RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking)

Registered & Corporate Office:

Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

Selection of Partner For

“IT Services to RCIL Customer”

EOI No: RCIL/EOI/CO/ITP/2023-24/IT services to RCIL customer/07 dated 06.10.23

EOI NOTICE

RailTel Corporation of India Limited Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

EOI No: RCIL/EOI/CO/ITP/2023-24/IT services to RCIL customer/07 Dated 06.10.2023

RailTel Corporation of India Ltd., (here after referred to as RailTel) invites EOIs from RailTel's Empaneled Partners for the selection of suitable agency for "IT Services to RCIL Customer".

The details are as under:

1	Last date for submission of EOIs by bidders	12.10.2023 before15:00Hrs.
2	Opening of bidder EOIs	12.10.2023 at 15:30Hrs.
3	Earnest Money Deposit (EMD)	Rs. 5 Lakh
4	Number of copies to be submitted for scope of work	01 in Hard Copy

Prospective bidders are required to direct all communications related to this Invitation for EoI document, through the following Nominated Point of Contact persons:

Contact: Naresh Kumar
Position: DGM/IT
Email: naresh.kumar@railtelindia.com Telephone:
+91124 2714000 Ext 2222

NOTE:

I. **All firms are required to submit hard copy of their EOI submissions, duly signed by Authorized Signatories.**

II. **The EOI response is invited from empanelled partners of RailTel. Only RailTel empanelled partners are eligible for participation in EOI process.**

1. RailTel Corporation of India Limited–Introduction

RailTel Corporation of India Limited (RCIL), an ISO-9001:2000 organization is a Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control Operation and Safety System of Indian Railways and to contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

For ensuring efficient administration across India, country has been divided into four regions namely, Eastern, Northern, Southern & Western each headed by Regional General Managers and Headquartered at Kolkata, New Delhi, Secunderabad & Mumbai respectively. These regions are further divided into territories for efficient working. RailTel has territorial offices at Guwahati, & Bhubaneswar in East, Chandigarh, Jaipur, Lucknow in North, Chennai & Bangalore in South, Bhopal, and Pune & Ahmedabad in West. Various other territorial offices across the country are proposed to be created shortly.

RailTel's business service lines can be categorized into three heads namely B2G/B2B (Business to Government and Business to Business) and B2C (Business to customers):

Licenses & Services

Presently, RailTel holds IP-1, NLD and ISP (Class-A) licenses under which the following services are being offered to various customers:

CARRIER SERVICES

1. National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
2. Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
3. Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
4. Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

ENTERPRISE SERVICES

1. Managed Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
2. MPLS VPN: Layer-2 & Layer-3 VPN available for granularities from 64 Kbps to nx64 Kbps, 2 Mbps& above
3. Dedicated Internet Bandwidth: Experience the "Always ON" internet connectivity at your fingertips in granularities 2mbps to 155mbps

RETAIL SERVICES

RailWire: RailWire is the retail broadband service of RailTel. RailWire is a collaborative public private local entrepreneur (PPLE) model providing broadband services by leveraging the eco system available with different partners like RailTel, Access Network Provider, Aggregation Network Provider (AGNP) and Managed Service Provider (MSP) to offer high speed & cost-effective broadband to end customers. The model uses RailTel's nationwide Core fiber Backbone Network, Access Network available with Local entrepreneurs, FTTH Infrastructure providers etc. and Managed Service Partners/Application Service Providers having IT & management capabilities. The model has been tested for several years now with about 4 lakh+ home broadband users along with 5200+ local access network partners. It is noteworthy that this approach whereby about 54% of the revenue is ploughed back into the local community not only serves the underserved but also creates livelihoods and jobs in the local communities.

2. Objective of EOI

RCIL is implementing IT-ICT projects like providing Infra & Cloud Services, Application Development, ERP/E-Office Implementation and Consultancy Services for its customers. There is requirement of providing ICT Infra Items supply , installation and support for one of RCIL's government customer. RailTel will obtain best Rates from its empanelled partner and will submit a techno-commercial proposal to its customer by adding RailTel margin .If RCIL receive PO from customer RailTel may issue the purchase order to its selected partner on back to back basis.

3. Scope of Work

The vendor is required to provide SITC of Infra , operation & maintenance and one time migration for RCIL Customer as per SOR. Technical details are provided in EOI as under :

a) Annexure-II (Proposed SAP Migration)

b) Annexure-III (Scope of work for SAP Infra Help Desk)

c) Annexure-IV (Minimum technical specification for Items in SOR)

d) Annexure-V (Current DC & DR Architecture)

e) Annexure-VI (DC infra deployment)

f) Annexure-VII (DR infra deployment)

g) Annexure-VIII (BoM for NewGen)

4. Language of Proposals

The proposal and all correspondence and documents shall be written in English. The hardcopy version will be considered as the official proposal.

5. Proposal Preparation and Submission

The Applicant/bidder is responsible for all costs incurred in connection with participation in this EOI process, including, but not limited to, cost incurred in conduct of informative and other diligence activities, participation in meetings/ discussions/presentations, preparationof proposal, in providing any additional information required by RCIL to facilitate the evaluation process or all such activities related to the EOI response process. RCIL will in nocase be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

6. Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the bidder's risk and may result in rejection of its bid without any further reference to the bidder.

All pages of the documents shall be signed in by the bidder including the closing page in token of his having studied the EOI document and should be submitted along with the bid.

7. Payment terms

7.1. All payment terms shall be in accordance with agreement between RailTel and Customer.

7.2. RailTel will make payment to selected firm after receiving payment from customer and on submission of Tax invoice by Firm to RailTel.

7.3. Any penalty/deduction made by customer shall be passed on to the selected firm on proportionate basis.

7.4. Escalation (if any) shall be applicable every year to cover inflation and other associated costs as per agreement between RailTel and Customer and after approval from Railtel's Competent Authority.

8. Schedule of Rates (SOR)

SOR A : Infra SITC (all items with 3 years warranty/support)

S. No.	Item Description	Qty	Unit Rate	Total Rate	GST on Total Rate	Total Rate with GST
1	Server	10				
2	Storage 100 TB	1				

3	Suse	135				
4	Windows CAL for AD	2				
5	Windows Server	30				
6	Vsphere	40				
7	Ve Center	2				
8	Backup	1				
9	Management Switch	4				
10	Leaf Switch	2				
11	NewGen Licenses up-gradation cost (one time) as per BoM in Annexure VIII	LS				
12	ATS for NewGen licenses (per year charges)	3				
13	AMC for NewGen licenses (per year charges)	3				
14	NewGen App migration one time cost	LS				
15	Zimbra mail solution licenses upgradation cost (one time)	LS				
16	Annual technical support charges for zimbra mail solution (per year charges)	3				
17	Cable and accessories for installation	LS				
18	**SOR Total**					

Amount in words : ____

***Note: The minimum specification of all items listed above is provided under Annexure-IV**

9. Qualification for Participation

9.1. The Applicant should be an empanelled RailTel partner having a valid Permanent Account Number (PAN), Goods and Service Tax Identification Number (GSTIN). Copy of documents in this regard is to be submitted.

9.2. The Applicant should not be black listed during last three years by any State / Central Government / PSU / Autonomous Body as on the last date of EOI submission. A Self-Declaration on letter head is to be submitted in this regard.

9.3. There should not be any ongoing or past, arbitration case(s) between RCIL and Applicant on the last date of submission of EOI. Self-Declaration on letter head is to be submitted in this regard.

9.4. Bidder should have authorization from OEM VMware and NewGen for participating in this EOI. Proof of same is required to be submitted.

10. Evaluation criteria

Only technical qualified bidder will be eligible for opening the financial bid . Based on the lowest price offered under financial bid as mention under clause no 9 by the technical eligible bidder, L1 will be selected. If required, the L1 bidder may be called for negotiation. A Tender Committee would be carrying out the evaluations. RCIL shall evaluate the responses to this EOI and scrutinize the supporting documents / documentary evidence. Inability to submit the requisite supporting documents / documentary evidence, may lead to rejection. The decision of RCIL in the evaluation of EOI responses shall be final. During the EOI response evaluation, RCIL reserves the right to reject any or all the EOI responses.

11. Bidding Process

The bidder needs to submit the bid in sealed, signed and stamped envelope clearly mentioning of EOI number, EOI name, addressed to the EOI inviting officer as well as Bidding Agency Name and Contact person.

Packet I - Technical BID should consist the following:

1. Covering Letter
2. EMD fee through online transfer in RailTel bank account or DD
3. Signed and Stamped EOI Document
4. RailTel’s Empanelment letter/LOI
5. GST and PAN documents
6. Self Undertaking as per clause No. 25.1 and clause 25.2
7. Duly filled Annexure-I
8. Deviation statement and Clause wise compliance sheet (clause No.-22)
9. Self Declaration of Non Blacklisting as per Clause 9.2
10. Self Declaration of No past / ongoing arbitration with RCIL as per Clause 9.3
11. Authorization from OEM as per Clause 9.4
12. Format for Providing Bidder’s Information – Clause 21.
13. Any other relevant documents

Packet II - Financial BID as per Clause 8

1. Submission of Duly filled SOR as per Clause Number 8.

Both the Packets i.e. Packet – I and Packet – II should be separately put in a common Envelope. The envelope also needs to be sealed, signed and stamped clearly mentioning of EOI number, EOI name, addressed to the EOI inviting officer as well as Bidding Agency Name and Contact person.

12. Period of Validity of bids and Bid Currency

Bids shall remain valid for a period of 180 days from the date of issue of Customer PO to RailTel. The prices in the bid document to be expressed in INR only.

13. RCIL's Right to Accept/Reject Bids

RCIL reserves the right to accept or reject any bid and annul the bidding process or even reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or without any obligation to inform the affected bidder or bidders about the grounds for RailTel's action.

14. Earnest Money Deposit (EMD)/ Bid Security

14.1. The bidder shall furnish a sum as Earnest Money in the form of online transfer or Demand Draft from any scheduled bank in India in favour of "RailTel Corporation of India Limited" payable at New Delhi. RailTel Bank details for online EMD amount payment is as under:

Account No. 340601010050446
IFSC: UBIN0534064
Name: RailTel CO Collection A/c
Bank: Union Bank of India

14.2. The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the Purchase order and fails to furnish performance bank guarantee (security deposit) in accordance with clause 6.

14.3. Offers not accompanied with Earnest Money shall be summarily rejected.

14.4. Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible as but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

14.5. The successful bidder's EMD will be discharged upon the bidder's acceptance of the purchase order satisfactorily and furnishing the performance bank guarantee in accordance with clause 7.

14.6. Earnest Money will bear no interest.

15. Security Deposit / Performance Bank Guarantee (PBG)

15.1. In case RCIL submits PBG to its Customer then Successful bidder has to furnish security deposit in the form of Performance Bank guarantee (with same %age as mentioned in agreement with RailTel and its customer) of issued PO/ LOA value, the same should be submitted within 30 days of issue of LOA/PO, failing which a penal interest of 15% per annum shall be charged for the delay period i.e. beyond 30 (thirty) days from the date of issue of LOA/PO. This PBG should be from a Scheduled Bank and should cover warranty period plus three months for lodging the claim. The performance Bank Guarantee will be discharged by the Purchaser after completion of the supplier's performance obligations including any warranty obligations under the contract. The claim expiry of PBG shall be one year after PBG validity.

15.2. The Performa for PBG is given in Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately.

15.3. The security deposit/PBG shall be submitted to Corporate Office & will bear no interest.

15.4. A separate advice of the BG will invariably be sent by the BG issuing bank to the RailTel’s Bank through SFMS and only after this the BG will become acceptable to RailTel. It is therefore in interest of bidder to obtain RailTel’s Bank IFSC code, its branch and address and advise these particulars to the BG Issuing bank and request them to send advice of BG through SFMS to the RailTel’s Bank.

15.5. The security deposit/Performance Bank Guarantee shall be released after successful completion of Contract, duly adjusting any dues recoverable from the successful tenderer. Security Deposit in the form of DD/Pay Order should be submitted in the favour of “RailTel Corporation of India Limited” payable at New Delhi Only.

15.6. Any performance security upto a value of Rs. 5 Lakhs is to be submitted through DD/Pay order / online transfer only.

16. Deadline for Submission of Bids

Bids must be submitted to RCIL at the address specified in the EOI document not later than the specified date and time mentioned. If the specified date of submission of bids being declared a holiday for RCIL, the bids will be received up to the specified time in the next working day.

17. Late Bids

Any bid received by RCIL after the deadline for submission of bids will be rejected and/or returned unopened to the bidder.

18. Modification and/or Withdrawal of Bids

Bids once submitted will treated as final and no modification will be permitted. No correspondence in this regard will be entertained. No bidder shall be allowed to withdraw the bid after the deadline for submission of bids. In case of the successful bidder, he will not be allowed to withdraw or back out from the bid commitments.

19. Clarification of Bids

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the bidder for clarification. The response should be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

20. Variation in Contract

+/-50% variation may be operated on SOR or relevant items during the period of Project

Schedule with the approval of competent authority with similar terms and procedure as specified in the agreement.

In case of additional requirement under customer project for similar items as mentioned under clause number 8 “SOR”, RailTel may place additional purchase order to selected bidder with same commercials and terms & conditions. In case of additional requirement from customer for any sub item under SOR during contract period, additional PO can be issued to selected bidder as per customer requirement and after approval of RailTel competent authority.

21. Bidder’s Information

Company Name:	
Type of RCIL Business Partner	
Status of Applicant (Partnership, Company etc.)	
Number of Years of Experience	
Number of office locations in India (Provide details)	
Number of office locations globally (Provide details)	
Number of employees in India and global	

CONTACT DETAILS:			
First Name		Last Name	
Designation			
Address for correspondence			
Contact Number (Office Landline)			
Mobile Number			
Official Email ID			
GSTN No			
PAN No			
Bank Account No			
IFSC Code			

Registered Address of Company	

22. Format for statement of Deviation/Compliance

The following are the particulars of deviations from the requirements of the Instructions to bidders:

SN	CLAUSE No.	Deviation (NIL or Yes)	REMARKS (Including Justification for deviation)	Fully Complied (Yes or No)

Note: In case of no deviation, bidder shall fill up above format with NIL deviation and submit along with Bid document.

23. Period of Association/Validity of Agreement

The initial contract period shall be for the period of 3 years from commissioning of project, however the contract period can be terminated earlier or extended further based on requirement of customer on same terms and conditions and as per approval of RailTel competent authority.

24. Special Terms and conditions

24.1. Selected firm will Provide O&M after successful commission of Appliance, hardware & software items initially for the period of three years which can be further extended as per requirement from RailTel's Customer.

24.2. The items number (1 to 10) mentioned under "SOR", shall be property of RailTel. During contract period, selected bidder shall have not any claim to the hardware/software procured against the SOR items.

24.3. **Delivery Timelines:** 06-08 Weeks from the date of placing Work Order.

25. Preference to make in India:

The provisions of the revised "Public Procurement (Preference to Make in India) Order 2017" dated. 15.06.2017 & dated 16.09.2020 (or subsequent revisions, if any till opening of tender) by Department of Promotion of Industry and Internal Trade (DPIIT), GoI shall apply to this tender.

25.1. Local Content:

i. Only Class-I local suppliers (meeting minimum 50% local content) & Class-II local suppliers (meeting minimum 20% local content) are eligible to participate in this EOI.

ii. Minimum Local Content shall be 50% for purchase preference or as per the Notification No. 18-

10/2017-IP dated 29th August 2018 issued by Department of Telecommunications, Ministry of Communications and Notification No. 33(1)/2017-IPHW dated 14.09.2017issued by MeitY or latest notification issued till opening of tender.

iii. Among all qualified bids, the lowest bid will be termed as L1. If L1 is Class-I local supplier, the contract will be awarded to L1. If L1 is not Class-I local supplier, the lowest bidder among the Class-I local supplier, will be invited to match the L1 price subject to local supplier's quote price falling with in the margin of purchase preference of 20%, and the contract shall be awarded to such Class-I local supplier subject to matching the L1 price. In case such lowest eligible Class-I local supplier fails to match the L1 price, the Class-I local supplier with the next higher bid within the margin of purchase preference of 20%, shall be invited to match the L1 price and so on and contract shall be awarded accordingly. In case none of the Class-I local supplier within the margin of purchase preference of 20%, matches the L1 price, the contract may be awarded to the L1 bidder. Please refer clause-4.A.41.1 of Chapter-4Aof this tender.

iv. As per para 9 of PPP-MIII order 16.09.2020, bidder shall be required to indicate percentage of local content and provide self-certification in his bid (without mention of any price) that the item offered meets the local content requirement for Class-I/Class-II local supplier, as the case may be and shall also give details of the location(s) at which the local value addition is made. In case of procurement for a value in excess of Rs. 10 Crores, the bidder shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. Bidder shall upload the certificate along with their techno-commercial bid. The bidder shall also provide calculation of Local Content with price Break-up of "Local Content" and "Imported Content" for each SOR item as per DPIIT's PMI Policy and its clarifications and same shall be uploaded by the bidder along with their price bid. In case of any false declaration, action shall be taken in line with the provisions of the PPP-MIII order. Performa for self-certification regarding local content is given in the Notification No. 18-10/2017-IP dated 29th August 2018 issued by Department of Telecommunications.

v. Self-certification of bidder on the letter head shall be required to be submitted along with bid. "We____ (name of the bidder) hereby certify to meet the mandatory Local Content requirements of the Project Work under this EOI i.e. _% (to be filled by the work center) quoted vide offer No.__ dated__ against RAILTEL EOI No.__ by M/s. __ (Name of the bidder).

vi. Office Memorandum Dated 19.02.2020 (or latest) issued by Department of Telecommunications, Ministry of Communications shall be applicable for Clause 10(d) of Public Procurement (Preference to Make in India) Order, 2017.

vii. Official website of Department of Promotion of Industry and Internal Trade (DPIIT) i.e."https://dpiit.gov.in/public-procurements" may be referred by tenderers for above mentioned orders or any revision issued. Frequently Asked Question (FAQ) available there may also be referred by tenderers

25.2. **Bidders sharing a land border with India:**

Office Memorandum F.No.6/18/2019-PPD dated 23.07.2020 by Ministry of Finance, Department of Expenditure, Public Procurement Division shall also apply to this EOI. A certificate as per Annexure-I of referred order shall be submitted by all the bidders regarding their compliance with this order. If such certificate given by a bidder whose bid is accepted is found to be false, this would be a ground for immediate termination and further legal action in accordance with law. Registration should be valid at the time of submission of bids and at the time of acceptance of bids. In respect of supply otherwise than by tender, registration should be valid at the time of placement of order

26. Other Terms and Condition

1. Bidders are requested to quote their best prices.
2. Unless otherwise specified all prices quoted must remain firm except for statutory variation in taxes and duties during contractual delivery period. Any increase in taxes and duties after expiry of the delivery period will be to vendor account.
3. Offer should preferably be typewritten and any correction or over- writing should be initialed. Rates to be indicated both in words and figures.
4. Sealed offer in envelope super scribing tender enquiry number and due date of opening must be sent by Registered or Speed Post or to be dropped in the Tender Box specified for the purpose. Offers received after specified date and time are liable to be rejected.
5. Offer should be valid for a minimum period of 180 days from the date of issue of Customer PO to RailTel.
6. Printed conditions on the back side of the offers will be ignored.
7. Any increase in taxes and duties after expiry of the delivery period will be to supplier's account. This will be without prejudice to the rights of RCIL for any other action including termination.
8. RCIL shall have the right to terminate the contract by giving 30 days notice without assigning any reasons thereof. However, in the event of any breach of terms of the contract, RCIL will have right to terminate the contract by written notice to the Seller.
9. FORCE MAJEURE: Any delay or failure to perform the contract by either party caused by acts of God or acts of Government or any direction or restriction imposed by Government of India which may affect the contract or the public enemy or contingencies like strikes, riots etc. shall not be considered as default for the performance of the contract or give rise to any claim for damage. Within 7 days of occurrence and cessation of the event(s), the other party shall be notified. Only those events of force majeure which impedes the execution of the contract at the time of its occurrence shall be taken into cognizance.
10. In case of any dispute or difference arising out of the contract which cannot be resolved mutually between RCIL and vendor, it shall be referred to a Sole Arbitrator to be appointed by the CMD, RCIL.
11. The Arbitration and Conciliation Act, 1996 and rules made there under shall apply to the Arbitration Proceedings.
12. The contract shall be governed by and construed according to the laws in force in India and subject to exclusive jurisdiction of the Courts of Delhi only.
13. RCIL may place the order in full or partial manner based on customer requirement.
14. Joint ventures and consortiums are not allowed.

27. Format for COVERING LETTER

COVERING LETTER (To be on company letter head)

EoI Reference No: RCIL/EOI/CO/ITP/2023-24/IT services to RCIL customer/07 dated 06.10.23

Date:

To,

DGM/IT
RailTel Corporation of India Ltd.
Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar,
New Delhi 110023

Dear Sir,

SUB: Participation in the EoI Process

Having examined the Invitation for EoI document bearing the reference number _______________ released

by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document. I/We also agree to keep this offer open for acceptance for a period of 180 days from the date of issue of Customer PO to RailTel and in default thereof,

If our application is accepted, we undertake to abide by all the terms and conditions mentioned in the said Invitation for EoI document.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Invitation for EoI document, are true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our EoI is liable to be rejected.

Authorized Signatory
Name
Designation
Contact Details

28. Proforma for Performance Bank Guarantee Bond

Form No. 1

PROFORMA FOR PERFORMANCE BANK GUARANTEE BOND
(On Stamp Paper of Rs one hundred)

(To be used by approved Scheduled Banks)

1. In consideration of the RailTel Corporation of India Limited, having its registered office at Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023 having agreed to exempt ……………………………………………………………(Hereinafter called “the said Contractor(s)”) from the demand, under the terms and conditions of an Purchase Order No.………………………………dated……………made between……………………………and…………………………………….. for (hereinafter called “ the said Agreement”) of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs. ……………………….(Rs ………….. only). We ……………………………… (indicate the name of the Bank) hereinafter referred to as “the Bank”) at the request of……………………….……. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs……………..…. against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, …………………………………………………………. Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs . ………………………

3. We, ……………………………………….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Tenderer(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Tenderer(s) shall have no claim against us for making such payment.

4. We, ………………………………………… Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the …………… We shall be discharged from all liability under this Guarantee thereafter.

5. We,………………………………………… (indicate the name of Bank) further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) / Tenderer(s).

(indicate the name of Bank) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

…………the day of 2021

for ………………………………………………..
(indicate the name of the Bank)

Witness

1. Signature Name

2. Signature Name

Note: Claim Period of BG will be 365 days more than the BG Validity date.

RailTel Bank Detail for SFMS:

- To mandatorily send the Cover message at the time of BG issuance.
- IFSC Code of ICICI Bank to be used **(ICIC0000007)**.
- Mention the unique reference(**RAILTEL6103)**in field 7037

Annexure-I

Self Undertaking on Letter Head

DGM/IT, **Dated: …………….**
RailTel Corporation of India Ltd.
…………………………………
………………………………....
………………………………....

Sub: Undertaking

Ref: EOI No…….………………..dated………………

Dear Sir,

Over and above all our earlier conformations and submissions as per your requirements of the EOI, we confirm that,

A. I/We have not been black-listed or debarred currently by Central Govt./State Govt./CPSU in India or anywhere globally by Government for security reasons either in Individual capacity or as a member of partnership firm/LLP/JV/Society/Trust.

B. We Certify that,

(i) All proposed hardware and software components in scope of supplies when shipped by ________, does not contain embedded malicious code that would activate procedures to:-

a. Inhibit the desired and designed function of the equipment.
b. Cause physical damage to the user or equipment during the exploitation.
c. Tap information resident or transient in the equipment/networks.

(ii) We, ___________ will be considered to be in breach in case physical damage or malfunctioning is caused due to activation of any such malicious code in embedded software and thus be liable to repair, replace or refund the price of the infected software if reported (or, upon request, return) to the party supplying the software to Customer, if different than ________

(iii) Security breach or damages to system, if any, so caused by any embedded malicious code or otherwise, due to the act of either OEM or bidder or both, the OEM as well as the bidder would be considered liable jointly or severally and shall be banned for conducting any business with RailTel. Also the present contract, may liable to be terminated by the purchaser.

C. We certify that our offered products are genuine, have our own manufacturing setups and IPR for the hardware(s)/software(s), and not have 3rd party manufacturing from any company blacklisted in India or abroad (due to proven backdoor access and data vulnerability) or any company sharing land border with India. The Intellectual Property Rights (IPR) of all offered product and source code of all offered software including camera firmware, switch firmware etc. are not residing in countries sharing land borders with

India. Proof of IPR & source code will be provided by the OEM.

or

IPR of offered products and source code of offered software including camera firmware, switch firmware etc. are residing in ……………country (Please mention the country name) and OEM has been registered with the Competent Authority of Govt. of India and are eligible to be considered(evidence of valid registration by the competent authority is enclosed)

In case any breach or false declaration is found at any stage, immediate strict penal action can be taken by RailTel.

Seal and signature of the authorized representative of Bidder

Place:
Date:

Annexure-II

Proposed SAP system Migration - Classical Method (SAP system copy option)

- Tech Stack - ECC, CRM, SRM, BW, Java system, Sybase)
- Existing SAP Instance Detail
- Environment VM, s Clustered Non-Clustered OS
- Production 40 14 26 Suse Linux
- Dev 16 0 16 Suse Linux
- QA 11 0 11 Suse Linux

SOW

- Infrastructure and landscape assessment
- Design and develop Migration Solution Approach
- Develop Migration Test Plan
- Build and Deploy SBX Environments and Connectivity
- Build and Deploy Dev Environments and Connectivity
- Build and Deploy QA Environments and Connectivity
- Build Pod Environments and Connectivity
- Execute Mock Integration Test
- Pre-Go-Live Readiness Check
- Go Live and Support
- 4 Weeks of Hyper-Care Support
- Phase Wise Plan
- Phase 1 Pilot Project SAP Sandbox Build and system Migration
- Connection checks
- Testing
- Sign off and confirmation
- Phase 2 Migration Build and migration of Dev. QA and Production
- system
- Inclusion
- SAP Basics Support for Migration
- SAP system Build and data migration support
- DB support specific to Migration and SAP only

Annexure-III

Scope of work for SAP Infra Help desk

1 Operations and Maintenance of IT infrastructure.

2.1 Help Desk Services .

- The SI will depute staff who will be contactable via phone and mail to provide assistance to the Users and address their queries and concerns. This assistance will be provided during the Service Hours as per the location classification and responsibility matrix, which will be covered in the Operations Manual to be provided by System Integrator and duly approved by RVNL. During all other hours, users can leave their message via email. The requests received on email will be taken during the next working day. A proper escalation procedure, as mentioned in the duly approved Operational Manual, will be followed if the problem cannot be resolved. Shared resources of operational and technical support group will provide this service at all locations. The help desk service will serve as a single point of contact for all incidents and service requests. The service will provide a Single Point of Contact (SPOC) and also escalation / closure of incidents for the user departments. The Help desk services would be for Infrastructure Facility Management and Application support across all offices of RVNL. The activities shall include
  - Provide Help Desk facility during agreed service period window for reporting user department incidents / issues / problems with the IT infrastructure & ERP Application related issues.
  - Provide necessary channels for reporting issues to the help desk. The incident reporting channels could be specific email account and Telephone (toll Free)
  - Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.
  - Creation of knowledge base on frequently asked questions to assist users in resolving basic issues themselves.
  - Track each incident / call to resolution.
  - Provide feedback to callers.
  - Analyze the call statistics.
  - Creation of knowledge base on frequently asked questions to aid users.
  - Continuous monitoring of the physical as well as the IT infrastructure at the DC, CUSTOMER offices to ensure application availability as per agreed SLAs.
  - Monitoring shall be done with the help of and EMS monitoring tools and system logs/counters and therefore the reports and alerts can be auto-generated.
  - Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed between the System Integrator and the user department. The escalation matrix shall be developed by the System Integrator in discussion with RVNL.

- Analyze the incident / call statistics and provide monthly reports including but not limited to 1) Type of incidents / calls logged 2) Incidents / calls resolved 3) Incidents / calls open 4) Root Cause analysis For frequently occurring incidents.
- The System Integrator shall provide Help Desk facility during the working hours for reporting issues / problems with the IT infrastructure as well as Non IT components. The System Integrator shall provide a service desk facility and set up all necessary channels for reporting issues to help desk.
- Initiate a “Problem Management Record” or “PMR” to document service outages using a Problem Management System as stated in the approved Operational Manual.
- Update concerned Authority of CUSTOMER with complete and accurate system status. Notify RVNL’s designated personnel of systems or equipment failures, or of an emergency, according to the Operational Documentation.
- Maintain an updated on-line help-desk telephone number listing in the Escalation Matrix.
- Call tracking and closure.
- Problem escalation in case of service levels not adhered to.

- Provide detailed contact list of Help Desk Support to RVNL. Receive log and dispatch or transfer calls. Make the guidelines for prioritization of calls and escalation procedure for approval by RVNL. Prioritize problem calls as per the defined Severity Codes.
- Perform problem analysis and identify the problems.
- Arrange for on-site/off-site support for resolution of problem. Intimate concerned CUSTOMER Authority of all the emergencies and equipment failures. Resolve performance issues of third party vendors, if any. Maintain the escalation procedure and notify the concerned person(s) as per the contact list provided by RVNL. Shall be primarily responsible for resolving third party service provider (if any) performance issues. Provide monthly reports to CUSTOMER on calls handled by Help desk.

Annexure – IV

Minimum Technical Specification:

1. Server:

a. CPU Should be populated with 2 Nos. of latest generation Intel Xeon GOLD CPU, each CPU should be 48 core and 2.4 GHz or better.
b. Configured Memory should be at-least of 1.5 TB.
c. Should support VMware, vSphere & VSAN Enterprise Lic., RedHat cloud or Similar etc.
d. Platinum rated redundant Power Supply in 1+1 from day one.
e. SAP Certification: Server should be SAP HANA certified.
f. Chipset- Intel C620 series or higher.
g. Server should support Zero-touch repository manager and self-updating firmware system.
h. Should provide effective protection, reliable detection & rapid recovery using: - Hardware Root of Trust and Signed firmware updates.
i. 3 Years of onsite warranty and support.

2. Storage:

Existing Storage Model- Hitachi Vantara E1090
Requirement: Total 100 TB in DC & DR
Disk type may be considered as below:
a) 7.6 TB SSD Drive
b) 2.4 TB HDD SAS Drive

3. SUSE:

a) SUSE Linux Enterprise for SAP Licences with 3 years Warranty / Support.

4. Windows CAL for AD:

a) Windows Client Access License (CAL) as per requirement.

5. Windows server:

a) MS Windows Server latest version with 3 years of enterprise support License per 16 core.

6. Virtualization:

VSphere enterprise edition

7. Virtualization:

a) Vcenter enterprise edition

8. Storage with backup:

Existing Backup solution-
Hitachi Vantara E790 with Commvault backup tool

Indicative Requirement: 50 TB in DC and 50 TB in DR to provide backup of unlimited operating and database instances on existing backup solution.

9. Management Switch:

a) 48 ports 10/100/1000gb copper based managed switches for out of band management of all equipment within DC.

b) Switch should have 48 X 10/100/1000Base-T autosensing ports complying to IEEE 802.3, IEEE 802.3u and 802.3ab standard, supporting half duplex mode, full duplex mode and auto negotiation on each port with 4 x SFP+ uplink ports

c) Switch should support stacking with dedicated stacking ports whenever required in future. Stacking bandwidth should be min 80 Gbps with dedicated stacking ports.

d) Switch should support IPv4 and IPv6 from day One

e) Switch should have non-blocking switching fabric of minimum 488 Gbps or more and should have Forwarding rate of minimum 650 Mbps

f) Switch should support power supply redundancy.

10. Leaf Switch:

a) 48 x 1G/10G/25G Multi Mode Fiber Interface populated with 48*10G multi mode interfaces

b) 6 x 40G /100G ports fully populated using multimode 100G SR Transceivers, for uplink connectivity

c) Similar no. of 100G SR transceivers should be additional supplied for fabric controller/spine switch for uplink connectivity termination.

d) should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data centre.

e) Switch should support VXLAN routing

f) Switch and optics should be from the same OEM, Proposed Leaf switch is to be connect with RailTel’s existing Leaf-Spine architecture i.e., CISCO ACI.

g) Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.

11. NewGen:

Running Version	Current Version (for upgradation)
OmniDocs 8.1	Omnidocs 11

12. Zimbra Mail Solution:

a) License upgrade from existing Business Email+ edition to Professional edition.

b) Support and Subscription (including upgrade, update, patches etc) for the upgraded edition.

Annexure –V

Current DC & DR Architecture

1. Introduction

1.1. Overview

CUSTOMER intends to implement an Integrated IT solution to meet its business needs. The Integrated IT Solution for CUSTOMER would aim to automate its business functions and would include all the Project Implementing Units (PIUs) as well as corporate office.

Incumbent service provider is implementing an integrated IT solution for CUSTOMER comprising the following key applications:

- SAP based ERP system
- Document Management System
- Geographical Information System
- Video conferring Solution
- Email SystemThe solution will connect 21 project implementing offices (PIUs) of CUSTOMER from which employees will connect and use these applications.

As part of the solution, Incumbent service provider will set up the Data Center as a hosted facility in Noida and a cloud based DR site at Bangalore. Both the facilities MPLS/Internet Link will be offered through Sify and Vodafone (Service Provider).

1.2. Purpose of the document

The purpose of this document is to present a description of the components and the features of IT infrastructure deployed at the Data Center.

Based on the RFP received from CUSTOMER and our understanding CUSTOMER intends to implementintegrated IT solution and underlying IT Infrastructure for the same.

1.3. Implementation Sites

Following is the list of locations included as a part of the project as per RFP:

Location
Data Center (DC) – Noida
Disaster Recovery Site (DR) - Bangalore

Sr. No	PIU Location
1	Corporate Office/Delhi PIU
2	Secunderabad
3	Bhubaneswar
4	Raipur -1
5	Chennai
6	PIU Kolkata (Majerhat)
7	PIU Kolkata (Tollygunge)
8	Raipur
9	Bhopal – II
10	Jodhpur
11	Waltair
12	Kota
13	Lucknow
14	Kanpur
15	Rishikesh
16	Patna
17	Ahmedabad
18	Bangalore
19	Pune
20	Mumbai
21	PIU Kolkata (Kalighat)

2. Solution Details

2.1. Rack Diagram at the Data Center

RACK-01

U	Equipment Description	Make	Model	Serial No
42	Access Switch-01	Cisco	Nexus 5548	SSI185209AE
41	SAN Switch-01	Brocade	6520	CHQ2533L01G
40				
39				
38				
37				
36				
35				
34				
33	Directory Server & Domain Naming Server-01	CISCO	C240	FCH1917V1EQ
32				
31	Web Server-01	CISCO	C240	FCH1917V0C6
30				
29	Web Server-02	CISCO	C240	FCH1917V17A
28				
27	EMS Server -01	CISCO	C240	FCH1917V0XN
26				
25				
24				
23	Mbook-01	CISCO	C240	FCH1917V1H5
22				
21	GIS Server -01	CISCO	C240	FCH1917V1EN
20				
19	Mail Server -01	CISCO	C240	FCH1917V1ER
18				
17	Application Server 01	CISCO	C460	FCH1917V211
16				
15				
14				
13		CISCO	C460	FCH1929V11S

12	Reporting/Analytics Server-01			
11				
10				
9	Database server - 01	CISCO	C460	FCH1925V1XS
8				
7				
6				
5	DMS Server -01	CISCO	C460	FCH1928V0UJ
4				
3				
2				
1				

Rack-02

U	Equipment Description	Make	Model	Serial No
42	Access Switch-02	Cisco	Nexus 5548	SSI185209AJ
41	IPS/IDS-01	Radware	Defence Pro 2412	31411016
40				
39	External Firewall-01	Cisco	ASA 5585-X	JMX1924806T
38				
37	Internal Firewall-01	Cisco	ASA 5585-X	JMX1924806P
36				
35	Proxy Solution -01	Bluecoat	SG900	1515240015
34	Proxy Solution -AV-01	Bluecoat	AV1200	4313220073

33	Server Load Balancer - 01	Array	APV 2600T-S1	1537G8435
32	SSL VPN-01	Array	AG1100	1538G8470
31	Video conferencing Server (TelePresence-01)	Cisco	MCU 5320	FOC1917N9ST
30	WAN Router-01	Cisco	1002-X	FOX1906GH5Y
29				
28	FCIP router-01	Brocade	7800	ASS2534L009
27	Server Load Balancer - 02	Array	APV 2600T-S1	1537G8438
26	Internet Router-01	Cisco	2951	FGL194111CW
25				
24	Application Firewall-01	Palo Alto	5020	2501001765
23				
22	Core Switch-01	Cisco	Nexus 7010	FXS1831Q17K
21				
20				
19				
18				
17				
16				
15				
14				
13				
12				
11				
10				
9				
8				
7				
6				
5				
4				
3				
2				
1				

	RACK-03			
U	**Equipment Description**	**Make**	**Model**	**Serial No**
42	Web Server-04	Cisco	C240	FCH1917V0RL
41				
40	Backup/Archival Server -01	Cisco	C240	FCH1917V1EF
39				
38	Web Server-03	Cisco	C240	FCH1917V0RP
37				
36	GIS Server -02	Cisco	C240	FCH1917V1F9
35				
34	EMS Server -02	Cisco	C240	FCH1917V197
33				
32				
31				
30				
29				
28	Mail Security & Antispamsolution -01	Cisco	C380	FCH1913V0YP
27				
26	EMS Server -04	Cisco	C240	FCH1917V1MW
25				
24	Radware Absolute Vision	Radware		31506021
23				
22	Management Switch-01	D-Link		F3Y94F4000037
21				
20				
19				
18	Virtual Tape Library	Quantum	Dxi-6902	SX44601226 SX44601226
17				

16				
15				
14				
13				
12				
11				
10	SAN Storage	Hitachi	HUS-150	717 DF850-CBLR1-93043431
9				
8				
7				
6				
5				
4				
3				
2				
1				

Rack-04

U	Equipment Description	Make	Model	Serial No
42	Access Switch-03	Cisco	Nexus 5548	SSI185209AV
41	SAN Switch-02	Brocade	6520	CHQ2527L010
40				
39	SMS Gateway,Antivirus & OTP Server-02	Cisco	C240	FCH1919V2VA
38				
37				
36				
35				
34				
33	Netapp	Netapp	FAS8020	21639040683
32				
31				
30				
29	Mail Server -02	Cisco	C240	FCH1917V0PV
28				

27				
26				
25	AAA Module/Single Sign onServer 02	Cisco	C240	FCH1916V1LU
24				
23	EMS Server -03	Cisco	C240	FCH1920V005
22				
21	Directory Server & DomainNaming Server-02	Cisco	C240	FCH1917V1G2
20				
19	Database Encryption Server-01	Safenet	K250	HUNK-T2ZG-QH6X-K
18				
17	Application server -02	Cisco	C460	FCH1921V1CN
16				
15				
14				
13	Reporting/Analytics Server-02	Cisco	C460	FCH1920V10H
12				
11				
10				
9	Database server -02	Cisco	C460	FCH1925V1M7
8				
7				
6				
5	DMS Server -02	Cisco	C460	FCH1924V26Z
4				
3				
2				
1				

Rack-05

U	Equipment Description	Make	Model	Serial No
42	Access Switch-04	Cisco	Nexus 5548	SSI185209AH

41		Cisco		FCH1912V227
40	Video conferencing Server (BE7000)		UCS-C240M3	
39	External Firewall-02	Cisco	ASA 5585	JMX1924806U
38				
37	Internal Firewall-02	Cisco	ASA 5585	JMX1924806Q
36				
35	WAN Router-02	Cisco	ASR 1002-X	FOX1906GH44
34				
33	FCIP Router-02	Brocade	7800	ASS2534L00D
32	Proxy solution-02	Bluecoat	SG900	1515240011
31	Proxy solution-AV- 02	Bluecoat	AV1200	4313220078
30	Internet Router-02	Cisco	2951	FGL194111CV
29				
28	Video conferencing Server (TelePresence Content-01)	Cisco	C220	FCH1920V1UB
27	Video conferencing Server for laptop/desktop/smart devices (BE6000)	Cisco	UCSC220 M3BE	FCH1918V0NQ
26	AAA Module-01	Cisco	3415	FCH1922V009
25	Application Firewall- 02	Palo Alto	PA 5020	2501001741

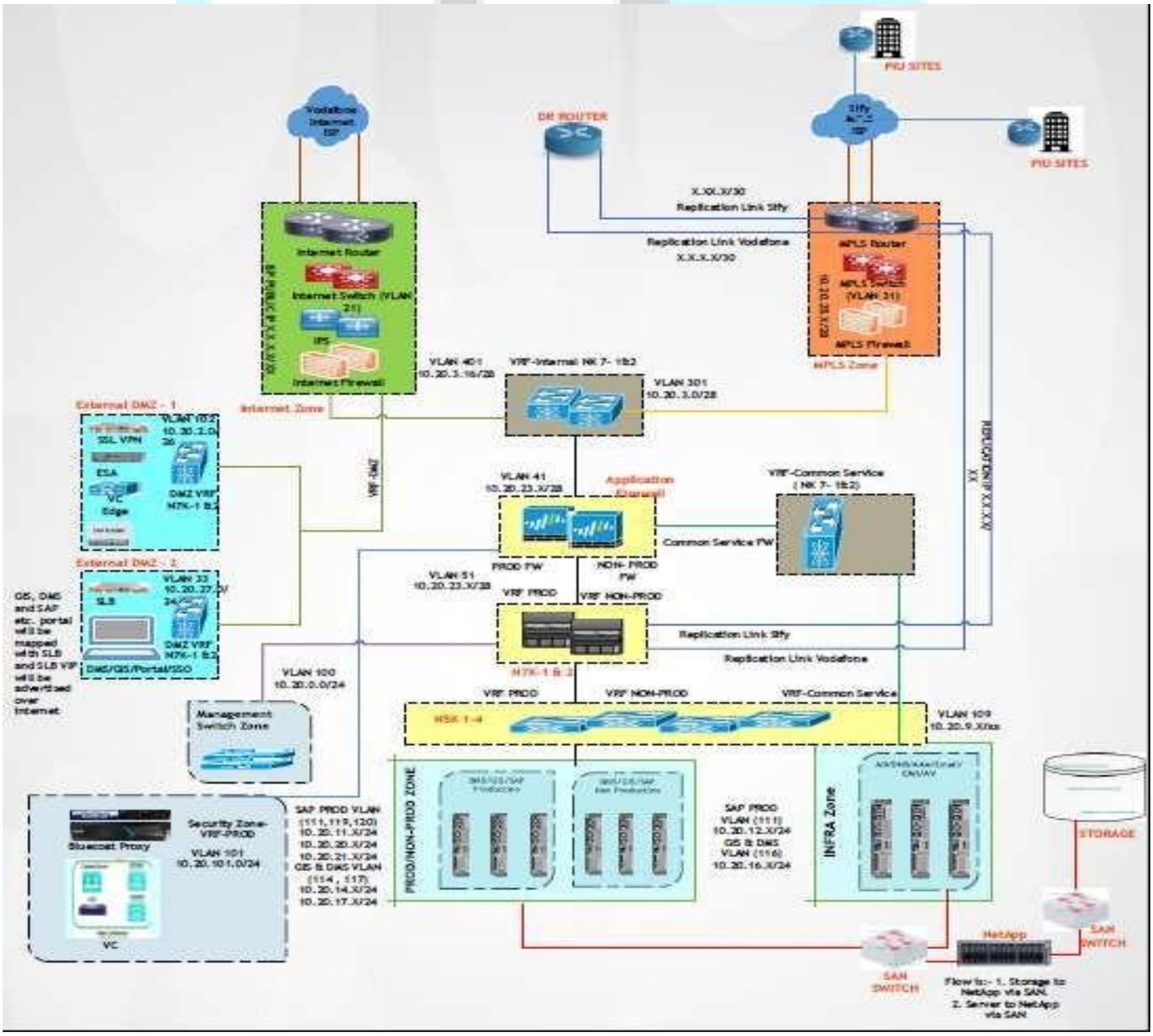
24				
23	Management Switch- 02	D-Link		F3Y94F4000038
22	Core Switch-02	Cisco	Nexus 7010	FXS1832Q40N
21				
20				
19				
18				
17				
16				
15				
14				
13				
12				
11				
10				
9				
8				
7				
6				
5				
4				
3				
2				
1				

	Rack-06			
U	Equipment Description	Make	Model	Serial No
42				
41				
40				
39				
38	Mbook Dev/quality	Cisco	C240	FCH1919V20B
37				
36				
35				
34				
33				
32				
31				
30				
29				
28				
27				
26				
25				
24				
23				
22				
21				
20				
19				
18				
17				
16				
15				
14				
13				
12				
11				
10				
9				
8				
7				
6				
5				

4				
3				
2				
1				

2.2. Network & Security Details

2.2.1. Overall Architecture



The above architecture diagram shows the physical topology view of datacenter. It consists ofthree major WAN networks namely MPLS, Internet and Management network connectivity.

Here three virtual firewalls are created from the Application Firewall i.e.

1. **Production Firewall**
   In this we have only the production servers which will be protected by firewall andsegregated by VRF like: GIS, DMS, SAP etc.

2. **Non-Production Firewall**
   In this we have only the Dev & Quality servers which will be protected by firewall andsegregated by VRF like: GIS, DMS, SAP etc.

3. **Common Services Firewall**
   In this we have only the common services like Ad, DNS, AAA, Mail Server, AV etc. whichwill be protected by firewall and segregated by VRF.

In Every Virtual Firewall, we will have multiple security Zone.

The above firewalls are further segregated via VRF (Virtual Routing & Forwarding) for Zoning. Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) networkrouters that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented withoutusing multiple devices.
From the server farm view below are the major zones available in existing setup:

- Internet DMZ
- Production MZ
- Security Zone
- Management
- Common Zone

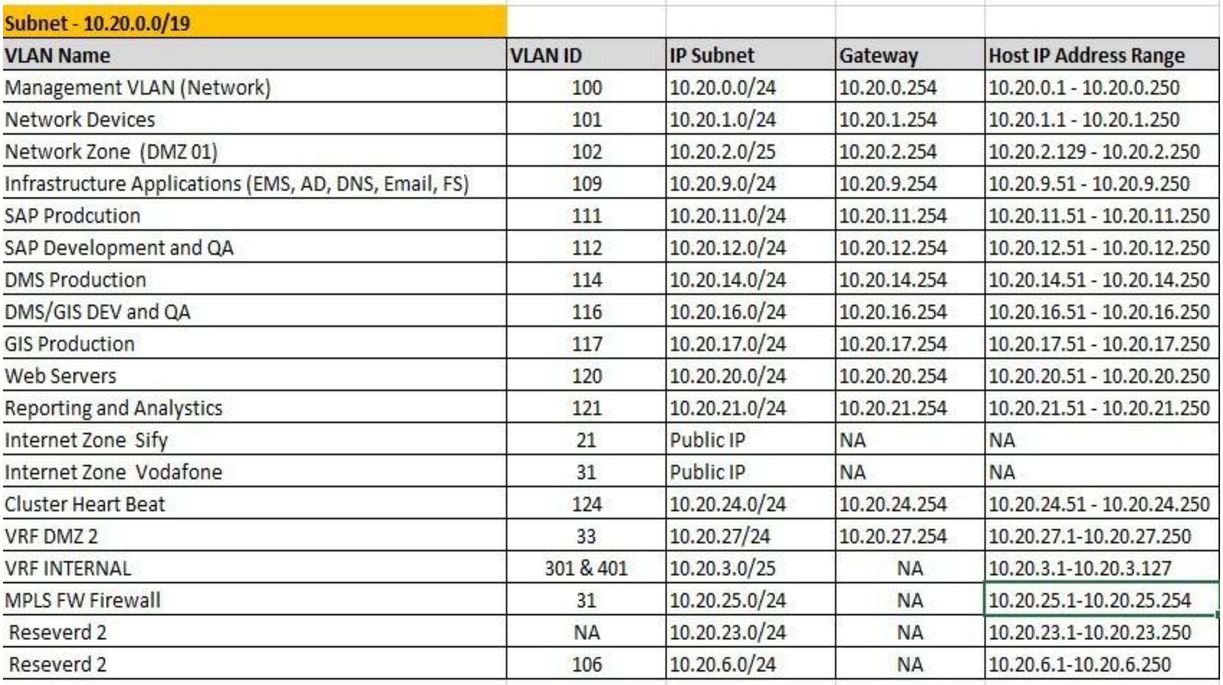
28.1. Zone Service Mapping

This section portrays the list of services mapped to their respective blocks / zones. These have been categorized and grouped in different zones based on their functional and access requirements

INTERNET DMZ-1	ESA, SAP ROUTER, VC Edge and SSL VPN
INTERNET DMZ -2	SLB, GIS, DMS, SAP, and MAIL portal (mapped with SLB)
SECURITY ZONE	VC servers and Forward Proxy.

MANAGEMENT	Dedicated management network for all servers,devices and users.
MZ	SAP/NON-SAP PROD and NON-PROD Servers SQL Database, Apps, portal apps, Archival,Reserved.
Common Zone	AD, DNS, AAA, Mail Servers and AV SMS/OTP
High Speed Layer2/layer3/ Aggregation	DC Interconnect + Intranet Services comprising of connectivity between various network Core security segments within DC.

The current datacenter networks are assigned with 10.20.x.x IP ranges respectively and has been further divided into various subnet according to zones & services inside the zones as required.



Subnet - 10.20.0.0/19				
VLAN Name	**VLAN ID**	**IP Subnet**	**Gateway**	**Host IP Address Range**
Management VLAN (Network)	100	10.20.0.0/24	10.20.0.254	10.20.0.1 - 10.20.0.250
Network Devices	101	10.20.1.0/24	10.20.1.254	10.20.1.1 - 10.20.1.250
Network Zone (DMZ 01)	102	10.20.2.0/25	10.20.2.254	10.20.2.129 - 10.20.2.250
Infrastructure Applications (EMS, AD, DNS, Email, FS)	109	10.20.9.0/24	10.20.9.254	10.20.9.51 - 10.20.9.250
SAP Prodcution	111	10.20.11.0/24	10.20.11.254	10.20.11.51 - 10.20.11.250
SAP Development and QA	112	10.20.12.0/24	10.20.12.254	10.20.12.51 - 10.20.12.250
DMS Production	114	10.20.14.0/24	10.20.14.254	10.20.14.51 - 10.20.14.250
DMS/GIS DEV and QA	116	10.20.16.0/24	10.20.16.254	10.20.16.51 - 10.20.16.250
GIS Production	117	10.20.17.0/24	10.20.17.254	10.20.17.51 - 10.20.17.250
Web Servers	120	10.20.20.0/24	10.20.20.254	10.20.20.51 - 10.20.20.250
Reporting and Analystics	121	10.20.21.0/24	10.20.21.254	10.20.21.51 - 10.20.21.250
Internet Zone Sify	21	Public IP	NA	NA
Internet Zone Vodafone	31	Public IP	NA	NA
Cluster Heart Beat	124	10.20.24.0/24	10.20.24.254	10.20.24.51 - 10.20.24.250
VRF DMZ 2	33	10.20.27/24	10.20.27.254	10.20.27.1-10.20.27.250
VRF INTERNAL	301 & 401	10.20.3.0/25	NA	10.20.3.1-10.20.3.127
MPLS FW Firewall	31	10.20.25.0/24	NA	10.20.25.1-10.20.25.254
Reseverd 2	NA	10.20.23.0/24	NA	10.20.23.1-10.20.23.250
Reseverd 2	106	10.20.6.0/24	NA	10.20.6.1-10.20.6.250

28.2. Subnet Details based on Zone Mapping

The Data Center Architecture is layered as below:

- Internet/WAN Edge Layer
- Collapsed Distribution/Core Layer

- Access Layer

A summary of the network and the security implemented at various levels is given below:

1. **Internet / WAN EDGE Layer:**

This layer consists of two major connection types for link level redundancy, one is internet Edge for those users accessing Data Center network through internet (Internet Users) and another one is MPLS WAN Edge for CUSTOMER PIU location internal users (Intranet Users).

Internet Edge layer equipped with 2 Cisco2901 router and 2 Cisco5585 ASA Firewall. Both devices configured in active-passive mode. The Internet connection is provided by two different ISPs. Primary 10 Mbps Internet connection from SIFY and Secondary 10 Mbps Internet connection from Vodafone. Both of these internet links are terminated on 2 different routers to provide link level as well as hardware level redundancy.

Intranet/MPLS Edge layer is equipped with 2 ASR1002 series router and 2 Cisco5585 ASA Firewalls. ASR Routers and ASA Firewalls are configured in Active-passive mode. Primary 20 Mbps MPLS connection is provided by SIFY and Secondary 20 Mbps MPLS connection is provided by VODAFONE. Both of these MPLS links are terminated on 2 different routers to provide link level as well as hardware level redundancy.

Both internet Edge routers are configured with static routing to connect with their own ISPs. The internet links will be provided at DC and will be used to access the Web servers, Video Conferencing meeting links and Email gateways. The all internet access will egress out from DC and the contents will be controlled using Bluecoat Proxy SSG 900.

Both Internal WAN Edge router and MPLS WAN Edge routers are using BGP Routing protocol to form neighbor ship with their ISPs. IBGP is configured and will be used between two internal Edge routers or MPLS WAN Edge routers.

Internet Firewalls are configured as Active – passive mode. All the traffic from internet will pass through this Firewalls. Firewall will be configured with three Zones. First Zone is Inside

Zone, Second Zone is Outside Zone and third Zone is DMZ Zone. Outside zone will be facing towards incoming Internet Traffic. Inside zone will be facing towards incoming DC LAN Traffic. DMZ Zone will be facing towards web facing Servers. All the Web based servers are mapped with Public IP address in the ASA Firewall for accessing through Internet. Access-lists are created and configured to permit or deny the access from the internet to DC Servers and will provide access to only authentic users. Link failover for WAN is configured on the Internet Firewall. Internet Firewall keep on monitoring the both ISP Links using IP SLA. If Primary ISP Internet links goes down, Internet Firewall will forward all the traffic automatically via Secondary ISP Internet link. Once the Primary ISP internet link comes up again, Internet Firewall is configured to automatically forward all the Traffic via Primary ISP Internet link. Both Firewalls are configured for LAN Failover. If any of the Firewall goes down the other Firewall will act as active firewall and Forward the Traffic.

Internal/Intranet Firewalls are also configured in Active-passive mode, and is configured in such a way that all the traffic from PIU must pass through this firewalls. Firewall will be configured with three Zones. First Zone is Inside Zone, Second Zone is Outside Zone and third Zone is DMZ Zone. Outside zone will be facing towards incoming MPLS WAN Traffic. Inside zone will be facing towards incoming DC LAN Traffic. DMZ Zone will be facing towards web facing Servers. All the Web based servers are mapped with Public IP address in the ASA Firewall for accessing through Internet. Only PIUs subnets are allowed to pass through this Firewall. Both Firewalls are configured for LAN Failover. If anyone Firewall goes down the other Firewall become active and Forward the Traffic. Access lists are created in this Firewallto control the DC Server access from the PIUs.

DMZ Zone has all the web servers like Email Security Appliances, E-mail Server, Web Portal and all other servers which required access through web. All the Internet users only have access permission only till DMZ Zone Servers in order to secure the DC LAN from unwanted Internet users.

Security:

This zone includes systems such as Internet routers, and other systems that do not reside behind the Firewalls. Internet user/web clients navigating through websites hosted on the Web infrastructure are part of this Untrusted Zone.

Devices Placed on the Internet zone:

- Internet Router (CISCO 2951)
- IPS/IDS (DefensePro 2412)
- External Firewall (ASA5585-X)

IPS will protect applications and networks against known and emerging network security threats such as:

- ➢ DoS and DDoS attacks
- ➢ Internet pipe saturation
- ➢ Attacks on login pages
- ➢ Attacks behind CDNs, and SSL-based flood attacks
- ➢ Protects infrastructure against network and application downtime
- ➢ Application vulnerability exploitation
- ➢ Malware spread
- ➢ Network anomalies
- ➢ Information theft and other emerging cyber-attack

Firewall Rule information:

Production Traffic Rule need to be added in the implementation stage.

After Implementation, any request come for port opening that request will go to CUSTOMER for approval. After approval of CUSTOMER port will be open in the Firewall.

Allow			
Source	Destination	Port	Remark
Any	Web Server	80 (HTTP)	For allowing communication to web server from outside world over HTTP
Any	Web Server	443 (HTTPS)	For allowing secure communication to webserver from outside world

Any	Application Server	3389 (TCP/UDP)	For taking remote connection of servers fromoutside world
Remote Site IP	Local Server IP	500 (ISAKMP)	For allowing VPN connectivity
Any	Mail Server	143 (IMAP)	For allowing remote user to download mail frommail server
Any	Mail Server	25 (SMTP)	For sending messages to a mail server for **relaying**
Any	NetworkDevice	22 (TCP/UDP)	For allowing user to access network device overSSH
Any	NetworkDevice	23 (TCP /UDP)	For allowing user to access network device overtelnet
Any	FTP Server	21 (TCP/UDP)	For allowing users to download files from FTP server
ANY	DNS Server	53 (TCP/UDP)	Resolving DNS with internal users and servers
ANY	NTP	123 (TCP/UDP)	UDP over port 123
			Deny
Source	Destination	Port	Remark
Any	Any	Any	Block all traffic by default and explicitly allowonly specific traffic to known services

28.3. **Port Testing Procedures for Firewall-**

Firewall port testing flow and results (from internet i.e. public IP)

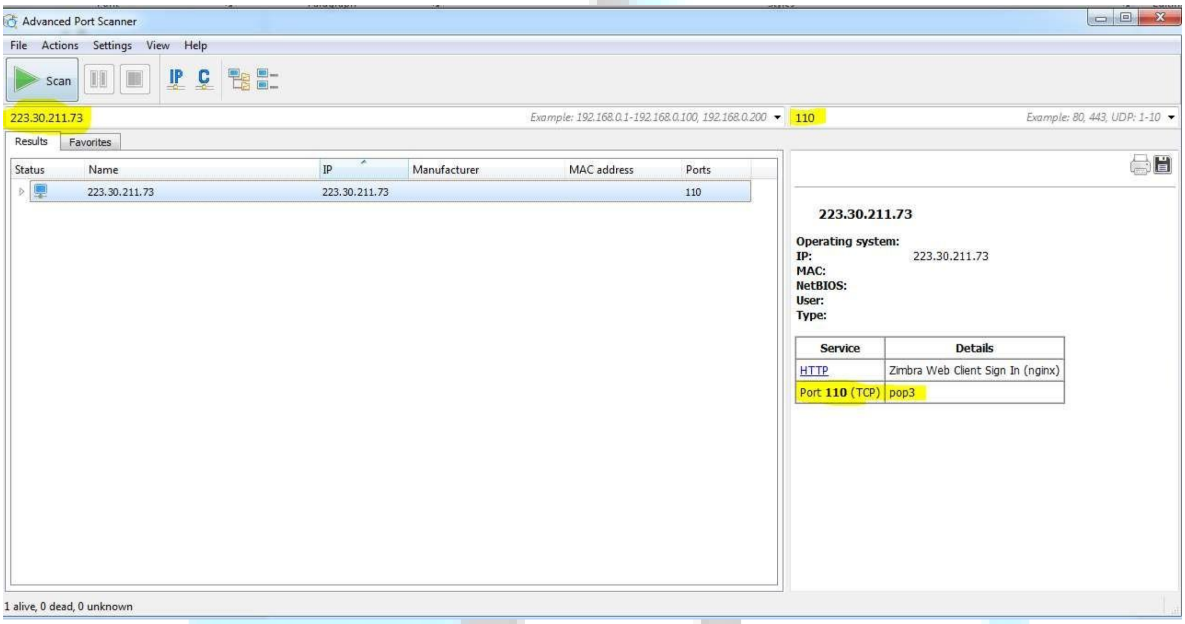
There are many tools from which we can check and test firewall port. We can scan open portvia port scanner tools and we can also check with manual via telnet to check the IP port status.

Below is snap with step to check the port status.

Step1: Open port scanner tools

Step2: Type the server IP (public) with port number (you can search all open port also at atime)

Step3: click on scan button and wait for the result (if port is open then port service will beshown as shown in below.



223.30.211.73 — Example: 192.168.0.1-192.168.0.100, 192.168.0.200

110 — Example: 80, 443, UDP: 1-10

Status	Name	IP	Manufacturer	MAC address	Ports
	223.30.211.73	223.30.211.73			110

223.30.211.73

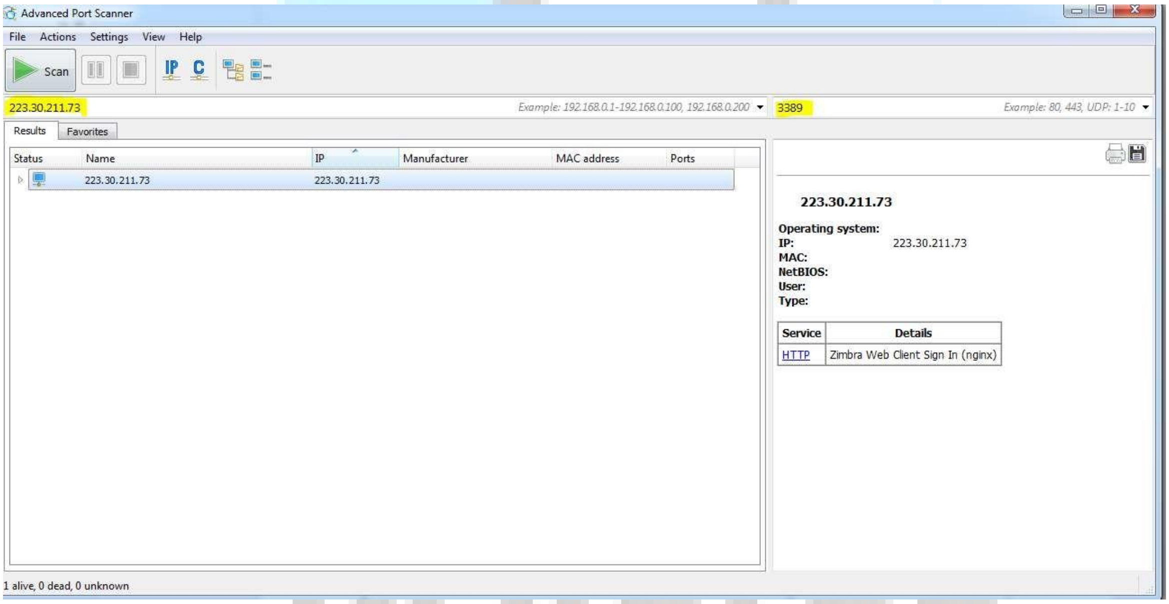
Operating system:
IP: 223.30.211.73
MAC:
NetBIOS:
User:
Type:

Service	Details
HTTP	Zimbra Web Client Sign In (nginx)
Port **110** (TCP)	pop3

1 alive, 0 dead, 0 unknown

Step 4: If port is not open then it will not show (please see the second snap for reference)

Note: In this picture, searched port number is 3389 and after scanning it is not showing anyDetails



223.30.211.73 — Example: 192.168.0.1-192.168.0.100, 192.168.0.200

3389 — Example: 80, 443, UDP: 1-10

Status	Name	IP	Manufacturer	MAC address	Ports
	223.30.211.73	223.30.211.73			

223.30.211.73

Operating system:
IP: 223.30.211.73
MAC:
NetBIOS:
User:
Type:

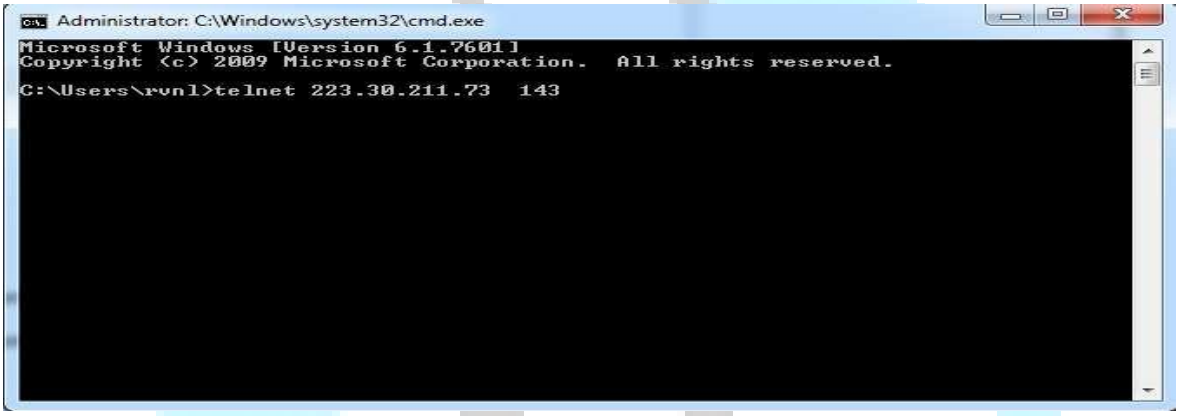
Service	Details
HTTP	Zimbra Web Client Sign In (nginx)

1 alive, 0 dead, 0 unknown

Firewall port testing flow and results (from telnet i.e. Public IP)

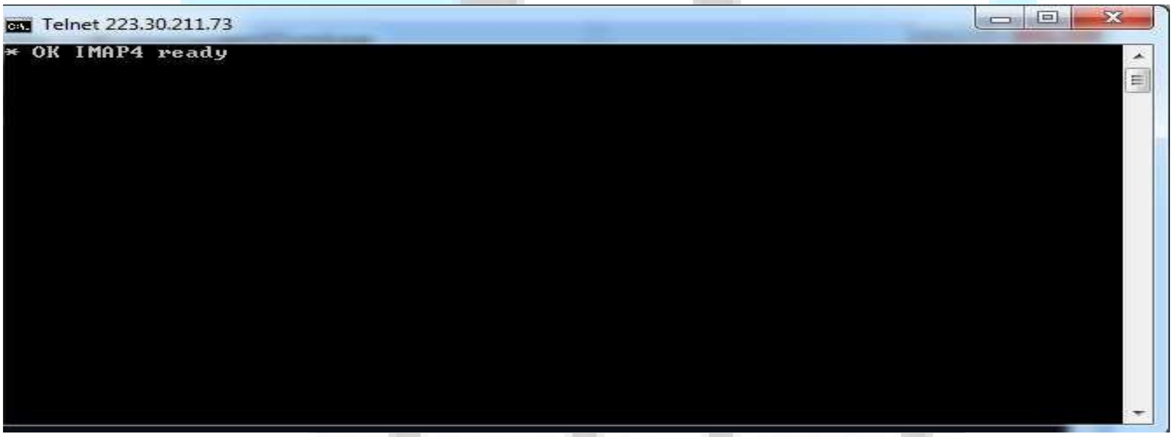
Step 1: Open command prompt or telnet software

Step 2: Type telnet “Ip address” “port number” and enter



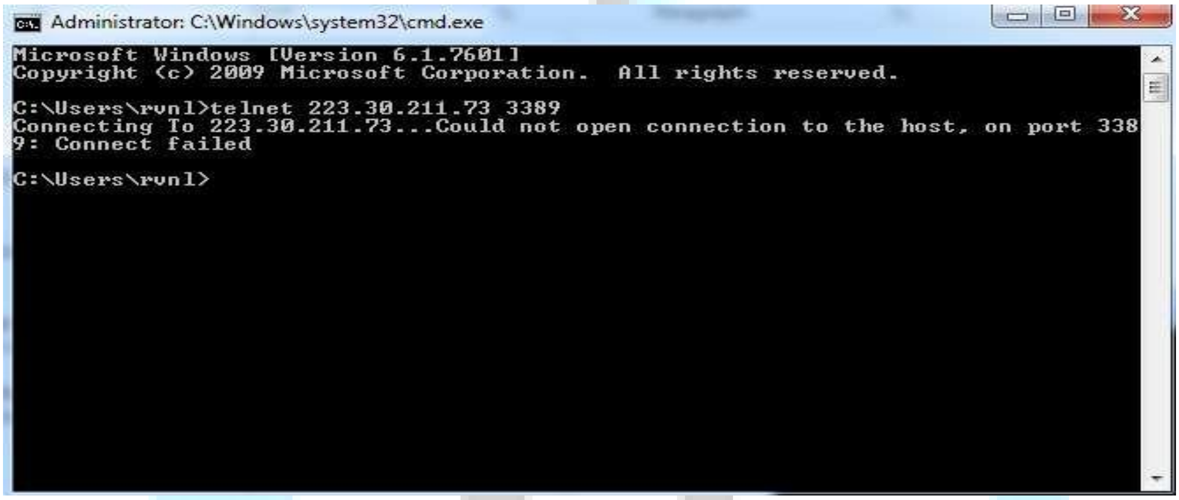
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\rvnl>telnet 223.30.211.73  143
```

Step 3: If port is open them you will be able to login telnet with desire port.



```
* OK IMAP4 ready
```

Step 4: If not then it will not login telnet with desire port.



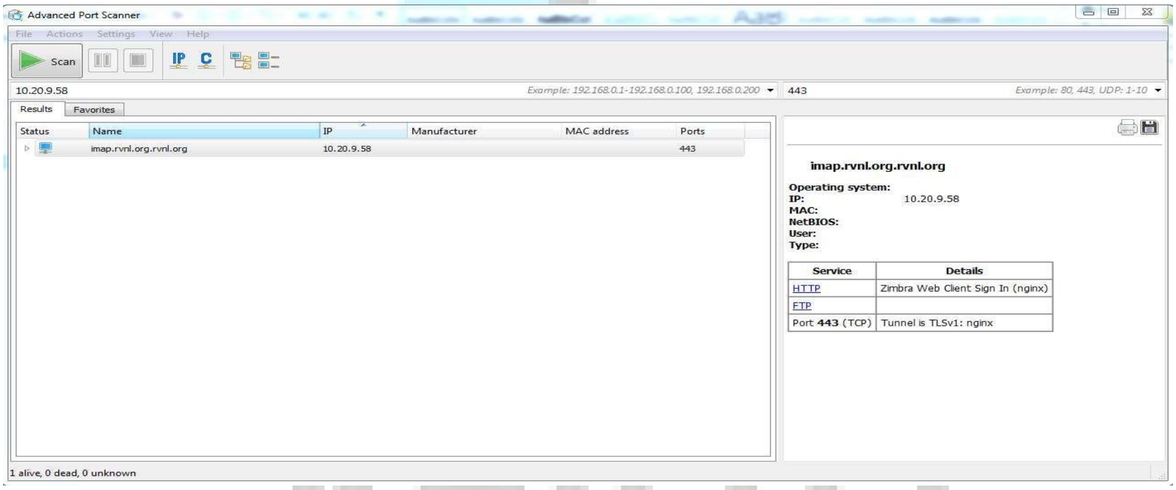
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\rvnl>telnet 223.30.211.73 3389
Connecting To 223.30.211.73...Could not open connection to the host, on port 338
9: Connect failed

C:\Users\rvnl>
```

Firewall port testing flow and results (from MPLS i.e. Private/Internal IP):

Step 1: Open port scanner tools

Step 2: Type the private server IP with port number (you can search all open port also at atime)

Step 3: click on scan button and wait for the result (if port is open then port service will beshown as shown in below.



10.20.9.58 — Example: 192.168.0.1-192.168.0.100, 192.168.0.200

443 — Example: 80, 443, UDP: 1-10

Status	Name	IP	Manufacturer	MAC address	Ports
	imap.rvnl.org.rvnl.org	10.20.9.58			443

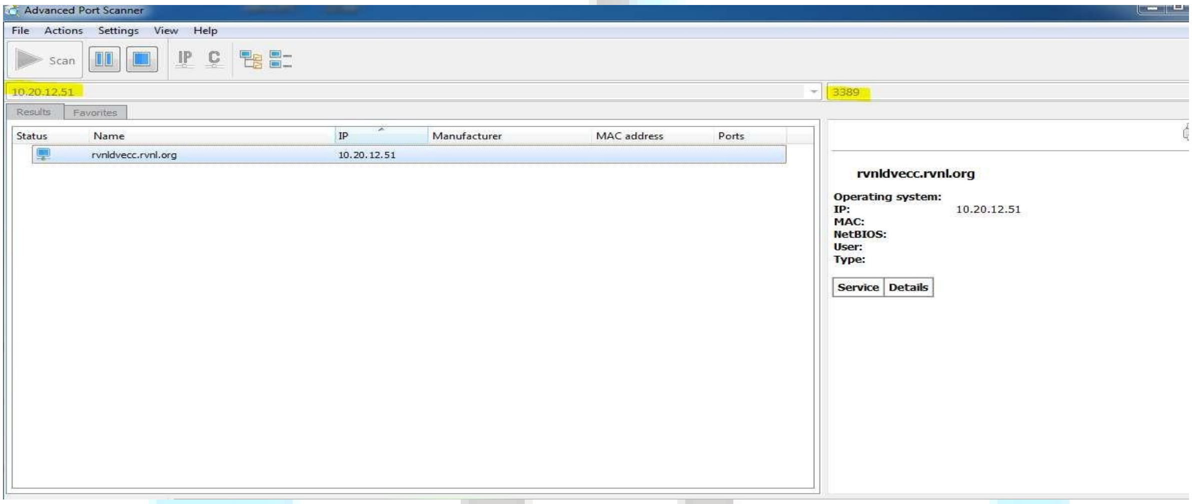
imap.rvnl.org.rvnl.org

Operating system:
IP: 10.20.9.58
MAC:
NetBIOS:
User:
Type:

Service	Details
HTTP	Zimbra Web Client Sign In (nginx)
FTP	
Port **443** (TCP)	Tunnel is TLSv1: nginx

1 alive, 0 dead, 0 unknown

Step 4: If port is not open then it will not show (please see the second snap for reference)



10.20.12.51

3389

Status	Name	IP	Manufacturer	MAC address	Ports
	rvnldvecc.rvnl.org	10.20.12.51			

rvnldvecc.rvnl.org

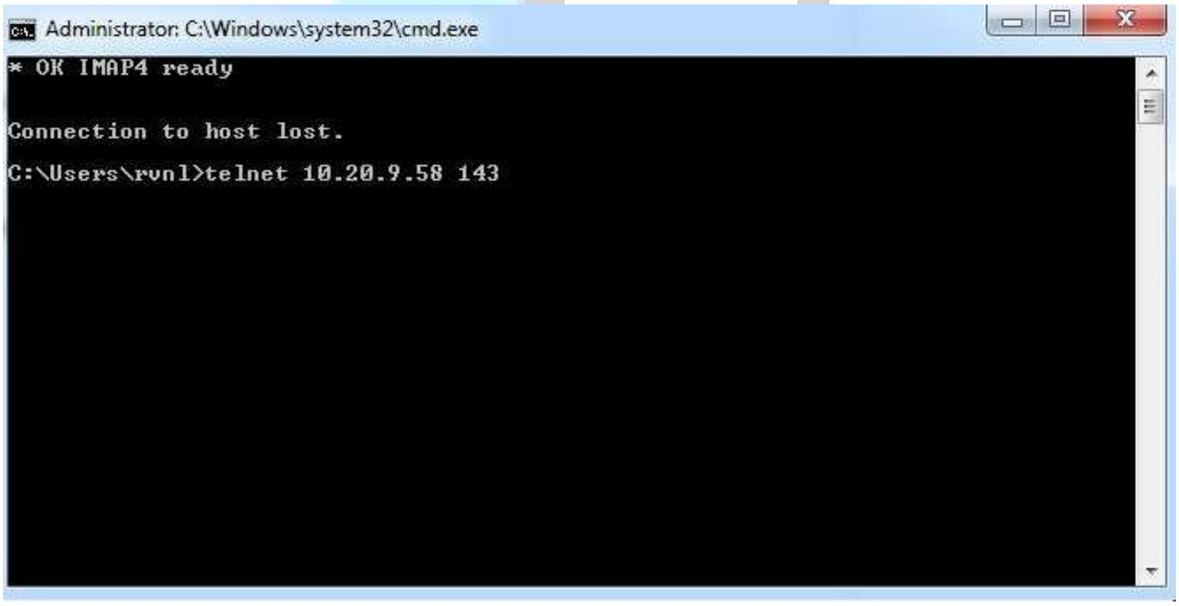
Operating system:
IP: 10.20.12.51
MAC:
NetBIOS:
User:
Type:

<u>Firewall port tester flow and results (from telnet i.e. Private/Internal IP):</u>

Step 1: Open command prompt

Step 2: Type telnet “private IP address” “port number” and enter

Step 3: If port is open them you will be able to login telnet with desire port.



```
* OK IMAP4 ready

Connection to host lost.
C:\Users\rvnl>telnet 10.20.9.58 143
```

Step 4: If not then it will not login telnet with desire port.

2. Collapsed distribution/Core Layer:

In this Collapsed distribution/core layer, Core Switches (Nexus 7010), Application Firewall, IPS/IDS, SSL VPN Devices and Blue coat Proxy devices are placed, and configured to cater different services and policies like, Access lists, firewall rules, traffic routing, QoS etc.

This layer being a gateway for Core layer to Server farm. Any sources trying to access the Data Center Server farm must pass through this core switch first and connected security devices. Internet Firewall and Internal Firewalls are connected their downlink in this core switch.

Both Nexus 7010 devices are banded as single logical switch using vPC. Two 10GB Fiber cables are used to form the vPC peer between two Nexus 7010, these two Fiber ports are connected as vPC as peer link between two Nexus 7010.

Through one Ethernet cable vPC keep alive link is configured between two Nexus 7010 used to carry the routing update between the two Nexus 7010. One switch is being Primary Core switch,Routing and Forwarding the traffics. When the Primary switch goes down secondary will take over the Routing and Forwarding Responsibility. In this action of time, End Servers does not face any interruption in the Traffic flows.

All the devices (Security, Load balancer and Proxy) connecting with Core switch N7K using port channel to provide the high bandwidth and high availability. This layer is secured using Cisco ASA firewalls for external and internal traffic, which will ingress and egress within the data center. The Radware’s DefensePro IPS will be deployed in the core network to check for security including distributed denial of service (DDoS) mitigation and SSL-based protection to fully protect applications and networks against known and emerging network security threats such denial of service attacks, DDoS attacks, Internet pipe saturation, attacks on login pages, attacks behind CDNs, and SSL-based flood attacks.

All the down layer switches (Nexus 5k) are connected with core switch using vPC connection.

Each down layer Switch having one physical connection (10 GB Fiber cable) to each core switch. Advantage of using vPC is all the uplink bandwidths are available for data traffic. Four vPC linksare created on the both Nexus 7010 switches to provide the down link connection the Nexus 5000 devices.

The Data Center network will be managed using Out of Band (OOB) network called asmanagement network (10.20.0.0/24). The dedicated Layer 2 switches will be deployed to connect the management interfaces for All Network devices, Security devices, UCS servers, storage and SAN Switches.

Security:

This zone would include systems such as public facing organizational web servers (and the application servers they communicate to) and other systems that need to be accessed by third parties. In this Architecture, this Zone will be created using logical separation.

Devices Placed on the DMZ zone:

- Email Security Appliance
- Video Conference Server-Edge
- SSL VPN
- Server Load Balancing (SLB)

Servers Placed on the DMZ zone:

Production Traffic Rule need to be added in the implementation stage.

Post Implementation required ports and protocols opening request will be submitted to the CUSTOMER approval.

S.NO	Physical Server Name	VM Name	Role	LAN IPADDRESS	Mapping Device in DMZ
1	DCSCLPRD-MAIL01	MTA1 + Proxy	Email Server	10.20.9.51	ESA and SLB

2	DCSCLPRD-MAIL02	MTA2 + Proxy	Email Server	10.20.9.54	ESA and SLB
3	DCSNCPRD-WEB04	RVNLPRSAPROUTER	SAP Router	10.20.20.58	SAP Router itself will placed in DMZ
4	DCSCLPRD-SAP01	RVNLPRSRMAP1	SAP SERVER (SRM)	10.20.11.69	Array LB
	DCSCLPRD-SAP02	RVNLPRSRMAP2		10.20.11.70	
5	DCSNCPRD-RA01	RVNLPREPAP1	SAP SERVER (EP)	10.20.21.57	Array LB
6	DCSNCPRD-RA02	RVNLPREPAP2		10.20.21.58	
6	DCSCLPRD-DMS01	RVNLPRDMSAP1	DMS	10.20.14.12	Array LB
7	DCSCLPRD-DMS02	RVNLPRDMSAP2		10.20.14.14	
8	DCSCLPRD-GIS01	RVNLPRGISAP1	GIS	10.20.17.3	Array LB
	DCSCLPRD-GIS02	RVNLPRGISAP2		10.20.17.5	
14	SSO-01		SSO server	10.20.9.72	Array LB
15	SSO-02		SSO server	10.20.9.82	Array LB

Firewall Rule information:

Production Traffic Rule need to be added in the implementation stage.

Post Implementation, any request come for port opening that request will go to CUSTOMER for approval. After approval of CUSTOMER port will be open in the Firewall.

Allow			
Source	Destination	Port	Remark
LAN Server Gateway IP inDMZ	LAN Server IPs	Application Specific Ports	Allow the traffic from DMZ to Servers in the LAN Server Farms based on the Services

Deny			
Source	Destination	Port	Remark
Any	Any	Any	Block all traffic by default and explicitly allowonly specific traffic to known services

3. Access Layer:

In this layer, Four Nexus 5000 series are placed. These switches having uplink connection to core switches. To provision, High-availability and load balancing, four Nexus 5000 switches are divided into two vPC domain. Nexus 5000 switch -1 and Nexus 5000 switch-2 are forming separate vPC peering between them using Two 10 GBPS Fiber cables. Nexus 5000 switch -3 and Nexus 5000 switch-4 are forming separate vPC peering between them using Two 10 GBPS Fiber cables.

This layer is designed to provide the high speed redundant connectivity to server, storage components that will host applications. The servers will be configured using Virtual Port Channels (vPCs) and will be connected physically connected to two different access switches to appear to a downstream server to be coming from a single device using a Port Channel. This will provide redundancy and high bandwidth using both links with 20Gbps connectivity. The server and devices will be connected using the LACP (IEEE 802.3ad) for link aggregation.

Enterprise management system server is connected in this layer.

All the devices will be configured in such a way to send the SNMP traps and log message tothe EMS system for monitoring and management using SNMP v2, WMI protocols. Logging willbe enabled on all network devices to send syslog alerts to EMS system. If any devices goes down Alert trigger will be shown in the EMS Server.

Security:

This is the most secure zone any traffic coming from the Internal, External and DMZ networkwill be physically isolated and scanned using Firewalls and IPS. Any traffic flow this zone towards internet will be secured using explicit proxy deployment ensuring no data loss.

In this zone, Data Center Core Architecture for Servers, Application Servers will be placed and installed in LAN Network. Only traffic/VLAN/IP subnet coming from different CUSTOMER trusted PIU’s will allowed here, all the other traffic will be denied.

Internet access to LAN zone will be provided by using Bluecoat proxy device SG900. Blue coat SG900 will be deployed in explicit mode. The explicit deployment mode will provide the below features:

- Used when a web gateway is deployed in a larger network, and the design of the networkrequires there to be no single point of failure,
- Allows the web gateway to be located on the network in any location that is accessibleby the users and the device itself has access to the Internet,
- Optimizing the data traffic processed by the web gateway and ability to ease redundancy implementation for web gateways in CUSTOMER environment.

Devices Placed on the MZ zone:

- Production & Non-Production Server (GIS, DMS, SAP etc.)

Firewall Rule information:

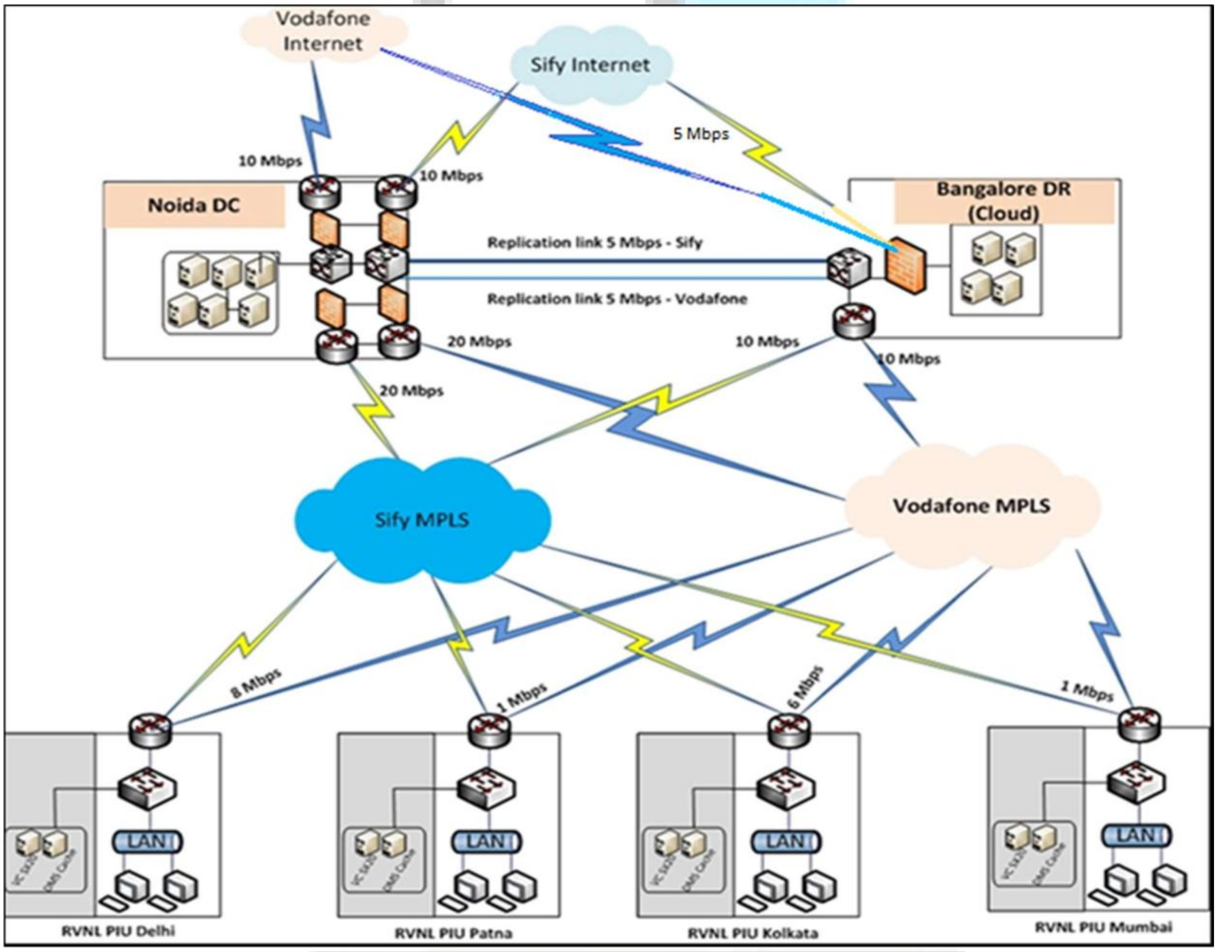
Production Traffic Rule need to be added in the implementation stage.

After Post Implementation, any request come for port opening that request will go to CUSTOMER for approval. After approval of CUSTOMER port will be open in the Firewall.

Allow			
Source	Destination	Port	Remark
PIU Location IP	Web server	80	For allowing communication to web server from PIU Location over HTTP
PIU Location IP	Web server	443	For allowing secure communication to web serverfrom PIU Location
PIU Location IP	Application server	3389	For taking remote connection of servers from PIU Location
PIU Location IP	Mail server	IMAP	For allowing remote user to download mail frommail server: Port 143 **-** this is the default IMAP non-encryptedport **Port 993** - this is the port you need to use if youwant to connect using IMAP securely
PIU Location IP	Mail server	SMTP	For allowing remote user to download mail from mail server, Standard protocol for sending emails across the Internet.

			Port 25 - this is the default SMTP non-encryptedport **Port 465 -** this is the port used, if you want to send messages using SMTP securely (SMTP)
PIU Location IP	Network Device	22	For allowing user to access network device over SSH
PIU Location IP	Network Device	23	For allowing user to access network device overtelnet
PIU Location IP	FTP server	21	For allowing users to download files from FTP server
PIU Location IP	Active directory	389 636 3268 3269	Directory, Replication, User and Computer Authentication, Group Policy, Trusts
PIU Location IP	Active directory	88	User and Computer Authentication, Forest LevelTrusts
PIU Location IP	Active directory	53	User and Computer Authentication, Name Resolution, Trusts
PIU Location IP	Active directory	137	User and Computer Authentication,
PIU Location IP	Active directory	139	User and Computer Authentication, Replication
Deny			
Source	Destination	Port	Remark
Any	Any	Any	Block all traffic by default and explicitly allow only specific traffic to known services

2.2.2. WAN Connectivity Solution



s

L & T InfoTech has finalized M/s Vodafone’s & M/s Sify’s (Service Provider) MPLS Services to provide dedicated Connectivity between CUSTOMER offices and DC/ DR. Vodafone & Sify are also providing Internet Services at DC and DR and Point to Point replication link between DC and DR. Link from Vodafone & Sify will be used to maintain redundancy.

The WAN connectivity redundancy between DC and DR will based on the BGP routing protocol features. DC subnets configured for same networks in the Primary router, will also beadvertised in Vodafone routers with back door routes. DR routers will advertise the default route with Autonomous System (AS) appended. To ensure Business continuity, the ingress and egress traffic will switch to the DR cloud location.

The dedicated redundant replication link has been provisioned to replicate between DC and DR, to make sure the data is available with high availability feature in the applications. During disaster at primary DC, the critical applications will be made available from DR sites with agreed RPO. DNS entries will be updated for critical application to be accessed from DR location.

28.4. **IP Routing deployment:**

The setup will be configured with dynamic routing making use of BGP v4. The below section highlights the routing deployment:

- The MPLS core routers at DC will be configured with eBGP peering with primary Sifyand eBGP peering with Vodafone.
- iBGP protocol will run between primary and backup router.
- The backup router will advertise the DC subnet using BGP backdoor to avoid any loopsduring normal conditions when primary and backup routers are up
- PIU location router will be configured with eBGP peering between Sify and Vodafone
- Vodafone MPLS network will honor Sify CE private AS numbers to be routed in Vodafone MPLS network this will enable loop free routing and use Vodafone connectionas backup.
- The DC internet core router will be configured will the eBGP to Sify and Vodafone
- iBGP will be configured between internet router to act as failover
- Sify provided public IP address subnet will be routed via Vodafone in its routing
- Both services provider syncing the AS and IP Subnet will help to configure internet routing without multi-home connection eliminating CUSTOMER network from becoming thetransvers network for public domain.

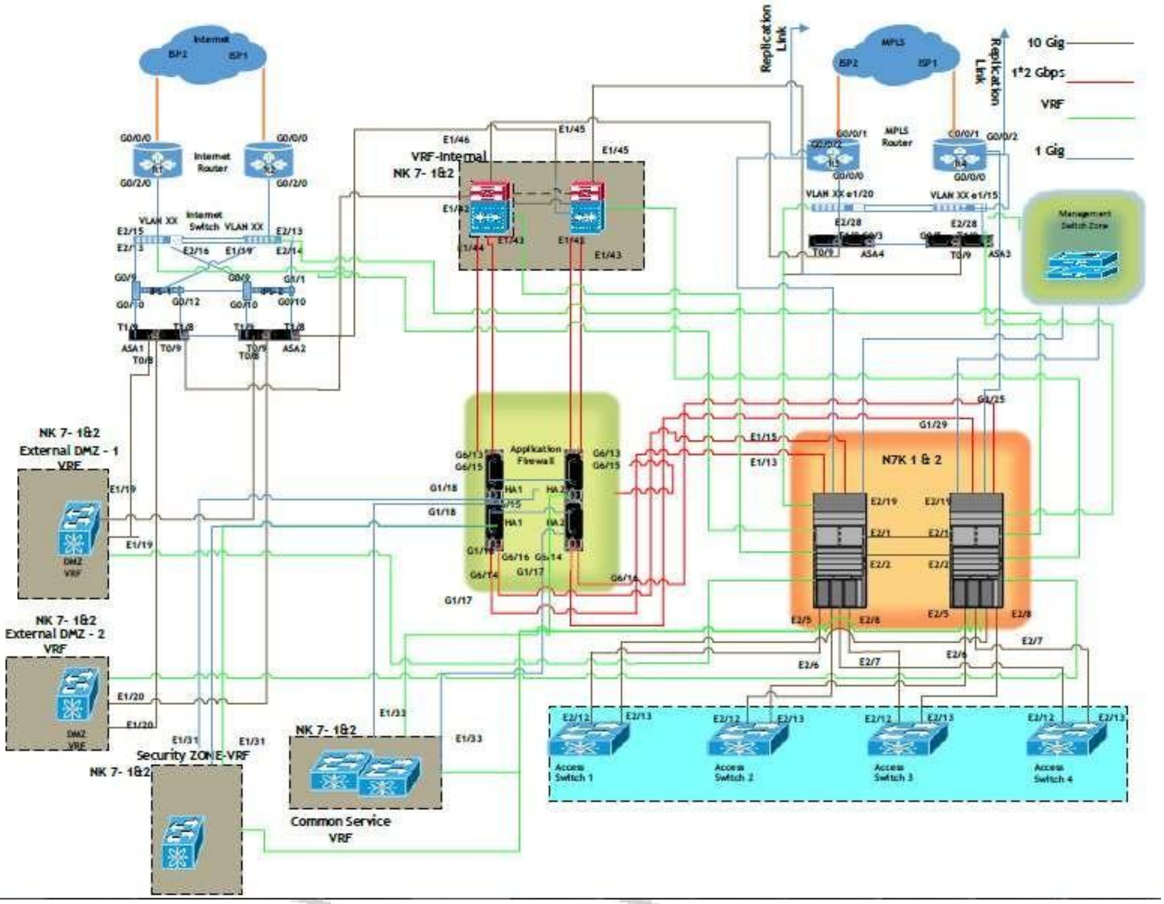
Default route will be advertised from DC to MPLS network and default route with backdoorwill be injected in network from DR MPLS router make the failover active.

28.5. 2.2.2.1. Security for WAN (MPLS)

All the CUSTOMER HQ and PIU offices will be accessing centralized services and application hosted in co-located data centers via WAN connectivity. RNVL has provisioned / used MPLS Cloud technology / circuits in secure Point to Multi Point topology mode. The MPLS cloud services has taken from Sify (Primary) and Vodafone (Backup) those are dedicated virtual MPLS tunnels build only for CUSTOMER where no other than CUSTOMER network traffic is allowed to traverse over WAN links. For each WAN circuit connectivity, a dedicated (point to point) eBGP session/ connection with password security has established between Provider Edge (PE) router and Customer Edge (CE) routers that is installed in CUSTOMER offices. Access to MPLS cloud core infrastructure is being monitored and managed in secure way by MPLS service provider.

Service Provider follows a comprehensive Network Monitoring and Management process to monitor and manage CUSTOMER networks. At the nerve center of this entire process is service providers – Sify’s homegrown tool, Beacon™ and customer facing portal as IONI which is a comprehensive network infrastructure management and monitoring solution designed to aid Service Provider in managing networks. Vodafone is using HP Openview and IBM Tivoli for Network Monitoring and customer facing portal as on Web Self Care - https://fls.vodafone.in/WSC/wscLogout.action.

2.3. Low-level DC Architecture



With respect to the layer 3 architecture explained in earlier section and based on the devices being proposed to be placed in each segment, the layer 1 Network and Security architecture diagram is shown above. The proposed Layer 1 architecture is prepared by examining and ensuring each of the points mentioned below.

- caters connectivity of all devices as finalized in the Network and Security device sizinglayer of each zone is distributed across
- ports based on the connectivity type multiple line cards in core switch for better
- multiple links are proposed to be connected to any core, different line cards ports
- Port numbers are based on the module placement inside a device
- protocol that shall be used on each segment (like VRF, vPC)
- prepared in line with the Layer-1 connectivity diagram shown above

2.4. Server Details

2.4.1. SAP Server Details

2.4.1.1. Production servers

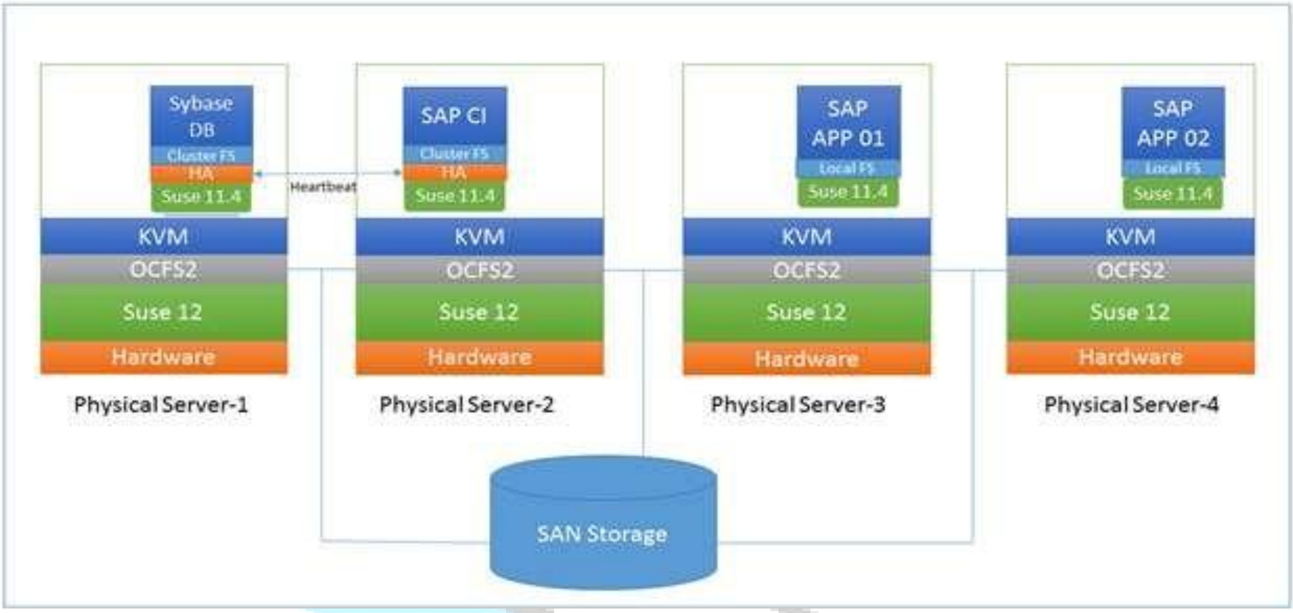
Sl.No	Physical Server	Serial	Physical Server Hostname	Physical Server Management IP
1	UCSC-C460-M4 (App/DB) Physical 1	FCH1917V211	DCSCLPRD-SAP01	10.20.0.51
2	UCSC-C460-M4 (App/DB) Physical 2	FCH1921V1CN	DCSCLPRD-SAP02	10.20.0.52
3	UCSC-C460-M4 (App/DB) Physical 3	FCH1925V1XS	DCSCLPRD-SAP03	10.20.0.53
4	UCSC-C460-M4 (App/DB) Physical 4	FCH1925V1M7	DCSCLPRD-SAP04	10.20.0.54
5	UCSC-C460-M4 (Reporting/Analytics) Physical 1	FCH1929V11S	DCSNCPRD-RA01	10.20.0.55
6	UCSC-C460-M4 (Reporting/Analytics) Physical 2	FCH1920V10H	DCSNCPRD-RA02	10.20.0.56
7	UCSC-C240-M3S (Web Server) Physical 1	FCH1917V0C6	DCSNCPRD-WEB01	10.20.0.57
8	UCSC-C240-M3S (Web Server) Physical 2	FCH1917V17A	DCSNCPRD-WEB02	10.20.0.58
9	UCSC-C240-M3S (Web Server) Physical 3	FCH1917V0RP	DCSNCPRD-WEB03	10.20.0.59
10	UCSC-C240-M3S (Web Server) Physical 4	FCH1917V0RL	DCSNCPRD-WEB04	10.20.0.60

2.4.1.2. Development & Quality Servers

Sl.No	Physical Server	Serial	Physical Server Hostname	Physical Server Management IP
11	UCSC-C240-M3S (DEV) Physical 1	FCH1917V1GA	DCSNCDEV-SAP01	10.20.0.63
12	UCSC-C240-M3S (DEV) Physical 2	FCH1917V0UH	DCSNCDEV-SAP02	10.20.0.64
13	UCSC-C240-M3S (QA) Physical 1	FCH1917V17N	DCSNCQA-SAP01	10.20.0.65
14	UCSC-C240-M3S (QA) Physical 2	FCH1916V26U	DCSNCQA-SAP02	10.20.0.66

15	UCSC-C240-M3S (QA) Physical 3	FCH1917V1G1	DCSNCQA-SAP03	10.20.0.67
16	UCSC-C240-M3S (QA) Physical 4	FCH1917V1EX	DCSNCQA-SAP04	10.20.0.68
17	UCSC-C240-M3S (QA) Physical 5	FCH1917V0R H	DCSNCQA-SAP05	10.20.0.69

2.4.1.3. HA for SAP Components



- SAP Cluster will be created using “SUSE Linux Enterprise High Availability Extension”
- KVM Virtualization technology will be used for deploying SAP Servers. For example,Virtual machine “DB” for SAP database & CI for SAP “CI”
- An Active-Active cluster type will be created between DB & CI virtual machine
- A Clustered File System from Storage allocated to both DB & CI Nodes. For example, Clustered LVM (CLVM) and OCFS2 file system will be used between virtual machines
- Cluster will have, Two virtual IP one will be mapped DB host & and another for CI host
- Therefore in case of failure of one node the filesystem and VIP will be moved to anotheravailable node and will start the required services automatically. For example, DB filesystem & VIP1 will move to secondary node, i.e CI node and start the SAP DB service automatically and vice versa in case of CI node failure
- Once the failed node came back to normal the Suse cluster will automatically failback the Filesystem and start the required services automatically

- There is auto recovery is enabled for critical services. For example, DB service and CI service. If any of the services is killed accidently by the user or it becomes unresponsive the cluster will try to restart the service automatically

If the physical host or virtual machine is unstable or frequent reboot, cluster service will stop the services that was monitored by cluster to avoid any data loss or corruption.

2.4.2. Non-SAP Server Details

2.4.2.1. Production servers

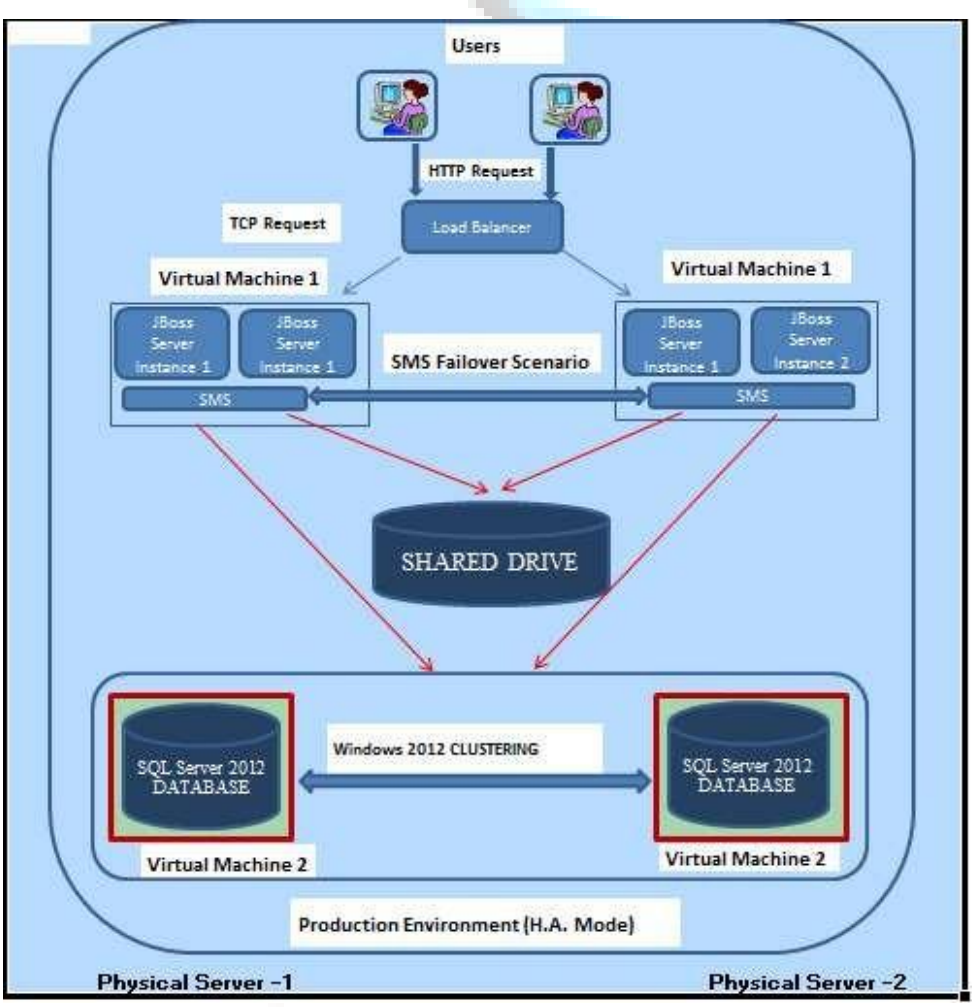
Sl.No	Physical Server	Serial	Physical Server Name	Physical Server Management IP
1	UCSC-C240-M3S (Mail Server-1)	FCH1917V1ER	DCSCLPRD-MAIL01	10.20.0.70
2	UCSC-C240-M3S (Mail Server-2)	FCH1917V0PV	DCSCLPRD-MAIL01	10.20.0.71
3	UCSC-C240-M3S (EMS) Physical 1	FCH1917V0XN	DCNCPRD-EMS01	10.20.0.73
4	UCSC-C240-M3S (Backup)	FCH1917V1EF	DCNCPRD-Backup	10.20.0.77
5	UCSC-C240-M3S (GIS server-1)	FCH1917V1EN	DCSCLPRD-GIS01	10.20.0.78
6	UCSC-C240-M3S (GIS server-2)	FCH1917V1F9	DCSCLPRD-GIS02	10.20.0.79
7	UCSC-C460-M4 (DMS Server-1)	FCH1928V0UJ	DCSCLPRD-DMS01	10.20.0.80
8	UCSC-C460-M4 (DMS Server-2)	FCH1924V26Z	DCSCLPRD-DMS02	10.20.0.81
9	UCSC-C240-M3S (AD/DNS-1)	FCH1917V1EQ	DCSCLPRD-PDC01	10.20.0.82
10	UCSC-C240-M3S (AD/DNS-2)	FCH1917V1G2	DCSCLPRD-BDC02	10.20.0.83
0	UCSC-C240-M3S (Testing/Training)	FCH1917V0EM	DCNCL-TRAINING	10.20.0.84
11	UCSC-C240-M3S (SMS/OTP/AV-1)	FCH1917V1G7	DCSCLPRD-SMS01	10.20.0.88
12	UCSC-C240-M3S (SMS/OTP/AV-2)	FCH1919V2VA	DCSCLPRD-SMS02	10.20.0.89
13	UCSC-C240-M3S (AAA-1)	FCH1917V18U	DCSCLPRD-AAA01	10.20.0.90
14	UCSC-C240-M3S (AAA-2)	FCH1916V1LU	DCSCLPRD-AAA02	10.20.0.91
15	UCSC-C240-M3S (EMS) Physical 2	FCH1917V197	DCNCPRD-EMS02	10.20.0.74
16	UCSC-C240-M3S (EMS) Physical 3	FCH1920V005	DCNCPRD-EMS03	10.20.0.75

17	UCSC-C240-M3S (EMS) Physical 4	FCH1917V1MW	DCNCPRD-EMS04	10.20.0.76
18	TCS UCS M3 Physical 1	FCH1920V1UB	DCSCLPRD-VC01	10.20.0.92
19	UCS C220 M3BE (VC-BE6K) Physical 1	FCH1918V0NQ	DCSCLPRD-VC02	10.20.0.93
20	UCS 240 M3 CIT 2 - Content Server	FCH1912V227	DCNCPRD-CS01	10.20.0.94

2.4.2.2. Development, Quality and Training & Testing Servers

Sl.No	Physical Server	Serial	Physical Server Name	Physical Server Management IP
1	UCSC-C240-M3S (Testing/Training)	FCH1917V0EM	DCNCL-TRAINING	10.20.0.84
2	UCSC-C240-M3S (DMS/GIS QA)	FCH1913V1PG	DCSNCQA-DMSGIS	10.20.0.61
3	UCSC-C240-M3S (DMS/GIS DEV)	FCH1917V0F4	DCSNCDEV-DMSGIS	10.20.0.62

2.4.2.3. HA for DMS & GIS Servers



- High Availability will be maintained for DMS & GIS using 2 numbers of servers
- HA in Database virtual machine will be maintained using Windows 2012 Standard Cluster
- HA in DMS Application will be maintained using Server Load Balancer (Array Network Appliances)

2.5. Active Directory

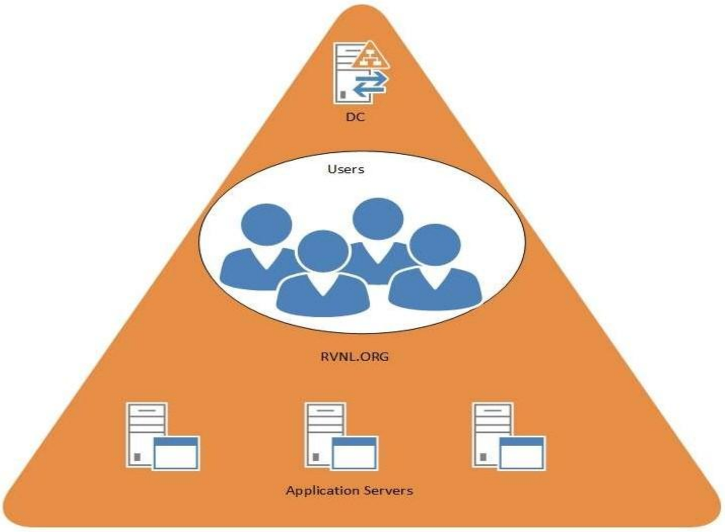
2.5.1. Active Directory Domain Design

2.5.1.1. Forest Model

The business and technical requirements for RVNL's new Active Directory design do not present any reason to implement more than one forest. The administration of the new CUSTOMER Active Directory infrastructure will be centralized. Furthermore, there are no special cases where a complete separation of administration is necessary, thus making the primary driving factor for additional forests a moot point.

2.5.1.2. Domain Model

As the CUSTOMER network is well connected by high speed network links, there is no need to consider segregating Active Directory replication at the domain level to control network traffic. The newCUSTOMER forest will consist of a single domain which will be utilized across the entire Active Directory environment.

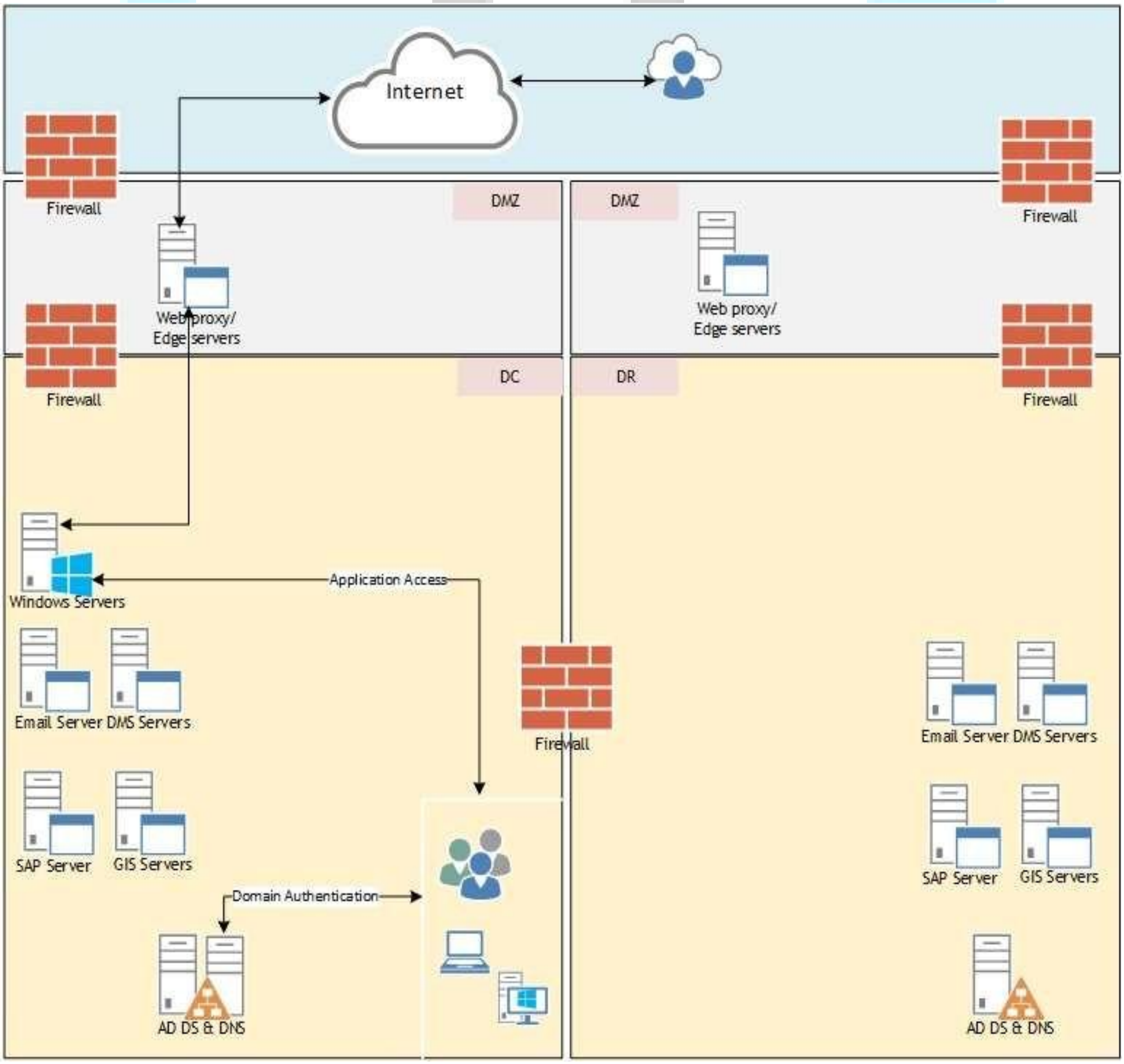


The new domain will have the following names:

- DNS Name – RVNL.org
- NetBIOS Name – RVNL

In the unlikely event that the CUSTOMER need to deploy an additional domain, it is logical to either deploy that domain as a child of RVNL.org (e.g. domain2.RVNL.org) or as a separate tree in the RVNL.org forest (e.g. RVNL2.org). This flexibility exists regardless of whether or not an empty root domain is deployed as part of the forest design.

2.5.2. Active Directory Solution Diagram



2.5.2.1. Active Directory Forest and Domain Functional Level

In Active Directory Domain Services (AD DS), domain controllers can run different versions of Windows Server operating systems. The functional level of a domain or forest depends on which versions of Windows Server operating systems are running on the domain controllers in the domain or forest. The functional level of a domain or forest controls which advanced features are available in the domain or forest.

All Domain Controllers are proposed to be in Windows 2012 R2 standard edition with Windows 2012 Native Forest\Domain functional Level

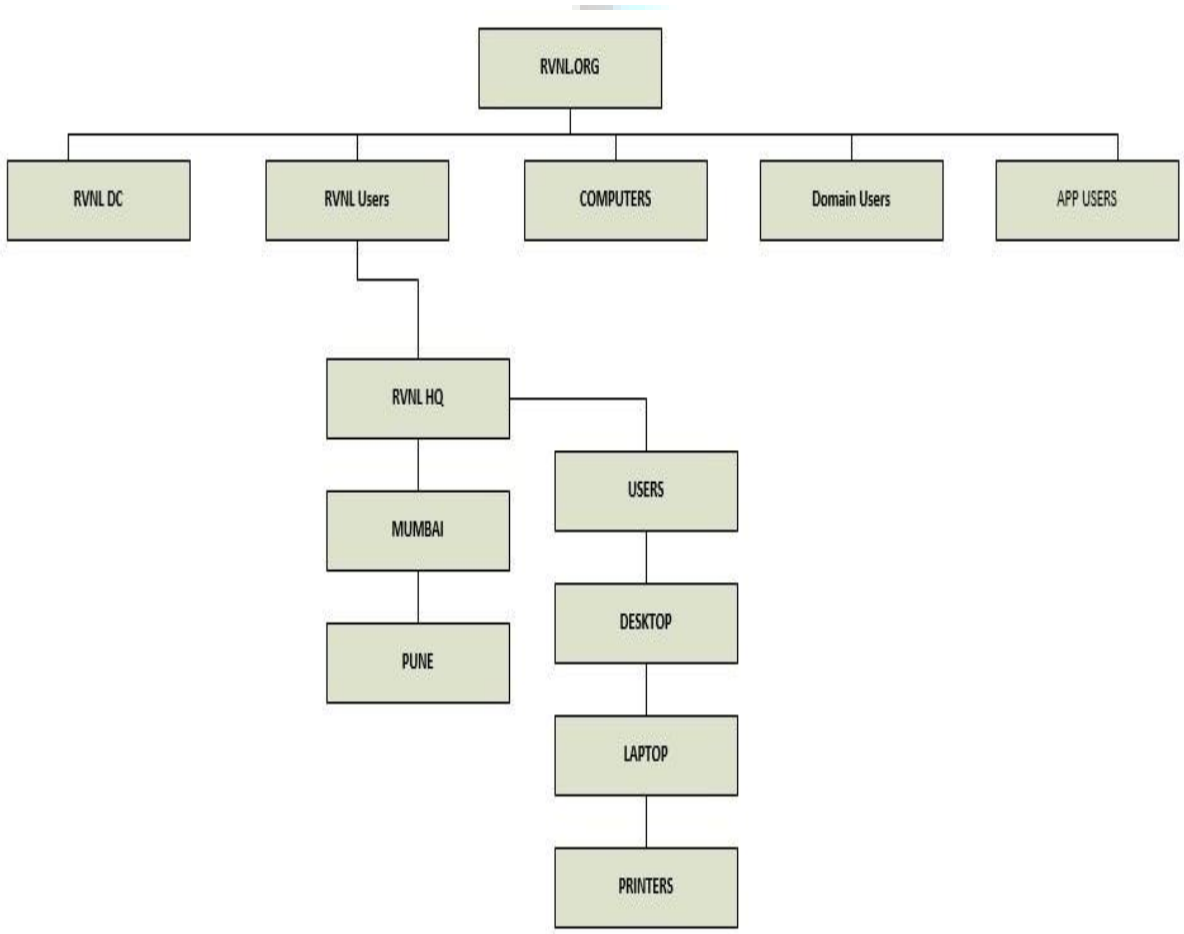
2.5.2.2. Active Directory FSMO Design

All domain controllers are of RVNL.org domain must have Global catalog server to readily avail searchable directory service and partial representation of every object in domain. For any given Active Directory Site with a Global Catalog, all the GC’s should be used for replication.

All FSMO Roles of domain will be maintained in PDC (Primary Domain Controller) which will be located at Primary Datacenter in Noida.

2.5.2.3. Recommended OU Structure

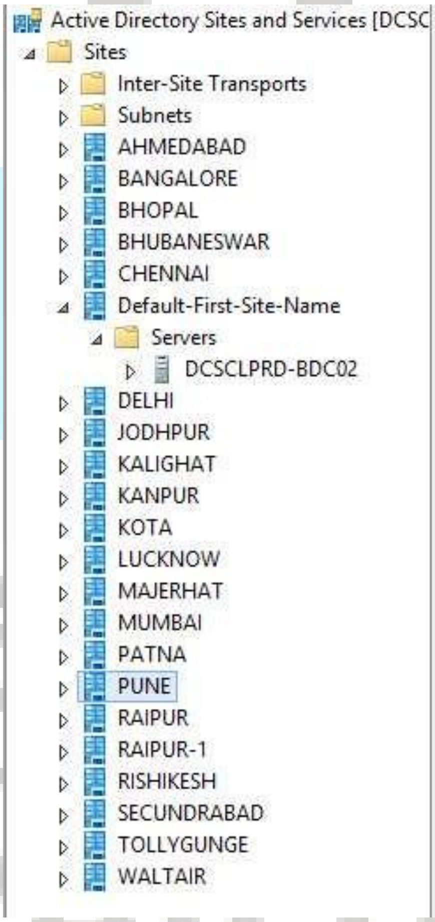
Based on CUSTOMER IT infrastructure, OU will created based on PIU location and GPO will pushed onOU


RVNL.ORG
RVNL DC
RVNL Users
COMPUTERS
Domain Users
APP USERS
RVNL HQ
USERS
MUMBAI
DESKTOP
PUNE
LAPTOP
PRINTERS

2.5.3. Active Directory Sites Design

Microsoft Active Directory Sites are designed to map the Physical Infrastructure with Logical Infrastructure and assist logon / Replication within Active Directory Domain Controllers located across multiple regions.

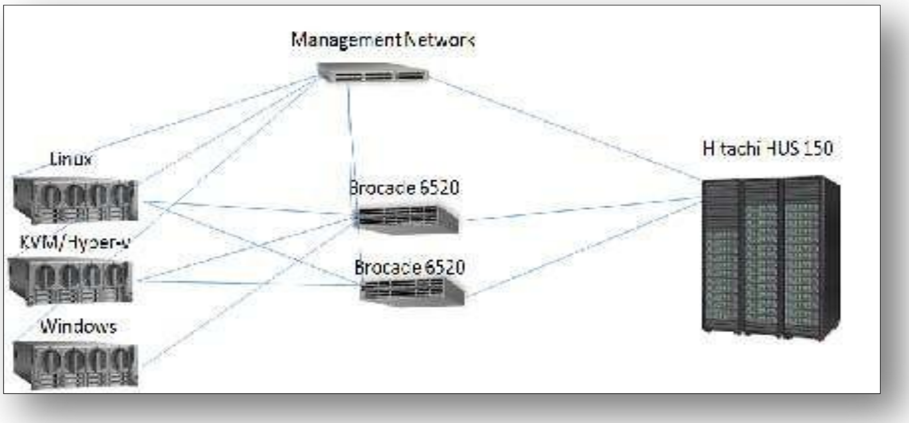
CUSTOMER spread across 26 PIU's (Branch Offices) with 1200 Users. As per the requirement, Incumbent service provider have proposed to 2 Domain Controllers in Primary Datacenter and 1 Domain controller in DR DC. Remaining Sites are provisioned for future growth.



- Active Directory Sites and Services [DCSC
  - Sites
    - Inter-Site Transports
    - Subnets
    - AHMEDABAD
    - BANGALORE
    - BHOPAL
    - BHUBANESWAR
    - CHENNAI
    - Default-First-Site-Name
      - Servers
        - DCSCLPRD-BDC02
    - DELHI
    - JODHPUR
    - KALIGHAT
    - KANPUR
    - KOTA
    - LUCKNOW
    - MAJERHAT
    - MUMBAI
    - PATNA
    - PUNE
    - RAIPUR
    - RAIPUR-1
    - RISHIKESH
    - SECUNDRABAD
    - TOLLYGUNGE
    - WALTAIR

2.6. Storage

To host the SAP ECC, Zimbra email data and other Applications, **1 Hitachi HUS 150** will be deployed at Data Center. Server to Storage connectivity will be through Brocade 6520 SAN switches. Architecture of Storage & Server connectivity is listed below. There is no single Point of Failure in the present Architecture. Each Storage connected Servers will be connected through 2 numbers of SAN switches. Also, each Storage connected Servers have two numbers of HBA. Therefore, there will not be connectivity failure even in case of 1 switch & 1 HBA failure in a server. Storage have built in full redundancy to maintain high availability



- High Redundancy (Dual controllers),
- Highly Scalable up to 2PB,
- I/O Multi-pathing,
- Auto Tiering feature for configuring RAID in storage,
- Dual SAN and Network Switch port (each having bandwidth of 8G) per controller
- Storage Zones will be created for different environment,
- Brocade 6520 SAN Switches with 48 Ports with each port of 8G will be configured in High Availability mode,
- Disk capacity of **34TB (15 * 1.2TB SAS 10K RPM, 44 * 300GB SAS 15K RPM, 8 * 400GB SAS)** will be deployed in production Data Center. Usable Space is **20TB**
- Disks in Storage configured with RAID5 for higher performance & availability

- Provide appropriate IOPS to run Business and Infrastructure applications,
- Equipped with high-end tools and software Ex. Replication, Monitoring,
- Network efficient replication.

The **Hitachi HUS 150** Storage is capable of providing the tiering on the basis of read and writefrequency of data. Most frequently accessed data will reside on Tier 2 for better performance. **Hitachi HUS 150** storage have SAS with **34TB (15 * 1.2TB SAS 10K RPM, 44 * 300GB SAS 15K RPM, 8 * 400GB SAS) disk capacity**, which will keep frequently read data on the same to provide better and faster query response. This will contribute towards enhancing application performance and end user satisfaction.

Redundancy like high availability on storage controllers (dual controller), redundant power, Replication and so on to ensure storage uptime and availability.

- Achieve 15 minutes of RPO and RTO for mission critical applications to provide data availability and performance to CUSTOMER business during Disaster scenario.

2.6.1. Storage Disk Pool & LUN Mapping with Server

Pool Details

DP Pool	Tier Mode	Raid Level	Total (TB)
0	Enabled	RAID5 (6D+1P)	24.2

LUN Details

VOL	Capacity (GB)	Consumed Capacity (GB)	No of Paths	Mapped Server
1	3072	882.3	2	DCSCLPRD-MAIL01 DCSCLPRD-MAIL02
2	600	413	2	DCNCL-TRAINING
3	4608	2150.4	2	DCSCLPRD-SAP01 DCSCLPRD-SAP02 DCSCLPRD-SAP03 DCSCLPRD-SAP04

4	2764	814.5	2	DCSCLPRD-SAP01 DCSCLPRD-SAP02 DCSCLPRD-SAP03 DCSCLPRD-SAP04
5	1024	288.4	2	DCSCLPRD-SAP01 DCSCLPRD-SAP02 DCSCLPRD-SAP03 DCSCLPRD-SAP04
6	5120	2764	2	DCSNCPRD-WEB01 DCSNCPRD-WEB02 DCSNCPRD-WEB03 DCSNCPRD-WEB04
7	5120	719.1	2	DCNCPRD-Backup
8	400	1	2	DCSCLPRD-DMS01 DCSCLPRD-DMS02
9	600	1	2	DCSCLPRD-DMS01 DCSCLPRD-DMS02

2.6.2. SAN Switch Zoning with Servers:

Alias Details

SR#	SAN Switch	Machine	Alias
1	DCNCPRD_Fabric01	DCSCLPRD-SAP01	RVNL_PRD_APPDB01_HBA1
3	DCNCPRD_Fabric01	DCSCLPRD-SAP02	RVNL_PRD_APPDB02_HBA1
5	DCNCPRD_Fabric01	DCSCLPRD-SAP03	RVNL_PRD_APPDB03_HBA1
7	DCNCPRD_Fabric01	DCSCLPRD-SAP04	RVNL_PRD_APPDB04_HBA1
9	DCNCPRD_Fabric01	DCSNCPRD-WEB01	RVNL_PRD_WEB01_HBA1
11	DCNCPRD_Fabric01	DCSNCPRD-WEB02	RVNL_PRD_WEB02_HBA1
13	DCNCPRD_Fabric01	DCSNCPRD-WEB03	RVNL_PRD_WEB03_HBA1
15	DCNCPRD_Fabric01	DCSNCPRD-WEB04	RVNL_PRD_WEB04_HBA1
17	DCNCPRD_Fabric01	DCSCLPRD-DMS01	RVNL_PRD_DMS01_HBA1
19	DCNCPRD_Fabric01	DCSCLPRD-DMS02	RVNL_PRD_DMS02_HBA1
21	DCNCPRD_Fabric0	DCSCLPRD-	RVNL_PRD_MAIL01_HBA1

	1	MAIL01	
23	DCNCPRD_Fabric01	DCSCLPRD-MAIL02	RVNL_PRD_MAIL02_HBA1
25	DCNCPRD_Fabric01	DCNCPRD-Backup	RVNL_BACKUP_SERVER_HBA1
2	DCNCPRD_Fabric02	DCSCLPRD-SAP01	RVNL_PRD_APPDB01_HBA2
4	DCNCPRD_Fabric02	DCSCLPRD-SAP02	RVNL_PRD_APPDB02_HBA2
6	DCNCPRD_Fabric02	DCSCLPRD-SAP03	RVNL_PRD_APPDB03_HBA2

8	DCNCPRD_Fabric02	DCSCLPRD-SAP04	RVNL_PRD_APPDB04_HBA2
10	DCNCPRD_Fabric02	DCSNCPRD-WEB01	RVNL_PRD_WEB01_HBA2
12	DCNCPRD_Fabric02	DCSNCPRD-WEB02	RVNL_PRD_WEB02_HBA2
14	DCNCPRD_Fabric02	DCSNCPRD-WEB03	RVNL_PRD_WEB03_HBA2
16	DCNCPRD_Fabric02	DCSNCPRD-WEB04	RVNL_PRD_WEB04_HBA2
18	DCNCPRD_Fabric02	DCSCLPRD-DMS01	RVNL_PRD_DMS01_HBA2
20	DCNCPRD_Fabric02	DCSCLPRD-DMS02	RVNL_PRD_DMS02_HBA2
22	DCNCPRD_Fabric02	DCSCLPRD-MAIL01	RVNL_PRD_MAIL01_HBA2
24	DCNCPRD_Fabric02	DCSCLPRD-MAIL02	RVNL_PRD_MAIL02_HBA2
26	DCNCPRD_Fabric02	DCNCPRD-Backup	RVNL_BACKUP_SERVER_HBA2

Zoning Details:

SR#	SAN Switch	Zone Name	Members Alias
1	DCNCPRD_Fabric01	RVNL_PRD_CTRL_APPDB01_HBA1	RVNL_PRD_APPDB01_HBA1 RVNL_CTRL_1B RVNL_CTRL_0C
2	DCNCPRD_Fabric02	RVNL_PRD_CTRL_APPDB01_HBA2	RVNL_PRD_APPDB01_HBA2 RVNL_CTRL_0B RVNL_CTRL_1D
3	DCNCPRD_Fabric01	RVNL_PRD_CTRL_APPDB02_HBA1	RVNL_PRD_APPDB02_HBA1 RVNL_CTRL_1B RVNL_CTRL_0C
4	DCNCPRD_Fabric02	RVNL_PRD_CTRL_APPDB02_HBA2	RVNL_PRD_APPDB02_HBA2 RVNL_CTRL_0B RVNL_CTRL_1D
5	DCNCPRD_Fabric01	RVNL_PRD_CTRL_APPDB03_HBA1	RVNL_PRD_APPDB03_HBA1 RVNL_CTRL_1B RVNL_CTRL_0C
6	DCNCPRD_Fabric02	RVNL_PRD_CTRL_APPDB03_HBA2	RVNL_PRD_APPDB03_HBA2 RVNL_CTRL_0B RVNL_CTRL_1D

7	DCNCPRD_Fabric01	RVNL_PRD_CTRL_APPDB04_HBA1	RVNL_PRD_APPDB04_HBA1 RVNL_CTRL_1B RVNL_CTRL_0C
8	DCNCPRD_Fabric02	RVNL_PRD_CTRL_APPDB04_HBA2	RVNL_PRD_APPDB04_HBA2 RVNL_CTRL_0B RVNL_CTRL_1D

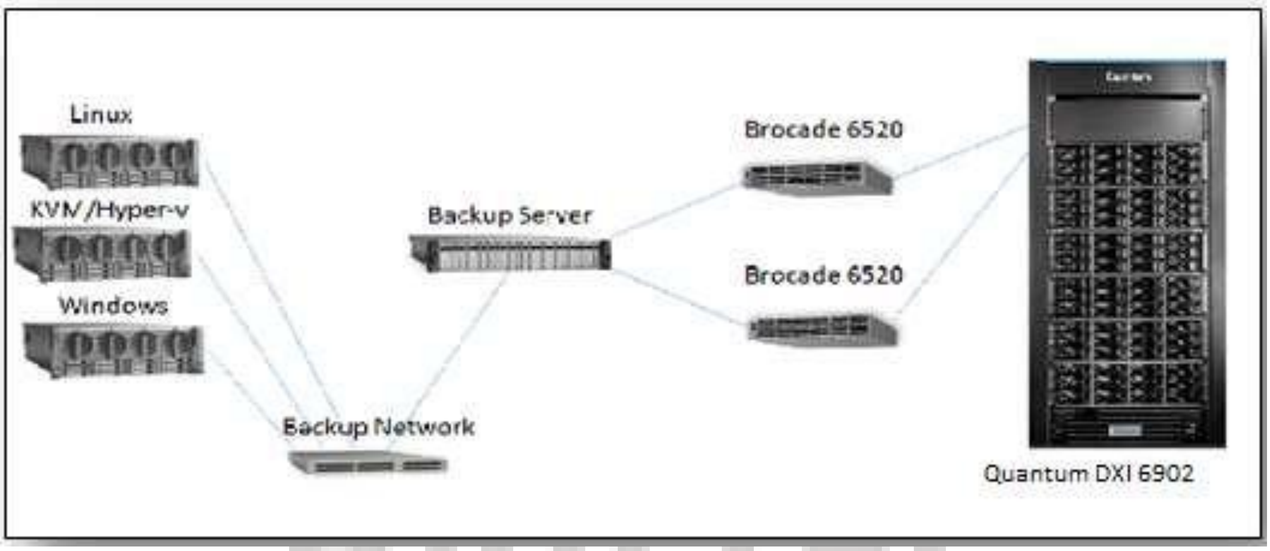
9	DCNCPRD_Fabric01	RVNL_PRD_CTRL_WEB01_HBA1	RVNL_PRD_WEB01_HBA1 RVNL_CTRL_0D RVNL_CTRL_1B
10	DCNCPRD_Fabric02	RVNL_PRD_CTRL_WEB01_HBA2	RVNL_PRD_WEB01_HBA2 RVNL_CTRL_1D RVNL_CTRL_0B
11	DCNCPRD_Fabric01	RVNL_PRD_CTRL_WEB02_HBA1	RVNL_PRD_WEB02_HBA1 RVNL_CTRL_0D RVNL_CTRL_1B
12	DCNCPRD_Fabric02	RVNL_PRD_CTRL_WEB02_HBA2	RVNL_PRD_WEB02_HBA2 RVNL_CTRL_1D RVNL_CTRL_0B
13	DCNCPRD_Fabric01	RVNL_PRD_CTRL_WEB03_HBA1	RVNL_PRD_WEB03_HBA1 RVNL_CTRL_0D RVNL_CTRL_1B
14	DCNCPRD_Fabric02	RVNL_PRD_CTRL_WEB03_HBA2	RVNL_PRD_WEB03_HBA2 RVNL_CTRL_1D RVNL_CTRL_0B
15	DCNCPRD_Fabric01	RVNL_PRD_CTRL_WEB04_HBA1	RVNL_PRD_WEB04_HBA1 RVNL_CTRL_0D RVNL_CTRL_1B
16	DCNCPRD_Fabric02	RVNL_PRD_CTRL_WEB04_HBA2	RVNL_PRD_WEB04_HBA2 RVNL_CTRL_1D RVNL_CTRL_0B
17	DCNCPRD_Fabric01	RVNL_PRD_CTRL_DMS01_HBA1	RVNL_PRD_DMS01_HBA1 RVNL_CTRL_0B
18	DCNCPRD_Fabric02	RVNL_PRD_CTRL_DMS01_HBA2	RVNL_PRD_DMS01_HBA2 RVNL_CTRL_1C
19	DCNCPRD_Fabric01	RVNL_PRD_CTRL_DMS02_HBA1	RVNL_PRD_DMS02_HBA1 RVNL_CTRL_0B
20	DCNCPRD_Fabric02	RVNL_PRD_CTRL_DMS02_HBA2	RVNL_PRD_DMS02_HBA2 RVNL_CTRL_1C
21	DCNCPRD_Fabric01	RVNL_PRD_CTRL_MAIL01_HBA1	RVNL_PRD_MAIL01_HBA1 RVNL_CTRL_0D RVNL_CTRL_1A
22	DCNCPRD_Fabric02	RVNL_PRD_CTRL_MAIL01_HBA2	RVNL_PRD_MAIL01_HBA2 RVNL_CTRL_1D RVNL_CTRL_0A

23	DCNCPRD_Fabric01	RVNL_PRD_CTRL_MAIL02_HBA1	RVNL_PRD_MAIL02_HBA1 RVNL_CTRL_0D RVNL_CTRL_1A
24	DCNCPRD_Fabric02	RVNL_PRD_CTRL_MAIL02_HBA2	RVNL_PRD_MAIL02_HBA2 RVNL_CTRL_1D RVNL_CTRL_0A
25	DCNCPRD_Fabric01	RVNL_CTRL_BACKUP_HBA1	RVNL_BACKUP_SERVER_HBA1 RVNL_CTRL_1B
26	DCNCPRD_Fabric02	RVNL_CTRL_BACKUP_HBA2	RVNL_BACKUP_SERVER_HBA2 RVNL_CTRL_0B

2.7. Backup

2.7.1. Backup Solution

In order to ensure a data copy is retained and for faster restoration, Virtual Tape Library (VTL) will be deployed in Data Center. **HDPS Backup Software** will be used for data backup& restoration. The data will be backed up in Quantum DXi 6902. Architecture of Backup Setup is depicted below

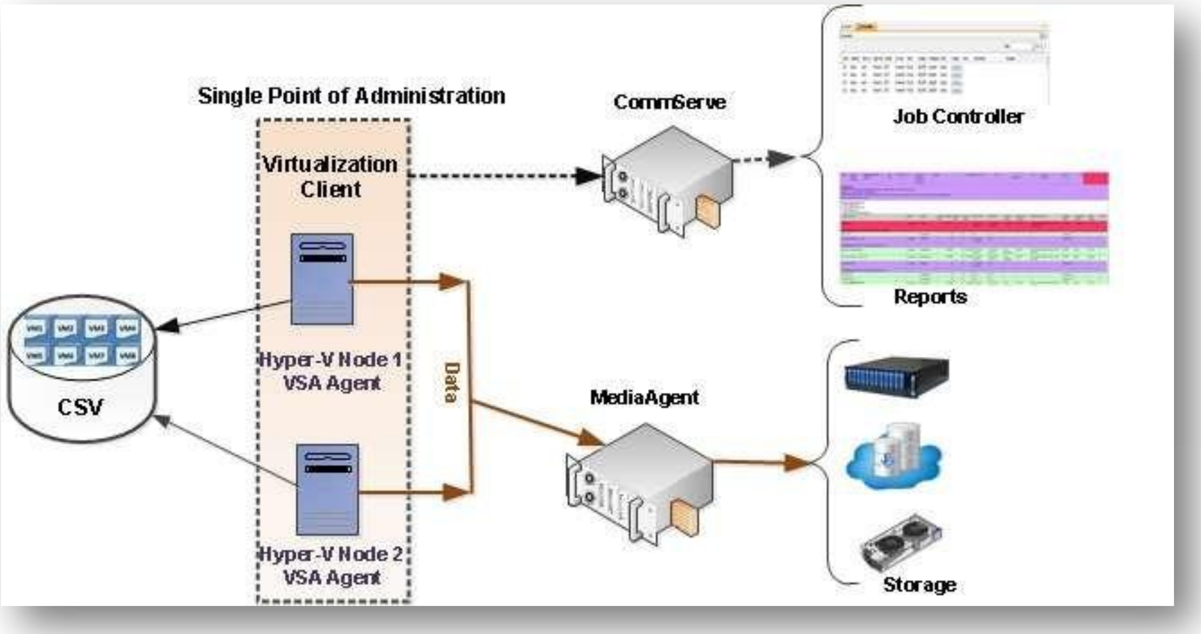


- I/O Multi-pathing will be enabled,
- Data de-duplication, Acceleration, encryption will be enabled,
- High Redundancy (Dual controllers),

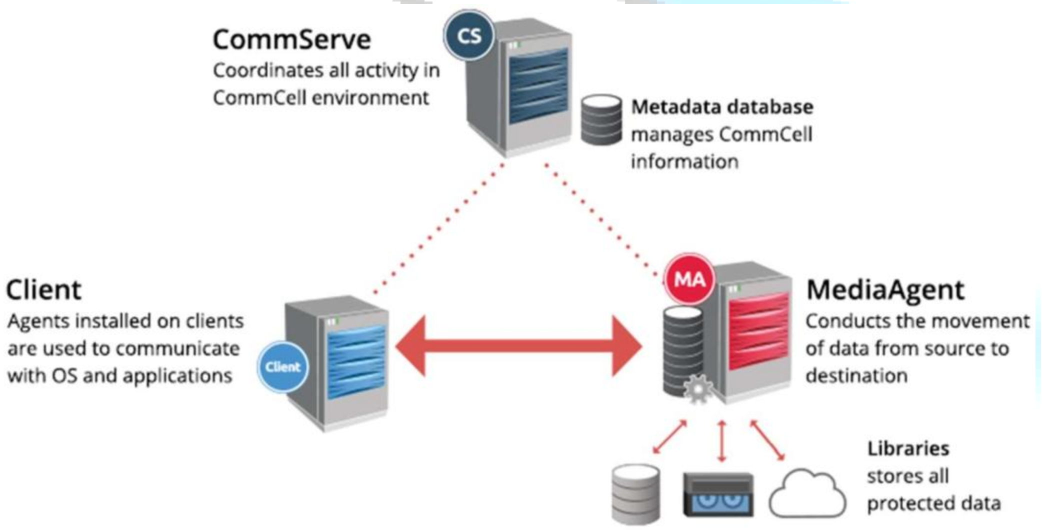
- 34TB of raw disk capacity will be deployed,
- Disk with 10K rpm
- Provide appropriate IOPS for faster restores,
- Volume Group and LUNs as per details mentioned in "Server-VM" file

2.7.2. Backup Architecture

2.7.2.1. Microsoft Hyper V, and SuSe KVM



2.7.2.2. Host, Media Agent, Backup Server and the Storage


CommServe
Coordinates all activity in CommCell environment
CS
Metadata database manages CommCell information
Client
Agents installed on clients are used to communicate with OS and applications
Client
MA
MediaAgent
Conducts the movement of data from source to destination
Libraries stores all protected data

Backup flow path

a) Data travels from the Production and the Non-Production servers through a LAN to thebackup server, the backup server backs up the data on the VTL through the SAN.

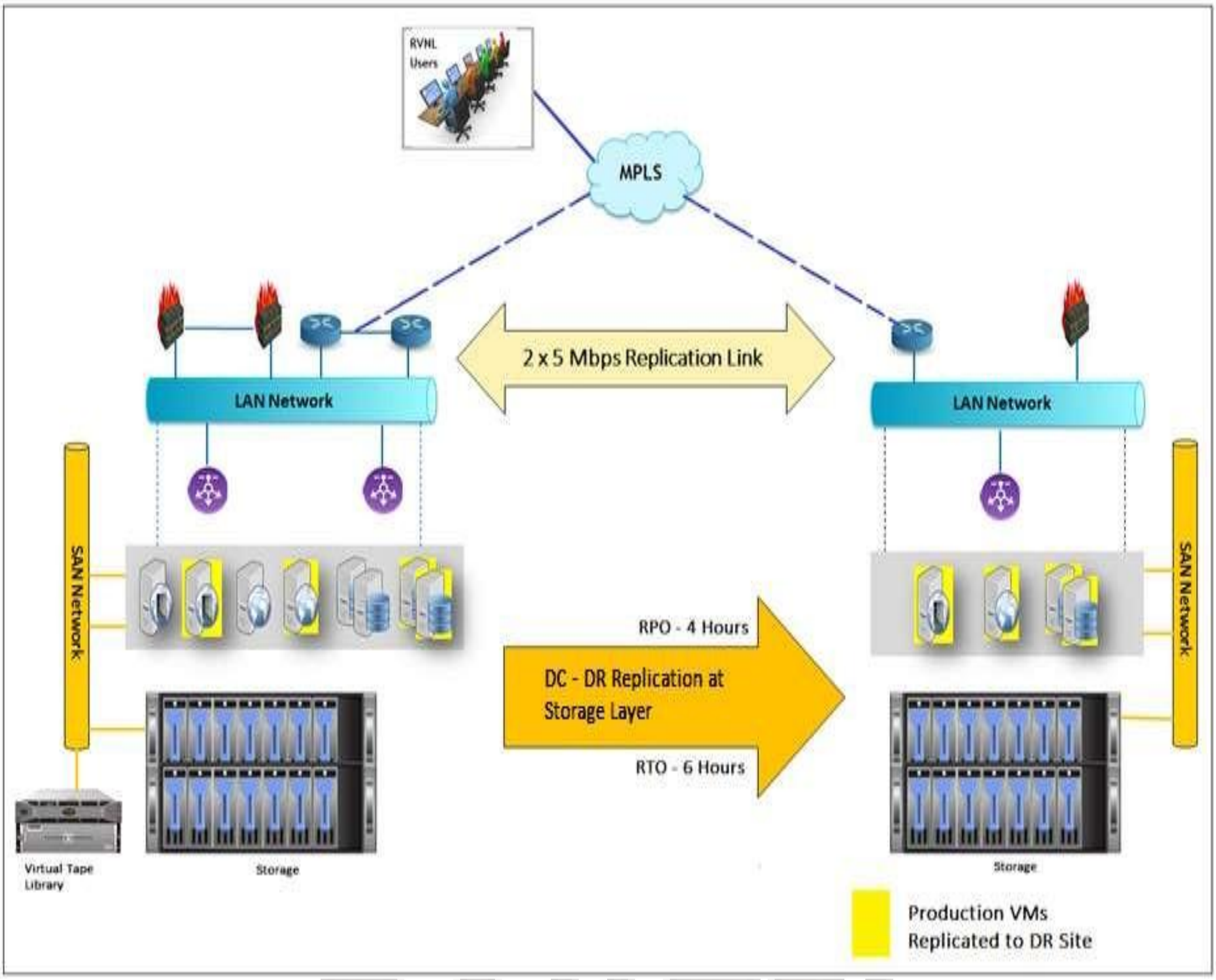
b) There are two port paths from the servers connected to Network switch A and NetworkSwitch B.

c) There are four port paths from the VTL to move the data through SAN switch A and SANswitch B.

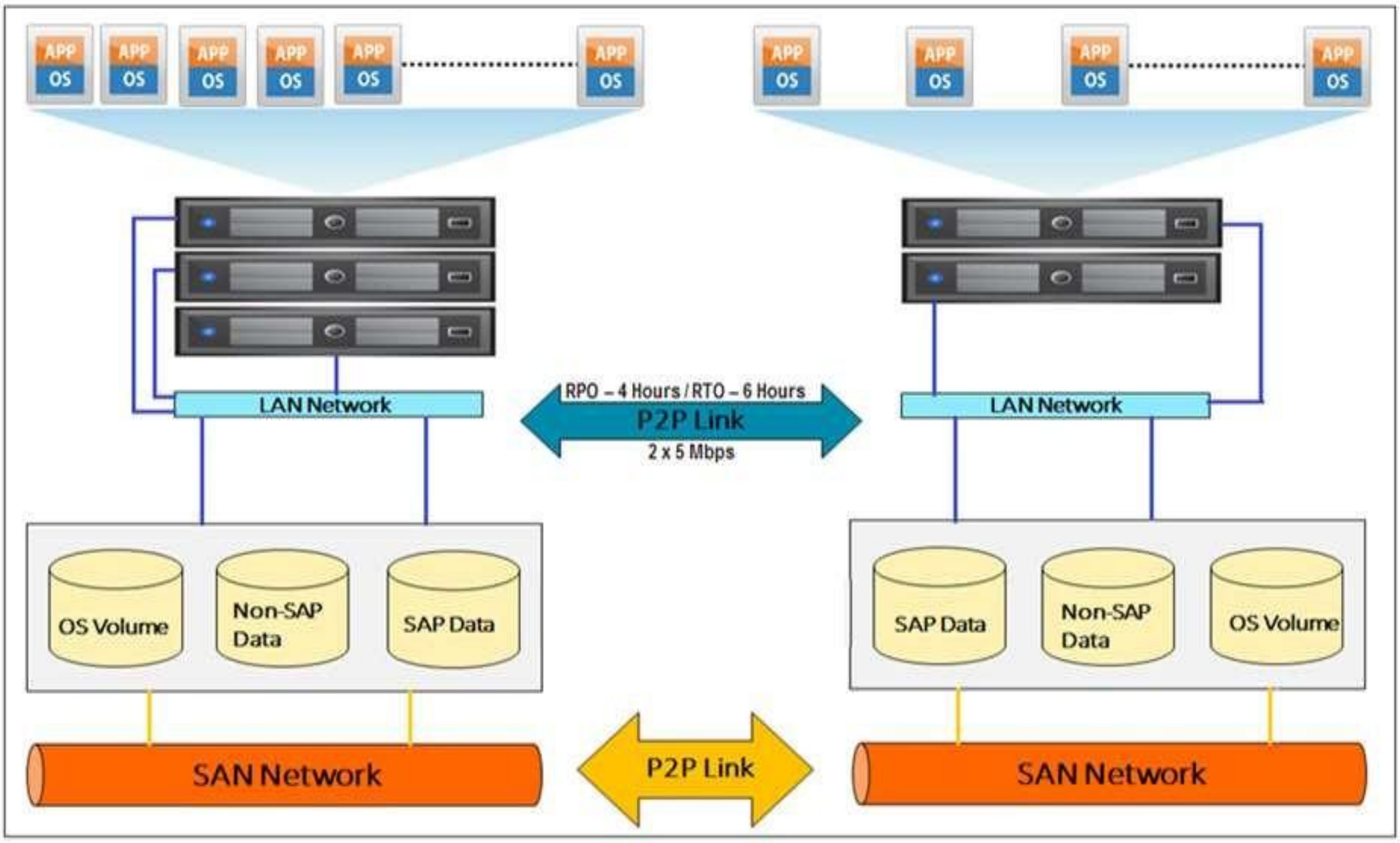
For further details on Backup policy and strategy refer the document in the “Reference”section.

3. DC-DR Connectivity

3.1. DC-DR Connectivity



3.2. DC-DR Replication



4. References

Sl. No.	Document Name	Document Description	Location
1	Backup Strategy Document	Backup Strategy, Policies design document	Solman Server
2	AD/DNS Design Document	AD/DNS design details	Solman Server
3	DC Security Design Document	DC Security, Network Design features	Solman Server
4	Email Design Document	Email Design features	Solman Server
5	VC Design Document	VC Design features	Solman Server

1. Introduction

1.1.Overview

CUSTOMER intends to implement an Integrated IT solution to meet its business needs. The Integrated IT Solution for CUSTOMER would aim to automate its business functions and would include all the Project Implementing Units (PIUs) as well as corporate office.

Incumbent service provider is implementing an integrated IT solution for CUSTOMER comprising the following key applications:

- SAP based ERP system
- Document Management System
- Geographical Information System
- Video conferring Solution
- Email System

The solution will connect 21 project implementation Units/ Offices (PIUs) of CUSTOMER from which employees will connect and use these applications.

As part of the solution, Incumbent service provider will set up the Data Center as a hosted facility in Noida and cloud based DR site at Bangalore. At each of the DC DR Site the connectivity is offered through MPLS/Internet Links by ISP’s Sify and Vodafone (Service Provider) in redundant mode.

The purpose of setting up Disaster Recovery (DR) site is to provide continuity of operations in the event of failure of Primary Data Centre (DC). The DR solution is majorly based on Infrastructure and cloud as a service and is deployed at Sify’s Tier-III Data Centre in Bangalore.

1.2. Purpose of the document

The purpose of this document is to present a description of the services, components and features of IT infrastructure deployed at the Disaster Recovery Site. The details mentioned in the document are based on the requirements mentioned in the RFP for Integrated ERP Project.

1.3. Details of the Disaster Recovery Site

The Disaster Recovery center is based out following address:

SIFY Technologies Pvt Ltd

Plot No.76/77, 3rd Floor, Cyber Park, Doddathogaur
Village, Electronic City Phase 1,Bangalore – 560100.

Scope of work and service details-

Sr. No.	Category	Component
One Time Installation		
1	Colo Rack	Colo Rack readiness
2	Rack and stack withcabling	Sify supplied Compute and storage Hardware Rack andStack in Colo Rack and inter rack cabling
3	Rack and stack withcabling	Client supplied Network devices and hardware rack andstack in Colo Rack and inter rack cabling
4	Configuration information	All configuration information to be provided by Client forall devices
5	Monitoring Agent	Monitoring agent installation (For instance always power ON)
6	Storage installation	Storage installation as per configuration informationprovided by client
7	Data replicationconfiguration	One time storage replication configuration
8	Hypervisor Installation	Hypervisor installation as per confirmation from client
9	VM creation on hypervisor	Virtual Machine Configuration as per configurationinformation provided by client
10	OS Installation	Operating system installation
11	Antivirus installation	Antivirus installation
12	DB, APP Installation	Database, Application Installation
13	Network devices installation	All network devices installation which are supplied by Client
14	Any Other device/service installation'	Installation of any other device/services
Managed Services		

15	KVM Hypervisor Support	KVM Hypervisor Support
16	HyperV Hypervisor Support	HyperV Hypervisor Support
17	Data Replication	Data Replication Monitoring and Managemnet
18	Email Security Appliance	Monitoring and Management of Cisco ESA-380
19	IPS	Monitoring and Management of Radware DP-2412
20	Web Application Firewall	Monitoring and Management of Palo Alto WAF-5020
21	Load Balancer	Monitoring and Management of Array Network APV-2600T
22	Proxy	Monitoring and Management of Bluecoat SSG 900
23	SSL VPN	Monitoring and Management of Array NetworkAG 1100
24	AAA	Monitoring and Management of Cisco SNS 3145-K9
25	Database Encryption	Monitoring and Management of Safenet KS-250
26	Firewall at DR site	Monitoring and managemnet of Firewall supplied by Sify
27	Vendor Management	Vendor co-ordination for sify supplied hardware
28	DR monitoring	Monitoring of DR instances, where DR replication by sifyprovided monitoring tool
29	Monitoring setup	Monitoring setup for all hardware and software
30	Required Access/resources for Sify Team	Required access/resources for sify team to monitor andmanage device/services for client

2. Solution Requirements for DR Site

- The disaster recovery center has been setup in Bangalore, India to ensure continuity ofoperations in the event of failure of primary data center.
- The DR solution implemented is based on cloud services offered by Sify which has a Tier IIIData Center in Bangalore.
- The cities for Data Center – Noida & Disaster Recovery Center – Bangalore are in twodifferent seismic zones.
- The solution implemented for CUSTOMER has two sites, one active (Data Center in Noida) and one passive (Disaster Recovery center in Bangalore). Each site is a self-contained system
- Incremental backups will be taken periodically and sent across to the DR site. RPOmaintained is 4 hrs.
- During normal operations, the active site will serve the requests. The passive site will not be performing any work but will remain on standby. This is the period during which the Compute environment for the application (except Video Conferencing which is not available in DR) will be available but with a low compute resource allocation. The application environment will be installed and ready for use at the instance of full computeDR Database Storage will be replicated on an ongoing basis and will be available in full as per designed RTO of 6 hrs. & RPO of 4 hrs.
- Redundant Network connectivity is maintained at DR by provisioning links from two ISPs –Sify & Vodafone.
- DR will be invoked under following circumstances:
  - Process & Hardware/infra failure- No DR call out for failure < 1 day (Ref table “DRInvoke Incident for details”)
  - Primary Site Application landscape & Hardware/infra failure- DR call out forfailure > 1 day (Ref table “DR Invoke Incident for details”)
  - During DR call out, entire DC application landscape will be made available at DRsite not for individual application.
- DR Invoke Incident Details-

Sr#	Incident	Resolution time	DR to be invoked
1	Power Outage	< 1 hour	No

2	Server/OS crash	< 1 hour	No
3	Fire/Explosion	> 1 day	Yes
4	Earthquake	> 1 day	Yes
5	Grid Failure	> 1 day	Yes
6	Acts of Terrorism/ Social unrest	> 1 day	Yes
7	DC Server hardware failure	> 1 day	Yes
8	WAN Link/ Communication Failure at DC	> 1 day	Yes
9	Virus Attack, Hacking	> 1 day	Yes

2.1 DR Invoke Process

The following steps would be conducted sequentially to start the DR services from DR.

Disaster Recovery Scenario		
Sr. No	**Activity**	**Owner**
	Prerequisites	
P-1	Communication to CUSTOMER Authority	DR Lead
P-2	Communication to all DR Drill team	DR Lead
P-3	Plan of action if DR Drill exceed time	DR Lead
P-4	Communication to ISP if required	DR Lead
P-5	Suspend all backup at Main Site during drill	Storage Team
P-6	Suspend all Application Batch Jobs at Main Site DC	ApplicationOwner
P-7	Setup for Bridge Communication	DR Lead
	Disaster Declaration	
1	**Declare Data Centre site availability**	DR Lead
1.1	Initiate DR Availability Process	DC-DR Lead
1.2	Inform Module Leads	DR Lead
1.3	Inform External Vendors	DR Lead
	DC to DR Failover Process	
2.1	**Isolating the DC Setup from External World**	Network Team
2.1.1	Disable all WAN Links / Routers at DC	Network Team
2.1.2	Confirm that DC Network is Down	Network Team
2.2	**Connecting the DR Setup to External World**	

2.2.1	Enable all WAN Links / Routers at DR	Network Team
2.2.2	DNS route to DR site	Network Team
2.2.3	Firewall rules to be updated	Network Team
2.2.4	Network Netting and Routes to updated for DR Connectivity	Network Team
2.2.5	Enable routing to all PIU's from DR site	Network Team
2.2.6	Internal DNS entry to be updated at DR site	Network Team
2.3	**Verify all Physical Servers and VMs are Up & Running at DR Site**	
2.4	**AD-DNS**	
2.4.1	Check last replication (Sysvol/NTDS and GPO)	Admin Team
2.4.2	Freeze the FSMO role on DC AD	Windows Team
2.4.3	Transfer the FSMO role	Windows Team
2.4.4	Restart Sysvol and Netlogon service	Windows Team
2.5	**DMS**	
2.5.1	Shutdown DMS application at DC.	Windows Team
2.5.2	Stop DB services at DC	Windows Team
2.5.3	Check the Last replication file on DR	Windows Team
2.5.4	Configure DB at active mode	Windows Team
2.5.5	Check PN file	Windows Team
2.5.6	Start DB services	Windows Team
2.5.7	Access from DR site	Windows Team
2.5.8	start Jboss services on respective server	Application Team
2.6	**GIS**	
2.6.1	Shutdown GIS Application at DC	Application Team
2.6.2	Stop DB services at DC	Windows Team
2.6.3	Check the Last replication file on DR	Windows Team
2.6.4	Configure DB at active mode	Windows Team
2.6.5	Start DB services	Windows Team
2.6.6	Start ArcGIS server services	Windows Team
2.6.7	Start ArcGIS map services in ArcGIS manager	GIS Team
2.6.8	Start the GIS application in IIS	GIS Team
2.7	**SAP Activity at DC & DR**	
2.7.1	SAP Standalone DC Systems - Shut down all applications, Shut down DB(GUI, Portals, Solman, DMS, SRM)	SAP Team
2.7.2	SAP Team to confirm the shutdown to Linux Team	SAP Team
2.7.3	SAP Clustered Systems - Make Resource groups offline gracefully	Linux Team
2.7.4	Verify no DB & application is up and running	Linux Team
2.7.5	SAP Team to confirm the shutdown to Linux Team	SAP Team

2.7.6	Unmount Filesystem from Cluster & Standalone Servers	Linux Team
2.7.7	Linux Team to confirm the FS Unmount to SAP Team	Linux Team
2.7.8	Intranet Setup	Network Team
2.7.9	SAP Team to Confirm to Linux Team to start DR activity	SAP Team
2.7.10	Make all DR LUNs ID as Write Enabled & inform Application Team to proceed	Linux Team
2.7.11	Storage Team to confirm the LUNs Status to Linux Team	Linux Team
2.7.12	SAP DR Systems – Mount all filesystems in global Zone, Start the LocalZones	Linux Team
2.7.13	Initiate startup of Listener & DB, Start the Applications, VerifyApplication functionality	SAP Team
2.7.14	Confirm SAP Setup is Down at DC & Up at DR Site	SAP Lead
2.8	**Verification of Standalone Supporting Applications**	
2.8.1	Ensure VPN Connectivity shutdown at DC and started from DR Site	Network Team
2.8.2	Ensure SSO functionality shutdown at DC and started from DR Site	respective vendor
2.8.3	Ensure Email functionality shutdown at DC and started from DR Site	respective vendor
2.8.5	Ensure SMS-OTP functionality shutdown at DC and started from DR Site	respective vendor
2.8.6	Ensure EMS functionality shutdown at DC and started from DR Site	respective vendor
2.8.7	Ensure Antivirus functionality shutdown at DC and started from DR Site	Admin Team
2.9	**Declare Availability of DR Site for Testing**	
3.0	**Connecting the DR Setup to External World**	

3. Solution Details

Under the DR Setup compute infrastructure is cloud based support by nine (9) appliances supplied by L&T, other technical support shall be provided and managed by Sify as DR Service provider, and details are discussed in subsequent sections under this document.

Primarily data replication would be enabled from Primary DC Site to DR, in case of SAP systems it will be purely Storage based replication and for non-SAP systems, it will be native and DFS based replication.

The underlying sub-sections will contain details about the DR Solution specific to:

- Rack Layout
- Overall architecture
- Network connectivity Details
- Storage Details
- Replication methodology used
- IP details for DR

3.1. Rack Layout

	RACK-01(FSR-16)						
U	**Equipment Description**	**Make**	**Model**	**Power (In Watt)**	**Serial No**	**Hostname**	**Remarks**
42	Access Switch-01	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
41	Router -Cisco 1841	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
40	IPS - Radware						
39		Radware	DP-2412	451(2)	31412056	DRNWDPRD_IPS01	Power rating from Datasheet
38							

37	Fortigate 100D	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model
36	DELL N3024 Switch	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model
35	Brocade 300	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model	Under Sify’s cloud model
34	RADWARE AP SoluteVision	Radware	ODS-VL	168	31506004	DRNWDPRD-IPSMGR01	Power rating from Datasheet
33	AAA	Cisco	SNS 3145-K9	650	FCH2003V1TY	DRNWDPRD-ACS01	Power rating from datasheet
32	Array Network APV A2600	Array	APV 2600T	143.19(2)	1537G8439	DRNWDPRD-SLB01	Power rating from datasheet
31	Array Network APV AG1100	Array	AG1100	134	1538G8477	DRNWDPRD-SSL01	Power rating from datasheet
30	Proxy - Blue Coat	Bluecoat	SG900	400	1515240013	DRNWDPRD-PRXY01	Power rating from datasheet
29							
28	WAF - Palo Alto	Palo Alto	PA-3020	450(2)	1801028675	DRNWDPRD_WAF 01	Power rating from datasheet
27	Database Encryption - SafeNet Keysecure K250	Safenet	K250	60	KS-250-74DL-AAUE-AET-2-H	DRNWDPRD-DBENC01	Power rating from datasheet
26							
25	Email Security Appliance - Cisco ESA	Cisco	C380	650(2)	FCH2003v197	DRNWDPRD-ESA01	Power rating from datasheet
24							
23							
22							
21							
20							

19							
18							
17							
16	NEC Server Express 5800	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
15	NEC Server Express 5800	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
14	NEC Server Express 5800	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
13	NEC Server Express 5800	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
12							
11							
10							
9	Netapp Controller	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
8							
7							
6	NETAPP Disc SelfArray	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model	Under Sify's cloud model
5							
4							
3							
2							
1							

🟩 Items supplied & managed by Sify as a part of DR cloud serviceItems

🟦 supplied by Incumbent service provider

Note: For DR, Incumbent service provider as an SI has supplied only 9 appliances. Rest all infra isprovisioned and managed by Sify as a part of DR cloud service.

3.2. IP Management

Subnet - 10.30.0.0/19

VLAN Name	VLAN ID	IP Subnet	Gateway	Host IP Address Range
Sify MGMT	100	192.168.94.0/24	192.168.94.254	192.168.94.1-192.168.94.254
L&T Management VLAN	104	10.30.0.0/24	10.30.0.254	10.30.0.1-10.30.0.254
Network Devices Data Segment (Like Proxy etc...)	101	10.30.1.0/2	10.30.1.254	10.30.1.1 - 10.30.1.254
Server Farm- Non-Infra VMs like SAP, DMS & GIS)	111	10.30.11.0/24	10.30.11.254	10.30.11.1 - 10.30.11.254
Server farm- Infra VMs like AD, SMS/OTP, AV , EMS etc.	109	10.30.9.0/24	10.30.9.254	10.30.9.1 - 10.30.9.254

4. Function of Appliances deployed at DR Site

The detailed functioning of each of the nine appliances deployed at DR sites has been discussedunder this section, the details of appliances as per table below and functioning is mentioned in the subsequent sections as under:

Sr. No.	Device	OEM	Model	Qty.	Serial No.
1	Email Security Appliance	Cisco	ESA-380	1	FCH2003V197
2	IPS	Radware	DP-2412	1	31412056
3	Web Application Firewall	Palo Alto	WAF-3020	1	1801028675

4	Load Balancer	Array Networks	APV-2600T	1	1537G8439
5	Proxy	Blue Coat	SSG 900	1	1515240013
6	SSL VPN	Array Networks	AG 1100	1	1538G8477
7	AAA	Cisco	SNS 3145-K9	1	FCH2003V1TY
8	Database Encryption	SafeNet	KS-250	1	KS-250-74DL-AAUE-AET-2-H
9	IPS Management	Radware	Absolute Vision	1	31506004

Security protocols of the supplied devices is as follows:

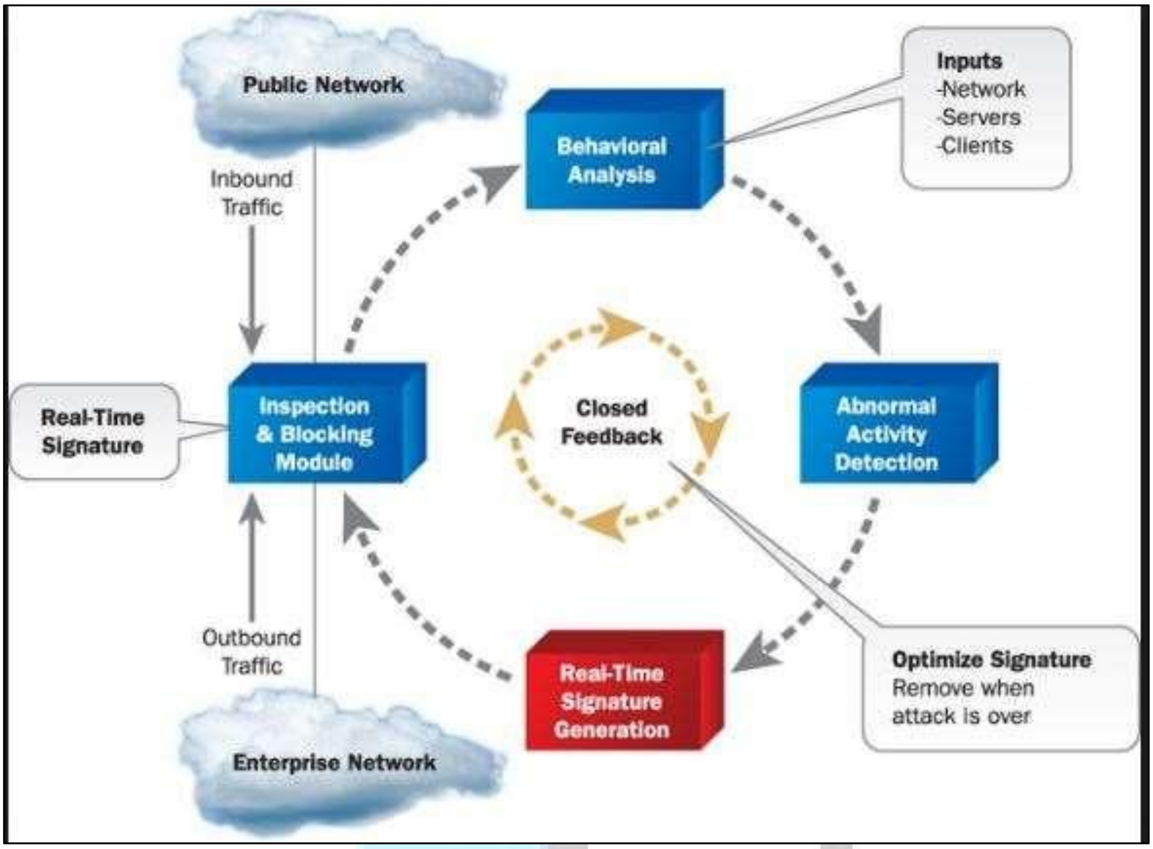
Sr. No.	Device	Protocols
1	Load Balancer	HTTPS port no 8888, SSH-22,SNMP
2	SSL VPN	HTTPS port no 8888, SSH-22, HTTPS-443,SNMP
3	Email Security Appliance	HTTPS-443,SSH-22,SNMP, MAIL ports(pop, IMAP, SMTP and with secure)
4	IPS	HTTPS-443,SSH-22,SNMP
5	Proxy	HTTPS-8080,SSH-22,SNMP,HTTP-80
6	AAA	HTTPS-443,SSH-22,SNMP,TACAS and RADIUS port
7	IPS Management	HTTPS-443,SSH-22,SNMP
8	Web Application Firewall	HTTPS-443,SSH-22,SNMP,ICMP
9	Database Encryption	HTTPS-443,SSH-22,SNMP

4.1. IPS and IPS Management

At perimeter layer the Users/connections need to pass through Radware Defense Pro IPS. This device will be configured as DoS (uses one computer and one Internet connection to flood a targeted system or resource) and DDoS (uses multiple computers and Internet connections to flood the targeted resource) protection device and will maintain business continuity by protecting CUSTOMER application infrastructure against existing and emerging network-based threats. Additionally, it will provide below features based on the latest signature, virus definition configured on these devices.

- Network and Application-Resource misuse
- Malware attack and spreading
- Authentication defeat and information theft
- Proactive signature updates
- Preventing the known attacks, including worms, Trojans, bots, SSL-based attacks, and VoIP attacks,
- Automatically generated real-time signatures prevent non-vulnerability–based attacks and zero-minute attacks such as network and application floods, HTTP page floods, malware propagation, Web application hacking, brute force attacks aiming to defeat authentication schemes.

Defense Pro will provide the Protection to DR Network without blocking legitimate users traffic and with no need for human intervention using Radware Absolute Vision Security Management appliance.



4.2. Proxy Solution

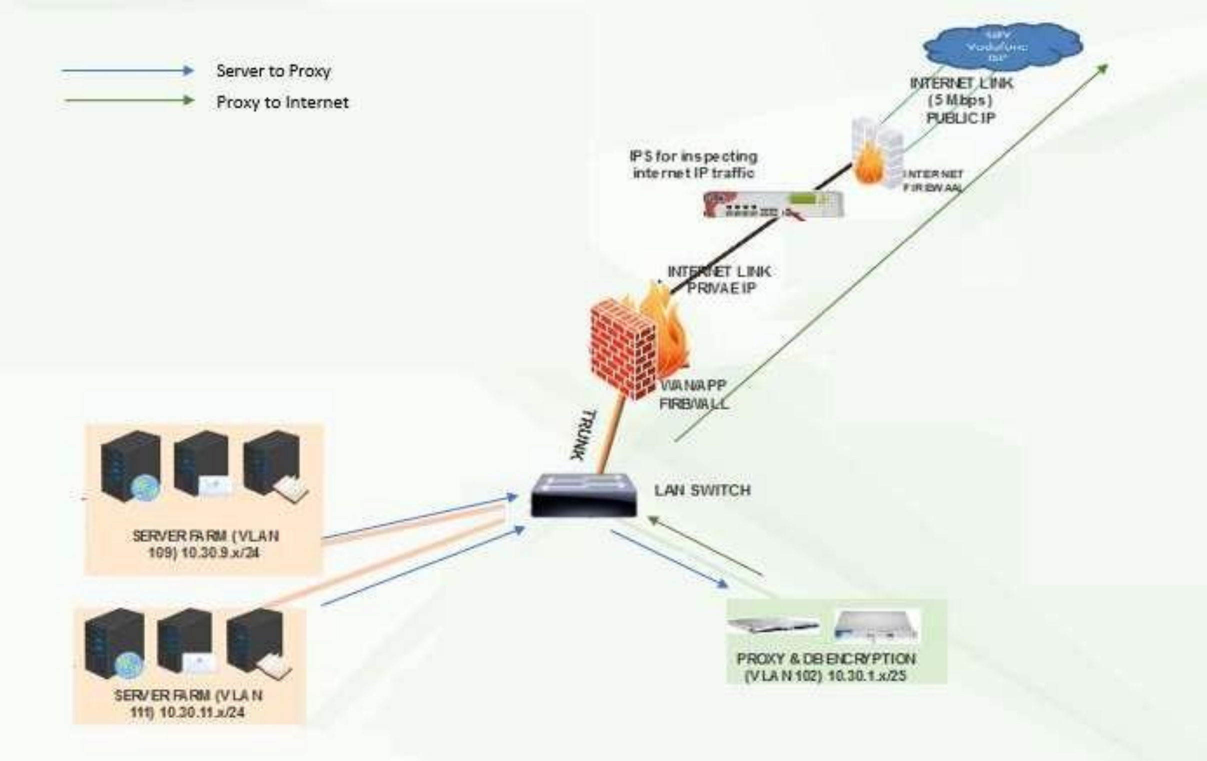
Bluecoat has been deployed on DC as internet proxy for the Web Traffic filtering for downstream servers towards internet. Internet request which will comes from downstream servers will be validated via bluecoat proxy for malicious traffic and filter unwanted content. Limiting or blocking the access to social websites and other unwanted websites.

The data traffic and management traffic are segregated by using different interfaces for management connections and data connections

Blue Coat ProxyAV1200, configured as part of the Security and Policy Enforcement Center, offers advanced malware detection at the gateway in collaboration with Blue Coat ProxySG appliances. ProxyAV appliances provide in-line threat protection and malware scanning of web content at the gateway. Together, ProxyAV and ProxySG provides greater performance and the lowest hardware footprint requirements, so it can protect against viruses, Trojans, worms, spyware and other forms of malicious content.

Work Flow:

1. DR Server trying to access internet will have the flow process as the request will be firstrouted to Bluecoat proxy SG900 via Application firewall.
2. If request access is granted via advance filtering, then the request is forwarded tointernet Firewall placed in the below flow diagram.
3. WAN firewall the request goes to IPS.
4. Then Traffic will forward to Internet Firewall from IPS after packet inspections
5. From Internet Firewall traffic will go to internet sites



4.3. AAA

Cisco Secure Access Control Server (ACS) is an access policy control platform that helps you comply with growing regulatory and corporate requirements. By integrating with your other access control systems, it helps improve productivity and contain costs. It supports multiple scenarios simultaneously, including:

Device administration: Authenticates administrators, authorizes commands, and provides an audit trail

Remote Access: Works with VPN and other remote network access devices to enforce access policies

Network admission control: Communicates with posture and audit servers to enforce admission control policies

Authentication-

All system / server level authentication of the CUSTOMER IT infrastructure components will utilize a centralized directory service (LDAP or AD system) in as per CUSTOMER defined policies, standardsand technical controls.

Authorization-

All system level authorization will be RBAC (Role Based Access Control) authorization that is implemented through a centralized directory service (LDAP or AD system) in conjunction with CUSTOMER standards.

Accounting-

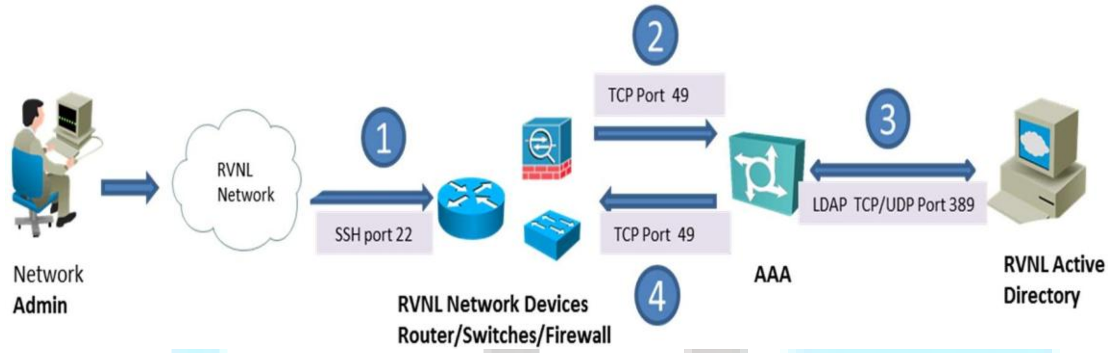
Audit logging will be configured for the following:

Account Management (user/group creation, modification, deletion)

Logon Events (logon, logoff, account lock-out)

Any additional events can be subsequently enabled for audit based on specific furtherrequirements.

AAA Appliance Call flow process



For session request:

1. Network administrator logs (Protocol SSH port 22) onto a network device

2. The network device sends a TACACS+ (TCP Port 49) access request to AAA

3. AAA uses an identity store (AD) to validate the user's credentials (LDAP TCP or UDP port389).

4. AAA sends a TACACS+ (TCP Port 49) response to the network device that applies the decision. The response includes parameters, such as the privilege level that determines thelevel of administrator access for the duration of the session

4.4. Load Balancer

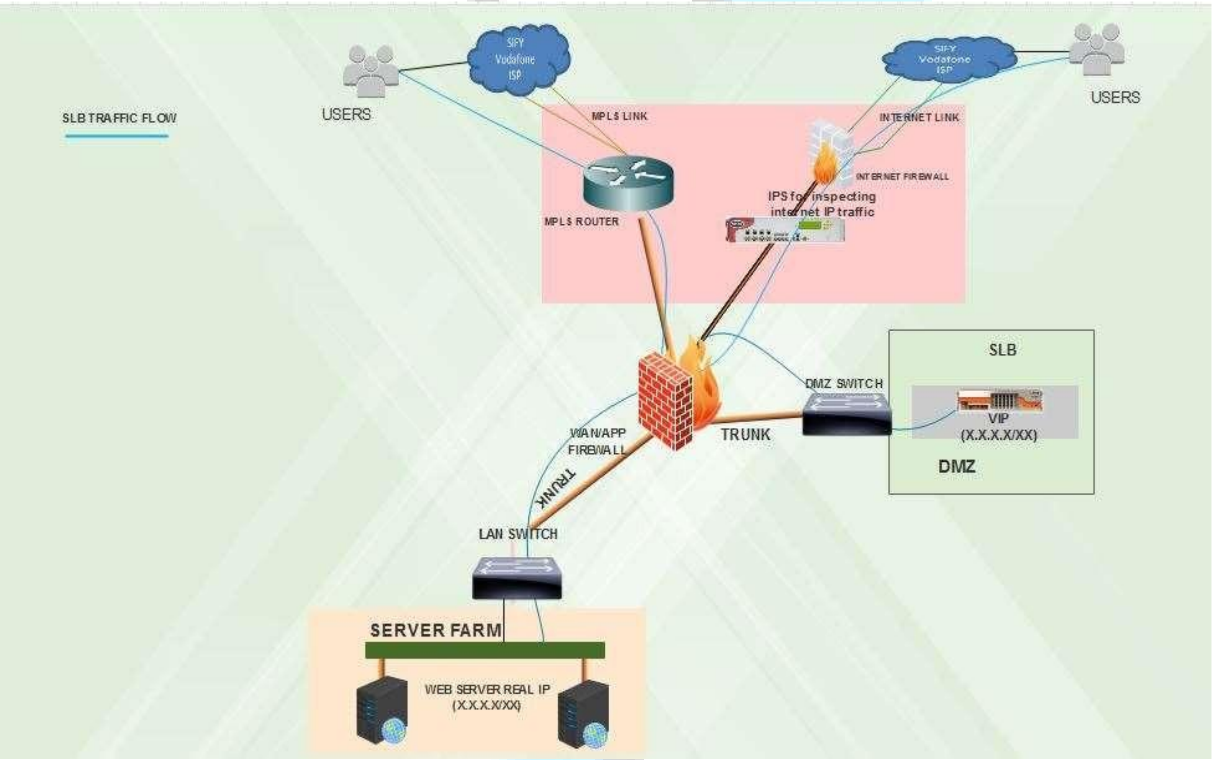
Array Networks APV -2600T Load balancer would be used to efficiently distribute incoming network traffic across a group of backend servers over cloud at CUSTOMER DR Site (here in after server may be referred as VMs over cloud). In this manner, it would perform the following functions:

Distributing client requests or network load efficiently across multiple cloud based servers. It would act as the “traffic cop” sitting in front of servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which may result to performance degrade.

In DR under load balanced environment if a single server goes down, the load balancer redirectstraffic to the remaining online servers or VMs. Whenever a new server would be added to the server group, the load balancer would automatically start sending requests to it.

In this manner, array load balancer at DR would performs the following functions:

- Distributing incoming client requests or network load efficiently across multiple servers
- Ensuring high availability and reliability by sending requests only to servers that are online
- Providing the flexibility to add or subtract servers as demand arises



1. Users will use FQDN in browser. Internet DNS Server will resolve FQDN to portal Public IP address and route the traffic to DR Internet firewall.
2. Internet firewall will translate the traffic from SLB hosted portal Public IP address to portal Private IP and Forward that SLB Traffic to DMZ zone based on the Firewall policy.
3. IPS will inspect the traffic to identify the SSL Based DoS and DDoS attacks. Once thetraffic inspected by IPS, It will be forwarded to WAN Firewall
4. Once portal traffic reach SLB devices, SLB will resolved actual IP and test the availabilityand based on the availability
5. SLB will route the traffic to the relevant application servers via WAN Firewall.
6. WAN firewall will inspect and filter the traffic based on the Firewall policy and forwardthe traffic to Application/Portal server via Switch.

Security Architecture- SLB and APP Access Data Flow via MPLS

The traffic will come from MPLS route in this section.

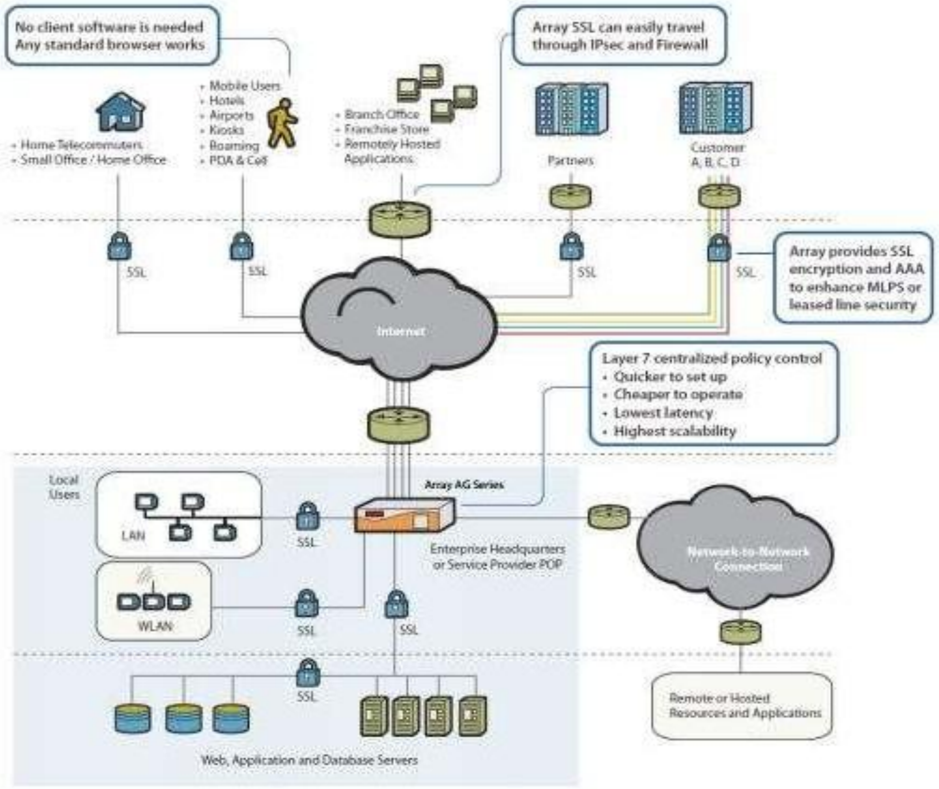
1. Users will use FQDN in browser. Internal DNS Server will resolve FQDN to portal privateIP address and route the traffic to DR MPLS Router.
2. DR MPLS router Route the SLB traffic to DMZ zone via WAN firewall
3. Based on the rules MPLS router will route the traffic to DMZ (SLB) via WAN firewall.
4. Once portal traffic reach SLB devices, SLB will resolve actual IP and test the availability and based on the availability
5. SLB will route the traffic to the relevant application servers via WAN Firewall.
6. WAN firewall will inspect and filter the traffic based on the Firewall policy andforward the traffic to Application/Portal server via Switch.

4.5. SSL VPN

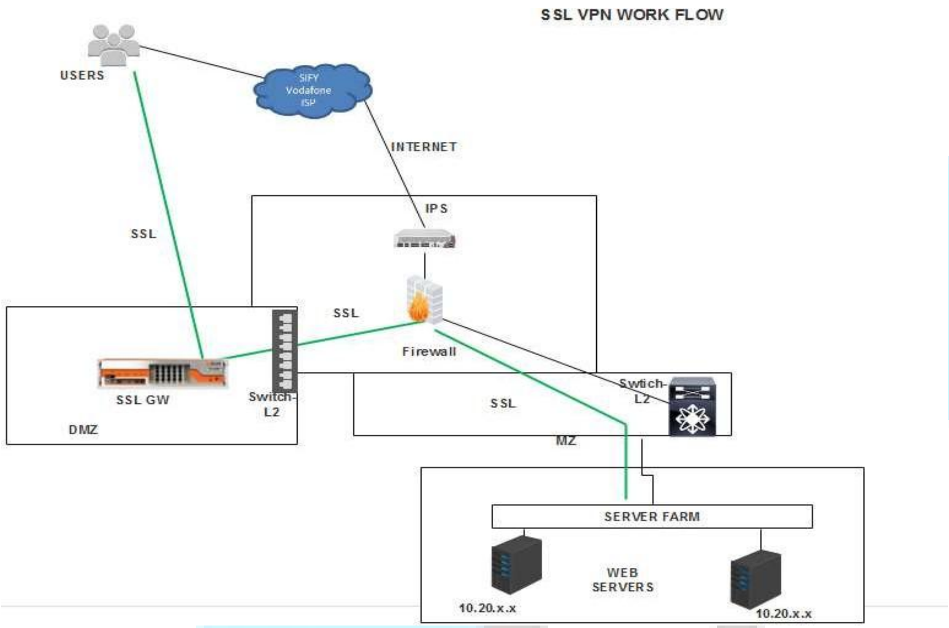
An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It's used to give remote users with access to Web applications, client/server applications and internal network connections.

A virtual private network (VPN) provides a secure communications mechanism for data and other information transmitted between two endpoints. An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security protocol.

SSL VPN Work Flow: Device



ARRAY SSL VPN: Actual Data Flow



Work Flow:

1. Users will use FQDN to logon to SSLVPN device. Internet DNS Server will resolve FQDN toSSL VPN Public IP address and route the traffic to DR Internet firewall via IPS.
2. IPS will inspect the traffic to identify the SSL Based DoS and DDoS attacks. Once thetraffic inspected by IPS, It will be forwarded to Internet Firewall
3. Internet firewall will translate the traffic from SSL VPN Public IP address to SSL VPN Private IP and Forward that SSL VPN Traffic to DMZ zone based on the Firewall policy.
4. once SSL VPN traffic reach SSL VPN devices, it will prompt for username and Password with OTP information. once user Enter their USER Credential, this credential cross verifiedwith SSO Identify Server for authorization.
5. once traffic authorised by Web SSO Identify Server, then it will be forwarded to web SSOAccess gateway (Proxy gateway)
6. when user try to access any application linked in SSL VPN, it will try to reach the application server (SAP, DMS and GIS) via Server Load balancer (SLB)
7. SLB will route the traffic to the relevant application servers via WAN Firewall.
8. WAN firewall will inspect and filter the traffic based on the Firewall policy and forwardthe traffic Application/Portal server via switch.