of rule override which can be authorized to use an override code issued from the security administrator based on the end user's justification.		
8	The solution should support the deployment of agent, policy assignments, reporting, DLP incident management using the Central Management Console.		
9	The agent should protect itself from unauthorized removal or service stoppage.		
10	The solution should have an option to Encrypt/Quarantine/Monitor/Delete sensitive files found during endpoint discovery.		
F	**Incident Management**		
1	The solution should provide the ability to detect Policy violation which retains the source IP address, destination IP address, protocol, sender e-mail address, recipients e-mail address		
2	The solution should provide ability by which Incidents can be assigned automatically to reviewers.		
3	The solution should provide the ability for Incidents to be sorted by severity level, sender, recipient, source, destination, protocol, and content type.		
4	Incident views can be customized based on content pertinent to the reviewer's role and preferences.		
5	The solution should provide an inbuilt Case Management Tool.		
6	The solution should provide the ability for Case content to be exported with full content and attachments for review by an external reviewer.		
I	**DLP Reporting**		
1	The solution should generate reports in PDF, Excel or CSV format.		
2	The solution should develop reports built around stakeholder requirements such as top Policy Violations, Senders, Content Type, Protocol, Historical Reports etc.		
L	**Support**		
1	The solution should be proposed with Premium Support i.e. One Level higher than the base level support directly from the OEM.		

2	The support provided should provide a single point of contact for account management and escalation		
3	The OEM should provide a utility to collect product and system information to assist Support in diagnosing issues		
4	Product upgrades should be easily be downloadable from the OEM Official Website		
5	The OEM should provide a service which delivers the latest OEM product information by email — patch and upgrade notification; and critical alerts that require immediate attention.		

Security Information & Event Management (SIEM) Solution

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
	Specifications		
1.	The proposed solution must include Next Gen SIEM, Security Analytics, Big Data Analytics with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have central data repository which should act as common data lake for SIEM, UEBA & SBDL		
2.	The proposed SIEM solution should be consistent in Gartner's Leaders Quadrant across last 10 years (2014-2024)		
3.	The proposed solution must be able to handle 5000 EPS / 130 GB of data /logs per day from day one without dropping or queuing of logs as per the requirement. There should not be limitations on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.		
4.	To virtually segregate different types of data, proposed solution should support unlimited virtual storage groups or indexes. Each index/ virtual storage group should be used for searching specific data and retention period should be configurable as per indexes.		
5.	The proposed solution should be DR ready and must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.		

6 .	The proposed solution must be be deployed on pre-requiste hardware and must be able to take peak load of 35000 EPS / 900 GB per day of data from day one with minimujm of ten indexer server clusters to ensure the optimal performance all the time.		
7 .	The proposed solution should provide a test/dev license as part of the solution. It should also provide a tool in-built or integrable, that allows to create test bed environment which can help to simulate blue team and red team attacks to test use cases, train analysts etc.		
8 .	The proposed soluton must be able to achive high availability for indexing cluster without the need of any third party software.		
9 .	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.		
10 .	Machine learning should be embedded across the platform (SIEM, SBDL & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.		
11 .	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data throughout the retention period of online 180 days and 365 days of archival. Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re-ingesting security analyst would save storage cost and identify and pin point attack intime.		
12 .	The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques.		

13 .	Log Filtering – Not all logs are needed for the compliance requirements, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator. Solution should be able to work seamlessly in an air gapped environment.		
14 .	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc.		
15 .	The proposed solution must support caching mode of transfer for data collection, to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection.		
16 .	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click. The Dashboard should be accessible from the endpoints as & when required.		
17 .	The Proposed solution must offer all the below built-in threat detection techniques out of the box: Detect Web Application Threats. Detect APT Threats Integrate with any Honeypot/Deception solutions Integrate with any NBAD tools Detect threats indicated by advisories Give visibility of endpoints also by integrating with EDR, Antivirus etc. for endpoint analytics.		
18 .	The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel. Same query string should also be capable of being used for SBDL & SIEM.		
19 .	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

20 .	The proposed solution must be auto-scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per the requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.		
21 .	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO.		
22 .	The proposed solution must support a configurable replication factor of N where it can tolerate the failure of N-1 peer nodes or should handle failure of a node in the solution.		
23 .	The proposed solution must be software based allowing flexible deployment models and architecture and should be horizontally and vertically scalable.		
	Supported Data Sources		
24 .	The proposed solution must be able to support both real-time and on-demand access to data sources from files, network ports, database connections, custom APIs and interfaced incl. text, XML, JSON and other evolving format.		
25 .	The proposed solution must be able to read data input from the following log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b. Windows Events Logs c. Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.		
26 .	The proposed solution must be able to accept the following indicative live data streams feeding through the network: a. Syslog Messages		

	b. Security Alerts c. JSON streaming over HTTP/HTTPS		
27.	The proposed solution must support the decoding of the following indicative network protocols from log data or picking the meta data from network traffic: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP, NFS, Oracle (TNS), LDAP/AD, PostgreSQL, Sybase/SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI		
28.	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.		
29.	The proposed solution must come with atleast 1200 out of the box correlation /detection rules to ensure and align with various industry security frameworks, allowing to readily monitor for potential threats across the systems.		
	Index, Search, Filter, Analyze and Investigate		
30.	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem. Indicative Use Case: If the system performance is degraded or Memory/CPU utilization is high then Analyst can know from single console weather this is due to a DDOS Attack or Malware outbreak or due to some IT issue. This helps to reduce the false positive and improve response time.		
31.	The proposed solution must be able to build an unstructured index or store data in its original format without any rigid schema.		

32 .	The proposed solution's licensing should be based on post filtering of events. If log events are filtered, then they should not be counted in license.		
33 .	Proposed solution should forward data to multiple destinations apart from its own SIEM processing/data storage layer. Log collector should be able to forward data to multiple destinations.		
34 .	The proposed solution will be continuously used in the SOC so that solution builds specific repository which includes categories like including event types, tags, lookups, parsing/normalizing, actions and saved searches etc. It should help to discover and analyze various aspects in data. For example, event types should enable analyst to quickly classify and group similar events; then use to perform analytics on events.		
	Monitor, Alert and Reporting Functions		
35 .	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.		
36 .	The proposed solution must be able to execute automated corrective or follow-on actions via scripted alerts.		
37 .	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or re-indexing so that complex report or user defined reports can be built.		
38 .	The proposed solution must be able to support sophisticated statistical and summary analysis by pipelining advanced search commands together in a single search.		

39 .	The proposed solution must be able to support mathematics functions to perform calculations on field values, examples Converting bytes to kilobytes, mega-bytes, absolute value functions, highest integers, standard deviation, command length etc.; Finding the time duration between time stamp values. These functionalities should be available as a search, report, alert or dashboard etc. so that analyst can build any kind of report required.		
40 .	The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs. Indicative Use Case: Predicting Malware spread based on previous malware attack patterns.		
41 .	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment. It should quickly compare resources and capacity utilization across many hosts Indicative Use case: Visibility of services running on servers are also critical to monitor. These could be impacted due to any security incident. Overall performance of the system may get impacted etc. Hence if a SOC analyst have all this view from central platform, then this helps to reduce the time to identify and fix any issue.		
42 .	The proposed solution must possess built-in feature for anomaly detection: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results		
	Machine Learning		

43 .	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre- defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.		
44 .	The proposed solution machine learning capabilities must include API access, role-based access controls for machine learning models.		
45 .	The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open source libraries like NLP, Python etc.		
46 .	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.		
	Search and Reporting		
47 .	Reports can be scheduled in a dynamic fashion with schedule windowing and prioritization to improve run priority of high value scheduled reports and manage concurrently running reports to meet the requirements of completing reports under 24 hours. The report should be parameterized, and the user should be able to scale the parameter as needed. And Out of box aging analysis of incident should be available.		
48 .	The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing URL parameters to any third party website. The Report should be scalable IP-wise, device- wise, user-wise, data-wise, location-wise based on requirement between any two dates.		
49 .	The product internal logs must be ingested within the product for ease of troubleshooting and investigation and those logs do not consume the product license.		

50 .	The solution must provide granular license utilization down to devices, log sources and data store or additional lookups of devices to agencies by the minute and the retention of granularity can be extended to the project requirement.		
51 .	The solution must provide the same search language for search, investigate, alert, report and visualize license utilization. A proper error handling screen should be available.		
52 .	The solution's reports should run fast on large data sets. Proposed solution should use next generation functionalities like creating set of data from the main index or data store. This will avoid running the queries on large index or full index and faster response for searching and reporting.		
	Fields, Schema and Log Parsing		
53 .	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization. Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time.		
54 .	The solution must allow the adding/modifying/removing of log parsers without impacting log collection from the web interface. Should have agentless Log Collection & AI-driven Log Analysis.		
55 .	The solution must provide a field extraction wizard that is used to create parsers and allow testing and validation with existing live or historical data within the system from the web interface.		
56 .	Old data should be parsed with new parser without re-ingesting or re-indexing the data.		
	Security Analytics Platform		

57.	The proposed solution must provide the following capabilities as a Security Analytics Platform: a. One single syntax that can be used universally for search queries, alerts, reports or dashboards, SIEM and preferably for SBDL also. b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure c. Risk management technique to apply risk scores to any asset or user based on relative importance or value to the business d. Threat intelligence technique that automatically collect, aggregate, indicators of compromise from threat feeds. The solution should have capability to alert in case duplicate indicators of compromise is added.		
58.	The proposed solution must be fully integrated with the datalake platform without the need to duplicate the collected raw logs.		
59.	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user.		
60.	The proposed solution must be able to assign any arbitrary risk score based on self defined query based on any correlated events, statistical analysis, threat indicator match. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

61 .	The proposed solution must be able to retrieve from any threat feeds without restriction, retrieve threats in various ASCII/UTF- 8 file formats like text, csv, xml. Must be able to automatically parse IOC from STIX and Open IOC formats. Must be able to support multiple transport mechanisms such as TCP or Trusted Automated exchange of Indicator Information (TAXII).		
62 .	The proposed solution must be able to support atleast 8 out the following indicative list: Network HTTP Referrer, User Agent, Cookie, Header, Data, URL IP Domain Endpoint File Hash, Name, Extension, Path and Size Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data Process Name, Arguments, Handle Name, Handle Type Service Name, Description Certificate Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm Email Email Address, Subject Body		
63 .	Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioral based use cases.		
64 .	Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time		

65 .	The proposed solutions should use multiple technologies like using distance formula, geo Database, etc. to detect geographically improbable access		
66 .	The proposed solutions should use randomness to measure domain names that can be potentially from malware domain generated algorithms. Indicative Use Case: Detect DGA using randomness. Domain generation algorithms (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of domain names hence above methodologies are required in proposed solution to detect such attacks		
67 .	The proposed solution should use statistic functions or techniques like percentile or standard deviation to detect unusual activities that can be applied to insider or fraudulent use cases. Other analysis: Find common or rare events using cluster or most commonly and widely used means clustering method Find percentage of times two fields exist in the same events correlating all the fields. Indicative Use Case: Analyst should be able to see an overview of the co-occurrence of fields in data. It should give the percentage of times that the two fields exist in the same events. This will help analyst to see the relationship among all the fields in a set of results		
68 .	The proposed solution should find relationship between pairs of fields by change in randomness in pair of fields. Indicative Use Case: This helps to predict the value of another field by knowing the value of one field.		
69 .	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to		

	be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per the requirements.		
70 .	The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.)		
	Incident Response		
71 .	The proposed solution must provide investigation auditing capability to enable analysts to easily: Track searches and activities Review activities at any point Select and place into timeline for temporal analysis Help remember searches, steps taken, provide annotation support		
72 .	The solution must be able to provide a built-in facility to centralize incident analysis of entities in one location.		
73 .	The proposed solution should be able to trigger actions. These actions can be automatically triggered by correlation alerts or offences or manually run on an ad hoc basis from the Incident.		
74 .	The proposed solution should have integration with major commercially available tools OOTB for triggering actions or integration with all commercially available SOAR for initiating action to be taken.		
75 .	The proposed solution should integrate with SOAR & UEBA if required in future		

Key Management System (KMS) Encryption

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1	The solution should be configured in HA at DC and standalone in DR. Should have Geo-Redundant KMS Clustering.		
2	The HSM solution would be a hardware, tamperproof box having support for operating systems like Windows and Linux. Should have Quantum-safe Cryptography Support.		
3	Should have at least 4 Gigabit Ethernet ports. Should have IPV4 and IPV6 support. Should have port bonding.		
4	Should have Asymmetric Support for various cryptographic algorithms: Full Suite B support, Asymmetric Key RSA (1024-4096 bits), DSA, Diffie-Hellman, ECDSA, ECDH, ECC Should have Hybrid cryptographic algorithms(PQC+ Traditional)		
5	Should have minimum 10 partitions from day one. Each partition should be protected with unique set of user id and password to grant access. Solution should follow CCA IVG guidelines. Minimum Performance: RSA-2048: 5,000 TPS and 10000 TPS for AES. Should have Throughput & Performace with FPGA-Based		
6	Cryptographic APIs: PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL. Should have Centralized Key management with RBAC & JIT Access.		
7	HSM must support Multi-Factor Authentication with hardware USB smartcards/tokens with M of N operations authorization. Should have Biometric-Based MFA & Adaptive authentication.		
8	HSM should be P&PW compliant (Declaration of Conformity should be attached)		
9	HSM should support 10 tps RSA 2048 Key Generation speed		
10	HSM generated session keys should always be encrypted even in the memory and never be stored as plaintext		

11	HSM should support storing minimum 130000 AES keys in HSM. Keys should always remain securely inside the HSM, and should not be stored in software in any form throughout the key lifecycle		
12	Should have 5G Cryptographic Mechanisms for Subscriber Authentication: Milenage, Tuak, and COMP128		
13	HSM should only support embedded ASIC chip for crypto-operations and should not use Open SSL versions.		
14	Should generate High quality keys through external Quantum RNG seeding		
15	HSM has to avoid decryption of communication with HSM Client on the appliance - it has to perform such operations directly on the HSM card itself		
16	Solution should have Random Number Generation complying with AIS 20/31, DRG4 along with NIST 800-90A compliant CTR-DRBG		
17	Should support Digital Encryption algorithm for block chain		
18	The proposed HSM box / cryptographic module should be minimum FIPS 140-3 level 3 certified. FIPS certification should be in the name of the proposed OEM and not from a third party.		
19	The proposed module / firmware should be Common Criteria EAL 4+ certified. Certification has to be in the name of proposed OEM. Should have automated compliance reports for DPDPA 2023, GDPR, and NIST 800-57		
20	The system should support separation-of-duties and policies to be enforced and integrate with existing users and groups from AD and LDAP		
21	Solution should provide REST based APIs for Administration of HSM.		
22	HSM supports the capability to run the custom code inside the HSM .		
23	All the keys should be encrypted and backed up on FIPS approved Backup appliance and not be available in file at any point. Backup HSM should not require constant power in order to take backup or perform restore. Should have Air-Gapped & Multi-site Encrypted key backup.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

24	Application keys should be securely backed up at min. one additional location other than Data Center and DR. Back Up HSMs required for three locations should be included in the solution. Should have Blockchain-Based Key Auditing & logging		
25	FIPS approved Backup appliance should not be capable of performing any crypto -operations besides backup and restore		
26	Should detect cover removal in addition to Alarm triggers for motion, voltage and temperature		
27	Solution should prevent privileged users from examining and even accessing critical resources. Should have AI-Driven Anomaly detection for Unauthorized key Usage.		
	Encryption Solution within DC and DR		
28	The encryption solution can be virtual or hardened appliance with HSM as Root of Trust (RoT)		
29	The Encryption solution should be done at File/Folder level with FIPS approved mechanisms & should not require any downtime while data encryption occurs. Should have End-to-End Encryption for Hybrid Cloud & Multi-Tenant Environments.		
30	The system can be able to send e-mail notifications to specific addresses when system alarms are triggered. Should trigger automatic notifications for certificate expiry.		
31	The Solution should support agent based and agent less/proxy scanning of large volumes of data, stored both on premise and in the cloud. This includes the scanning of local disks, network file shares, big data like Hadoop, as well as Cloud storage provider.		
32	API Support –REST (JWT), KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, C, Java API's and libraries for integration in to custom applications. Should have Zero-Trust API Access with Mutual Authentication.		
33	Should have the functionality of entire Key life-cycle tasks including generation, caching, versioning, rotation, destruction, import and export as well as provide abilities to manage certificates and secrets. Key Versioning should not require any downtime for the application.		

	Should have Automate key rotation & Expiry polices with AI-driven insights.		
34	Solution should Identify "trusted applications" – binaries which are approved to perform encryption/decryption of business-critical files.		
35	Solution should be able to check the integrity of those "trusted applications" with signatures to prevent polymorphic malware from getting into approved binaries.		
36	The solution should enforce ransom ware protection per volume with minimal configuration and no modification to any applications		
37	Solution must have Fine-grained Access Control to prevent access to Ransom ware hackers.		
38	Solution must have Application White listing feature to prevent Ransom ware attacks. Solution should Block Un-trusted Binaries from Encrypting Data.		
39	Solution should define who (user/group) has access to specific protected files/folders and what operations (encrypt / decrypt / read / write / execute) they can perform.		
40	Solution should prevent privileged users from examining and even accessing critical resources.		
41	The solution should factor necessary connectors /agents to centrally encrypt Database servers, Application servers, File and Folder servers, Storage and Tape Libraries.		
42	The proposed solution should be certified / tested with Scality and RedHat Ceph Storage apart from other leading OEMs like Dell, NetApp, etc.		
43	Solution should have the capability to discover sensitive data. The Data discovery and classification solution is not intended for end user as in the case of DLP but to identify and protect Sensitive and PII data lying in the Gov Drive. Publicly available support / compatibility report with proposed encryption OEM has to be furnished in case of a third-party discovery solution (other than encryption OEM) is being proposed.		
44	The solution should support any solution which has capability of PDF exporting of Scanned data report. Publicly available support / compatibility report with proposed encryption OEM has to be furnished in case of a third-party discovery solution (other than encryption OEM) is being proposed.		

45	The Solution should be able to discover sensitive data and provide Intelligent Remediation by encryption. Publicly available support / compatibility report with proposed encryption OEM has to be furnished in case of a third-party discovery solution (other than encryption OEM) is being proposed.		
	Encryption Solution for Data in Motion between DC and DR		
46	Solution should factor Layer 2, 3 and 4 Network Encryption to be designed and implemented for traffic between DC and DR.		
47	The solution should with throughput: minimum 1 GBPS encryption speed with latency under 1 ms with virtual appliance along with server /appliance based.		
48	Network Encryptors should not require Smart cards to do the authentication and backup, all the authentication between devices should be based on the X.509 certificates.		
49	Latency of Network Encryptors should be below 10µs when they are deployed on the 1Gb links, independently of the packet/Ethernet frame size. Should ensure high quality of real time applications such as VoIP and video.		
50	Network Encryptors should support TACACS+ for remote authentication and SNMPv3 protocol.		
51	The network encryption should be transparent to the L2 and L3 core network.		
52	The cryptographic unit should be tamper-proof. The unit detects tamper assaults and reacts accordingly by its tamper response (zeroing all secret keys and secret security parameters).		
53	The System shall support multi-tenancy using multiple domains, Clustering and high availability and Backup.		
54	Point-point connection has to support Transmission security to prevent statistical analysis on the encrypted data.		
	General		
55	SI should factor 5-year comprehensive 24x7 maintenance services from OEM		

56	Each of the Proposed OEM/ OEMs should have at least 25 support engineers in India on its payroll on the date of bid submission. Undertaking from OEM to be furnished.		
57	Each of the proposed OEMs in this tender should have their own office in India and should have been present in India for at least 5 years. Proof of the same to be furnished.		
58	All the OEMs of the proposed products should have their own RMA and Customer Support center in India. Proof of the same to be furnished.		
59	Bidder / SI has to furnish MAF for the proposed OEMs		

Privileged Access Management (PAM)

S.N	Specifications	Compliance (Yes/No)	References (Document/Page No.)
A	**Architecture and Performance**		
1	The solution shall be used as the sole gateway connecting user's workstation to the managed systems for privileged access.		
2	The solution shall initiate the login session from the workstation to the managed systems using a session proxy (via a login portal).		
3	The solution shall not require network topology changes in order to assure all privileged sessions are controlled by the solution.		
4	The solution shall be based on agentless architecture and Implement Zero Trust Network Access (ZTNA) for both password and session management.		
5	The solution shall support high availability in Active-Passive mode with automatic and manual failover within the same site or cross different sites without the need of additional tools or licenses. Also Enable Geo-Redundant PAM Deployment with Multi-Site HA.		
6	The solution shall support at least tens of thousands managed systems and accounts.		
7	The solution shall support not less than 300 concurrent recording sessions for each node and be able to scale up to support thousands of concurrent sessions.		
8	The solution shall support out-of-the-box archiving capability for recorded session without incurring any additional cost or resources other than the storage requirement.		
9	The solution shall have the capability to cache selected credentials externally. These credentials can be used for application-to-application connections also to mitigate temporary outage of PAM infrastructure.		
B	**Asset Management and Discovery**		

1	The solution shall have bulk loading capability to import managed systems, privileged accounts, users, and other necessary objects.		
2	The solution shall have the capability to record system information for managed systems including but not limited to IP address, DNS name, platform type & version.		
3	The solution shall allow administrator to define custom attributes for both managed system and privileged account.		
4	The solution shall have the capability to discover and inventory all privileged and non-privileged accounts in known and unknown systems including but not limited to: Windows, Unix/Linux, Mac OS, Directories (AD/LDAP), Databases and Network Devices. AI-driven automated account discovery & Onboarding.		
5	The solution shall provide distributed discovery engine capability that allows asset to be discovered across different isolated network segments and geographical regions and report discovery result back centrally.		
6	The solution shall have the capability to discover Windows Services and Scheduled Tasks so that privileged credentials used by them can be managed automatically.		
7	The solution shall have the capability to discover Active Directory domain accounts and automatically link discovered accounts to specific member servers for user to request for access.		
8	The solution shall have the capability to discover software that are installed and ports are open in the target system.		
9	The solution shall have the capability to group target systems based on discovered and custom defined system attributes.		
10	The solution shall have the capability to group systems and accounts based on the result of AD/LDAP query.		
11	The solution shall have the capability to send email notification to designated personnel upon discovering new target systems or found systems are no longer reachable.		
12	The solution shall have the capability to discover new privileged accounts and on-board them for password management automatically.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

	Should have automated Risk-based access approval.		
C	**Credential Management**		
1	The solution shall support password management for the following platforms out-of-the-box: Automated Password Rotation & Just-in-time(JIT) Privilege Elevation.		
1.1	**Operating Systems:** Linux, Mac OS, Windows Desktop, Windows Server		
1.2	**Databases:** MongoDB, MySQL, Oracle, PostgreSQL, SQL Server		
1.3	**Directories:** Active Directory, LDAP		
1.4	**Devices:** WAF (F5 and Imperva), Checkpoint, Cisco IOS, Dell iDRAC, Fortinet, HP Comware, HP iLo, Juniper (JunOS), Palo Alto Networks		
1.5	**Applications:** VMware vSphere API, VMware vSphere SSH, Office 365		
2	Beside out of the box supported platforms, the solution shall have the flexibility and user-friendly interface to configure custom platform to manage account password. The custom platform feature must be easy to use and allow user (the customer) to perform configuration without involvement from product vendor.		
3	The solution shall support definition of multiple password policies and ability to enforce one password policy for multiple managed systems and individual password policy for each managed system.		
4	The solution shall have the flexibility to define schedule to reset and randomize passwords on per managed system and account basis without knowledge of existing passwords.		
5	The solution shall have the flexibility to reset and randomize passwords for selected accounts upon check-in to eliminate risk of passwords being compromised.		
6	The solution shall support time-based password retrieval whereby requested password is reset automatically upon expiration of granted timeframe.		
7	The solution shall have the capability to unlock account upon changing its password.		
8	The solution shall have the capability to set password change frequency based on date and time.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

9	The solution shall have the capability to change password at one go for single, group and all managed systems based on specific criteria.		
10	The solution shall have the flexibility to support on-demand manual password change by authorized user.		
11	The solution shall have the capability to enforce password integrity by automatically resetting account passwords that failed verifications or no longer synchronized with the passwords stored in the solution.		
12	The solution shall have the capability to automatically change Windows Services and Scheduled Tasks logon password and optionally restart the Services when corresponding privileged account password is changed by the solution.		
13	The solution shall have the capability to perform password verification against managed account and notify 'out of sync' passwords.		
14	The solution shall have the capability to synchronize password for selected accounts that reside in multiple systems with different platform type.		
15	The solution shall maintain password history for managed privileged accounts and provide easy way to view old passwords through solution's web interface.		
16	The solution shall support SSH key management through automated storage of SSH keys and rotation of SSH keys according to a defined schedule. Should have FIDO2 & Biometric Authentication support		
17	The solution shall support SSH key generation with DSA & RSA key types and configurable key size.		
18	The solution shall have the capability to change SSH key at one go for single, group and all managed systems based on specific criteria.		
19	The solution shall have the flexibility to support on-demand manual SSH key change by authorised user.		
20	The solution shall have "Disable at Rest" functionality for Microsoft Active Directory and Entra ID managed accounts, providing Just-in-Time capabilities.		
D	**Session Management**		

1	The solution shall support monitoring and recording of privileged session access through standard protocols RDP and SSH. Automatic logon without exposing privileged account password must be supported for this type of access. Should have AI-based session anomaly detection & threat scoring.		
2	The solution shall support monitoring and recording of privileged session for any client application access for Windows thick clients including but not limited to vSphere Client, Microsoft SQL Management Studio, SQL Developer, SAPGui, Toad, etc. and web browsers. Automatic logon without exposing privileged account password must be supported for this type of access.		
3	The solution shall allow administrators to add and configure any new client application access with session monitoring and auto logon capabilities.		
4	The solution's session recording feature shall support the use of Commercial off-the-shelf (COTS) client tools: Windows Remote Desktop for RDP access and user's preferred SSH client such as PuTTY/SecureCRT for SSH access.		
5	The solution shall have the capability to limit the number of sessions a user can open for certain set of privileged accounts at one time.		
6	The solution shall have the capability to allow users to make direct connection to managed system via their favorite RDP and SSH clients without the need of log into solution's web interface. Session recording, auto logon and without exposing privileged account password features shall still apply to this way of access.		
7	The solution shall have the capability to display on-screen message with countdown timer to notify user before approved access exceeds the requested time frame.		
8	The solution shall have configuration option to automatically terminate a requested remote access session should the approved access exceeds the requested time frame.		
9	The solution shall have the capability of keystroke logging for all type of access including RDP, SSH, Web and GUI based application clients. The keystroke must be searchable. Should have Real-time user behavior Analytics(UBA)		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

10	The solution shall have the capability to mask password for RDP and SSH session even if keystroke is being recorded.		
11	The solution shall have the capability to lock the SSH session when a blacklisted command is executed and optionally send email notification to designated personnel upon detecting the execution of those commands.		
12	The solution shall have the capability for authorized user to search across all types of recording by keystroke, date/time, user name, target system name and privileged account name.		
13	The solution shall allow authorized user to replay selected recording from web interface without the need of installing third party client software.		
14	The session replay capability shall support playback from point in time in the timeline and searched keyword instead of playing from the beginning of the recording.		
15	The session replay capability shall support fast forward playback.		
16	The solution shall allow authorized user to provide review comment while replaying recorded session and indicate recorded session has been reviewed.		
17	The solution shall support live monitoring of sessions from web interface without the need of installing third party client software. Should have Automated session termination for policy violations.		
18	The solution shall support real-time session intervention which allows authorized user to lock or terminate a session remotely when suspicious activity is performed.		
19	The solution shall capture all changes carried out by administrators in audit trail including user name, time stamp, activity performed, IP address		
20	The solution shall have the flexibility to enable users to connect securely to remote target systems through the session recording feature using accounts which are not managed by the solution.		
21	The solution shall have the capability to archive recorded sessions to long term storage to cater for long retention requirement.		

22	The solution shall have the capability to replay archived session using the application itself without administrator's intervention. The archived session should be secured and encrypted so that it cannot be accessed outside the solution.		
23	The solution shall have the capability to ensure integrity of recorded sessions to prevent tampering.		
24	The solution shall support privileged session with auto logon for Windows platform where smart card authentication enabled.		
25	The solution shall support privileged SSH session in restricted shell access environments.		
E	**Administration & Workflow**		
1	The solution shall ensure proper segregation of duties with Role Based Access Control (RBAC) capability such that roles and accesses are properly defined.		
2	The solution shall minimally support requester, approver and reviewer roles for segregation of duties.		
3	The solution shall have the capability to dynamically group managed accounts based on criteria including but not limited to platform type, platform version, domain name, IP address, system name, account name, account privilege, etc. so that they can be effectively granted to appropriate users for request.		
4	The solution must ensure personal accountability when user granted privileged password and session for shared account.		
5	The solution shall support policy driven workflow and allow easy configuration through web interface to route password and session request to appropriate approver(s).		
6	The solution shall have the flexibility to specify zero, one or multiple approvers for single, group or all managed accounts for dual control. The solution shall have the flexibility to allow this configuration to be applied to one or groups of managed accounts.		
7	The solution shall have the flexibility to allow multiple users requesting the same account password and session for the same managed system in the same time period.		
8	The solution shall have the capability to restrict time frame and frequency that users can request password and session to managed systems. The solution shall have the flexibility to allow this configuration to be applied to one or groups of managed accounts.		

IFD	Co-opted Member	CRPF	BSF	SSB	CISF	NSG	NCIIPC	M-V	M-IV	M-III	M-II	M-I	PO

9	The solution shall have the capability to restrict IP address of user's computer where password and session requests are made. The solution shall have the flexibility to allow this configuration to be applied to one or groups of users.		
10	The solution shall have the flexibility to allow multiple approval polices to be assigned to one managed account for the same requester. This is to support the use cases such as a privileged account doesn't require approval during office hour but approval is required after office hour.		
11	The solution shall be configurable to allow authorised user to bypass approvals for selected privileged account for emergency case.		
12	The solution shall have the capability to send notification via email to requester and/or approvers when request for password or session has been made.		
13	The solution shall have the capability to send notification via email to requester and/or approvers when approver has approved or rejected the request.		
14	The solution shall have the capability to send notification via email to designated personnel for any password or session request regardless approval requirement.		
15	The solution shall have the capability to send notification via email to designated personnel in the event of password change failure.		
16	The solution shall have the capability to send notification via email to designated personnel in the event that password in the solution doesn't match the one in managed system.		
17	The solution shall have the capability to allow customization of email templates.		
18	The solution shall have the capability to purge old system logs according to retention period configurations.		
F	**End User Interface**		
1	The solution shall provide a single HTML5 web interface for users to perform activities related to privileged account such as request, approval, session replay and audit trail retrieval, etc. and administrators to manage privilege accounts, user profiles, groups, organizations, roles and policies.		

2	The solution shall support the following web browsers: • Microsoft Edge • Internet Explorer • Google Chrome • Mozilla Firefox • Apple Safari		
3	The solution shall have self-service interface that allows user to view and search privileged accounts granted for access.		
4	The solution shall have self-service interface for authorised user to retrieve credentials and request session for privileged access for a time-limited or one time access.		
5	The solution shall allow user to specify start date/time, duration and reason when requesting privileged account password and session.		
6	The solution shall allow user to view and search old, existing and pending requests.		
G	**Audit, Reporting and Analytics**		
1	The solution shall support auditing and accountability where each transaction is logged for every request. Should have customizable Role-Based dashboards & Reports		
2	The solution shall have the ability to generate all reports by frequency, on-demand or as scheduled tasks.		
3	The solution shall support minimally these report format: CSV, Excel, PDF, PowerPoint, MHTML, Word, TIFF and XML.		
4	The solution shall provide minimally following types of report out-of-the-box without any additional component and no additional cost.		
5	Account password age report that provides last password change date and age for each managed account.		
6	User activities report that provides a detailed transactional view of password and session request and approval activities.		
7	Entitlement report that details who has access to which accounts.		
8	Password change activity report that details password change reason and result.		
9	Password change schedule report that provides details of upcoming scheduled password change.		

10	Password reset upon release reconciliation report that shows end of request reset statuses of managed account passwords to provide auditable evidence that passwords have been reset appropriately after being released.		
11	Asset inventory report that provides list of all managed and unmanaged systems, IT assets discovered grouped by operating system.		
12	Account inventory report that provides list of all managed and unmanaged accounts.		
13	Account delta report that provides delta change for added and removed accounts according to daily, weekly and monthly periods.		
14	Managed vs unmanaged accounts report that provides a list of target system accounts and indicates which are under password management.		
15	Service account usage report that provides a detailed list of what systems are using a service account to start one or more Windows services.		
16	Regulatory compliance report that provides insight to regulatory standards (but not limited to): COBIT, ISO-27002, ITIL, NIST 800 and PCI. Should have Automate DPDPA 2023, GDPR, and NIST compliance Reports.		
17	The solution shall have the ability to deliver reports through email or to shared folder automatically based on predefined schedule so that user doesn't have to generate or retrieve report manually.		
18	The solution shall support rich reporting content including but not limited to text, table, graphics, chart, bar, etc.		
19	The solution shall have the capability to allow creation of customized report.		
20	The solution shall have advanced threat analytics capability that pinpoints specific, high-risk users and systems by correlating low-level privilege, vulnerability, and threat data from a variety of sources.		
H	**Authentication, Security and Compliance**		
1	The solution shall have configuration option to turn on only FIPS 140-2 validated cryptography for encrypting sensitive data including passwords, keys and session recordings and all other secure communications.		

2	The solution must be accredited with Common Criteria certificate.		
3	The solution shall not contain any hard coded credentials that cannot be managed.		
4	The solution shall have the capability to integrate with multiple enterprise authentication methods including Active Directory, LDAP, Smart Card, RADIUS and built-in authentication mechanism.		
5	The solution shall support Integrated Windows Authentication and SAML for single sign on.		
	The solution shall support the enforcement of strong authentication with RADIUS Two Factor Authentication (2FA).		
7	The solution shall have the capability to integrate with AD/LDAP directories with following capabilities:		
7.1	(a) Authenticate and logon to the solution using AD/LDAP account credential.		
7.2	(b) Make use of AD/LDAP group for authorization within the solution.		
7.3	(c) Auto provisioned/de-provisioned of the identity within the solution whenever a user had been added or deleted from the AD/LDAP.		
7.4	(d) Support multiple Active Directory forests and domains.		
8	The solution shall have the capability to temporarily revoke selected users to prevent the users from accessing the solution to make privilege access request. When integrating with AD/LDAP for authentication, revoking user in the solution shall not disable or lock the AD/LDAP account.		
9	The solution shall have the capability to integrate with Hardware Security Module (HSM) out-of-the-box using PKCS#11 standard.		
I	**System Management and API**		
1	The solution shall have the capability of performing auto update when newer version of software is available.		
2	The solution shall have the capability to send email notification to designated personnel when newer version of software packages is available or have been installed automatically.		

3	The solution shall have the capability to perform scheduled regular and ad-hoc backup on its operating state configurations.		
4	The solution shall have the capability to restore its operating state configurations from backup.		
5	The solution shall have the capability to send system health information based on predefined thresholds via syslog.		
6	The solution shall have the capability to send system health information based on predefined thresholds via SNMP trap.		
7	The solution shall have the capability to send system health information based on predefined thresholds via email.		
8	The solution shall offer a Software Development Kit (SDK) that can address corner cases, using API's available for virtually all platforms to allow real-time, programmatic access to passwords. The SDK allows applications and individuals to access the password store independently, without using the product's original interface.		
9	The solution shall provide RESTful API with comprehensive features that allows management of the solution programmatically including but not limited to add/modify/remove managed systems/accounts, update access policies, add/remove users, retrieval of privileged account credential, request and launch privileged session, etc. Should allow Implement secure API Gateway with RBAC & OAuth 2.0 support		
10	The solution shall provide API documentation and sample API programs in at least following programming languages: Python, C#, Java, PowerShell, Ruby and Unix Shell Script.		
11	The solution shall provide command line utility with similar capability as the API. The command line utility must be supported on Windows, Linux, AIX, HP-UX and Solaris platforms.		
J	**Integrations**		

1	**SIEM Integration** - The solution shall have out of the box integration with SIEM. The type of events shall include but not limited to system health based predefined thresholds, system configuration changes, user login/logoff, user request for privileged access, approver approve/reject request. Should have expand integration with SOAR & XDR for automated threat response.		
2	**Vulnerability Management Integration** - The solution shall have out of the box integration with following Vulnerability Management solutions as credential provider for authenticated scan: Tenable Nessus/Qualys Cloud Suite		
3	**Cloud Integration** - The solution shall have out of the box integration with following Cloud and virtualization platforms to discover online/offline virtual machines: Amazon AWS/ Google Cloud/ Microsoft Azure		

Backup Software for Tape Library & NL-SAS (250TB Capacity)

S.N	Feature	Specifications	Compliance (Yes/No)	References (Document/Page No.)
1	Backup Software Overview	Capacity: The backup solution that should be sized appropriately for backup of front-end data of 250TB (30% DB, 70% File System) as per below mentioned retention policies: a) Daily Incremental Backup – retained for 14 days. b) Weekly Full Backup for all data types–retained for min 21 days. Scalability: The solution should be quoted with adequate provision for future capacity expansion on demand and in modular architecture rather than fixed configuration.		

		The proposed backup solution shall offer comprehensive data protection across physical, virtual, and cloud environments, with the ability to deploy on Windows and Linux platforms, ensuring consistent and scalable data management.		
		The proposed backup solution shall provide a unified management interface for hybrid deployments, delivering a single pane of glass to manage infrastructure seamlessly, regardless of deployment location.		
		Proposed backup solution should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup via NFS, and CIFS protocols.		
		The proposed backup solution shall provide centralized backup policies for consistency across all hybrid environments, including automated policy-based management with workflow automation to ensure uniform data protection standards		
		The proposed backup solution shall enable automated recovery with pre-defined workflows, integrated data management, and lifecycle policies from a single interface, avoiding the need for manual configurations or separate tools required by other solutions.		
2	Application-Aware Backups	The proposed backup solution shall provide application-aware support for Microsoft Exchange, SQL Server, SharePoint, Oracle, and SAP HANA, PostgreSQL, MySQL, and MongoDB enabling application-consistent backups across all hybrid deployments.		
		The proposed backup solution shall provide granular recovery for emails, databases, and application components, including point-in-time recovery for SAP HANA, Oracle, and Unix-based systems, without relying on manual configurations or third-party tools.		

3	Security, Ransomware Protection	The backup solution shall offer automated scanning of backup files for malware using signature-based and forensic analysis techniques, with the ability to quarantine detected threats and recover clean data.		
		The backup solution shall offer automated anomaly detection to identify unusual patterns in backup data and potential ransomware activity. It must support multi-person authorization for executing critical recovery tasks to prevent unauthorized actions.		
		The backup solution shall provide air-gapped backups to isolate backup data from the primary network, preventing ransomware access and ensuring data integrity.		
		The backup solution shall include mount protection to prevent unauthorized access or modifications to backup data during recovery operations.		
		Native integration with SIEM and SOAR platforms for real-time threat monitoring, alerts, and incident response.		
4	Hypervisor Support and Storage Vendor Integration	The proposed backup solution shall support VMware, Hyper-V, Nutanix AHV, RHEL OpenShift, OpenStack, Kubernetes, Oracle (VM) and virtual environments on AIX, Solaris, and HP-UX.		
		The backup software shall support integration with storage vendor technologies like NetApp SnapDiff, Isilon ChangeList, or equivalent ensuring faster and more efficient NAS backups.		
		The provided backup software shall provide Full support for NDMP backups, enabling efficient protection of NAS devices.		
		The backup software shall support Granular VM and file-level recovery across hypervisors.		

		The backup software shall offer agentless backups for virtual environments with application-consistent snapshots.		
5	Snapshots, NDMP, and NAS Support	The backup solution shall support application-consistent snapshots across multiple storage arrays, ensuring data integrity and seamless recovery for enterprise applications.		
		The backup solution shall provide comprehensive NDMP support and integrate with storage vendor technologies to optimize backup performance and minimize recovery times.		
		The backup software shall provide efficient backups for large NAS environments with minimal impact on production systems.		
6	Deduplication and Data Efficiency	The backup solution shall provide global deduplication across physical, virtual, and cloud environments to optimize storage utilization and minimize network bandwidth consumption.		
		The backup solution shall enable deduplication from disk to tape natively, without the need for third-party appliances, ensuring efficient data transfer and storage optimization.		
		The backup software shall provide efficient data transfer for large datasets, ensuring optimized resource usage across hybrid cloud deployments.		
7	Automation and Workflow	The backup solution shall support advanced automation for backup policies, recovery workflows, and disaster recovery orchestration.		
		The proposed backup solution shall be customizable workflows to reduce manual interventions and ensure policy enforcement across environments.		
		The proposed backup software shall provide automated scheduling for routine backups and custom tasks with minimal administrative overhead.		

8	Reporting, Analytics, and Compliance	The proposed backup shall provide a real-time reporting with built-in analytics for performance tracking, capacity planning, and compliance auditing.		
		The proposed backup shall have capability with centralized dashboards for monitoring resource usage, job success rates, and recovery readiness.		
		The proposed backup software shall be customizable reports to meet organizational and regulatory compliance requirements.		

Date: 22.04.2025

22/4/25
Sh. Kurian Varghese, SI(Comn)
SSB Rep.

Sh. Anil Kamboj,
Insp(T) CRPF Rep.

22/4/25
Sh. Ramvir Singh,
Insp(T) BSF

22/04/25
Sh. Ajit Singh, AC III
NSG

22/4/25
Sh. Anil Kumar,
DC(Exe) CISF

22-4-25
Sh. Sardar Singh, AC(Office)
IFD Member

Sh. M.C. Joshi, Consultant ITBP
Co-Opted Member

Sh. Anshuman Bhattacharya, Director NCIIPC
Co-Opted Member

Sh. Pardeep Kumar,
DC(Tele), M-V

22/4/25
Sh. Himanshu Tiwari,
2IC(GD), M-IV

22/4/25
Sh. Amit Tiwari,
2IC(Tele), M-III

22/4/25
Sh. Piyush Kushwaha,
Comdt(Tele), M-II

Sh. Sanjay Kori,
IPS, DIG, M-1

Sh. Abdul Ghani Mir, IPS ADG(HQ)
PO