Note : All The queries raised by Bidders has been clarify as below however for more clarification may please see tender document and Corrigendum-II. Incase of any ambiguity ,Tender document and Corrigendum-II will be superseed .All bidders are requested to go through the Tender document and Corrigendum-II carefully.

SL#	RFP Volume Section and sub-section	Page no.	Clause/ Content in the RFP	Clarification sought/	Reason for Requesting the amendment	Change Request	RailTel Response	RailTel Remarks
	E-Risk							
1	SOR-B-2: Internet Firewall-3.1	43	**Should support at least 10 Gbps of NGFW Real world performance (includes FW, Application Visibility & IPS) from day one**	As Internet Firewall going to deply in perimeter, only NGFW will not able to protect from current sophisticated attacks. it is suggested to ask for Threat Protection which included FW, Application Control, IPS and Malware Protection.		Requesting you to modify the clause to "Should have at least 10 Gbps of NGFW and Threat Protection with Real world / Enterprise Traffic Mix performance (includes FW, Application Visibility, IPS and Malware Protection) from day one"	As Per RFP	
2	SOR-B-2: Internet Firewall-3.2	43	NG Firewall should support at least 4,00,0000 concurrent sessions	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. the firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling MINIMUM 40 million concurrent sessions		Requesting you to modify the clause to "NG Firewall should support at least 4,00,0000 concurrent sessions"	As Per RFP	
3	SOR-B-2: Internet Firewall-3.3	43	NG Firewall should support at least 50,000 connections per second	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. the firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling MINIMUM 380000 New Sessions per Sec.		Requesting you to modify the clause to "NG Firewall should support at least 380,000 connections per second"	As Per RFP	
4	SOR-B-2: Internet Firewall-5.2	43	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously	As IPv6 asked in RFP It is suggested to include **DNS64 and and DHCPv6 along with NAT66 and NAT64 for a complete IPv6 functionality**		Requesting you to modify the clause to "Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously and also support DNS64 and DHCPv6 along with NAT66 and NAT64 ."	As Per RFP	

5			New suggested Clause	There is no IPsec VPN Throughput mention in RFP		Pls mention Firewall should have atleast 30 Gbps of IPsec VPN Throughput	Not Required	
6			New suggested Clause	Requesting you to ask for internet Firewall should be from different OEM vendor than UTM because if there is an vulnerability with one firewall, the other firewall from a different vendor does not have that vulnerability. Hence there is more protection if the two firewalls are provided by two different vendors		Requesting you to add the clause "Proposed internet Firewall should be from different OEM than UTM for better security".	Not Required	
7			New suggested Clause	To reduce the information security threats and organisation adopts best practices to minimise threats.		Requesting you to kindly ask for "The Firewall vendor must have ISO 27001 certified"	Not Required	
Queries from EDSPL								
SL#	**RFP Volume Section and sub-section**	**Page no.**	**Clause/ Content in the RFP**	**Clarification sought/**		**Change Request**		
1	SOR-B-2: Internet Firewall-3.1	43	Should support at least 10 Gbps of NGFW Real world performance (includes FW, Application Visibility & IPS) from day one	As Internet Firewall going to deply in perimeter, only NGFW will not able to protect from current sophisticated attacks. it is suggested to ask for Threat Protection which included FW, Application Control, IPS and Malware Protection.		Requesting you to modify the clause to "Should have at least 10 Gbps of NGFW and Threat Protection with Real world / Enterprise Traffic Mix performance (includes FW, Application Visibility, IPS and Malware Protection) from day one"	As Per RFP	
2	SOR-B-2: Internet Firewall-3.2	43	NG Firewall should support at least 4,00,0000 concurrent sessions	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. the firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling MINIMUM 40 million concurrent sessions		Requesting you to modify the clause to "NG Firewall should support at least 4,00,0000 concurrent sessions"	As Per RFP	

3	SOR-B-2: Internet Firewall-3.3	43	NG Firewall should support at least 50,000 connections per second	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. the firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling MINIMUM 380000 New Sessions per Sec.		Requesting you to modify the clause to "NG Firewall should support at least 380,000 connections per second"	As Per RFP	
4	SOR-B-2: Internet Firewall-5.2	43	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously	As IPv6 asked in RFP It is suggested to include **DNS64 and and DHCPv6 along with NAT66 and NAT64 for a complete IPv6 functionality**		Requesting you to modify the clause to "Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously and also support DNS64 and DHCPv6 along with NAT66 and NAT64 ."	As Per RFP	
5			New suggested Clause	There is no IPsec VPN Throughput mention in RFP		Pls mention Firewall should have atleast 30 Gbps of IPsec VPN Throughput	Not Required	
6			New suggested Clause	Requesting you to ask for internet Firewall should be from different OEM vendor than UTM because if there is an vulnerability with one firewall, the other firewall from a different vendor does not have that vulnerability. Hence there is more protection if the two firewalls are provided by two different vendors		Requesting you to add the clause "Proposed internet Firewall should be from different OEM than UTM for better security".	Not Required	
7			New suggested Clause	To reduce the information security threats and organisation adopts best practices to minimise threats.		Requesting you to kindly ask for "The Firewall vendor must have ISO 27001 certified"	Not Required	
Juniper								
Sl.No	**Clause No**	**Page No**	**Description of the Clause as per Tender Document**	**Query**	**Reason for Requesting the amendment**	**Amendment Requested**		
1	VII	6	The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote only one OEM against one SOR	We understand that this will be a leaf-spine architecture with L3 Switch in SOR-A acting as Leaf and Core Switch in SOR-B acting as Spine.	In a fabric architecture leaf and spine should be from same OEM	It is recommended that Leaf and Spine be part of same SOR.	As Per Corrigendum-II	
2	1.3	13	The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multiprocessor based for enhanced performance. The Router should have multi-core Processor @ 2.1 GHz or more+D18	Request to remove the clock speed mentioned in the clause.	The processor specification does not guarantee device performance.	The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multiprocessor based for enhanced performance. The CPU should have sufficient clock speed to meet the performance requirements mentioned in the tender.	As Per Corrigendum-II	

3	1.6	13	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.	Please clarify the requirement of NAT at DC-GW router.	NAT would be done at ISP-PE/IGW. If required, then this can be achieved through the firewall which is part of UTM solution.	The router may have hardware assisted Network Address Translation (NAT) capability as per RFC 1631 as an optional feature.	As Per Corrigendum-II	
4	2.1	13	Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 100 Gbps or more.	It is recommended that the switch fabric should be upgradable to at least 200G per slot and a total backplane of at least 600Gbps	Since 40GE and 10GE interfaces are requested. 100Gbps performance is too low and won't provide wire speed/ line-rate performance.	Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 200G per slot and a total backplane of at least 600Gbps.	As Per Corrigendum-II	
5	2.2	14	Number of Slots: The router must be chassis based with minimum 3 numbers of Main interface slots. Only the main slots on the router chassis should be considered to comply with this requirement. All the 3 interface slots should be usable from day 1	Request to not restrict the number of slots on the device.	This will restrict participation and flexibility of solution provider	The router should have enough interface card slots to provide the interfaces requested in the tender. The router should have 25% free slots on Day 1 after populating all the interfaces requested in the tender.	As Per Corrigendum-II	
6	3.4	14	Router should support 26 Gbps of IPSEC performance and 8000 tunnels (internal/external).	Request to change the IPSec tunnel count to 6000.	This would allow more vendor participation	Router should support 26 Gbps of IPSEC performance and 6000 tunnels (internal/external).	As Per Corrigendum-II	
7	3.9	14	Software rollback feature	It is recommended that the software support configuration commit and rollback up to 10 configurations	This will improve high availability and robustness of the system	Software should support configuration commit and rollback up to 10 configurations	As Per Corrigendum-II	
8	4.2	14	The router should have Short Haul SFP enabled on all ports. The Router should have at least 8 ports 1GE and 8 Port x10GE from Day-1. The router should have support of 40GE &100GE interfaces for any future upgrade with additional line card hardware in same chassis.	Request to specify the number of 40GE and 100GE interfaces required in future.	This is required to dimension the backplane capacity of the offered solution.	The router should have Short Haul SFP enabled on all ports. The Router should have at least 8 ports 1GE and 8 Port x10GE from Day-1. The router should be able to support 4 numbers of 40GE & 4 numbers of 100GE interfaces in future with additional line card hardware in same chassis.	As Per Corrigendum-II	
9	5.3	15	The router should support minimum 6000 VRF instances from day one	Request to clarify the requirement for 6000 VRF on a DC-GW router	Most of the VRF creation will take place on upstream MPLS PE and not on DC-GW	The router should support minimum 30 VRF instances from day one	As Per Corrigendum-II	
10	5.12	15	The Router shall support selection of the best path for each application based upon reachability, delay, loss, jitter, MOS	This is SD-WAN functionality.	This feature is not required on DC-GW.	Request to remove this clause.	As Per Corrigendum-II	
11	8.2	16	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP and by some well known application types through Application Recognition techniques or Application Awareness techniques.	Application awareness is not a functionality required on DC-GW router.	Application awareness can be done on the UTM devices which is requested in the tender	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP and DSCP.	As Per Corrigendum-II	
12	8.6	16	The router shall support cRTP for VoIP.	Request cRTP as optional as DC-GW location will not have bandwidth availability constraint.	cRTP is not required high capacity DC-GW routers with high speed interfaces where bandwidth is not a constraint.	The router may support cRTP for VoIP as an optional feature.	As Per Corrigendum-II	
13	8.13	16	The router shall support 200k queues to offer granular QoS, policing and shaping capabilities.	This is in conflict with clause 8.7 which is sufficient for DC-GW requirement. Also, such high number of queues are not required on DC-GW.	High number of queues are required only when high number of subscribers are terminating on a node. Hence this won't be used on DC-GW router.	Request to remove this clause.	As Per Corrigendum-II	

14	9.6	17	The router shall support firewall service in hardware on all interfaces. The firewall performance shall be at least 4 Gbps.	Firewall is already part of UTM therefore not needed on DC-GW	Firewall function is already covered in UTM. The network performance will deteriorate if firewall inspection is repeated at multiple points within the same network (router and UTM)	Request to remove this clause.	As Per Corrigendum-II	
15	9.7	17	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.	Please clarify the requirement of NAT at DC-GW router.	NAT would be done at ISP-PE/IGW. If required, then this can be achieved through the firewall which is part of UTM solution.	The router may have hardware assisted Network Address Translation (NAT) capability as per RFC 1631 as an optional feature.	As Per Corrigendum-II	
16	9.12	17	The Router shall support Suite B Cryptographic Suites for Ipsec (RFC 4869)	It is recommended to use AES/3DES for cryptographic requirement.	RFC 4869 is only optional informational RFC and not a standard.	The Router shall support Suite B Cryptographic Suites for IPSec using AES/3DES	As Per Corrigendum-II	
17	10.3	17	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP	Request cRTP as optional as DC-GW location will not have bandwidth availability constraint.	cRTP is not required high capacity DC-GW routers with high speed interfaces where bandwidth is not a constraint.	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter and packet loss	As Per Corrigendum-II	
18	12.1	17	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum.	In order to allow more vendor participation, we request to modify the clause to support IPv6 features as requested in the tender.	IPv6 certification is not standard industry practice and only a specific vendor has this.	The proposed router should have complete IPv6 readiness as requested in the tender.	As Per Corrigendum-II	
19	2.9	18	Switch should have a minimum 40MB buffer of more.	We request to modify the minimum buffer to 32MB.	This will allow more vendor participation.	Switch should have a minimum 32MB buffer of more.	As Per Corrigendum-II	
20	3.3	18	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure	This is not applicable for fixed configuration spine/leaf switches. Please confirm.	Tender does not request for redundant controller in DC Spine and Leaf Switches.	Request to remove this clause.	As Per Corrigendum-II	
21	5.11	19	Switch platform should support MAC Sec in hardware	There is no benefit of MAC Sec on Spine and Leaf switches in a DC environment. This will add additional processing load on the switches.	All the connectivity of Switch is with nodes within the data center, which is a secured environment, hence MAC sec is not required in such scenario.	Request to remove this clause.	As Per Corrigendum-II	
22	6.4.c	19	Bi-Directional PIM	Please clarify the use case of Bi-Direction PIM on a DC fabric	PIM-SM can be used for multicast requirements in DC.	Request to remove this clause.	As Per Corrigendum-II	
23	1.4	34	Robustness : while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone	Request to clarify what is meant by "zone" in DC Fabric	Clause not clear		As Per Corrigendum-II	Zoning is required, Dynamic mobility of VM is required from production to production zone and production to non production zone. Zone should be defined in fabric controller.
24	1.8	35	Business Continuance- The fabric should be able to deploy applications across data center fabrics representing separate availability zones, to ensure that any network-level failures or configuration or policy definition errors that occur in one availability zone will not ever be propagated to the application's workloads running in a separate availability zone	Request to clarify what is meant by "zone" in DC Fabric	Clause not clear		As Per Corrigendum-II	The Fabric Should support this, so that if one Zone fails due to some reason, this would not effect in other zones in the DC

25	2.3	35	In case of Fixed Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated Equipped with 32* 40G Multimode QFP28 Each Leaf should connect to Each Spine using minimum 6 x 40G/100 G ports Multimode from day 1 to support desired Leaf Scale connectivity.	Please clarify connectivity architecture.	If each leaf should connect to each spine using 6 x 40G/100G, then each leaf should at least have 24 x 40G/100G uplink towards spine on Day 1. Please clarify the connectivity architecture. Please also clarify the desired leaf scale.		As Per Corrigendum-II	
26	3.1	35	Fabric must support various Hypervisor encapsulation including VXLAN and 802.1q natively without any additional hardware/software or design change.	It is recommended to have only VxLAN as the encapsulation protocol as it would also cover use cases where VMs must talk to bare metal servers.	To ensure interoperability between application running on VM and bare metal servers	Fabric must support Hypervisor encapsulation using VXLAN natively without any additional hardware/software or design change.	As Per Corrigendum-II	
27	3.5	35	Fabric must provide open programmable interface using python SDK, JSon SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.	Request to confirm that the fabric should support at least one of the mentioned open programmable interface	The desired functionality can be met using any of the mentioned protocols.	Fabric must provide open programmable interface using python SDK/JSon SDK/XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.	As Per Corrigendum-II	
28	3.12	36	Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc	Request to clarify what is meant by "fabric as stateless distributed firewall"	Clause not clear		As Per Corrigendum-II	
29	5.3	36	Fabric must support VM attribute based zoning and policy	Request to clarify the functionality required	Clause not clear		As Per Corrigendum-II	Zoning based on different VM attribute, Different policy in Fabirc with different VM Zoning
30	5.5	36	Fabric must support true multi - tenancy	Request to explain the meaning of "true multi-tenancy"	Clause not clear		As Per Corrigendum-II	Multi - tenancy/ Multi-Instance can be create to define different zone.
31	5.8	37	Fabric must act as a State-less distributed firewall with the logging capability	Request to clarify what is meant by "fabric as stateless distributed firewall"	Clause not clear		As Per Corrigendum-II	
32	6.6	37	Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated from day 1 to support desired Leaf Scale. Each Leaf should connect to Each Spine using minimum 4 x 40G/100 G ports connectivity	This conflicts with clause 2.3. Request to confirm the number of uplink ports required on the leaf switches	Connectivity Architecture not clear		As Per Corrigendum-II	
33	2.1	38	a. Minimum 36 ports support 40/100 Gbps QSFP28 ports. The switch should be populated with 32* 40G Multimode fiber transreceivers for downlink connectivity & 4*100G ports Switch should have a minimum 40MB buffer of more.	As per clause 6.6 and 2.3 the interface requirement on Spine switch is 32 ports. Please confirm the actual number of 40GE/100GE ports required on Spine Switch. Also confirm the connectivity for 4 x 100GE uplink requested on spine switches as there is no 100GE requested on the DC-GW router on Day 1. Request to share the connectivity diagram.	Connectivity Architecture not clear		As Per Corrigendum-II	
34	2.7	39	Switch should have a minimum 40MB buffer of more.	Request to change the minimum buffer requirement to 16MB as spine switch does not require high buffer memory.	This will add to latency on the spine switches. Hence it is not recommended.	Switch should have a minimum 16MB buffer of more.	As Per Corrigendum-II	
35	3.5	39	Switch should support minimum 7 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services.	Request to change the minimum switching capacity to 6.4Tbps	32 x 100GE switch will require only 6.4Tbps of switching capacity.	Switch should support minimum 6.4 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non-blocking capacity) including the services:	As Per Corrigendum-II	

36	5.11	40	Switch platform should support MAC Sec in hardware	There is no benefit of MAC Sec on Spine and Leaf switches in a DC environment. This will add additional processing load on the switches.	All the connectivity of Switch is with nodes within the data center, which is a secured environment, hence MAC sec is not required in such scenario.	Request to remove this clause.	As Per Corrigendum-II	
37	1	22	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years	Request to modify this clause such that firewall solution offered should be listed in the Gartner Magic Quadrant for Enterprise Firewall	This restricts participation and request to relax the clause.	The firewall solution offered must be listed in the Gartner Magic Quadrant for Enterprise Firewall	As Per Corrigendum-II	
38	2	22	Chassis platform should support at least 6 * 10G Gigabit ports and should be scalable to additional 8 * 40G in future. Solution should support 100G (QSFP28) Interfaces.	Interface requirement given for Day 1 is too low and not enough to meet the throughput of firewall.	To ensure 40Gbps of NGFW capability at least 5 x 10GE ports are required downlink and 5 x 10GE ports for uplink.	Chassis platform should support at least 10 * 10G Gigabit ports and should be scalable to additional 8 * 40G in future. Solution should support 100G (QSFP28) Interfaces.	As Per Corrigendum-II	
39	2	22	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	It is not recommended to have merchant silicon-based security solution as it is more vulnerable against attacks.	This is not recommended	Request to remove this clause.	As Per Corrigendum-II	
40	2	22	The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet.	It is not recommended to have merchant silicon-based security solution as it is more vulnerable against attacks.'[Consolidated Queries for e-Office_11April19-Responce.xlsx]Sheet1'!$E$74:$H$90	This is not recommended	Request to remove this clause.	As Per Corrigendum-II	
41	2	22	Proposed firewall should not consume more than 3 RU of rack space	This clause is restricting to offer the best security solution available.	This restricts participation.	Request to remove this clause.	As Per Corrigendum-II	
42	3	23	Firewall should support atleast 25,000,000 concurrent sessions with application visibility turned on or more	The concurrent sessions scale requested is too low for a 40Gbps NGFW.	Scale requested is too low.	Firewall should support at least 75,000,000 concurrent sessions with application visibility turned on or more	As Per Corrigendum-II	
43	3	23	Firewall should support atleast 300,000 connections per second with application visibility turned on or more	The connections per second scale requested is too low for a 40Gbps NGFW.	Scale requested is too low.	Firewall should support at least 1,500,000 connections per second with application visibility turned on or more	As Per Corrigendum-II	
44	4	24	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	The scale requested seems vendor specific. Hence request to change the signatures scale to 3500 or more. This is in line with latest TEC-GR for UTM devices.	This would allow more vendor participation	Should support more than 3,500 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined for better efficacy.	As Per Corrigendum-II	
45	4	24	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	The scale requested is not required for DC UTM solution	This would allow more vendor participation	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 100 million of URLs in more than 80 categories.	As Per Corrigendum-II	
46	4	25	Should support safe search for YouTube EDU enforcement	This is not applicable for a datacenter scenario hence request to delete this clause.	Not a relevant feature for DC.	Request to remove this clause.	As Per Corrigendum-II	
47	4	25	DNS Security	DNS security is not a part of UTM solution. Hence request to remove this requirement from NGFW.	DNS security is not covered by NGFW. Dedicated solutions are available for DNS security.	Request to remove this clause.	As Per Corrigendum-II	
48	1.1	43	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years	Request to modify this clause such that firewall solution offered should be listed in the Gartner Magic Quadrant for Enterprise Firewall	This restricts participation and request to relax the clause.	The firewall solution offered must be listed in the Gartner Magic Quadrant for Enterprise Firewall	As Per Corrigendum-II	

49	2.2	43	The appliance should have at least 8 * 1 GE and 8*10G ports from day one	Request to change the port configuration to multi rate (1GE/10GE) to allow more vendor participation.	This restricts participation.	The appliance should have at least 8 * 1 GE/10GE ports from day one	As Per Corrigendum-II	
50	5.9	43	Should support capability to receive contextual user information like username, IP address, authentication status, location and device information from 3rd party vendors	This is not a feature of Internet Firewall.	This functionality is achieved through NAC and not internet firewall	Request to remove this clause.	As Per Corrigendum-II	
51	8.2	45	Firewall/ Firewall's Operating System should be USGv6/IPv6 Certified/IPv6 logo ready	In order to allow more vendor participation, we request to modify the clause to support IPv6 features as requested in the tender.	IPv6 certification is not standard industry practice and only a specific vendor has this.	The proposed router should have complete IPv6 readiness as requested in the tender.	As Per Corrigendum-II	
Exato Technologies							As Per Corrigendum-II	
S.No.	**Tender Sr. No.**	**Page No.**	**Description/ Tender Clause**	**Queries/ Recommendation**	**Response**		As Per Corrigendum-II	
1	A. Scope of work Note 4.	13	Bidder has to provide all type of SFP's of same OEM, Patch Cords and other items required for Installation and Commissioning of complete solution.	It is advised to remove patch chords from the clause, since none of the active component OEM manufacture Patch chords of their own.			As Per Corrigendum-II	
2	SOR-A-2: Switch, Point 2.2		a. 48 x 1G/10G/25G Multi Mode Fiber Interface populated with 48*10G multimode interfaces	It is advised to consider Support for Fiber Channel 16 Gbps ports with or without additional licenses along with 48 x 1G/10G/25G Fiber ports. It will lead to future secure investment.			As Per Corrigendum-II	
3	Technical Specification for Firewall Point no. 8		Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement	Please clarify if Bidders need to consider the clause only in Firewall or on Overall Solution.			As Per Corrigendum-II	
4	New Clause		Request to add	Bidder should have atleast 1 x Valid CCIE R&S certified engineer in their team. Valid Certificate need to be submitted at the time of tender bid submission.			As Per Corrigendum-II	
Intec							As Per Corrigendum-II	
S.No	**page No**	**Clause No**	**Bid Clause Description**	**Clause Query / Changes**	**Justification**		As Per Corrigendum-II	
1	Page no. 30,	Network Access Control & Authentication, Clause no. C-2	Solution should have concurrent capacity for 2000 endpoints out of 50000 endpoint users from day one with scaling upto 50000 concurrent end point endpoints.	Please confirm that proposed solution should include license for 2000 endpoint from day one with capability to scale it to 50,000 in future by purchasing additional license.	To ensure all bidder quote the license without unncessailrly increasing cost of solution		As Per Corrigendum-II	
2	Page no. 33	Anti-Malware Protection for Endpoint Specification. Clause no. D-10	Total of 50000 Licenses should be factored for this End Points. Solution should have concurrent capacity for 2000 endpoints out of 50000 endpoint users from day one with scaling upto 50000 concurrent end point endpoints	Please confirm that proposed solution should include license for 2000 endpoint from day one with capability to scale it to 50,000 in future by purchasing additional license.	To ensure all bidder quote the license without unncessailrly increasing cost of solution		As Per Corrigendum-II	
3	Page no. 5	SOR-A-3: UTM	UTM Solution along with other appliances as per technical specification given in Chapter-3A: 2 SET	As per both the clauses, please clarify Total number of equipments would be required multiplied by Two set of quantities in Page no. 22 or only One set of quantities in Page no. 22	For Two set in page no. 5, the Total quantities of equipments would be double 1. Next Generation Firewall: 8 Qty 2. Network Behavior Analysis: 4 Qty 3. Network Access Control & Authentication: 4 Qty 4. Anti-Malware Protection for Endpoint: 4 Qty		As Per Corrigendum-II	
4	Page no. 22	SOR-A-3: UTM	1. Next Generation Firewall: 4 Qty 2. Network Behavior Analysis: 2 Qty 3. Network Access Control & Authentication: 2 Qty 4. Anti-Malware Protection for Endpoint: 2 Qty				As Per Corrigendum-II	
PaloAlto Networks							As Per Corrigendum-II	

S. No	Ietm Ref	Page No	Specification	Issue	Proposed Change		As Per Corrigendum-II	
1	Chapter 2, SOR, Clause VII	Pg 6	The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote only one OEM against one SOR	Limiting one OEM against one SOR limits participation of hetrogeneous OEM products in a single SOR. Since routing and switching products has been asked in each SOR hence cyber security OEMs will not be able to participate in the RFP. Ideally the cyber security prodcuts in each SOR MSUT be different from the routing and switching OEMs in an SOR in order to ensure better solution and wider participation	The Bidder should have authorization specific to this tender from respective OEM. Bidder to ensure routing and switching OEM is different from security OEM for products like UTM, Internet Firewall, Advance Endpoint, NBA and AAA etc		As Per Corrigendum-II	
2	Scope of Work	Pg 12	The Data Centre Solution should have “Secure tool” should provide application insights and inventory across DC's using auto generated application discovery and dependency mapping for workloads in various Dev, Test, Pre-Prod, Prod and other DC zones. It should provide an always on application blueprint for ever changing application relationships and inter-dependencies.	There is no mention of Secure Tool in SOR. The specifications are given in the scope of work section. Please clarify if "Secure Tool" is a requirement by elaborating in the SOR			As Per Corrigendum-II	
3	SOR -A3, UTM, NGFW	Pg 22	Chassis based security appliance should provide firewall, AVC and IPS functionality from day one	The security appliance should have advanced security features like network antivirus, Command and control prevention, zero day protection, DNS protection etc from day one for maximum effectiveness as only FW, AVC and IPS are no sufficient on their own for complete security	Chassis based security appliance should provide firewall, AVC, IPS/vulnerability protection, network antivirus, Command and control prevention, zero day protection, DNS protection functionality from day one		As Per Corrigendum-II	
4	SOR -A3, UTM, NGFW	Pg 22	Chassis platform should support at least 6 * 10G Gigabit ports and should be scalable to additional 8 * 40G in future. Solution should support 100G (QSFP28) Interfaces.	Rather than asking a single type of ports, it is recommended that different type of ports may be asked for. There is no mention of ports for HA and SYNC functionality, these should be asked for as well	Chassis platform should support at least 10 * 10G Gigabit ports with transceivers (4x 10G Copper, 6 x 10G SFP+) from day one and should be scalable to additional 6x 10G ports and 4 * 40G in future. Solution should support 100G (QSFP28) Interfaces.		As Per Corrigendum-II	
5	SOR -A3, UTM, NGFW	Pg 22	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 256 GB of RAM	The minimum RAM on device varies from one OEM to the other hence instead of asking for very high RAM a min value may please be asked for	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory (min 96 GB or higher)		As Per Corrigendum-II	

6	SOR -A3, UTM, NGFW	Pg 23	Should support 40 Gbps of NGFW (FW, AVC and IPS) real-world / production performance and should be scalable to 80 Gbps in future without replacing hardware.	Rather than asking only NGFW performnace it is recommended that Threat Prevention Throughput may please be asked for. Threat Prevention Throuhgput acounts for perfromance after enabling all functionalitites on the device. Railtel is already asking for malware prevention features on the same device, hence the same must be considered while asking for device perfromance	Should support 23 Gbps of Threat Prevention Throuhgput (FW, AVC, IPS, AV, C&C, Zero Day and logging enabled) real-world / production/ app mix performance		As Per Corrigendum-II	
7	SOR -A3, UTM, NGFW	Pg 23	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc. Firewall should support Next-Gen IPS (NGIPS) from day one. The same Firewall should support Advanced Malware Protection (AMP) for Networks, and URL Filtering.	The firewall must support inclusion of multiple policy aspects/objects in a single unified policy. AMP is a propreitry terminology used by Cisco hence the same may be deleted.	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc in a single rule in a single policy. Firewall should support Next-Gen IPS (NGIPS), zero day protection, antivirus, anti spyware protection from day one.		As Per Corrigendum-II	
8	SOR -A3, UTM, NGFW	Pg 23	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to- IPv4) & Nat46 (IPv4-to-IPv6) functionality	NPTv6, an equivaluent technology to NAT66 may please be considered	Firewall should support Nat66 (IPv6-to-IPv6)/NPTv6, Nat 64 (IPv6-to- IPv4) & Nat46 (IPv4-to-IPv6)functionality		As Per Corrigendum-II	
9	SOR -A3, UTM, NGFW	Pg 23	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
10	SOR -A3, UTM, NGFW	Pg 23	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
11	SOR -A3, UTM, NGFW	Pg 24	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	Different OEMs have different number of IPS signatures, the common min number is 10,000, hence the same may be asked for wider participation	Should support more than 10,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy		As Per Corrigendum-II	

12	SOR -A3, UTM, NGFW	Pg 24	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	Endpoint Quartantine is the function of a NAC solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
13	SOR -A3, UTM, NGFW	Pg 24	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
14	SOR -A3, UTM, NGFW	Pg 24/25	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	There is no defined number of URLs as such and categorization of URL varies from one OEM to the other, hence the number of categories may please be reduced to 60	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies millions of URLs in more than 60 categories.		As Per Corrigendum-II	
15	SOR -A3, UTM, NGFW	Pg 25	Should support safe search for YouTube EDU enforcement	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	
16	SOR -A3, UTM, NGFW	Pg 25	In order to allow the malware detection on a global scale, the network utilized to build the threat intelligence must process at least 80 billion DNS requests/day coming from at least 60 million daily users.	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	
17	SOR -A3, UTM, NGFW	Pg 25	The solution should support ability to enforce Web filtering policies, based on 62 categories. It must be possible to enforce the Web filtering policy independently form the security policy.	Web/URL Filtering policy is an integral part of the firewall security policy, it must not be asked independently of the security policy	The solution should support ability to enforce Web filtering policies, based on 62 categories. It must be possible to enforce the Web filtering policy uniformly with the security policy		As Per Corrigendum-II	
18	SOR -A3, UTM, NGFW	Pg 25	The network used to deliver the DNS security service must have experienced an uptime of at least 99.9% over the last 10 years.	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	

19	SOR -A3, UTM, NGFW	Pg 25	The analysis algorithms must make use multi-layer predictive detectors. As a mere example, these include (but are not limited to): § Analysis of DNS co-occurrences, § Analysis of Domains based on Natural Language Processing algorithms. § Detection of DGA via perplexity and entropy. § Detection of DNS traffic peaks § Soundwave analysis applied to DNS traffic § BGP anomalies detection.	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	
20	SOR -A3, UTM, NGFW	Pg 26	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted	A dedicated appliance may have scaling issues if the loggign rate is high, hence the option for VM based management solution may be provided	The management platform must be a dedicated OEM appliance/VM running on server. In case of VM option the compute to be provided by bidder based on OEM recommendation		As Per Corrigendum-II	
21	SOR -A3, UTM, NGFW	Pg 26	The centralized management platform must not have any limit in terms of handling logs per day	Every management platform has certain limit in handling max logs/day. Hence the specification asked may be deleted	May please be deleted		As Per Corrigendum-II	
22	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 33	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from endpoint specs	May please be deleted		As Per Corrigendum-II	
23	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 33	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	A network sandbox solution helps in analysis of advanced threats like zero day threats, and most advanced endpoint solutions need verdict from network sandbox for better and accurate results and prevention. It may be noted that a support for network sandbox has been asked for in the Internet firewall.	May please be deleted		As Per Corrigendum-II	
24	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 34	Solution should allow Users to chose to preview the new Policy UI.	As a security best practice the endpoint policy must be hidden from the user. Hence this clause may be deleted	May please be deleted		As Per Corrigendum-II	
25	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 34	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from endpoint specs	May please be deleted		As Per Corrigendum-II	

26	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 34	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	A network sandbox solution helps in analysis of advanced threats like zero day threats, and most advanced endpoint solutions need verdict from network sandbox for better and accurate results and prevention. Hence this clause may be deleted	May please be deleted		As Per Corrigendum-II	
27	SOR B-2, Internet Firewall, 2.1	Pg 43	The appliance based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance	The security appliance should have advanced security features like network antivirus, Command and control prevention, zero day protection, DNS protection etc from day one for maximum effectiveness as only FW, AVC and IPS are no sufficient on their own for complete security	The appliancebased security platform should be capable of providing firewall, AVC, IPS/vulnerability protection, network antivirus, Command and control prevention, zero day protection, DNS protection functionality from day one in a single appliance		Tender Document is Clear	
28	SOR B-2, Internet Firewall, 3.1	Pg 43	Should support at least 10 Gbps of NGFW Real world performance (includes FW, Application Visibility & IPS) from day one	Rather than asking only NGFW performnace it is recommended that Threat Prevention Throughput may please be asked for. Threat Prevention Throuhgput acounts for perfromance after enabling all functionalitites on the device. Railtel is already asking for malware prevention features on the same device, hence the same must be considered while asking for device perfromance	Should support at least 4.5 Gbps of Threat Prevention Throuhgput (FW, AVC, IPS, AV, C&C, Zero Day and logging enabled) real-world / production/ app mix performance from day one		Tender Document is Clear	
29	SOR B-2, Internet Firewall, 3.2	Pg 43	NG Firewall should support at least 4,00,0000 concurrent sessions	As per the device throuhgput the number of concurrent sessions may be reduced accordingly please	NG Firewall should support at least 3,00,0000 concurrent sessions		Tender Document is Clear	
30	SOR B-2, Internet Firewall, 3.2	Pg 43	Firewall should support Nat66 (IPv6-to-IPv6), Nat44 (IPv4 to IPv4) and IPv6 to IPv4 to IPv6 for translation/tunneling functionality.	NPTv6, an equivaluent technology to NAT66 may please be considered	Firewall should support Nat66 (IPv6-to-IPv6)/NPTv6, Nat 64 (IPv6-to- IPv4) & Nat46 (IPv4-to-IPv6)functionality		Tender Document is Clear	
31	SOR B-2, Internet Firewall, 3.2	Pg 43	Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		Tender Document is Clear	
Fortinet								
SL#	**RFP Volume Section and sub-section**	**Page no.**	**Clause/ Content in the RFP**	**Clarification sought**		**Change Request**	**RailTel Response**	**RailTel Remarks**

1	SOR-B-2: Internet Firewall-3.1	43	Should support at least 10 Gbps of NGFW Real world performance (includes FW, Application Visibility & IPS) from day one	As Internet Firewall going to deply in perimeter, only NGFW will not able to protect from current sophisticated attacks. it is suggested to ask for Threat Protection which included FW, Application Control, IPS and Malware Protection.		Requesting you to modify the clause to "Should have at least 10 Gbps of NGFW and Threat Protection with Real world / Enterprise Traffic Mix performance (includes FW, Application Visibility, IPS and Malware Protection) from day one"	Tender Document is Clear	
2	SOR-B-2: Internet Firewall-3.2	43	NG Firewall should support at least 4,00,0000 concurrent sessions	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. the firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling MINIMUM 40 million concurrent sessions		Requesting you to modify the clause to "NG Firewall should support at least 4,00,0000 concurrent sessions"	Tender Document is Clear	
3	SOR-B-2: Internet Firewall-3.3	43	NG Firewall should support at least 50,000 connections per second	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. the firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling MINIMUM 380000 New Sessions per Sec.		Requesting you to modify the clause to "NG Firewall should support at least 380,000 connections per second"	As Per Corrigendum-II	
4	SOR-B-2: Internet Firewall-5.2	43	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously	As IPv6 asked in RFP It is suggested to include **DNS64 and and DHCPv6 along with NAT66 and NAT64 for a complete IPv6 functionality**		Requesting you to modify the clause to "Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously and also support DNS64 and DHCPv6 along with NAT66 and NAT64 ."	Tender Document is Clear	
5			New suggested Clause	There is no IPsec VPN Throughput mention in RFP		Pls mention Firewall should have atleast 30 Gbps of IPsec VPN Throughput	Not required	

6			New suggested Clause	Requesting you to ask for internet Firewall should be from different OEM vendor than UTM because if there is an vulnerability with one firewall, the other firewall from a different vendor does not have that vulnerability. Hence there is more protection if the two firewalls are provided by two different vendors		Requesting you to add the clause "Proposed internet Firewall should be from different OEM than UTM for better security".	Not required	
7			New suggested Clause	To reduce the information security threats and organisation adopts best practices to minimise threats.		Requesting you to kindly ask for "The Firewall vendor must have ISO 27001 certified"	Not required	
RAH Infotech								
Sl. No.	**Page No**	**Clause No.**	**Clause in the RFP**	**Query**				
1	27	SOR-A-3 B1	Solution should provide a full featured Network threat analyzer capability to detect threats emerging from inside the network (i.e. ones that have not passed through a perimeter FW/IPS). This includes ability to establish "normal" traffic baseline through flow analysis techniques and the ability to detect deviations from normal baseline.	Two questions -				
				1. Request the buyer to kindly clarify the nature of threats perceived. Can you share the mix of devices/prevalent OS/applications so as to enable an assessment at vendor's end?			Tender Document is Clear	
				2. Request the buyer to clarify what format of flow records shall be made available and, what are the desired ingestion rates?			Tender Document is Clear	
2	27	SOR-A-3 B2	Should have an automated discovery function to identify network devices and capture information such as IP Addresses, OS, Services Provided, Other Connected Hosts.	This generally requires active scanning which can be disruptive. Could you please revert with an approximate count of assets?			Tender Document is Clear	
3	27	SOR-A-3 B3	Should capture singature/heuristics based alerts and block the same	Blocking requires integrating with perimeter or other network-based security controls. Request please update the inventory of assets that the tool is required to integrate with. Signature matching requires DPI. Please suggest what kind of flow data will be made available? Will the enriched flow-data include payload (per IEEE standard)?			Tender Document is Clear	
4	27	SOR-A-3 B9	Solution should generate a whitelist policy based on real-time application behavior and keep the policies up-t-date as applications evolves and more applications are added and modified. It should enforce the generated application whitelisted policy consistently across bare-metal, virtual and container workloads. It should track policy compliance.	Security is getting paranoid to a point of being zero-trust. It is our opinion that this requirement of whitelisting applications not only creates integration challenges and security posture gaps, it opens the environment to more risk by use of any form of whitelisting. Therefore, we request this requirement to be dropped. Let the system monitor 100% of network traffic and flows without any bias.			Tender Document is Clear	

5	27	SOR-A-3 B11	Solution should integrate with Microsoft Active Directory, RADIUS and, DHCP to provide user identity information in addition to IP Address information throughput the system and allow groups based on identity or Active Directory workgroup & provides full historical mapping of user name to IP Address logins in a searchable format	Request the buyer to clarify which of the three technologies is desired? Generally such integration modules are separately priced. In absence of this indicator, it is can overshoot the commercial without adding any material value to the solution. For DHCP integration, will you allow the use of DPI? If yes, will you allow the vendor to use DPI to auto-generate enriched flow-records for NBAD?			Tender Document is Clear	
6	27	SOR-A-3 B12	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantive VLANs	We believe this requirement is addressed in requirement #3. If they imply different techniques, request please clarify on both.			Tender Document is Clear	
7	27	SOR-A-3 B13	Should support the capability to alert the admin and provide mitogation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue	Request please share endpoint detection and response tool details. We believe that the responsibility of getting the endpoint vendor to share required integration API or SDK details lie with the buyer.			Tender Document is Clear	
8	27	SOR-A-3 B14	The system should be able to monitor flow data beween various VLANs	Request please update on the number of network segments/VLANs. Also, kindly update if you are okay with the vendor to tap various network segments to generate enriched flow data for its solution.			Tender Document is Clear	
9	28	SOR-A-3 B20	Solution should support capability to quarantine/remediate endpoint	Request please share endpoint detection and response tool details. We believe that the responsibility of getting the endpoint vendor to share required integration API or SDK details lie with the buyer.			Tender Document is Clear	
10	28	SOR-A-3 B23	Solution should have the capability to traci every process executed on the server and map behaviour deviations instantaneously to malware execution patterns. It should provide high fidelity alerts for both system generated and user defined events.	Request please share endpoint detection and response tool details. We believe that the responsibility of getting the endpoint vendor to share required integration API or SDK details lie with the buyer.			Tender Document is Clear	
11	28	SOR-A-3 B24	Should provide accurate inventory of the installed software packages on workloads in real-tie to quickly identify any known vulnerabilities and exposures. It should then provide actions to quarantine or restrict communications based on vulnerabilities or vulnerability score.	Request please share current asset inventory. This will be required for assessment and accurate feedback on what can or can't be covered by the tool. Also, we believe that sharing of credentials and installation of agents on endpoints is acceptable.			Tender Document is Clear	

12	28	SOR-A-3 B33	Solution should be able to collect security and network information of servers and clients without the usage of agents	Request please share the asset inventory and revert if its acceptable to share credentials.			Tender Document is Clear	
				We request that this requirement (and all related ones) be either dropped or, permit use of agents or, enable integration with endpoint detection and response to tools to facilitate collection of this data.			Tender Document is Clear	
13	28	SOR-A-3 B34	Solution include capability to monitor and display of each and every process, process ID, process owner, process mapping running on the server (Physical/VM form factor).	For better visibility and less load on the network, it makes sense to use agents to perform endpoint monitoring. Therefore, we request that the requirement be altered to permit use of or, integration with endpoint agents to collect such information.			Tender Document is Clear	
Network Access Control								
Sl. No.	**Page No**	**Clause No.**	**Clause in the RFP**	**Query**				
1	30	Serial No 6 in Section C	Should helps organisations to identify the number of endpoints that have a specified application installed and these applications should be classified into 13 categories	Application classification is not a function of the NAC. However NAC can help in whitelisting and blacklisting of applications. Please rephrase the clause to "Solution should be able provide complete asset inventory i.e hardware and software inventory and provide the ability to whitelist or blacklist any installed application"			As per RFP	
2	30	Serial No 2 in Section C	Solution should have concurrent capacity for 2000 endpoints out of 50000 endpoint users from day one with scaling upto 50000 concurrent end point endpoints.	NAC licensing is based on total number of IP enabled devices (endpoints) and not on concurrent users. Please specify the total number of IP enabled devices			As per RFP	
3	30	Serial No 13 in Section C	Support password settings for internal users and admin users, option should be available to choose if the password can contain any dictionary word or its characters in reverse order	Why dictionary word or its characters in reverse order. Password complexity are optional and vary Device to Device and OEM to OEM. Please rephrase the clause to "The NAC solution should provide the ability to set a complex password"			As per RFP	
4	31	Serial No 17 in Section C	Solution should support TACACS+ to simplify device administration and enhance security through flexible, granular control of access to network devices	As per security standards user authentication and device authentication should not be in same device, it must be seprate. Kindly delete this clause.			As per RFP	
5	31	Serial No 18 in Section C	TACACS+ device administration should support: i. Role-based access control ii. Flow-based user experience iii. Per Command level authorization with detailed logs for auditing	As per security standards user authentication and device authentication should not be in same device, it must be seprate. Kindly delete this clause.			As per RFP	

6	31	Serial No 19 in Section C	Solution should support capability to customize TACACS+ Services by specifying customer TACACS+ port number	As per security standards user authentication and device authentication should not be in same device, it must be seprate. Kindly delete this clause.			As per RFP	
7	31	Serial No 21 in Section C	Solution should be able to create TACACS+ profile like Monitor, Priviledge level, default, etc to control the initial login session of device administrator.	As per security standards user authentication and device authentication should not be in same device, it must be seprate. Kindly delete this clause.			As per RFP	
8	30	Section C	Request the clause to be added as it's an important NAC requirement	All the NAC functionality/features asked in the RFP should be available from day one			As per RFP	
9	30	Section C	Request the clause to be added as it's an important NAC requirement	The solution should have intelligence to be able to identify all network devices such as routers, switches, printers, IP cameras, etc which are still using factory default credentials on the network. It should be able to test factory default credentials for SSH, Telnet,SNMP, etc. It will help in determining which devices in organizations network are vulnerable to attack due to their use of weak credentials			As per RFP	
10	30	Section C	Request the clause to be added as it's an important NAC requirement	Solution should be able provide complete asset inventory i.e hardware and software inventory			As per RFP	
11	30	Section C	Request the clause to be added as it's an important NAC requirement	Solution should individually support all the three mentioned integration methods 802.1X , non-802.1X & Hybrid to completely manage the endpoint.			As per RFP	
12	30	Section C	Request the clause to be added as it's an important NAC requirement	Solution should not only relay on 802.1X for authentication & remediation , it should have verious other method to achieve the same such as SSH, Telnet and SNMP based authentication			As per RFP	
13	30	Section C	Request the clause to be added as it's an important NAC requirement	Solution should capable to block the access of endpoints which are connected on unmanaged switch and should able to integrate with all existing Network devices with no up-gradation require.			As per RFP	
14	30	Section C	Request the clause to be added as it's an important NAC requirement	Solution Should capable to achieve all feature & functionality (including full posture assessment) with complete agentless , Agent based & Dissolvable agent mode deployment			As per RFP	
15	30	Section C	Request the clause to be added as it's an important NAC requirement	Platform must be deployable in out-of-band model (with all feature & funcationility) to ensure network keeps functioning even if the solution goes down for whatever reason			As per RFP	

16	30	Section C	Request the clause to be added as it's an important NAC requirement	Should operate within a heterogeneous network with switches from multiple vendors (e.g. but not limited to- Cisco, Juniper, 3com, Nortel, Linksys, Extreme , Dlink , Avaya , Brocade Networks etc). NAC appliance should support vendor agnostic switch infrastructure. It must not only relay on 802.1x mechanism.			As per RFP	
17	30	Section C	Request the clause to be added as it's an important NAC requirement	The solution must support at least the following IOC types for IOC scanning:			As per RFP	
				CnC Address (Command and Control URL)			As per RFP	
				Process (Process Name, Process Hash, Process Hash Type)			As per RFP	
				File Exists (File Name, File Path)			As per RFP	
				Mutex (Mutex Name)			As per RFP	
				Registry Key (Path, Value)			As per RFP	
				Service (Service name)			As per RFP	
18	30	Section C	Request the clause to be added as it's an important NAC requirement	The solution should provide policies to address ransomware threats by providing ability to detect, evaluate and respond to vulnerabilities and threats used by these ransomwares. Policies should provide organization instant visibility, options for a fast and simple response, and the ability to track and segment devices that cannot be patched or mitigated.			As per RFP	
19	30	Section C	Request the clause to be added as it's an important NAC requirement	The proposed NAC solution should be able to provide capability to run custom scripts on Windows and Linux endpoints			As per RFP	
20	30	Section C	Request the clause to be added as it's an important NAC requirement	The solution must have tight integration out of the box with at least these Firewall vendors (CheckPoint, Cisco ASA, Fortinet, Juniper SRX, Palo Alto Networks and Forcepoint Stonesoft)			As per RFP	
21	30	Section C	Request the clause to be added as it's an important NAC requirement	The NAC solution must bi-directionally integrate with SMS/SCCM. The proposed NAC solution should detect devices with missing or broken SMS/SCCM agents before allowing network access. It should be able to automatically enroll devices with missing agents at the connection time and leverage SMS/SCCM for automated agent deployment. It must be able to leverage SMS/SCCM host properties within the NAC policies. Further, it must be able retrieve advertisements related to SMS/SCCM hosts, update SMS/SCCM clients with new advertisements, and update the SMS/SCCM server with new host information.			As per RFP	
Millenium								

Sl.No	SOR	Clause No	Page No	Description of the Clause as per Tender Document	Query	Reason for Requesting the amendment	Amendment Requested	
1	**SOR**	**VII**	**6**	**The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote only one OEM against one SOR**	**We understand that this will be a leaf-spine architecture with L3 Switch in SOR-A acting as Leaf and Core Switch in SOR-B acting as Spine.**	**In a fabric architecture leaf and spine should be from same OEM**	As Per Corrigendum-II	
2	**SOR-A-1-Router**	**1.3**	**13**	**The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multiprocessor based for enhanced performance. The Router should have multi-core Processor @ 2.1 GHz or more**	**Request to remove the clock speed mentioned in the clause.**	**The processor specification does not guarantee device performance.**	As Per Corrigendum-II	
3	**SOR-A-1-Router**	**1.6**	**13**	**The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.**	**Please clarify the requirement of NAT at DC-GW router.**	**NAT would be done at ISP-PE/IGW. If required then this can be achieved through the firewall which is part of UTM solution.**	Tender Document is Clear	
4	**SOR-A-1-Router**	**2.1**	**13**	**Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 100 Gbps or more.**	**It is recommended that the switch fabric should be upgradable to atleast 200G per slot and a total backplane of atleast 600Gbps**	**Since 40GE and 10GE interfaces are requested. 100Gbps performance is too low and wont provide wirespeed/linerate performance.**	Tender Document is Clear	
5	**SOR-A-1-Router**	**2.2**	**14**	**Number of Slots: The router must be chassis based with minimum 3 numbers of Main interface slots. Only the main slots on the router chassis should be considered to comply with this requirement. All the 3 interface slots should be usable from day 1**	**Request to not restrict the number of slots on the device.**	**This will restrict participation and flexibility of solution provider**	As Per Corrigendum-II	
6	**SOR-A-1-Router**	**3.4**	**14**	**Router should support 26 Gbps of IPSEC performance and 8000 tunnels (internal/external).**	**Request to change the IPSec tunnel count to 6000.**	**This would allow more vendor participation**	As Per Corrigendum-II	
7	**SOR-A-1-Router**	**3.9**	**14**	**Software rollback feature**	**It is recommended that the software support configuration commit and rollback upto 10 configurations**	**This will improve high availability and robustness of the system**	As Per Corrigendum-II	
8	**SOR-A-1-Router**	**4.2**	**14**	**The router should have Short Haul SFP enabled on all ports. The Router should have at least 8 ports 1GE and 8 Port x10GE from Day-1. The router should have support of 40GE &100GE interfaces for any future upgrade with additional line card hardware in same chassis.**	**Request to specify the number of 40GE and 100GE interfaces required in future.**	**This is required to dimension the backplane capacity of the offered solution.**	As Per Corrigendum-II	
9	**SOR-A-1-Router**	**5.3**	**15**	**The router should support minimum 6000 VRF instances from day one**	**Request to clarify the requirement for 6000 VRF on a DC-GW router**	**Most of the VRF creation will take place on upstream MPLS PE and not on DC-GW**	As Per Corrigendum-II	
10	**SOR-A-1-Router**	**5.12**	**15**	**The Router shall support selection of the best path for each application based upon reachability, delay, loss, jitter, MOS**	**This is SD-WAN functionality.**	**This feature is not required on DC-GW.**	As Per Corrigendum-II	

11	**SOR-A-1-Router**	**8.2**	**16**	**The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP and by some well known application types through Application Recognition techniques or Application Awareness techniques.**	**Application awareness is not a functionality required on DC-GW router.**	**Application awareness can be done on the UTM devices which is requested in the tender**	As Per Corrigendum-II	
12	**SOR-A-1-Router**	**8.6**	**16**	**The router shall support cRTP for VoIP.**	**Request cRTP as optional as DC-GW location will not have bandwidth availability constraint.**	**cRTP is not required high capacity DC-GW routers with high speed interfaces where bandwidth is not a constraint.**	As Per Corrigendum-II	
13	**SOR-A-1-Router**	**8.13**	**16**	**The router shall support 200k queues to offer granular QoS, policing and shaping capabilities.**	**This is in conflict with clause 8.7 which is sufficient for DC-GW requirement. Also such high number of queues are not required on DC-GW.**	**High number of queues are required only when high number of subscribers are terminating on a node. Hence this wont be used on DC-GW router.**	Tender Document is Clear	
14	**SOR-A-1-Router**	**9.6**	**17**	**The router shall support firewall service in hardware on all interfaces. The firewall performance shall be at least 4 Gbps.**	**Firewall is already part of UTM therefore not needed on DC-GW**	**Firewall function is already covered in UTM. The network performance will deteriorate if firewall inspection is repeated at multiple points within the same network (router and UTM)**	As Per Corrigendum-II	
15	**SOR-A-1-Router**	**9.7**	**17**	**The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.**	**Please clarify the requirement of NAT at DC-GW router.**	**NAT would be done at ISP-PE/IGW. If required then this can be achieved through the firewall which is part of UTM solution.**	Tender Document is Clear	
16	**SOR-A-1-Router**	**9.12**	**17**	**The Router shall support Suite B Cryptographic Suites for Ipsec (RFC 4869)**	**It is recommended to use AES/3DES for cryptographic requirement.**	**RFC 4869 is only optional informational RFC and not a standard.**	Tender Document is Clear	
17	**SOR-A-1-Router**	**10.3**	**17**	**Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP**	**Request cRTP as optional as DC-GW location will not have bandwidth availability constraint.**	**cRTP is not required high capacity DC-GW routers with high speed interfaces where bandwidth is not a constraint.**	As Per Corrigendum-II	
18	**SOR-A-1-Router**	**12.1**	**17**	**The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum.**	**In order to allow more vendor participation, we request to modify the clause to support IPv6 features as requested in the tender.**	**IPv6 certification is not standard industry practice and only a specific vendor has this.**	As Per Corrigendum-II	
19	**SOR-A-2-Switch**	**2.9**	**18**	**Switch should have a minimum 40MB buffer of more.**	**We request to modify the minimum buffer to 32MB.**	**This will allow more vendor participation.**	As Per Corrigendum-II	
20	**SOR-A-2-Switch**	**3.3**	**18**	**The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure**	**This is not applicable for fixed configuration spine/leaf switches. Please confirm.**	**Tender does not request for redundant controller in DC Spine and Leaf Switches.**	Tender Document is Clear	

21	**SOR-A-2-Switch**	**5.11**	**19**	**Switch platform should support MAC Sec in hardware**	**There is no benefit of MACSec on Spine and Leaf switches in a DC environment. This will add additional processing load on the switches.**	**All the connectivity of Switch is with nodes within the data center which is a secured environment, hence MACsec is not required in such scenario.**	Tender Document is Clear	
22	**SOR-A-2-Switch**	**6.4.c**	**19**	**Bi-Directional PIM**	**Please clarify the use case of Bi-Direction PIM on a DC fabric**	**PIM-SM can be used for multicast requirements in DC.**	As Per Corrigendum-II	
23	**SOR-B-1-Core Switch**	**1.4**	**34**	**Robustness : while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone**	**Request to clarify what is meant by "zone" in DC Fabric**	**Clause not clear**	Tender Document is Clear	Zoning is required. Dynamic mobility of VM is required from production to non production. Zone should be defined in febric control.
24	**SOR-B-1-Core Switch**	**1.8**	**35**	**Business Continuance- The fabric should be able to deploy applications across data center fabrics representing separate availability zones, to ensure that any network-level failures or configuration or policy definition errors that occur in one availability zone will not ever be propagated to the application's workloads running in a separate availability zone**	**Request to clarify what is meant by "zone" in DC Fabric**	**Clause not clear**	Tender Document is Clear	The Fabric Should support this, so that if one Zone fails due to some reason, this would not effect in other zones in the DC
25	**SOR-B-1-Core Switch**	**2.3**	**35**	**In case of Fixed Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated Equipped with 32* 40G Multimode QFP28 Multimode from day 1 to support desired Leaf Scale. Each Leaf should connect to Each Spine using minimum 6 x 40G/100 G ports connectivity**	**Please clarify connectivity architecture.**	**If each leaf should connect to each spine using 6 x 40G/100G, then each leaf should atleast have 24 x 40G/100G uplink towards spine on Day 1. Please clarify the connectivity architecture. Please also clarify the desired leaf scale.**	As Per Corrigendum-II	
SOR-B-1-Core Switch	**3.1**	**35**	**Fabric must support various Hypervisor encapsulation including VXLAN and 802.1q natively without any additional hardware/software or design change.**	**It is recommended to have only VxLAN as the encapsulation protocol as it would also cover use cases where VMs have to talk to bare metal servers.**	**To ensure interoperability between application runing on VM and bare metal servers**	**Fabric must support Hypervisor encapsulation using VXLAN natively without any additional hardware/software or design change.**	As Per Corrigendum-II	
SOR-B-1-Core Switch	**3.5**	**35**	**Fabric must provide open programmable interface using python SDK, JSon SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.**	**Request to confirm that the fabric should support atleast one of the mentioned open programmable interface**	**The desired functionality can be met using any of the mentioned protocols.**	**Fabric must provide open programmable interface using python SDK/JSon SDK/XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.**		
28	**SOR-B-1-Core Switch**	**3.12**	**36**	**Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc**	**Request to clarify what is meant by "fabric as stateless distributed firewall"**	**Clause not clear**	As Per Corrigendum-II	

29	**SOR-B-1-Core Switch**	**5.3**	**36**	**Fabric must support VM attribute based zoning and policy**	**Request to clarify the functionality required**	**Clause not clear**	Tender Document is Clear	Zoning based on different VM attribute, Different policy in Fabirc with different VM Zoning
30	**SOR-B-1-Core Switch**	**5.5**	**36**	**Fabric must support true multi - tenancy**	**Request to explain the meaning of "true multi-tenancy"**	**Clause not clear**	Tender Document is Clear	Multi - tenancy/ Multi-Instance can be create to define different zone.
31	**SOR-B-1-Core Switch**	**5.8**	**37**	**Fabric must act as a State-less distributed firewall with the logging capability**	**Request to clarify what is meant by "fabric as stateless distributed firewall"**	**Clause not clear**	As Per Corrigendum-II	
32	**SOR-B-1-Core Switch**	**6.6**	**37**	**Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated from day 1 to support desired Leaf Scale. Each Leaf should connect to Each Spine using minimum 4 x 40G/100 G ports connectivity**	**This is in conflict with clause 2.3. Request to confirm the number of uplink ports required on the leaf switches**	**Connectivity Architecture not clear**	As Per Corrigendum-II	
33	**SOR-B-1-Core Switch**	**2.1**	**38**	**a. Minimum 36 ports support 40/100 Gbps QSFP28 ports. The switch should be populated with 32* 40G Multimode fiber transreceivers for downlink connectivity & 4*100G ports with multimode 100G Transrecievers, for uplink connectivity**	**As per clause 6.6 and 2.3 the interface requirement on Spine switch is 32 ports. Please confirm the actual number of 40GE/100GE ports required on Spine Switch. Also confirm the connectivity for 4 x 100GE uplink requested on spine switches as there is no 100GE requested on the DC-GW router on Day 1. Request to share the connectivity diagram.**	**Connectivity Architecture not clear**	As Per Corrigendum-II	
34	**SOR-B-1-Core Switch**	**2.7**	**39**	**Switch should have a minimum 40MB buffer of more.**	**Request to change the minimum buffer requirement to 16MB as spine switch does not require high buffer memory.**	**This will add to latency on the spine switches. Hence it is not recommended.**	As Per Corrigendum-II	
35	**SOR-B-1-Core Switch**	**3.5**	**39**	**Switch should support minimum 7 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services:**	**Request to change the minimum switching capacity to 6.4Tbps**	**32 x 100GE switch will require only 6.4Tbps of switching capacity.**	As Per Corrigendum-II	
36	**SOR-B-1-Core Switch**	**5.11**	**40**	**Switch platform should support MAC Sec in hardware**	**There is no benefit of MACSec on Spine and Leaf switches in a DC environment. This will add additional processing load on the switches.**	**All the connectivity of Switch is with nodes within the data center which is a secured environment, hence MACsec is not required in such scenario.**	Tender Document is Clear	
Millenium for Security								
S. No	Ietm Ref	Page No	Specification	Issue	Proposed Change			

1	Chapter 2, SOR, Clause VII	Pg 6	The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote only one OEM against one SOR	Limiting one OEM against one SOR limits participation of hetrogeneous OEM products in a single SOR. Since routing and switching products has been asked in each SOR hence cyber security OEMs will not be able to participate in the RFP. Ideally the cyber security prodcuts in each SOR MSUT be different from the routing and switching OEMs in an SOR in order to ensure better solution and wider participation	The Bidder should have authorization specific to this tender from respective OEM. Bidder to ensure routing and switching OEM is different from security OEM for products like UTM, Internet Firewall, Advance Endpoint, NBA and AAA etc		As Per Corrigendum-II	
2	Scope of Work	Pg 12	The Data Centre Solution should have “Secure tool” should provide application insights and inventory across DC's using auto generated application discovery and dependency mapping for workloads in various Dev, Test, Pre-Prod, Prod and other DC zones. It should provide an always on application blueprint for ever changing application relationships and inter-dependencies.	There is no mention of Secure Tool in SOR. The specifications are given in the scope of work section. Please clarify if "Secure Tool" is a requirement by elaborating in the SOR			As Per Corrigendum-II	
3	SOR -A3, UTM, NGFW	Pg 22	Chassis based security appliance should provide firewall, AVC and IPS functionality from day one	The security appliance should have advanced security features like network antivirus, Command and control prevention, zero day protection, DNS protection etc from day one for maximum effectiveness as only FW, AVC and IPS are no sufficient on their own for complete security	Chassis based security appliance should provide firewall, AVC, IPS/vulnerability protection, network antivirus, Command and control prevention, zero day protection, DNS protection functionality from day one		As Per Corrigendum-II	
4	SOR -A3, UTM, NGFW	Pg 22	Chassis platform should support at least 6 * 10G Gigabit ports and should be scalable to additional 8 * 40G in future. Solution should support 100G (QSFP28) Interfaces.	Rather than asking a single type of ports, it is recommended that different type of ports may be asked for. There is no mention of ports for HA and SYNC functionality, these should be asked for as well	Chassis platform should support at least 10 * 10G Gigabit ports with transceivers (4x 10G Copper, 6 x 10G SFP+) from day one and should be scalable to additional 6x 10G ports and 4 * 40G in future. Solution should support 100G (QSFP28) Interfaces.		As Per Corrigendum-II	
5	SOR -A3, UTM, NGFW	Pg 22	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 256 GB of RAM	The minimum RAM on device varies from one OEM to the other hence instead of asking for very high RAM a min value may please be asked for	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory (min 96 GB or higher)		Tender Document is Clear	

6	SOR -A3, UTM, NGFW	Pg 23	Should support 40 Gbps of NGFW (FW, AVC and IPS) real-world / production performance and should be scalable to 80 Gbps in future without replacing hardware.	Rather than asking only NGFW performnace it is recommended that Threat Prevention Throughput may please be asked for. Threat Prevention Throuhgput acounts for perfromance after enabling all functionalitites on the device. Railtel is already asking for malware prevention features on the same device, hence the same must be considered while asking for device perfromance	Should support 23 Gbps of Threat Prevention Throuhgput (FW, AVC, IPS, AV, C&C, Zero Day and logging enabled) real-world / production/ app mix performance		As Per Corrigendum-II	
7	SOR -A3, UTM, NGFW	Pg 23	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc. Firewall should support Next-Gen IPS (NGIPS) from day one. The same Firewall should support Advanced Malware Protection (AMP) for Networks, and URL Filtering.	The firewall must support inclusion of multiple policy aspects/objects in a single unified policy. AMP is a propreitry terminology used by Cisco hence the same may be deleted.	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc in a single rule in a single policy. Firewall should support Next-Gen IPS (NGIPS), zero day protection, antivirus, anti spyware protection from day one.		As Per Corrigendum-II	
8	SOR -A3, UTM, NGFW	Pg 23	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to- IPv4) & Nat46 (IPv4-to-IPv6) functionality	NPTv6, an equivaluent technology to NAT66 may please be considered	Firewall should support Nat66 (IPv6-to-IPv6)/NPTv6, Nat 64 (IPv6-to- IPv4) & Nat46 (IPv4-to-IPv6)functionality		Tender Document is Clear	
9	SOR -A3, UTM, NGFW	Pg 23	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
10	SOR -A3, UTM, NGFW	Pg 23	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
11	SOR -A3, UTM, NGFW	Pg 24	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	Different OEMs have different number of IPS signatures, the common min number is 10,000, hence the same may be asked for wider participation	Should support more than 10,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy		As Per Corrigendum-II	

12	SOR -A3, UTM, NGFW	Pg 24	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	Endpoint Quartantine is the function of a NAC solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
13	SOR -A3, UTM, NGFW	Pg 24	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		As Per Corrigendum-II	
14	SOR -A3, UTM, NGFW	Pg 24/25	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	There is no defined number of URLs as such and categorization of URL varies from one OEM to the other, hence the number of categories may please be reduced to 60	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies millions of URLs in more than 60 categories.		As Per Corrigendum-II	
15	SOR -A3, UTM, NGFW	Pg 25	Should support safe search for YouTube EDU enforcement	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	
16	SOR -A3, UTM, NGFW	Pg 25	In order to allow the malware detection on a global scale, the network utilized to build the threat intelligence must process at least 80 billion DNS requests/day coming from at least 60 million daily users.	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	
17	SOR -A3, UTM, NGFW	Pg 25	The solution should support ability to enforce Web filtering policies, based on 62 categories. It must be possible to enforce the Web filtering policy independently form the security policy.	Web/URL Filtering policy is an integral part of the firewall security policy, it must not be asked independently of the security policy	The solution should support ability to enforce Web filtering policies, based on 62 categories. It must be possible to enforce the Web filtering policy uniformly with the security policy		As Per Corrigendum-II	
18	SOR -A3, UTM, NGFW	Pg 25	The network used to deliver the DNS security service must have experienced an uptime of at least 99.9% over the last 10 years.	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	

19	SOR -A3, UTM, NGFW	Pg 25	The analysis algorithms must make use multi-layer predictive detectors. As a mere example, these include (but are not limited to): § Analysis of DNS co-occurrences, § Analysis of Domains based on Natural Language Processing algorithms. § Detection of DGA via perplexity and entropy. § Detection of DNS traffic peaks § Soundwave analysis applied to DNS traffic § BGP anomalies detection.	The functionality is specific to Cisco may please be deleted	May please be deleted		As Per Corrigendum-II	
20	SOR -A3, UTM, NGFW	Pg 26	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted	A dedicated appliance may have scaling issues if the loggign rate is high, hence the option for VM based management solution may be provided	The management platform must be a dedicated OEM appliance/VM running on server. In case of VM option the compute to be provided by bidder based on OEM recommendation		Tender Document is Clear	
21	SOR -A3, UTM, NGFW	Pg 26	The centralized management platform must not have any limit in terms of handling logs per day	Every management platform has certain limit in handling max logs/day. Hence the specification asked may be deleted	May please be deleted		As Per Corrigendum-II	
22	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 33	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from endpoint specs	May please be deleted		As Per Corrigendum-II	
23	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 33	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	A network sandbox solution helps in analysis of advanced threats like zero day threats, and most advanced endpoint solutions need verdict from network sandbox for better and accurate results and prevention. It may be noted that a support for network sandbox has been asked for in the Internet firewall.	May please be deleted		As Per Corrigendum-II	
24	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 34	Solution should allow Users to chose to preview the new Policy UI.	As a security best practice the endpoint policy must be hidden from the user. Hence this clause may be deleted	May please be deleted		As Per Corrigendum-II	
25	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 34	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from endpoint specs	May please be deleted		As Per Corrigendum-II	

26	SOR -A3, UTM, Anti Malware Protection for Endpoint	Pg 34	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	A network sandbox solution helps in analysis of advanced threats like zero day threats, and most advanced endpoint solutions need verdict from network sandbox for better and accurate results and prevention. Hence this clause may be deleted	May please be deleted		As Per Corrigendum-II	
27	SOR B-2, Internet Firewall, 2.1	Pg 43	The appliancebased security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance	The security appliance should have advanced security features like network antivirus, Command and control prevention, zero day protection, DNS protection etc from day one for maximum effectiveness as only FW, AVC and IPS are no sufficient on their own for complete security	The appliancebased security platform should be capable of providing firewall, AVC, IPS/vulnerability protection, network antivirus, Command and control prevention, zero day protection, DNS protection functionality from day one in a single appliance		Tender Document is Clear	
28	SOR B-2, Internet Firewall, 3.1	Pg 43	Should support at least 10 Gbps of NGFW Real world performance (includes FW, Application Visibility & IPS) from day one	Rather than asking only NGFW performnace it is recommended that Threat Prevention Throughput may please be asked for. Threat Prevention Throuhgput acounts for perfromance after enabling all functionalitites on the device. Railtel is already asking for malware prevention features on the same device, hence the same must be considered while asking for device perfromance	Should support at least 4.5 Gbps of Threat Prevention Throuhgput (FW, AVC, IPS, AV, C&C, Zero Day and logging enabled) real-world / production/ app mix performance from day one		Tender Document is Clear	
29	SOR B-2, Internet Firewall, 3.2	Pg 43	NG Firewall should support at least 4,00,0000 concurrent sessions	As per the device throuhgput the number of concurrent sessions may be reduced accordingly please	NG Firewall should support at least 3,00,0000 concurrent sessions		Tender Document is Clear	
30	SOR B-2, Internet Firewall, 3.2	Pg 43	Firewall should support Nat66 (IPv6-to-IPv6), Nat44 (IPv4 to IPv4) and IPv6 to IPv4 to IPv6 for translation/tunneling functionality.	NPTv6, an equivaluent technology to NAT66 may please be considered	Firewall should support Nat66 (IPv6-to-IPv6)/NPTv6, Nat 64 (IPv6-to- IPv4) & Nat46 (IPv4-to-IPv6)functionality		Tender Document is Clear	
31	SOR B-2, Internet Firewall, 3.2	Pg 43	Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	The asked functionality pertains to NBA solution asked in the RFP, hence may please be deleted from NGFW specs	May please be deleted		Tender Document is Clear	
	Targus							
SOR	VII	6	The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote only one OEM against one SOR	We understand that this will be a leaf-spine architecture with L3 Switch in SOR-A acting as Leaf and Core Switch in SOR-B acting as Spine.	In a fabric architecture leaf and spine should be from same OEM	It is recommended that Leaf and Spine be part of same SOR.		

SOR-A-1-Router	1.3	13	The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multiprocessor based for enhanced performance. The Router should have multi-core Processor @ 2.1 GHz or more	Request to remove the clock speed mentione	The processor specification does not guarantee device performance.	The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multiprocessor based for enhanced performance. The CPU should have sufficient clock speed to meet the performance requirements mentioned in the tender.	
SOR-A-1-Router	1.6	13	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.	Please clarify the requirement of NAT at DC-G	NAT would be done at ISP-PE/IGW. If required then this can be achieved through the firewall which is part of UTM solution.	The router may have hardware assisted Network Address Translation (NAT) capability as per RFC 1631 as an optional feature.	
SOR-A-1-Router	2.1	13	Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 100 Gbps or more.	It is recommended that the switch fabric should be upgradable to atleast 200G per slot and a total backplane of atleast 600Gbps	Since 40GE and 10GE interfaces are requested. 100Gbps performance is too low and wont provide wirespeed/linerate performance.	Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 200G per slot and a total backplane of atleast 600Gbps.	
SOR-A-1-Router	2.2	14	Number of Slots: The router must be chassis based with minimum 3 numbers of Main interface slots. Only the main slots on the router chassis should be considered to comply with this requirement. All the 3 interface slots should be usable from day 1	Request to not restrict the number of slots on the device.	This will restrict participation and flexibility of solution provider	The router should have sufficient interface card slots to provide the interfaces requested in the tender. The router should have 25% free slots on Day 1 after populating all the interfaces requested in the tender.	
SOR-A-1-Router	3.4	14	Router should support 26 Gbps of IPSEC performance and 8000 tunnels (internal/external).	Request to change the IPSec tunnel count to 6000.	This would allow more vendor participation	Router should support 26 Gbps of IPSEC performance and 6000 tunnels (internal/external).	
SOR-A-1-Router	3.9	14	Software rollback feature	It is recommended that the software support configuration commit and rollback upto 10 configurations	This will improve high availability and robustness of the system	Software should support configuration commit and rollback upto 10 configurations	
SOR-A-1-Router	4.2	14	The router should have Short Haul SFP enabled on all ports. The Router should have at least 8 ports 1GE and 8 Port x10GE from Day-1. The router should have support of 40GE &100GE interfaces for any future upgrade with additional line card hardware in same chassis.	Request to specify the number of 40GE and 1	This is required to dimension the backplane capacity of the offered solution.	The router should have Short Haul SFP enabled on all ports. The Router should have at least 8 ports 1GE and 8 Port x10GE from Day-1. The router should be able to support 4 nos of 40GE & 4 nos of 100GE interfaces in future with additional line card hardware in same chassis.	
SOR-A-1-Router	5.3	15	The router should support minimum 6000 VRF instances from day one	Request to clarify the requirement for 6000 V	Most of the VRF creation will take place on upstream MPLS PE and not on DC-GW	The router should support minimum 30 VRF instances from day one	
SOR-A-1-Router	5.12	15	The Router shall support selection of the best path for each application based upon reachability, delay, loss, jitter, MOS	This is SD-WAN functionality.	This feature is not required on DC-GW.	Request to remove this clause.	

SOR-A-1-Router	8.2	16	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP and by some well known application types through Application Recognition techniques or Application Awareness techniques.	Application awareness is not a functionality r	Application awareness can be done on the UTM devices which is requested in the tender	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP and DSCP.	
SOR-A-1-Router	8.6	16	The router shall support cRTP for VoIP.	Request cRTP as optional as DC-GW location will not have bandwidth availability constraint.	cRTP is not required high capacity DC-GW routers with high speed interfaces where bandwidth is not a constraint.	The router may support cRTP for VoIP as an optional feature.	
SOR-A-1-Router	8.13	16	The router shall support 200k queues to offer granular QoS, policing and shaping capabilities.	This is in conflict with clause 8.7 which is sufficient for DC-GW requirement. Also such high number of queues are not required on DC-GW.	High number of queues are required only when high number of subscribers are terminating on a node. Hence this wont be used on DC-GW router.	Request to remove this clause.	
SOR-A-1-Router	9.6	17	The router shall support firewall service in hardware on all interfaces. The firewall performance shall be at least 4 Gbps.	Firewall is already part of UTM therefore not	Firewall function is already covered in UTM. The network performance will deteriorate if firewall inspection is repeated at multiple points within the same network (router and UTM)	Request to remove this clause.	
SOR-A-1-Router	9.7	17	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.	Please clarify the requirement of NAT at DC-GW router.	NAT would be done at ISP-PE/IGW. If required then this can be achieved through the firewall which is part of UTM solution.	The router may have hardware assisted Network Address Translation (NAT) capability as per RFC 1631 as an optional feature.	
SOR-A-1-Router	9.12	17	The Router shall support Suite B Cryptographic Suites for Ipsec (RFC 4869)	It is recommended to use AES/3DES for cryptographic requirement.	RFC 4869 is only optional informational RFC and not a standard.	The Router shall support Suite B Cryptographic Suites for Ipsec using AES/3DES	
SOR-A-1-Router	10.3	17	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP	Request cRTP as optional as DC-GW location will not have bandwidth availability constraint.	cRTP is not required high capacity DC-GW routers with high speed interfaces where bandwidth is not a constraint.	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter and packet loss	
SOR-A-1-Router	12.1	17	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum.	In order to allow more vendor participation, we request to modify the clause to support IPv6 features as requested in the tender.	IPv6 certification is not standard industry practice and only a specific vendor has this.	The proposed router should have complete IPv6 readiness as requested in the tender.	
SOR-A-2-Switch	2.9	18	Switch should have a minimum 40MB buffer of more.	We request to modify the minimum buffer to 32MB.	This will allow more vendor participation.	Switch should have a minimum 32MB buffer of more.	

SOR-A-2-Switch	3.3	18	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure	This is not applicable for fixed configuration s	Tender does not request for redundant controller in DC Spine and Leaf Switches.	Request to remove this clause.		
SOR-A-2-Switch	5.11	19	Switch platform should support MAC Sec in hardware	There is no benefit of MACSec on Spine and Leaf switches in a DC environment. This will add additional processing load on the switches.	All the connectivity of Switch is with nodes within the data center which is a secured environment, hence MACsec is not required in such scenario.	Request to remove this clause.		
SOR-A-2-Switch	6.4.c	19	Bi-Directional PIM	Please clarify the use case of Bi-Direction PIM on a DC fabric	PIM-SM can be used for multicast requirements in DC.	Request to remove this clause.		
SOR-B-1-Core Switch	1.4	34	Robustness : while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone	Request to clarify what is meant by "zone" in	Clause not clear			
SOR-B-1-Core Switch	1.8	35	Business Continuance- The fabric should be able to deploy applications across data center fabrics representing separate availability zones, to ensure that any network-level failures or configuration or policy definition errors that occur in one availability zone will not ever be propagated to the application's workloads running in a separate availability zone	Request to clarify what is meant by "zone" in	Clause not clear		Please Refer Above	
SOR-B-1-Core Switch	2.3	35	In case of Fixed Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated Equipped with 32* 40G Multimode QFP28 Multimode from day 1 to support desired Leaf Scale. Each Leaf should connect to Each Spine using minimum 6 x 40G/100 G ports connectivity	Please clarify connectivity architecture.	If each leaf should connect to each spine using 6 x 40G/100G, then each leaf should atleast have 24 x 40G/100G uplink towards spine on Day 1. Please clarify the connectivity architecture. Please also clarify the desired leaf scale.			
SOR-B-1-Core Switch	3.1	35	Fabric must support various Hypervisor encapsulation including VXLAN and 802.1q natively without any additional hardware/software or design change.	It is recommended to have only VxLAN as the encapsulation protocol as it would also cover use cases where VMs have to talk to bare metal servers.	To ensure interoperability between application runing on VM and bare metal servers	Fabric must support Hypervisor encapsulation using VXLAN natively without any additional hardware/software or design change.		
SOR-B-1-Core Switch	3.5	35	Fabric must provide open programmable interface using python SDK, JSon SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.	Request to confirm that the fabric should support atleast one of the mentioned open programmable interface	The desired functionality can be met using any of the mentioned protocols.	Fabric must provide open programmable interface using python SDK/JSon SDK/XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.		

SOR-B-1-Core Switch	3.12	36	Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc	Request to clarify what is meant by "fabric as stateless distributed firewall"	Clause not clear		
SOR-B-1-Core Switch	5.3	36	Fabric must support VM attribute based zoning and policy	Request to clarify the functionality required	Clause not clear		
SOR-B-1-Core Switch	5.5	36	Fabric must support true multi - tenancy	Request to explain the meaning of "true mult	Clause not clear		
SOR-B-1-Core Switch	5.8	37	Fabric must act as a State-less distributed firewall with the logging capability	Request to clarify what is meant by "fabric as stateless distributed firewall"	Clause not clear		
SOR-B-1-Core Switch	6.6	37	Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated from day 1 to support desired Leaf Scale. Each Leaf should connect to Each Spine using minimum 4 x 40G/100 G ports connectivity	This is in conflict with clause 2.3. Request to confirm the number of uplink ports required on the leaf switches	Connectivity Architecture not clear		
SOR-B-1-Core Switch	2.1	38	a. Minimum 36 ports support 40/100 Gbps QSFP28 ports. The switch should be populated with 32* 40G Multimode fiber transreceivers for downlink connectivity & 4*100G ports with multimode 100G Transrecievers, for uplink connectivity	As per clause 6.6 and 2.3 the interface requirement on Spine switch is 32 ports. Please confirm the actual number of 40GE/100GE ports required on Spine Switch. Also confirm the connectivity for 4 x 100GE uplink requested on spine switches as there is no 100GE requested on the DC-GW router on Day 1. Request to share the connectivity diagram.	Connectivity Architecture not clear		
SOR-B-1-Core Switch	2.7	39	Switch should have a minimum 40MB buffer of more.	Request to change the minimum buffer requirement to 16MB as spine switch does not require high buffer memory.	This will add to latency on the spine switches. Hence it is not recommended.	Switch should have a minimum 16MB buffer of more.	
SOR-B-1-Core Switch	3.5	39	Switch should support minimum 7 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services:	Request to change the minimum switching capacity to 6.4Tbps	32 x 100GE switch will require only 6.4Tbps of switching capacity.	Switch should support minimum 6.4 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services:	
SOR-B-1-Core Switch	5.11	40	Switch platform should support MAC Sec in hardware	There is no benefit of MACSec on Spine and Leaf switches in a DC environment. This will add additional processing load on the switches.	All the connectivity of Switch is with nodes within the data center which is a secured environment, hence MACsec is not required in such scenario.	Request to remove this clause.	
SOR-A-3: UTM	1	22	The Firewall solution offered must be rated as ‘leaders’ or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years	Request to modify this clause such that firewall solution offered should be listed in the Gartner Magic Quadrant for Enterprise Firewall	This restricts participation and request to relax the clause.	The firewall solution offered must be listed in the Gartner Magic Quadrant for Enterprise Firewall	

SOR-A-3: UTM	2	22	Chassis platform should support at least 6 * 10G Gigabit ports and should be scalable to additional 8 * 40G in future. Solution should support 100G (QSFP28) Interfaces.	Interface requirement given for Day 1 is too low and not enough to meet the throughput of firewall.	To ensure 40Gbps of NGFW capability atleast 5 x 10GE ports are required downlink and 5 x 10GE ports for uplink.	Chassis platform should support at least 10 * 10G Gigabit ports and should be scalable to additional 8 * 40G in future. Solution should support 100G (QSFP28) Interfaces.	
SOR-A-3: UTM	2	22	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	It is not recommended to have merchant silicon based security solution as it is more vulnerable against attacks.	This is not recommended	Request to remove this clause.	
SOR-A-3: UTM	2	22	The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet.	It is not recommended to have merchant silicon based security solution as it is more vulnerable against attacks.	This is not recommended	Request to remove this clause.	
SOR-A-3: UTM	2	22	Proposed firewall should not consume more than 3 RU of rack space	This clause is restricting to offer the best security solution available.	This restricts participation.	Request to remove this clause.	
SOR-A-3: UTM	3	23	Firewall should support atleast 25,000,000 concurrent sessions with application visibility turned on or more	The concurrent sessions scale requested is too low for a 40Gbps NGFW.	Scale requested is too low.	Firewall should support atleast 75,000,000 concurrent sessions with application visibility turned on or more	
SOR-A-3: UTM	3	23	Firewall should support atleast 300,000 connections per second with application visibility turned on or more	The connections per second scale requested is too low for a 40Gbps NGFW.	Scale requested is too low.	Firewall should support atleast 1,500,000 connections per second with application visibility turned on or more	
SOR-A-3: UTM	4	24	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	The scale requested seems vendor specific. Hence request to change the signatures scale to 3500 or more. This is inline with latest TEC-GR for UTM devices.	This would allow more vendor participation	Should support more than 3,500 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy.	
SOR-A-3: UTM	4	24	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	The scale requested is not required for DC UTM solution	This would allow more vendor participation	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 100 million of URLs in more than 80 categories.	
SOR-A-3: UTM	4	25	Should support safe search for YouTube EDU enforcement	This is not applicable for a datacenter scenario hence request to delete this clause.	Not a relavant feature for DC.	Request to remove this clause.	
SOR-A-3: UTM	4	25	DNS Security	DNS security is not a part of UTM solution. Hence request to remove this requirement from NGFW.	DNS security is not covered by NGFW. Dedicated solutions are available for DNS security.	Request to remove this clause.	
SOR-B-2: Internet Firewa	1.1	43	The Firewall solution offered must be rated as ‘leaders’ or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years	Request to modify this clause such that firewall solution offered should be listed in the Gartner Magic Quadrant for Enterprise Firewall	This restricts participation and request to relax the clause.	The firewall solution offered must be listed in the Gartner Magic Quadrant for Enterprise Firewall	

SOR-B-2: Internet Firewa	2.2	43	The appliance should have at least 8 * 1 GE and 8*10G ports from day one	Request to change the port configuration to multi rate (1GE/10GE) to allow more vendor participation.	This restricts participation.	The appliance should have at least 8 * 1 GE/10GE ports from day one		
SOR-B-2: Internet Firewa	5.9	43	Should support capability to receive contextual user information like username, IP address, authentication status, location and device information from 3rd party vendors	This is not a feature of Internet Firewall.	This functionality is achieved through NAC and not internet firewall	Request to remove this clause.		
SOR-B-2: Internet Firewa	8.2	45	Firewall/ Firewall's Operating System should be USGv6/IPv6 Certified/IPv6 logo ready	In order to allow more vendor participation, we request to modify the clause to support IPv6 features as requested in the tender.	IPv6 certification is not standard industry practice and only a specific vendor has this.	The proposed router should have complete IPv6 readiness as requested in the tender.		
Commercial Queries								
Note VII mentioned under Chapter 2 Schedule of Requirements	Note VII	6	The Bidder should have authorization specific to this tender from respective OEM.	RailTel has asked for only One OEM against One SOR. Please help understand what SOR would imply.	Only One OEM against One SOR (if it is will Limit submission to one specific OEM only.	Kindly withdraw this clause, enabling best solutions to be tabled from different OEMs	As Per Corrigendum-II	
			Bidder has to quote only one OEM against one SOR	SOR would mean SOR-A or SOR-B as a whole to be offered by One OEM or SOR-A, Item#1 to be offered by ONE OEM, Item# 2 can offered by the same or other OEM and likewise for SOR-B also separate line items can be offered by same or different OEM, but one line item completely shall be offered by One OEM.	There are different OEMs which are Subject Matter Experts in their respective domains.		As Per Corrigendum-II	
Note VIII mentioned under Chapter 2 Schedule of Requirements	Note VIII	6	Bidder has to quote for all SOR and evaluation will be done on totality.	RailTel Intends to place two separate POs for SOR A & SOR B, does this implies that it is also possible to Place SOR A on One Bidder & SOR B on another Bidder	We wish request RailTel help us to understand the objective of releasing two separate POs	Please clarify,	As Per Corrigendum-II	
			However, PO for SOR-A and SOR-B will be issued separately.			Also since RailTel Intends to release two separate purchase orders, we wish to request that the PQ also should be in line with the values of the two separate POs rather than one consolidated BID value.	As Per Corrigendum-II	
Tax Breakup for SOR	Annexure A	7	Column 11 under 'Price Per Unit (all inclusive) for delivery at destination (4+6+8+10)'	We believe Column 11 may not be required	Column mentions %, while this column is supposed to be total Price including all the breakup shared for a given item	please clarify	As Per Corrigendum-II	
5. Offline Submissions:	Sub Clause "c"	9	c. In case bidder happens to be an eligible MSME, the documentary evidence for same shall be submitted.	does this Bid allows the exemptions available for the MSME Registered vendors like exemption of EMD, Preference etc.	Since RailTel has asked for a Valid MSME Certificate	Please clarify and we also wish to request RailTel to Allow the MSME exemptions & preferences allowed under "Public Procurement (preference to make in India) Policy Order, 2017 issued by DIPP and Public Procurement Policy for Micro and Small Enterprises (MSEs) order, 2012" issued by MoSME."	Tender Document is Clear	

12.1 Technical Capability & Note VIII mentioned under Chapter 2 Schedule of Requirements & CHAPTER- 5	12.2.5, Note VIII & Clause 12.2.1	61, 7 & 71 respectively	at least one (1) project worth at least INR 7.78 Crore showcasing supply, design, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially in India in the last 3 years.		RailTel for many other bids have asked for the 1 Order of 35% Value, 2 order of 20% value & 3 orders of 15% value.	Kindly allow 2 orders of 20% value & 3 orders of 15% value in the field of SITC of IT Project also in addition of 1 Order of 35% Value	Tender Document is Clear	
BID DATA SHEET (BDS)					Also since RailTel intends to place two separate orders then the Qualifying criteria should also be matching the 2 separate orders.		Tender Document is Clear	
Sl. No.	**Page No**	**Clause No.**	**Clause in the RFP**	**Query**				
1	27	SOR-A-3 B1	Solution should provide a full featured Network threat analyzer capability to detect threats emerging from inside the network (i.e. ones that have not passed through a perimeter FW/IPS). This includes ability to establish "normal" traffic baseline through flow analysis techniques and the ability to detect deviations from normal baseline.	Two questions - 1. Request the buyer to kindly clarify the nature of threats perceived. Can you share the mix of devices/prevalent OS/applications so as to enable an assessment at vendor's end? 2. Request the buyer to clarify what format of flow records shall be made available and, what are the desired ingestion rates?			As Per Tender Document and Corrigrndum- II	
2	27	SOR-A-3 B2	Should have an automated discovery function to identify network devices and capture information such as IP Addresses, OS, Services Provided, Other Connected Hosts.	This generally requires active scanning which can be disruptive. Could you please revert with an approximate count of assets?			As Per Tender Document and Corrigrndum- II	
3	27	SOR-A-3 B3	Should capture singature/heuristics based alerts and block the same	Blocking requires integrating with perimeter or other network-based security controls. Request please update the inventory of assets that the tool is required to integrate with. Signature matching requires DPI. Please suggest what kind of flow data will be made available? Will the enriched flow-data include payload (per IEEE standard)?			As Per Tender Document and Corrigrndum- II	
4	27	SOR-A-3 B9	Solution should generate a whitelist policy based on real-time application behavior and keep the policies up-t-date as applications evolves and more applications are added and modified. It should enforce the generated application whitelisted policy consistently across bare-metal, virtual and container workloads. It should track policy compliance.	Security is getting paranoid to a point of being zero-trust. It is our opinion that this requirement of whitelisting applications not only creates integration challenges and security posture gaps, it opens the environment to more risk by use of any form of whitelisting. Therefore, we request this requirement to be dropped. Let the system monitor 100% of network traffic and flows without any bias.			As Per Tender Document and Corrigrndum- II	

5	27	SOR-A-3 B11	Solution should integrate with Microsoft Active Directory, RADIUS and, DHCP to provide user identity information in addition to IP Address information throughput the system and allow groups based on identity or Active Directory workgroup & provides full historical mapping of user name to IP Address logins in a searchable format	Request the buyer to clarify which of the three technologies is desired? Generally such integration modules are separately priced. In absence of this indicator, it is can overshoot the commercial without adding any material value to the solution. For DHCP integration, will you allow the use of DPI? If yes, will you allow the vendor to use DPI to auto-generate enriched flow-records for NBAD?			As Per Tender Document and Corrigrndum- II
6	27	SOR-A-3 B12	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantive VLANs	We believe this requirement is addressed in requirement #3. If they imply different techniques, request please clarify on both.			As Per Tender Document and Corrigrndum- II
7	27	SOR-A-3 B13	Should support the capability to alert the admin and provide mitogation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue	Request please share endpoint detection and response tool details. We believe that the responsibility of getting the endpoint vendor to share required integration API or SDK details lie with the buyer.			As Per Tender Document and Corrigrndum- II
8	27	SOR-A-3 B14	The system should be able to monitor flow data beween various VLANs	Request please update on the number of network segments/VLANs. Also, kindly update if you are okay with the vendor to tap various network segments to generate enriched flow data for its solution.			As Per Tender Document and Corrigrndum- II
9	28	SOR-A-3 B20	Solution should support capability to quarantine/remediate endpoint	Request please share endpoint detection and response tool details. We believe that the responsibility of getting the endpoint vendor to share required integration API or SDK details lie with the buyer.			As Per Tender Document and Corrigrndum- II
10	28	SOR-A-3 B23	Solution should have the capability to traci every process executed on the server and map behaviour deviations instantaneously to malware execution patterns. It should provide high fidelity alerts for both system generated and user defined events.	Request please share endpoint detection and response tool details. We believe that the responsibility of getting the endpoint vendor to share required integration API or SDK details lie with the buyer.			As Per Tender Document and Corrigrndum- II
11	28	SOR-A-3 B24	Should provide accurate inventory of the installed software packages on workloads in real-tie to quickly identify any known vulnerabilities and exposures. It should then provide actions to quarantine or restrict communications based on vulnerabilities or vulnerability score.	Request please share current asset inventory. This will be required for assessment and accurate feedback on what can or can't be covered by the tool. Also, we believe that sharing of credentials and installation of agents on endpoints is acceptable.			As Per Tender Document and Corrigrndum- II

12	28	SOR-A-3 B33	Solution should be able to collect security and network information of servers and clients without the usage of agents	Request please share the asset inventory and revert if its acceptable to share credentials. We request that this requirement (and all related ones) be either dropped or, permit use of agents or, enable integration with endpoint detection and response to tools to facilitate collection of this data.			As Per Tender Document and Corrigrndum- II
13	28	SOR-A-3 B34	Solution include capability to monitor and display of each and every process, process ID, process owner, process mapping running on the server (Physical/VM form factor).	For better visibility and less load on the network, it makes sense to use agents to perform endpoint monitoring. Therefore, we request that the requirement be altered to permit use of or, integration with endpoint agents to collect such information.			As Per Tender Document and Corrigrndum- II
S.No	**Clause No.**	**Section, Point No, Page no.**	**Content of RFP Requiring Clarification**	**Change Request**	**Remarks**		As Per Tender Document and Corrigrndum- II
1	SOR-A-3: UTM	SN No 2, point no 6, Page no 22	Proposed firewall should not consume more than 3 RU of rack space	Pls delete this point	Rack Unit of an appliance varies from OEM to OEM depending on the hardware architecture and physical dimensions. 3 RU is very much restricted to one single OEM. Request Railtel to remove this point and let the bidders quote as per the functional requirement of the RFP.		As Per Tender Document and Corrigrndum- II
2	SOR-A-3: UTM	SN No 3, point no 5, Page no 23	Firewall should have integrated redundant hot-swappable fan tray / modules	Firewall should have integrated redundant hot-swappable fan tray / modules / power supplies	Hot swappable fan tray / modules are not supported by manu OEM and will restric to a particular OEM. It's suggested to include Hot swap power supplies which is a legitimate ask from RPS point of view.		As Per Tender Document and Corrigrndum- II
3	SOR-A-3: UTM	SN No 4, point no 1, Page no 23	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc. Firewall should support Next-Gen IPS (NGIPS) from day one. The same Firewall should support Advanced Malware Protection (AMP) for Networks, and URL Filtering.	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc. Firewall should support Next-Gen IPS (NGIPS) from day one. The same Firewall should support Anti-Malware & Anti-Virus Protection for Networks, and URL Filtering.	Advanced Malware Protection (AMP) is a Cisco specific terminology. Request to change the same to anti-malware and anti-virus. Pls refer - https://www.cisco.com/c/en_in/products/security/amp-appliances/index.html		As Per Tender Document and Corrigrndum- II
4	SOR-A-3: UTM	SN No 4, point no 4, Page no 23	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	Should support Static, RIP, OSPF, OSPFv3 and BGP	NGFW will function as a firewall and not router, so specific version of BGP is not required. Request to remove BGPv6.		As Per Tender Document and Corrigrndum- II

5	SOR-A-3: UTM	SN No 4, point no 18, Page no 24	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.	Pls delete this point	NBA is a Cisco specific terminology, so request Railtel to remove this point from the specification. Pls refer - https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.pdf		As Per Tender Document and Corrigrndum- II	
6	SOR-A-3: UTM	SN No 4, point no 18, Page no 24	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	Should support access to community resources and ability to easily customize security to address new and specific threats and applications quickly	Open based Application ID is a Cisco specific terminology, so request Railtel to remove this point from the specification. Pls refer - https://blogs.cisco.com/security/cisco-announces-openappid-the-next-open-source-game-changer-in-cybersecurity		As Per Tender Document and Corrigrndum- II	
7	SOR-A-3: UTM	SN No 5, point no 3, Page no 25	Should support safe search for YouTube EDU enforcement	Should support safe search	Request for the change.		As Per Tender Document and Corrigrndum- II	
8	SOR-A-3: UTM	SN No 6, point no 2, Page no 25	The solution must offer several deployment options: either via an internal forwarder, or pointing the forwarder of the existing authoritative DNS to the recursive service, or pointing the DNS configured on the Internal Proxy to the recursive service, without any additional physical hardware.	The solution must offer transparent deployment options without any dependency on existing DNS server.	Request for the change as the data is specific to Cico Umbrella - Pls refer https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella		As Per Tender Document and Corrigrndum- II	
9	SOR-A-3: UTM	SN No 6, point no 4, Page no 25	The solution must be able to protect at least from the following categories of malware: botnets, exploit kits, drive-by, phishing.	The solution must be able to protect at least from the following categories of malware: botnets, exploit kits, drive-by, phishing (from endpoints).	Normally phishing attacks are generated from endpoints, so request Railtel to specify the same.		As Per Tender Document and Corrigrndum- II	
10	SOR-A-3: UTM	SN No 6, point no 6, Page no 25	In order to allow the malware detection on a global scale, the network utilized to build the threat intelligence must process at least 80 billion DNS requests/day coming from at least 60 million daily users.	In order to allow the malware detection on a global scale, the network utilized to build the threat intelligence must process at least 80 billion DNS requests or IOCs/day coming from at least 60 million daily users or block 100 million unkown attacks/year.	Request for the change as the data are specific to Cisco. Pls refer - https://umbrella.cisco.com/blog/2016/12/14/cisco-umbrella-1-million/		As Per Tender Document and Corrigrndum- II	

11	SOR-A-3: UTM	SN No 6, point no 7, Page no 25	The analysis algorithms must make use multi-layer predictive detectors. As a mere example, these include (but are not limited to): § Analysis of DNS co-occurrences, § Analysis of Domains based on Natural Language Processing algorithms. § Detection of DGA via perplexity and entropy. § Detection of DNS traffic peaks § Soundwave analysis applied to DNS traffic § BGP anomalies detection.	Pls delete this point	Pls delete this point as this is specific to Cisco Umrella. Pls refer - 1) https://docs.umbrella.com/investigate-api/docs/co-occurrences-for-a-domain 2)https://umbrella.cisco.com/blog/2015/03/05/nlp-apt-dns/ 3) https://docs.umbrella.com/investigate-ui/docs/dga-detection-system-1 4)https://umbrella.cisco.com/blog/2015/11/19/opendns-cracks-predictive-security/		As Per Tender Document and Corrigrndum- II
11	SOR-A-3: UTM	SN No 6, point no 8, Page no 25	The solution should support ability to enforce Web filtering policies, based on 62 categories. It must be possible to enforce the Web filtering policy independently form the security policy.	Pls delete this point	This point is repeating to point no SN No 5, point no 2, Page no 25. Request Railtel to delete this point.		As Per Tender Document and Corrigrndum- II
12	SOR-A-3: UTM	SN No 6, point no 9, Page no 25	The solution must have ability to Protect against phishing threats automatically leveraging global network data and predictive intelligence to discover internet infrastructure used to host phishing sites.	The solution must have ability to Protect against phishing threats automatically leveraging global network data and predictive intelligence to discover internet infrastructure used to host phishing sites. **This point is included in Advance Endpoint specification (page 32).**	Normally phishing attacks are generated from endpoints, so request Railtel to change and include this point in the endpoint protection specification.		As Per Tender Document and Corrigrndum- II
13	SOR-A-3: UTM	SN No 6, point no 10, Page no 25	The network used to deliver the DNS security service must have experienced an uptime of at least 99.9% over the last 10 years.	The network used to deliver the DNS security service must have experienced an uptime of at least 99.9% over the last 5 years.	Request change.		As Per Tender Document and Corrigrndum- II
14	SOR-A-3: UTM	SN No 6, point no 11, Page no 25	The solution must have ability to block over 200 apps and automatically enable app settings and policy configuration.	Pls delete this point	This point is repeating to point no SN No 4, point no 10, Page no 23. Request Railtel to delete this point.		As Per Tender Document and Corrigrndum- II
15	SOR-A-3: UTM	SN No 7, point no 3, Page no 26	The management platform must be able to store record of 15000 user or more	The management platform must have 1 x 2TB hot swap HDD and 32 GB RAM from day 1.	Pls mention the storage requirement.		As Per Tender Document and Corrigrndum- II
16	SOR-A-3: UTM	SN No 7, point no 5, Page no 26	The management platform must domain multi-domain management	Pls delete this point	Request change.		As Per Tender Document and Corrigrndum- II
17	SOR-A-3: UTM	SN No D, point no 10, Page no 33	Software footprint should be small <50MB and should support interactive and/or silent install. Total of 50000 Licenses should be factored for this End Points. Solution should have concurrent capacity for 2000 endpoints out of 50000 endpoint users from day one with scaling upto 50000 concurrent end point endpoints.	Software footprint should be small <50MB and should support interactive and/or silent install. Total of 50000 Licenses should be factored for this End Points.	Request change, as number of endpoints has to be mentioned from day 1 and there is no concurrence of license which can be factored in endpoint security licensing scheme.		As Per Tender Document and Corrigrndum- II

18	SOR-A-3: UTM	SN No D, point no 27, Page no 33	The solution shall be capable of working in Windows, Windows Server &Linux operating systems	The solution shall be capable of working in Windows operating systems	Request change, since the solution is primarily focused on protecting endpoints.		As Per Tender Document and Corrigrndum- II	
19	SOR-A-3: UTM	SN No D, point no 28, Page no 33	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	Pls delete this point	Request change.		As Per Tender Document and Corrigrndum- II	
20	SOR-A-3: UTM	SN No D, point no 30, Page no 33	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	The proposed solution should utilize network sandboxing for protecting against zero day attacks/malwares.	Request change, since the solution should leverage on network sandboxing for preventing unknown and zero day threats. This has also been mentioned in point no 1.		As Per Tender Document and Corrigrndum- II	