Nokia Clarification

S.No	Tender Clause and page number	Clause description	Modification required	Justification
1	a) CGNAT Gateway , clasue no:27 Page no: 20	CGN should have capabilities extracted the information such as user/MSISDN from RADIUS accounting messages and inserted into logs and exporting them to a system logging server, as well as providing load balancing and UDP monitoring of high-speed logging servers.	Mapping of username/MSISDN to NAT flow logs is function of logging server correlation engine . Please relax this clause for CGN device , username to flow correlation should be requirment on the logging server	standard NAT flow logs data does not have field for username . All large scale deployments use NAT flow logging server for this correlation.
2	a) CGNAT Gateway , clasue no:14 Page no: 18	Platform shall support high availability using active passive and active-active setup	Please clarify if 1+1 chassis redundancy is required at each site or intra chassis redundancy at line card and controller is ok . SOR has mention of only single chassis per site.	1+1 chassis will increase the over all capex & space/power requirement of the project . Chassis failure rate is very less , 1+1 chassis redundacy is required only in case of georedundant DC & DR sites .
3	a) CGNAT Gateway , clasue no:15 Page no: 18	Failover shall support stateful session mirroring to ensure that in case of active unit failure the system can handle the active connections seamlessly without interruption	Please clarify if 1+1 chassis redundancy is required at each site or intra chassis redundancy at line card & controller level is ok . SOR has mention of only single chassis per site. We request to modify this clause as "CGN device must support redundancy with minimum 600k NAT session setup rate to ensure minimum disruption." Request is to relax Statefull session mirroring for active unit failure case.	With high setup rate (600k sessions per second) and with given redundancies, 99.999% availability can be achieved. further it is also needed to configure same IP Address pool on both devices and the convergence in case of chassis failure also involve routing convergence which is depends on other network components . So session mirroring will not result in immediate traffic shift.
4	a) CGNAT Gateway , clasue no:28(iv) Page no: 20	Solution shall be able to provide the web filtering and security function for HTTP and HTTPS traffic	Please relax the web filtering for HTTPs only at domain level . Clause should be modified as " Web filteriing and security function for URL/URI level for HTTP and URL level for HTTPs .	HTTPs traffic is encrypted and it not possible to decrypt use traffic on ISP gateway .
5	a) CGNAT Gateway , clasue no:28(Vii) Page no: 20	Solution shall have the capability to inspects all incoming and outgoing traffic, using a real-time Anti-Virus inspection .	Please restict the scope to URL filtering only . Anti-virus inspection would require a complete IDS/IPS system which is a separate solution .	Anti-virus inspection should be implemented centerally at ISP gateway level . IDS/IPS at each Wi-Fi gateway will add to overall capex of the project.

Inspira Clarifications

1	11.2.5, pg 37	The tenderer should present at least one (1) project worth at least INR 1.25 Crores showcasing supply, design, installation, testing, commissioning, implementation of WI-FI Gateway/BNG/BRAS and operations projects for WI-FI Gateway solutions commercially in India in the last 3 years.	The tenderer should present at least one (1) project worth at least INR 1.25 Crores showcasing supply, design, installation, testing, commissioning, implementation of WI-FI Gateway/BNG/BRAS/ Routers and operations projects for WI-FI Gateway solutions/ Routing solution commercially in India in the last 3 years.	All wifi gateways, BNG, BRAS are working on Routing profile with routing as core part, Request to please consider Routing experience as well.

2	11.1.2, Pg 46	The Tenderer/bidder should have supplied and provision of similar offered security/WI-FI Gateway solution with satisfactory working as to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.	The Tenderer/bidder should have supplied and provision of similar offered security/WI-FI Gateway/ Routing solution with satisfactory working as to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.	All wifi gateways are working on Routing profile with routing as core part, Request to please consider Routing experience as well.
3	1.2.5, pg 46	The tenderer should present at least one (1) project worth at least INR 1.25 Crores showcasing supply, design, installation, `testing, commissioning, implementation and operations projects for Wi-Fi Gateway solutions commercially in India in the last 2 years.	The tenderer should present at least one (1) project worth at least INR 1.25 Crores showcasing supply, design, installation, `testing, commissioning, implementation and operations projects for Wi-Fi Gateway solutions / Routing solutions commercially in India in the last 2 years.	All wifi gateways are working on Routing profile with routing as core part, Request to please consider Routing experience as well.
4	a) CGNAT Gateway , clasue no:27	CGN should have capabilities extracted the information such as user/MSISDN from RADIUS accounting messages	Mapping of username/MSISDN to NAT flow logs is function of logging server correlation engine .	standard NAT flow logs data does not have field for username . All large scale deployments use NAT flow
5	a) CGNAT Gateway , clasue no:14 Page no: 18	Platform shall support high availability using active passive and active-active setup	Please clarify if 1+1 chassis redundancy is required at each site or intra chassis redundancy at line card and controller is ok . SOR has mention of only single chassis per site.	1+1 chassis will increase the over all capex & space/power requirement of the project . Chassis failure rate is very less , 1+1 chassis redundacy is required only in case of georedundant DC & DR sites .
6	a) CGNAT Gateway , clasue no:15 Page no: 18	Failover shall support stateful session mirroring to ensure that in case of active unit failure the system can handle the active connections seamlessly without interruption	Please clarify if 1+1 chassis redundancy is required at each site or intra chassis redundancy at line card & controller level is ok . SOR has mention of only single chassis per site. We request to modify	With high setup rate (600k sessions per second) and with given redundancies, 99.999% availability can be achieved. further it is also needed to configure same IP Address pool on both devices and the convergence
7	a) CGNAT Gateway , clasue no:28(iv) Page no: 20	Solution shall be able to provide the web filtering and security function for HTTP and HTTPS traffic	Please relax the web filtering for HTTPs only at domain level . Clause should be modified as " Web filteriing and security function for URL/URI level	HTTPs traffic is encrypted and it not possible to decrypt use traffic on ISP gateway .
8	a) CGNAT Gateway , clasue no:28(Vii) Page no: 20	Solution shall have the capability to inspects all incoming and outgoing traffic, using a real-time Anti-Virus inspection .	Please restict the scope to URL filtering only . Anti-virus inspection would require a complete IDS/IPS system which is a separate solution .	Anti-virus inspection should be implemented centerally at ISP gateway level . IDS/IPS at each Wi-Fi gateway will add to overall capex of the project.

FORTINET Clarifications

5	Platform shall be able to handle at least 500K new connections per second	It is requested to reduce the connections per second to 400K in order to allow other leading OEMs to participate	Considering 20 Million concurrent connections, 500K connections per second is very high. Request to reduce it to 300 - 400K in order to have parity with concurrent connections required in rfp.
7	Proposed platform shall have dual redundant DC power supply	Today mostly all leading CGNAT / Firewall solutions which can cater to the RFP requirement are available with hot swappable redundant AC power supplies. Request you to please give option of AC or DC power supplies to allow more participation	This will allow more participation from Gartner listed leading security OEMs

A10 Networks

Solution shall have the capability to inspects all incoming and outgoing traffic, using a real-time Anti-Virus inspection .	Gateway level antivirus is deployed offline in ISP's as not all the traffic needs to pass through it, it integrates with inline devices using ICAP protocol.	We recommend to modify the clause to "URL filtering device must support ICAP integration with gateway level security devices such as Antivirus and DLP"

ERICSSON				
Chapter – 2	-	Schedule of Requirement	CGNAT is not mentioned in the SOR, please clarify.	-
a) CGNAT Gateway	28 (vii)	Solution shall have the capability to inspects all incoming and outgoing traffic, using a real-time Anti-Virus inspection.	Gateway level antivirus is deployed offline in ISP's as not all the traffic needs to pass through it, it integrates with inline devices using ICAP protocol.	We recommend to modify the clause to "URL filtering device must support ICAP integration with gateway level security devices such as Antivirus and DLP"
b) Wi-Fi Access GATEWAY Specification	iv	-	We understand that redundant Supervisor Engine is not required, since GeoRedundancy is already asked to take care of box failure. Please confirm.	Controller card and power supply redundancy needed. Line card redundancy not required

INVENTUM	
1	NAT64 in the network scenarios required by Railtel would necessitate use of a DNS64 server. Is the supply of this server part of this tender in the CGNAT?
2	The CGNAT unit will not be doing user authentication. Please confirm.
3	Tender clause 23.w : If the CGNAT unit is not doing user authentication, then can we assume that the definition of a subscriber is a unique IPv6/IPv4 address?
4	The Web filtering module specifies that it may be used in bridge mode. However deployment of CGNAT itself means it’s a routed unit. How would a bridge mode work in this case?
5	AV Scanning - please specify what ports and protocols are expected to be scanned?
6	Syslog server monitoring - please specify ways since Syslog uses UDP and has no confirmation mode.
7	Tender clause #20 - Please specify what RFC does the “IPv4 to IPv6 conversion" refer to?
8	Tender clause #27 - Will this be implemented using copy accounting where a specific set of RADIUS servers forward accounting data to CGNAT unit or does the CGNAT unit have to dissect