TENDER NO: ***SCCC/EST/2023/002***

UEN Registration No.: 201309577Z

TENDER FOR IT INFRASTRUCTURE TECH REFRESH AND MANAGED IT SERVICES AT THE SINGAPORE CHINESE CULTURAL CENTRE

INVITATION TO TENDER

1. Singapore Chinese Cultural Centre invites your tender to offer for the IT infrastructure tech refresh and managed IT services to Singapore Chinese Cultural Centre (SCCC).

2. The following documents that form part of this Tender Document have been prepared to enable prospective vendors to tender for the above-mentioned works that would meet the SCCC's requirements and specifications. These forms may be obtained from **https://singaporeccc.org.sg/tenders-quotations/**

   - Tender Guidelines
   - Conditions of Contract
   - Draft Banker's Guarantee
   - Technical Specification
   - Tenderer's Offer (FORM A)
   - Tenderer's Profile (FORM B)
   - Price Schedule of Tenderer's Offer (FORM C)
   - Tenderer's Proposal – Equipment Specifications (FORM D)
   - Tenderer's Proposal – Equipment Support and Maintenance (FORM E)
   - Tenderer's Proposal – Software Support (FORM F)
   - Tenderer's Proposal – Training (FORM G)
   - Major Projects completed by Tenderer's Company within the 3 years (FORM H)
   - Current Projects undertaken by Tenderer's Company (FORM I)
   - Profile of Tenderer's Project Team (FORM J)
   - Tenderer Compliance List (FORM K)

3. The Tenderer is required to complete and submit the following documents in sealed envelope, together with all technical data on the equipment and any other supporting data or relevant information in a ring bound A4 folder, in duplicate, to SCCC before the closing date of tender:

   - Tenderer's Offer (FORM A)
   - Tenderer's Profile (FORM B)
   - Price Schedule of Tenderer's Offer (FORM C)
   - Tenderer's Proposal – Equipment Specifications (FORM D)
   - Tenderer's Proposal – Equipment Support and Maintenance (FORM E)
   - Tenderer's Proposal – Software Support (FORM F)
   - Tenderer's Proposal – Training (FORM G)
   - Major Projects completed by Tenderer's Company within the 3 years (FORM H)
   - Current Projects undertaken by Tenderer's Company (FORM I)
   - Profile of Tenderer's Project Team (FORM J)
   - Tenderer Compliance List (FORM K)

4. The closing date for submission of tender is **29 December 2023, 2.00pm**.

5. A compulsory site briefing will be conducted on 5 December 2023 at 2pm at 1 Straits Boulevard, Singapore 018906. You are required to register for the briefing at the following email estates@singaporeccc.org.sg by 1 December 2023, 2pm.

6. Schedule of payments is thirty (30) days after the successful completion of the Acceptance Test.

7. Liquidated damages will be charged at 5% of tender award per week for each week's delay (and a proportionate part of this amount for delay for any period of less than a week).

TENDER GUIDELINES

1. DEFINITIONS

1.1 All terms used in the Tender Guidelines, which are defined under clause 1 of the Conditions of Contract, shall have the meanings so described to them.

2. SUBMISSION OF TENDER

2.1 The tenderer shall complete and sign the Tender's Offer and complete all parts of this Tender Document required to be completed by a tenderer.

2.2 The Tenderer shall submit this Tender Document in a seal envelope deposit by hand into the Tender Box located at SCCC by the stipulated date and time. The tenderer shall mark the top left-hand corner of the envelope with:

SCCC/EST/2023/002
29 December 2023, 2.00pm
Tenders in sealed envelopes are to be deposited into the Tender Box located at 1 Straits Boulevard, L1 Lift lobby. Singapore Chinese Cultural Centre

2.3 Tenders submitted after the stipulated date and time will not be accepted.

2.4 The Tenderer shall also submit samples of the goods and/or packages if SCCC so requests.

- Such samples shall be delivered at the site and by the time stipulated in the Invitation to Tender and should be marked clearly with the Tender number, item number and the name of the tenderer. Failure to provide the required samples at the stipulated time may render the tender liable to be disqualified.

- The tenderer shall indicate whether he wishes the samples to be returned. If no indication is given, SCCC shall not be obliged to return any samples to the tenderer.

- All cost, including but not limited to all shipping and transportation duties incurred in providing and delivering such samples to SCCC shall be borne by the Tenderer.

2.5 Tenderers shall submit the tender and supporting brochures/handbooks in the number of sets as specified in the Invitation to Tender. One set is to be marked "original" and the other set is to be marked "copy".

2.6 All expenses incurred in the preparation of this tender shall be borne by the Tenderer.

3. GOODS AND SERVICES TAX (GST)

3.1 The tenderer shall not include any Goods and Services Tax (GST) in the Price Schedule of Tender's Offer.

3.2 The tenderer shall declare his GST status in his tender. He shall clearly indicate whether he is, or whether he will be a taxable person under the GST Act. He shall, if available, furnish the GST registration number to SCCC.

3.3 If the Tenderer is a taxable person under the Singapore GST Act, SCCC will pay the Tenderer, in addition to the rates and prices proposed, the GST chargeable on the supply of Goods and Services provided pursuant to this tender.

3.4 A Tenderer who declares himself to be a non-taxable person under the GST Act but who becomes a taxable person after the award of the tender shall forthwith inform SCCC of his change in GST status. He shall be entitled to claim from SCCC any GST charged on the supply of the Goods or Services made by him after his change in GST status.

4. QUERIES

Any queries in respect of this Tender Document or any matter related thereto may be submitted in writing to **estates@singaporeccc.org.sg** before **15 December 2023, 5.00pm.**

4.1 SCCC reserves the absolute right not to entertain or respond to any query, which, in the SCCC's opinion, is inappropriate or improper.

4.2 On submitting his tender, the Tenderer shall be deemed to have examined this Tender Document and site conditions and satisfied himself with regard to any query on this Tender Document.

5. PRESENTATION

5.1 The Tenderer shall, on the request of SCCC, make a presentation on such aspects of his tender as may be required by SCCC.

6. VALIDITY PERIOD

6.1 Tenders submitted shall remain valid for acceptance for a period of 180 days commencing on the closing date. This validity period may be extended by mutual consent in writing of SCCC and the Tenderer.

7. AWARD

7.1 SCCC shall be under no obligation to accept the lowest or any tender.

7.2 SCCC shall normally not enter into correspondence with any tenderer regarding the reasons for non-acceptance of a tender.

7.3 SCCC reserves the right to accept portion of each tender as SCCC may decide.

7.4 The Letter of Acceptance issued by SCCC shall create a binding contract on the part of the tenderer to supply to SCCC the goods and/or services offered in the tender.

7.5 The Contract shall be governed by the Conditions of Contract.

7.6 SCCC shall notify a successful tenderer of its acceptance of his tender, whether in whole or in part, by sending a purchase order or letter of acceptance by post to that tenderer and the posting of the purchase order or the letter of acceptance shall be deemed good service of such notice.

7.7 SCCC may at its discretion require the tenderer to sign a written agreement.

7.8 SCCC may make awards to more than one tenderer.

8. VARIATIONS

8.1 SCCC reserves the right to negotiate with the tenderer, where exceptional circumstances so necessitate, to vary any provision or part of this Tender Document without reference to any other party. Any such variation shall be subject to the mutual consent in writing of SCCC and the Tenderer.

9. SECURITY DEPOSIT

Within ten (10) days of the Date of Contract, the tenderer shall deposit with SCCC, if so requested by SCCC, the Security Deposit or the Banker's Guarantee, as the case may be, required under the Conditions of Contract

10. INSURANCE

Within ten (10) days of the Date of Contract, the tenderer shall deposit with SCCC copies of the insurance policies and premium receipts therefore required under the Conditions of Contract.

CONDITIONS OF CONTRACT

1. DEFINITIONS

SCCC:	Singapore Chinese Cultural Centre
Tenderer:	The company who submits this Tender Document
Contractor:	The Tenderer whose tender has been accepted in whole or in part
Contract Price:	The sum stated in the Form of Tender by the contractor as the price for carrying out and completion of the works
Works:	The supply, delivery to and installation at the Site of the equipment and/or services in conformance and accordance with the Technical Specifications and drawings
Site:	The premises on SCCC, (Shenton way) or any other site designated by SCCC
System Completion Date:	The date which all equipment and/or services shall be functional/ready as specified in the Technical Specifications
Warranty Period:	The period during which the contractor, at his own expense, shall make good to the satisfaction of SCCC and shall promptly attend to any defects whatsoever in the works as per clause 5 of the Condition of Contract
Acceptance Test:	Any applicable functional and/or compliance testing carried out as per clause 6 of the Condition of Contract
Performance Requirements:	The acceptance standards of the Acceptance Test as per clause 7 of the Condition of Contract
Security Deposit:	A refundable sum that placed with SCCC by the Contractor as security for the due performance and observance of the Contractor's obligation to this Contract as per clause 19 of the Condition of Contract
Banker's Guarantee:	A letter issued from a bank undertaking the guaranteed payment of Security Deposit upon demand by SCCC for the purpose stated in clause 19 of the Condition of Contract

2. SCOPE OF CONTRACT

2.1 The contractor shall carry out and complete the supply of all items of goods and/or services in accordance with the contract in every respect and to the directions and satisfaction of SCCC. Unless otherwise stated in the contract, all goods shall be newly manufactured goods.

2.2 The contractor shall do or supply all things, free of charge, which are not expressly specified in this Tender Document, but which may be necessary for the proper completion of the Works, or obviously required to be done or supplied in the context of this Tender Document and/or in view of the conditions on the Site.

3. DOCUMENTATION

3.1 The contractor shall undertake to supply SCCC with one (1) complete set of comprehensive documentation on all aspects of the equipment/services including documentation to be used for planning, design, installation, operation, maintenance, administration and training purposes. All sets of such documentation shall be of the latest version.

3.2 In the event of any conflict between the provisions of any documentation or information or data supplied by the contractor including the supporting data, and the provisions of this tender document exclusive of the supporting data, the provisions of this Tender Document shall prevail unless SCCC agrees otherwise in writing.

4. SYSTEM COMPLETION DATE

4.1 The contractor undertakes that the equipment/services shall be delivered, fully installed and operational within the specified period. The contractor shall be entitled to a reasonable extension of time for delays caused by the following:

- force majeure; or
- damage or delay not caused by or due to the wilful act or default or negligence of the contractor or his employees, agents or any person for whom the contractor is responsible.

provided that:

- in respect of all the above events, the contractor has not himself been at fault in failing to guard against or prevent or minimise such delays or damage; and
- the contractor shall make his claim in writing to SCCC for any extension of time within seven (7) days of the date he claims such event took place failing which he shall be deemed to have waived any right he may have hand to such extension.

4.2 In the event of failure by the contractor to deliver any item of goods or complete the performance of services by the date specified in the contract other than due to the circumstances provided above, SCCC shall have the right:

- to cancel all or any items of goods or services from the contract without compensation and obtain them from other sources and all increased costs thereby incurred shall be deducted from any moneys due or to become due to the contractor or shall be recoverable as damages; or,
- to require the contractor to pay or allow SCCC to deduct from any moneys due or become due to the contractor's sum, calculated at the rate as specified in the Invitation To Tender as liquidated damages until the goods are delivered and the services are performed.

5. WARRANTY PERIOD

5.1 There shall be a warranty period during which the contractor, at his own expense, shall make good to the satisfaction of SCCC and shall promptly attend to any defects whatsoever in the works.

5.2 The duration of the warranty period shall be the period specified in the "Tenderer's Proposal – Equipment Support and Maintenance" and "Tenderer's Proposal - Software Support" commencing the day following the date of the successful completion of the Acceptance Test or the last test to be conducted. When SCCC does not require any test to be conducted, the warranty period shall commence the day following the date on which the equipment is fully installed and operational. Provided always that the duration of the warranty period shall not be less than one (1) year.

5.3 Where SCCC considers appropriate, it may in its absolute discretion require a separate warranty period in respect of each or any item or part of the equipment delivered. The duration of any such warranty period shall be the specified period, commencing the day following the date of the successful completion of the last test conducted on the said item or part of the Equipment or if SCCC so agrees from the date such item or part of the equipment is installed and operational. Provided always that the duration of any such warranty period shall not be less than one (1) year.

6. ACCEPTANCE TEST

6.1 If SCCC so required, the equipment and/or service will be subject to an acceptance test conducted by SCCC in accordance with such procedure(s) and method(s) as SCCC may in its absolute discretion deem fit for the purpose of confirming and verifying that the functions, features and performance of the Equipment meet the requirements and standards stipulated in the Technical Specifications.

6.2 The Acceptance Test shall be conducted and completed within a period of thirty (30) days from the date of completion of the installation of the equipment. This period may be extended upon mutual agreement to ninety (90) days.

6.3 SCCC may conduct such other tests on each item or part of the equipment in accordance with such procedure(s) and method(s) as SCCC may in its absolute discretion deem fit for the purpose of confirming and verifying that the functions, features and performance of such item or part meet with the requirements and standards stipulated in the Technical Specifications which are applicable to such item or part. Such tests may be conducted at the discretion of SCCC, in addition to or substitution of the Acceptance test and shall be completed before the expiry of the period stipulated.

7. PERFORMANCE REQUIREMENTS

7.1 The equipment when installed must comply with such performance requirements as may be mutually agreed to in writing between SCCC and the Contractor in order to be acceptable to SCCC.

8. WARRANTIES

8.1 The contractor warrants to SCCC that the equipment is suitable for and shall meet the requirements set out in the Technical Specifications.

8.2 The contractor warrants that the equipment when operational shall meet the standards of the Acceptance Test and such other test(s) conducted and the Performance Requirements.

8.3 The Contractor warrants that all information and data given in the tender submission documents are accurate.

8.4 All equipment and materials and supporting documentation not mentioned or included in this Tender Document but which may be necessary for the proper operation and functioning of equipment to the standards of the Acceptance Test and such other test(s) conducted and the Performance Requirements shall be provided by the Contractor to SCCC free of charge.

8.5 The contractor warrants that the performance of this contract and the use of the equipment by SCCC shall not infringe any patent, copyright, trade secret or other property right of any third party and the contractor shall obtain without charge to SCCC any licences as are necessary for the purposes of this contract from any third parties in respect of such rights.

9. SUPPORT AND MAINTENANCE SERVICES

9.1 The contractor shall provide the support and maintenance services as set out in "Tenderer's Proposal – Equipment Support and Maintenance" and "Tenderer's Proposal - Software Support" documents.

10. TRAINING

10.1 The contractor shall carry out the training as set out in the "Tenderer's Proposal – Training" document.

11. FUTURE PURCHASES

11.1 At any time up to the end of the Warranty Period or, where there are more than one warranty period under this contract, the last warranty period, SCCC shall be entitled to purchase from the contractor any additional quantity of the equipment and materials set out in the Price Schedule of Tenderer's Offer which are marketed by the Contractor at a price not exceeding the price for the same set out therein.

12. COMPLIANCE WITH LAW

12.1 The contractor shall comply with and satisfy all requirements under all laws and regulations relevant or applicable to the performance of his obligations under this Contract and shall indemnify SCCC in respect of all costs and expenses and any liabilities whatsoever which may be incurred under or in connection with such laws and regulations.

13. PROPERTY & RISK

13.1 The property in any items or part of the Equipment shall pass to SCCC on delivery to the site and the risk therein shall pass on the expiry of the warranty period that relate to the item or part of the Equipment so delivered.

14. VARIATIONS

14.1 Any variation of the provisions of this contract shall be subject to the mutual consent on writing of SCCC and the Contractor.

15. ASSIGNMENT

15.1 The contractor shall not transfer or assign the contract or any part, share or interests therein.

16. EQUIPMENT AND MATERIALS

16.1 All equipment and materials supplied shall be new and in strict conformance with the Technical Specifications and shall be of good quality and suitable for their required purpose.

17. PROCEDURE ON SITE

17.1 The contractor shall keep upon the site a competent supervisor who shall attend to the Works at all time. Any instructions given to the supervisor by SCCC shall be deemed to be given to the contractor.

17.2 The contractor shall, if required by SCCC, furnish to him a list of the names, nationalities and other particulars of the employees and workmen engaged for or by him for the purpose of the Works.

17.3 The Contractor shall be responsible for the proper behaviour of employees and workmen engaged for or by him and shall remove any such employee or workmen who is not acceptable to SCCC and the contractor shall indemnify SCCC against any claims by such employee or workmen arising from such removal.

17.4 Unless prior arrangements are made with and agreed to in writing by SCCC, the Contractor shall carry out all works on the site under his contract during SCCC's official working hours, i.e. Monday to Friday, from 8.00am to 12.00pm and 1.00pm to 6.00pm.

17.5 The contractor shall during the execution of the works take all necessary precautions to prevent damage to furniture, fittings and other properties on the site.

17.6 Where necessary, the contractor shall supply and place at appropriate places on the Site signs to give warning of work in progress.

17.7 The Contractor shall keep the Site clean and shall remove speedily from the site debris and rubbish generated by the works and properly disposes of the same.

17.8 SCCC shall not be liable for loss or damage to the Contractor's property placed or left on the Site or elsewhere on SCCC property.

18. PAYMENTS

18.1 Payment for the equipment shall be made by SCCC within **thirty (30) days** of the successful completion of the Acceptance Test or the last test to be conducted. Where SCCC does not require any test to be conducted, payment shall be made within **thirty (30) days** of the date on which the equipment is fully installed and operational.

19. SECURITY DEPOSIT

19.1 The Contractor shall place with SCCC by way of a cheque or banker's draft a security deposit for a sum equal to **10%** of the Contract Price as security for the due performance and observance of the Contractor's obligation to this Contract.

19.2 SCCC may accept a banker's guarantee for the purpose stated in lieu of Security Deposit to be furnished in the form of the Draft Banker's Guarantee or such other form as may be acceptable to SCCC.

19.3 The Security Deposit shall be refundable after the expiry of the Warranty Period or, where there is more than one warranty period under this Contract, the last such warranty period subject to the Contractor having rectified any defects in the Works to the satisfaction of SCCC and/or any claims that SCCC may have under this Contract.

19.4 SCCC may retain **Ten percent (10%)** of the Contract Price if the security deposit is not made upfront. Such monies retained shall be payable to the Contractor after the expiry of the Warranty Period or, where there are more than one warranty period under this Contract, the last warranty period subject to the Contractor having rectified any defects in the Works to the satisfaction of SCCC and any claims which SCCC may have under this contract.

20. LATE COMPLETION

20.1 If the proposed Contractor fails to complete the installation of the equipment/or service or the Equipment is not fully operational by the System Completion Date, the Contractor shall be liable to pay liquidated damages at the rate specified in the Invitation to Tender.

21. TERMINATION

21.1 SCCC may terminate this Contract with immediate effect by giving notice in writing to the Contractor on any one of the following grounds:

- If the Contractor has wholly suspended work without justification or is failing to proceed with due diligence and due expedition and following expiry of two weeks' written notice from SCCC to that effect has failed to take effective steps to recommence work or is continuing to proceed without due diligence or expedition, as the case may be;

- If the Contractor refuses or persistently fails or neglects to comply with the instructions of SCCC issued under the provisions of this Contract and following expiry of two weeks written notice from SCCC to that effect has failed to take effective steps to comply with the said instructions; and

- If the Contractor becomes bankrupt or insolvent or makes a composition with creditors or if, being a company, a winding-up order of any kind is made in respect of the Contractor, or if a receiver or manager is appointed over the Contractor's undertaking or assets or possession of or execution on any part of such undertaking or assets is taken or levied by creditors.

21.2 Upon termination under sub-clause 21.1

- SCCC may engage other contractors to complete those parts of the Works uncompleted by the Contractor and the Contractor shall be liable to SCCC for all additional costs incurred thereby. The Contractor shall also pay liquidated damages for delay calculated in accordance with Clause 20 as if he had himself completed the Works on the date of actual completion by those other contractors engaged by SCCC;

- SCCC may withhold payment of any monies payable to the Contractor until the Works are completed and the damages payable to SCCC arising from such termination are quantified and ascertained by SCCC (such quantification and ascertainment to be made within a reasonable time) and if the aggregate amount of such damages and all monies paid to the Contractor under this Contract exceeds the Contract Price, such excess amount shall constitute a debt payable to SCCC by the Contractor; and

- the Contractor shall remove from the Site, if required by SCCC any temporary structures, plants, tools, goods, materials and equipment brought thereon by or for the Contractor and if the Contractor fails to do so within the time stipulated in the said notice for such removal, SCCC shall be entitled to store, remove, sell or otherwise deal with or dispose of the same and the Contractor shall be liable to and shall indemnify SCCC for or against any costs, expenses and liabilities whatsoever incurred by SCCC in so dealing with or disposing the same. In the event that the said

temporary structures, plants, tools, goods, materials and equipment are sold, the proceeds after the deduction therefrom of such monies as are due to SCCC from the Contractor shall be held for the Contractor for a period of not less than one month from the date of posting of a notice to the Contractor to collect the said proceeds from SCCC and if the said Contractor fails to collect the same from SCCC within the said period, he shall be deemed to have disclaimed any rights to or interests in the said proceeds. The Contractor shall not be entitled to make any claims whatsoever against SCCC or its employees or agents for any action taken by SCCC in accordance with the provisions of this sub-clause.

21.3 The rights of SCCC specified under clause 21 shall be in addition to such other rights and remedies as SCCC may have or be entitled to against the Contractor for breach of contract or otherwise.

22. NON-DISCLOSURE

22.1 The tenderer agrees not to disclose, reveal or divulge to any person or entity any information concerning the organisation, business, finances, transactions or other affairs of SCCC which may come to the tenderer's knowledge at any time during or after the agreement term, unless SCCC grants written consent of such a disclosure. If need to be, all tenderers are required to enter into a non-disclosure agreement with SCCC.

23. INDEMNITIES

23.1 The Contractor shall indemnify and keep SCCC indemnified against all claims, demands, actions, judgements, damages, costs and expenses for personal injury or death arising directly or indirectly from the Works or the performance of this Contract unless the same are due to the act or neglect of SCCC or its employees or agents.

23.2 The Contractor shall indemnify and keep SCCC indemnified against all claims, demands, actions, judgements, damages, costs and expenses for damage to property which are caused directly or indirectly by any act or omission or negligence of the Contractor, his employees or agents or any person for whom the Contractor is responsible or due to any circumstances within the Contractor's control.

23.3 The Contractor shall indemnify and keep SCCC indemnified against all claims, demands, actions, judgements, damages, costs and expenses in respect of any infringement or alleged infringement of any patent, copyright, trade secret or other property right which infringement or alleged infringement arise directly or indirectly from the performance of this Contract or use of the Equipment or any matter relating thereto unless such infringement or alleged infringement is due solely to the use of any specifications or drawings provided by SCCC.

23.4 None of the indemnities shall be defeated or reduced by reason of the fact that SCCC may have neglected or omitted to exercise any powers of supervision or control whatsoever that may have under this contract.

24. THIRD PARTY INSURANCE

24.1 As a condition precedent to the commencement of the Works, the Contractor shall insure:-

- Against his and SCCC's liabilities and that of SCCC's employees in respect of or in connection with personal injuries or death arising directly or indirectly from the Works or the performance of this Contract.

- Against his and SCCC's liabilities and that of SCCC's employees in respect of or in connection with any damage to property (other than the Works) arising directly or indirectly from the Works or the performance of this contract; and

- Against his and SCCC's liabilities and that of SCCC's employees in respect of any liability to the Contractor's employees or workmen or such persons engaged for the purposes of the Works under the Workmen's Compensation Act with any amendments, modifications thereto or re-enactment thereof or any law.

- Such insurance shall be taken out with an insurer approved by SCCC for such period(s) and on such terms as SCCC may require and in default of production of a satisfactory relevant policy or premium receipt or current certificate of insurance from such insurer SCCC may itself insure against the risks described in sub-clause 23.1 and recover the costs thereof from the Contractor and/or deduct such cost from any sums due to the contractor.

25. WAIVER

25.1 The failure by SCCC to enforce at any time or any period any one or more of the terms or conditions of this contract shall not be a waiver of them or of the right at any time subsequently to enforce all terms or conditions of this Contract.

26. NOTICE

27. Any notice to be served on the Contractor under this contract may be sent by post in an envelope addressed to the Contractor at his place of business or residence last known to SCCC or at the Contractor's registered office, as the case may be, and any notice so posted shall be deemed to have been given at the time when the same would normally be delivered in the ordinary course of post.

28. ARBITRATION

28.1 Any dispute or difference between the parties in connection with this Tender Document or this Contract or any matter related thereto shall be referred to arbitration in Singapore in accordance with the Arbitration Act with any amendments, modifications thereto or re-enactments thereof.

29. APPLICABLE LAW

29.1 This Tender Document and this Contract shall be construed in accordance with and governed by the Laws of Singapore.

DRAFT BANKER'S GUARANTEE

To : Singapore Chinese Cultural Centre
1 Straits Boulevard, #11-01
S(018906)

RE : << WORKS>>

WHEREAS << Name and Address of Contractor>> ("the contractor") has entered into a contract ("the Contract") with you on the terms of the Form of Tender dated the __ day of __ in a Tender Document ("the Tender Document") submitted by the Contractor to you for the above Works which are more particularly described in the Tender Document;

AND WHEREAS by the provisions of the Conditions of Contract ("the Conditions of Contract") in the Tender Document the Contractor is required to make a deposit with you in cash in the amount S$_____("the Security Deposit") as a security deposit for the due performance and observance of the Contractor's obligations under the Contract;

AND WHEREAS we [name and address of banker] …… have requested you to accept an unconditional guarantee in lieu of the security deposit and you have agreed to accept the same.

NOW IN CONSIDERATION OF THE PREMISES :

1. We guarantee to pay to you forthwith upon demand made to us in writing a sum or sums not exceeding in the aggregate the sum of Singapore Dollars (S$……) ("the Guaranteed Sum"). We will pay you the Guaranteed Sum or part thereof as may be requested by you without any proof that you are entitled to reimburse yourself with or utilise such sum or that the Contractor is in default or is in breach of any agreement with you. We will however accept for the account of the guarantee any sum returned by you to us.

2. We expressly agree and declare that this guarantee shall not be prejudiced diminished or affected in any way nor shall we be released or otherwise exonerated by any act omission fact circumstance matter or thing which but for this provision might operate too or otherwise exonerate us including without limitation any arrangement whatsoever made between yourself and the Contractor with or without our consent or knowledge including any alteration in the obligations undertaken by the Contractor or any forbearance by you in respect of those obligations.

3. The Guarantee shall take effect immediately and shall continue until (expiry date of warranty period) and thereafter shall be extended from year to year without request until the Contractor shall have discharged all his obligations under the Contract or the Contract is terminated by SCCC, whichever shall first occur.

4. You may make more than one claim under this Guarantee provided that the claims in aggregate do not exceed the Guaranteed Sum.

5. All claims made by you under this Guarantee must be in writing to us not later than six months from the expiry of this Guarantee or any extension thereof.

Dated the__day of__ 20_____

SIGNED BY
[NAME]
AS
[DESIGNATION]
FOR AND ON BEHALF OF
[NAME OF GUARANTOR]

in the presence of
[NAME]
[DESIGNATION]
SIGNATURE
ADDRESS

TECHNICAL SPECIFICATIONS

1. LAN

1.1. General Network Requirements

1.1.1. The tenderer shall propose the network architecture of their proposed solution showing all the interconnections of servers, storages, switches, and workstations.

1.1.2. All the communication between the various components of the system shall be using TCP/IP

1.1.3. All the network switches shall support the following switch management and operation features:

1.1.3.1. SSH (version 1 & 2)

1.1.3.2. Telnet

1.1.3.3. Console

1.1.3.4. FTP

1.1.3.5. SFTP

1.1.3.6. HTTPS

1.1.3.7. Remote Monitoring (RMON) (RFC 1757) and RMON II (RFC 2021).

1.1.3.8. Simple Network Management Protocol (SNMP) Version 1, 2c and 3

1.1.4. Supports the IEEE 802.1AB LLDP neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network.

1.1.5. Provide support for voice over IP (VoIP) applications and additional TLVs for capabilities discovery, network policy, power over Ethernet (PoE), inventory management, and location information.

1.1.6. The network switch shall support Syslog logging.

1.1.7. The proposed network equipment shall be IPv6 ready and support the co-existence of IPv4 and IPv6.

1.1.8. The tenderer shall ensure sufficient and appropriate switches are provided to support the new proposed hyper-converged solutions in the system. All switches are to be rack-mountable into a standard 19” wide rack.

1.1.9. The tenderer shall ensure that the system supports integration through API for policies can be used to control and monitor the power consumed by PoE-powered endpoints, desktop and data- center IT equipment, and a wide range of building infrastructure.

1.2. Campus Core Switch

1.2.1. The Tenderer shall propose campus core switch.

1.2.2. The switch shall have the following features:

1.2.2.1 High performance of at least 3.6 Tbps with 2,000 Mpps throughput

1.2.2.2 800G of stateful software-defined services performance through DPU.

1.2.2.3 Support distributed stateful segmentation, east-west firewalling, NAT, IPSec encryption, and flow-based/session-based telemetry services—all delivered inline within the switch embedded DPUs, all the time, on every switch access port, closer to where critical enterprise applications run.

1.2.2.4 Simplifies operations via unified network and security automation and management with fabric Composing/Orchestration toolset.

1.2.2.5 Accelerates infrastructure service provisioning with fabric Composing/Orchestration toolset.

1.2.2.6 Network Analytics Engine—A first-of-a-kind, built-in framework for monitoring, troubleshooting, and capacity planning

1.2.2.7 Compact 1U switches with 1/10/25 GbE and 40/100 GbE connectivity.

1.2.2.8 Modular, Linux-based and built with OVSDB to support a database-centric operating system.

1.2.2.9 Support automation and programmability using built-in REST APIs and Python scripts.

1.2.2.10 Intelligent monitoring and visibility with the Network Analytics Engine.

1.2.2.11 Advanced Layer 2/3 feature set includes BGP, OSPF, VRF, and IPv6.

1.2.2.12 Distributed architecture with separation of data and control planes.

1.2.2.13 Includes independent monitoring and restart of individual software modules, and enhanced software process serviceability functions.

1.2.2.14 Allows individual software modules to be upgraded for higher availability.

1.2.2.15 RJ-45 Console Port

1.2.2.16 USB-A Host Port

1.2.2.17 Provide hardware warranty including power supply and fan until the end of sale of the switch.

1.2.2.18 Powerful QoS feature—Supports congestion actions, such as strict priority (SP) queuing and weighted fair queuing.

1.2.3 Resiliency and High Availability

1.2.3.1 Enables a distributed and redundant architecture by deploying two switches, with each switch maintaining independent control yet staying synchronized during upgrades or failover.

1.2.3.1 Virtual Router Redundancy Protocol (VRRP) – Allows groups of two routers to dynamically back each other up to create highly available routed environments.

1.2.3.3 Unidirectional Link Detection (UDLD) – Monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks

1.2.3.4 IEEE 802.3ad LACP—Supports up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm.

1.2.3.5 Redundant power supplies—Provides N+1 high reliability with hot swappable, redundant power supplies.

1.2.3.6 Redundant and load-sharing fans, and power supplies—Increases total performance and power availability while providing hitless, stateful failover.

1.2.3.7 Hot-swappable power supply and fan modules—Allows replacement of modules without any operational impact on other modules.

1.2.3.8 Separate data and control paths—Separates control from services and keeps service processing isolated; increases security and performance.

1.2.3.9 Rapid Per-VLAN spanning tree plus (RPVST+)

1.2.3.10 Support Ethernet Ring Protection Switching (ERPS), Supports rapid protection and recovery in a ring topology.

1.2.3.11 Support IEEE 802.3ad LACP supports up to 54 LAGs and 16 member per LAG with user selectable L1 to L4 hashing algorithm.

1.2.4. Performance

1.2.4.1 High-speed fully distributed architecture—Provides 3.6 Tbps for switching and 2,000 MPPS for forwarding. All switching and routing are wire-speed to meet the demands of bandwidth-intensive applications today and in the future.

1.2.4.2 Scalable system design—Provides investment protection to support future technologies and higher-speed connectivity.

1.2.5 Connectivity

1.2.5.1 High-density port connectivity 48 ports of 1/10/25 GbE (SFP/SFP+/SFP28) and 6 ports of 40/100 GbE (QSFP+/QSFP28) SFP+ ports with an optional 10GBASE-T Transceiver.

1.2.5.2 Jumbo frames—Supports high-performance backups and disaster recovery systems; provides a maximum frame size of 9 K bytes.

1.2.5.3 Loopback – Supports internal loopback testing for maintenance purposes and an increase in availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.

1.2.5.4 Packet storm protection—Protects against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds.

1.2.6 Management

1.2.6.1 Management interface control—Enables or disables these interfaces depending on security preferences: console port or reset button.

1.2.6.2 Industry-standard CLI with a hierarchical structure – Reduces training time and expenses and increases productivity in multivendor installations.

1.2.6.3 Management security—Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide SNMP access; and local and remote Syslog capabilities allow logging of all access.

1.2.6.4 SNMP v2c/v3—Provides SNMP read and trap support of the industry standard Management Information Base (MIB) and private extensions.

1.2.6.5 IPSLA—Monitor the network for degradation of various services, including monitoring voice. Monitoring is enabled via the NAE for history and for automated gathering of additional information when anomalies are detected.

1.2.6.6 sFlow (RFC 3176)—Increases total performance and power availability while providing hitless, stateful failover.

1.2.6.7 Remote monitoring (RMON) – Uses standard SNMP to monitor essential network functions and supports events, alarms, history, and statistics groups, as well as a private alarm extension group.

1.2.6.8 TFTP and SFTP support—Offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security.

1.2.6.9 Debug and sampler utility—Supports ping and traceroute for IPv4 and IPv6.

1.2.6.10 Network Time Protocol (NTP)—Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network. Can serve as the NTP server in the network.

1.2.6.11 IEEE 802.1AB Link Layer Discovery Protocol (LLDP)—Advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

1.2.6.12 Dual flash images – Provides independent primary and secondary operating system files for backup while upgrading.

1.2.6.13 Multiple configuration files – Easily stores the flash image.

1.2.6.14 Built-in programmable and easy-to-use REST API interface

1.2.6.15 Multiple configuration files can be stored to a flash image and allows rollback of any of these configurations without requires reboot.

1.2.6.16 Support Secure Sockets Layer (SSL) which encrypts traffic, allowing secure access to the browser-based management GUI in the switch.

1.2.6.17 ASIC-based wire speed network monitoring and accounting RFC 3176 sFlow.

1.2.7 Layer 2 Switching

1.2.7.1 VLAN—Supports up to 4,040 port-based or IEEE 802.1Q-based VLANs.

1.2.7.2 VXLAN—Supports static VXLAN. Allows to connect two or more VXLAN tunnel endpoints (VTEP).

1.2.7.3 Port mirroring—Duplicates port traffic (ingress and egress) to a local or remote monitoring port; supports four mirroring groups with an unlimited number of ports per group.

1.2.7.4 STP—Supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

1.2.7.5 Internet Group Management Protocol (IGMP)—Controls and manages the flooding of multicast packets in a Layer 2 network.

1.2.7.6 Rapid Per-VLAN spanning tree plus (RPVST+)—Allows each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs.

1.2.8 Layer 3 Services and Routing

1.2.8.1 Address Resolution Protocol (ARP) – Determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network.

1.2.8.2 Dynamic Host Configuration Protocol (DHCP)—DHCP services are offered within a client network to simplify network management. DHCP relay enables DHCP operation across subnets.

1.2.8.3 Domain Name System (DNS) – Provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

1.2.8.4 Policy Based Routing (PBR)—Enables using a classifier to select traffic that can be forwarded based on a policy set by network administrator.

1.2.8.5 Static IPv4 routing – Provides simple manually configured IPv4 routing.

1.2.8.6 Open shortest path first (OSPF)—Delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and a graceful restart for faster failure recovery.

1.2.8.7 Border Gateway Protocol 4 (BGP-4)—Delivers an implementation of the Exterior Gateway Protocol (EGP), utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; and scales to very large networks.

1.2.8.8 6in4 tunnels—Supports the tunneling of IPv6 traffic in an IPv4 network.

1.2.8.9 IP performance optimization – Provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.

1.2.8.10 Static IPv6 routing – Provides simple manually configured IPv6 routing.

1.2.8.11 Dual IP stack—Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

1.2.8.12 OSPFv3—Provides OSPF support for IPv6.

1.2.8.13 Equal-Cost Multipath (ECMP) – Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.

1.2.8.14 Generic Routing Encapsulation (GRE)—Enables tunneling traffic from site to site over a Layer 3 path.

1.2.9 Security

1.2.9.1 Access control list (ACL) Features—Supports powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices such as IP addresses. For instance, IT management devices could be grouped in this way. ACLs can also protect control plane services, such as SSH, SNMP, NTP, or web servers.

1.2.9.2 Remote Authentication Dial-In User Service (RADIUS)—Eases security access administration by using a password authentication server.

1.2.9.3 Terminal Access Controller Access-Control System (TACACS+) – Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security.

1.2.9.4 Management access security—provides for both on-box as well as off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can provide user authorization services.

1.2.9.5 Secure shell (SSHv2)—Uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers.

1.2.9.6 Support Remote Authentication Dial-In User Service (RADIUS)
1.2.9.7 Support Terminal Access Controller Access-Control System (TACACS+)
1.2.9.8 Support RadSec , RadSec enables RADIUS authentication and accounting data to be passed safely and reliably across insecure networks.

1.2.10 Multicast
1.2.10.1 Internet Group Management Protocol (IGMP)—Enables establishing multicast group memberships in IPv4 networks; supports IGMPv1, v2, and v3.
1.2.10.2 Multicast Listener Discovery (MLD)—Enable discovery of IPv6 multicast listeners; supports MLDv1 and v2.
1.2.10.3 IGMP/MLD Snooping—Prevent flooding of multicast traffic to non-listening ports.
1.2.10.4 Protocol Independent Multicast (PIM) – Supports one-to-many and many-to-many media casting use cases, such as IPTV over IPv4 and IPv6 networks; support for PIM Spare Mode (PIM-SM, IPv4, and IPv6).

1.2.11 Analytic
1.2.11.1 The switch should have an Analytic engine to monitors and analyzes events that can impact network health
1.2.11.2 Easy access to all network state information allows visibility and analytics
1.2.11.3 REST APIs and Python scripting for fine-grained programmability of network tasks
1.2.11.4 Continuous telemetry data with WebSocket subscriptions for event driven
1.2.11.5 Allows downloading of Analytic Agent from the manufacturer to extend the function and features of the switches in terms on visibility, analytic and automation.

1.3. Access Switch

The Tenderer shall propose access switches with the following features.

1.3.1. Key features
1.3.1.1. High performance 880 Gbps system switching capacity, 660 MPPS of system throughput, and up to 200 Gbps stacking bandwidth
1.3.1.2. Stackable Layer 3 switches with BGP, EVPN, VXLAN, VRF, and OSPF with robust security and QoS
1.3.1.3. Compact 1U switches with full density 1/2.5/5 GbE multi-gigabit, PoE and SFP+ models
1.3.1.4. Built-in high speed 10/25/50 GbE uplinks
1.3.1.5. Intelligent monitoring, visibility, and remediation with Network Analytics Engine
1.3.1.6. One touch deployment with mobile app
1.3.1.7. Support for automated configuration and verification
1.3.1.8. Dynamic segmentation enables secure and simple access for users and IoT
1.3.1.9. Easy access to all network state information allows unique visibility and analytics
1.3.1.10 REST APIs and Python scripting for fine-grained programmability of network tasks
1.3.1.11 A micro-services architecture that enables full integration with other workflow systems and services
1.3.1.12 Continual state synchronization that provides superior fault tolerance and high availability
1.3.1.13 Continuous telemetry data with WebSocket subscriptions for event-driven automation
1.3.1.14 All software processes communicate with the database rather than each other, helping to ensure near real-time state and resiliency, and allowing individual software modules to be independently upgraded for higher availability

1.3.1.15 Quad Core CPU with 8GB DDR4 RAM
1.3.1.16 USB-C Console Port
1.3.1.17 USB-A Host Port
1.3.1.18 Support Always on POE, which allows supply power to poe device even during reboot and firmware upgrade
1.3.1.19 Support Quick POE, supplies PoE power to powered devices as soon as the switch is plugged into AC power so device can initialize at same time as switch OS boots up

1.3.2 Quality of Service (QoS)
1.3.2.1 Strict priority (SP) queuing and Deficit Weighted Round Robin (DWRR)
1.3.2.2 Traffic prioritization (IEEE 802.1p) for real-time classification into eight priority levels that are mapped to eight queues
1.3.2.3 Layer 4 prioritization based on TCP/UDP port numbers
1.3.2.4 Class of Service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
1.3.2.5 Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums
1.3.2.6 Transmission rates of egressing frames can be limited on a per-queue basis using Egress Queue Shaping (EQS)
1.3.2.7 Large buffers for graceful congestion management
1.3.2.8 IP SLA for Voice to monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests.

1.3.3 Resiliency and High Availability
1.3.3.1 Virtual Router Redundancy Protocol (VRRP)—Allows groups of two routers to dynamically back each other up to create highly available routed environments.
1.3.3.2 Unidirectional Link Detection (UDLD)—Monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.
1.3.3.3 IEEE 802.3ad LACP—Supports up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm.
1.3.3.4 Redundant power supplies—Provides N+1 high reliability with hot swappable, redundant power supplies.
1.3.3.5 Redundant and load-sharing fans, and power supplies—Increases total performance and power availability while providing hitless, stateful failover.
1.3.3.6 Hot-swappable power supply and fan modules—Allows replacement of modules without any operational impact on other modules.

1.3.4 Scale and Simplicity
1.3.4.1 Support for up to 10 switches (or members) in a stack via chain or ring topology.
1.3.4.2 Support maximum stacking distance of 10 km.
1.3.4.3 Flexibility to create stacks that span longer distances, such as hundreds of meters to kilometers between sites using long-range 10/25/50 GbE transceivers
1.3.4.4 Flexibility to mix both modular and fixed models within a single stack to meet your deployment requirements
1.3.4.5 Simplified configuration and management as the switches act as a single chassis when stacked
1.3.4.6 A mobile app that provides support for a validated stack deployment to help ensure that all stack links and uplinks are connected properly

1.3.5 Connectivity

1.3.5.1 Compact 1U models support:

1.3.5.1.1 24 and 48 ports of multi-gigabit Ethernet IEEE 802.3bz (100 M/1/2.5/5 GbE) supporting high power.

1.3.5.1.3 High density 24 port SFP+ model, which is ideal for aggregation.

1.3.5.1.4 10/25/50 GbE uplink port connectivity.

1.3.5.2 Jumbo frames—Supports high-performance backups and disaster recovery systems; provides a maximum frame size of 9 K bytes.

1.3.5.3 Loopback – Supports internal loopback testing for maintenance purposes and an increase in availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.

1.3.5.4 Packet storm protection—Protects against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds.

1.3.6 Management

1.3.6.1 Management interface control—Enables or disables these interfaces depending on security preferences: console port or reset button.

1.3.6.2 Industry-standard CLI with a hierarchical structure – Reduces training time and expenses and increases productivity in multivendor installations.

1.3.6.3 Management security—Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide SNMP access; and local and remote Syslog capabilities allow logging of all access.

1.3.6.4 SNMP v2c/v3—Provides SNMP read and trap support of the industry standard Management Information Base (MIB) and private extensions.

1.3.6.5 IPSLA—Monitor the network for degradation of various services, including monitoring voice. Monitoring is enabled via the NAE for history and for automated gathering of additional information when anomalies are detected.

1.3.6.6 sFlow (RFC 3176)—Increases total performance and power availability while providing hitless, stateful failover.

1.3.6.7 Remote monitoring (RMON) – Uses standard SNMP to monitor essential network functions and supports events, alarms, history, and statistics groups, as well as a private alarm extension group.

1.3.6.8 TFTP and SFTP support—Offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security.

1.3.6.9 Debug and sampler utility—Supports ping and traceroute for IPv4 and IPv6.

1.3.6.10 Network Time Protocol (NTP)—Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network. Can serve as the NTP server in a customer network.

1.3.6.11 IEEE 802.1AB Link Layer Discovery Protocol (LLDP)—Advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

1.3.6.12 Dual flash images – Provides independent primary and secondary operating system files for backup while upgrading.

1.3.6.13 Multiple configuration files – Easily stores the flash image.

1.3.6.14 Allows configuration from Smart Phone or Tablet using the app which are downloadable from Google play store OR Apple App Store.

1.3.6.15 Built-in programmable and easy-to-use REST API interface

1.3.6.16 Multiple configuration files can be stored to a flash image and allows rollback of any of these configurations without requires reboot.

1.3.6.17 Support Cloud based or on-premises management.

1.3.7 Layer 2 Switching

1.3.7.1 VLAN support and tagging for IEEE 802.1Q (4094 VLAN IDs)

1.3.7.2 VXLAN encapsulation (tunneling) protocol for overlay network enables a more scalable virtual network deployment.

1.3.7.3 Port mirroring—Duplicates port traffic (ingress and egress) to a local or remote monitoring port; supports four mirroring groups with an unlimited number of ports per group.

1.3.7.4 STP—Supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

1.3.7.5 Internet Group Management Protocol (IGMP)—Controls and manages the flooding of multicast packets in a Layer 2 network.

1.3.7.6 Rapid Per-VLAN spanning tree plus (RPVST+)—Allows each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs.

1.3.7.7 Supports jumbo frame size of up to 9198 bytes

1.3.8 Layer 3 Services and Routing

1.3.8.1 Address Resolution Protocol (ARP) – Determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network.

1.3.8.2 Dynamic Host Configuration Protocol (DHCP)—DHCP services are offered within a client network to simplify network management. DHCP relay enables DHCP operation across subnets.

1.3.8.3 Domain Name System (DNS) – Provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

1.3.8.4 Policy Based Routing (PBR)—Enables using a classifier to select traffic that can be forwarded based on a policy set by [CustomerName]'s network administrator.

1.3.8.5 Static IPv4 routing – Provides simple manually configured IPv4 routing.

1.3.8.6 Open shortest path first (OSPF)—Delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and a graceful restart for faster failure recovery.

1.3.8.7 Border Gateway Protocol 4 (BGP-4)—Delivers an implementation of the Exterior Gateway Protocol (EGP), utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; and scales to large networks.

1.3.8.8 IP performance optimization – Provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.

1.3.8.9 Static IPv6 routing – Provides simple manually configured IPv6 routing.

1.3.8.10 Dual IP stack—Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

1.3.8.11 OSPFv3—Provides OSPF support for IPv6.

1.3.8.12 Equal-Cost Multipath (ECMP) – Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.

1.3.8.13 Support Generic Routing Encapsulation (GRE) to enables tunneling traffic over a Layer 3 path

1.3.8.14 Support switch to switch VXLAN encapsulation (tunneling) protocol for overlay network that enables a more scalable virtual network deployment

1.3.8.15 Routing Information Protocol version 2 (RIPv2) and RIPng

1.3.8.16 RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
1.3.8.17 Support switch-to-switch tunnels using VXLAN and BGP EVPN

1.3.9 Security
1.3.9.1 Access control list (ACL) Features—Supports powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices such as IP addresses. For instance, IT management devices could be grouped in this way. ACLs can also protect control plane services, such as SSH, SNMP, NTP, or web servers.
1.3.9.2 Remote Authentication Dial-In User Service (RADIUS)—Eases security access administration by using a password authentication server.
1.3.9.3 Terminal Access Controller Access-Control System (TACACS+) – Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security.
1.3.9.4 Management access security—provides for both on-box as well as off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can provide user authorization services.
1.3.9.5 Secure shell (SSHv2)—Uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers.
1.3.9.6 integrated trusted platform module (TPM) for platform integrity
1.3.9.7 Ensure critical device are still allow network access during RADIUS server failure
1.3.9.8 Support RadSec, RadSec enables RADIUS authentication and accounting data to be passed safely and reliably across insecure networks
1.3.9.9 Support ICMP throttling, defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic

1.3.10. Multicast
1.3.10.1 Internet Group Management Protocol (IGMP)—Enables establishing multicast group memberships in IPv4 networks; supports IGMPv1, v2, and v3.
1.3.10.2 Multicast Listener Discovery (MLD)—Enable discovery of IPv6 multicast listeners; supports MLDv1 and v2.
1.3.10.3 IGMP/MLD Snooping—Prevent flooding of multicast traffic to non-listening ports.
1.3.10.4 Protocol Independent Multicast (PIM) – Supports one-to-many and many-to-many media casting use cases, such as IPTV over IPv4 and IPv6 networks; support for PIM Spare Mode (PIM-SM, IPv4, and IPv6).
1.3.10.5 Multicast Service Discovery Protocol (MSDP) efficiently routes multicast traffic through core networks.

1.3.11 Convergence
1.3.11.1 LLDP-MED (Media Endpoint Discovery) defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
1.3.11.2 PoE allocations supports multiple methods (allocation by usage or class, with LLDP and LLDP-MED) to allocate PoE power for more efficient power management and energy savings.
1.3.11.3 CDPv2 uses CDPv2 to configure legacy IP phones
1.3.11.4 Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones

1.3.12 Analytic

1.3.12.1 The switch should have an Analytic engine to monitors and analyzes events that can impact network health

1.3.12.2 Easy access to all network state information allows visibility and analytics

1.3.12.3 REST APIs and Python scripting for fine-grained programmability of network tasks

1.3.12.4 Continuous telemetry data with WebSocket subscriptions for event driven automation

1.3.12.5 Allows downloading of Analytic Agent from the manufacturer to extend the function and features of the switches in terms on visibility, analytic and automation.

1.4. Compact Access Switch (12 ports)

The Tenderer shall propose compact access switches with the following features.

1.4.1. Connectivity, performance and standards

1.4.1.1 Minimum Quad Core CPU with 8GB DDR4 RAM

1.4.1.2 12 x 10/100/1000Base-T and 2 x 1/10G SFP ports, 2 x 1GbE ports. High performance 68 Gbps system switching capacity

1.4.1.3 Minimum 45.1 MPPS of system throughput.

1.4.1.4 Has the following ports

1.4.1.4.1 USB-A Host Port

1.4.1.4.2 OOBM Ethernet Port

1.4.1.5 support 802.3af/ 802.3at POE Standards and able to detect and power up pre-standard POE device

1.4.1.6 Support Always on POE

1.4.1.7 Support 8 members Stacking

1.4.1.8 Support maximum stacking distance of 10KM

1.4.1.9 Support all the below IEEE standards:-

1.4.1.9.1 IEEE802.1p

1.4.1.9.2 IEEE802.1Q

1.4.1.9.3 RFC1519 CIDR

1.4.1.9.4 RFC 1583 OSPF v2

1.4.1.9.5 RFC 5340 OSPF v3

1.4.1.9.6 RFC 4252 SSHv6 Authentication

1.4.1.9.7 RFC 4253 SSHv6 Transport Layer

1.4.1.10 Support 4094 VLAN IDs

1.4.1.11 Support Generic Routing Encapsulation (GRE)

1.4.1.12 Support VXLAN encapsulation (tunneling) protocol

1.4.2 High Availability and Resiliency

1.4.2.1 Support Uni-directional ink Detection (UDLD)

1.4.2.2 Support Rapid Per-VLAN Spanning Tree (RPVST+)

1.4.2.3 Support IEEE 802.3ad LACP supports up to 32 LAGs with user-selectable hashing algorithm

1.4.3 Quality of Service (QoS)

1.4.3.1 Support Traffic prioritization (802.1p)

1.4.3.2 Class of Service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ

1.4.3.3 Strict priority (SP)

1.4.3.4 Deficit Weighted Round Robin (DWRR)

1.4.3.5 Transmission rates of egressing frames can be limited on a per-queue basis using Egress Queue Shaping (EQS)

1.4.3.6 Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums.

1.4.3.7 IP SLA for Voice to monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests.

1.4.4 Management

1.4.4.1 Allows configuration from Smart Phone or Tablet using the app which are downloadable from Google play store OR Apple App Store

1.4.4.2 Built-in programmable and easy-to-use REST API interface

1.4.4.3 Multiple configuration files can be stored to a flash image and allows rollback of any of these configurations without requires reboot

1.4.4.4 Support Secure Sockets Layer (SSL) which encrypts traffic, allowing secure access to the browser-based management GUI in the switch

1.4.4.5 Support Cloud based or on-premises management

1.4.4.6 To simplify administration the switch is capable to receive the security setting such as user-role, access control list from policy manager, this allows the administrator to create the policy only once and deploy the same policy across the entire network.

1.4.4.7 Allow direct access to the manufacturer support website to download all future software/OS releases (when available) until the end of sale of the product.

1.4.5 Layer 3 Features

1.4.5.1 Routing Information Protocol version 2 (RIPv2) and RIPng

1.4.5.2 OSPFv2 and OSPFv3

1.4.6 Layer 2 Switching

1.4.6.1 VLAN support and tagging support IEEE 802.1Q (4094 VLAN IDs)

1.4.6.2 Supports jumbo frame size of up to 9198 bytes

1.4.6.3 VXLAN tunneling

1.4.7 Multicast

1.4.7.1 Support IGMPv1, v2, and v3

1.4.7.2 Support IGMP snooping

1.4.7.3 Support any-source multicast

1.4.8 Security

1.4.8.1 Integrated trusted platform module (TPM) for platform integrity

1.4.8.2 Access control list (ACL) support for both IPv4 and IPv6

1.4.8.3 ACLs also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis

1.4.8.4 Support Remote Authentication Dial-In User Service (RADIUS)

1.4.8.5 Ensure critical device are still allow network access during RADIUS server failure

1.4.8.6 Support Terminal Access Controller Access-Control System (TACACS+)

1.4.8.7 Support Control Plane Policing

1.4.8.8 Support RadSec

1.4.8.9 Support ICMP throttling

1.4.8.10 Allows tunneling of traffic from switches to transports user traffic to a Layer 7 firewall to enhanced security and visibility

1.4.9 Convergence

1.4.9.1 LLDP-MED (Media Endpoint Discovery) defines a standard extension of LLDP that stores values for
parameters such as QoS and VLAN to automatically configure network

devices such as IP phones

1.4.9.2 PoE allocations supports multiple methods (allocation by usage or class, with LLDP
and LLDP-MED) to allocate PoE power for more efficient power management and energy savings.

1.4.9.3 CDPv2 uses CDPv2 to configure legacy IP phones

1.4.9.4 Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute
and LLDP-MED to automatically configure a VLAN for IP phones

1.4.10 Analytic

1.4.10.1 The switch should have an Analytic engine to monitors and analyzes events that can impact network health

1.4.10.2 Easy access to all network state information allows visibility and analytics

1.4.10.3 REST APIs and Python scripting for fine-grained programmability of network tasks

1.4.10.4 Continuous telemetry data with WebSocket subscriptions for event driven automation

1.4.10.5 Allows downloading of Analytic Agent from the manufacturer to extend the function and features of the switches in terms on visibility, analytic and automation.

1.5 Datacenter Core Switch (Server Farm Switch)

The Tenderer shall propose datacenter core switches with the following features.

1.5.1. Key Features

1.5.1.1 Minimum 1.76 Tbps with 1,309 Mpps throughput

1.5.1.2 Simplifies operations via unified network automation and management with fabric Composing/Orchestration toolset.

1.5.1.3 Accelerates infrastructure service provisioning with fabric Composing/Orchestration
toolset.

1.5.1.4 Network Analytics Engine—A first-of-a-kind, built-in framework for monitoring,
troubleshooting, and capacity planning

1.5.1.5 Compact 1Uswitches variety of port density options. Including 1/10 GbE, 2/3.5/5/10G SmartRate GbE and 40/100 GbE connectivity.

1.5.1.6 Modular, Linux-based and built with OVSDB to support a database-centric operating
system.

1.5.1.7 Support core/aggregation in the campus or Top of Rack (ToR) and End of Row (EoR)
in the datacenter

1.5.1.8 Support automation and programmability using built-in REST APIs and Python scripts.

1.5.1.9 Intelligent monitoring and visibility with Network Analytics Engine.

1.5.1.10 Advanced Layer 2/3 feature set includes BGP, OSPF, VRF, and IPv6.

1.5.1.11 High availability with industry-leading redundancy, and redundant power supplies and fans

1.5.1.12 Distributed architecture with separation of data and control planes.

1.5.1.13 Includes independent monitoring and restart of individual software modules, and enhanced software process serviceability functions.

1.5.1.14 Allows individual software modules to be upgraded for higher availability.

1.5.1.15 Has RJ-45 Console Port and USB-A Host Port

1.5.1.16 Provide hardware warranty including power supply and fan until the end of sale of the switch.

1.5.2 Quality of Service (QoS)

1.5.2.1 feature—Supports congestion actions, such as strict priority (SP) queuing and weighted fair queuing.

1.5.3 Resiliency

1.5.3.1 Enables a distributed and redundant architecture by deploying two switches, with each switch maintaining independent control yet staying synchronized during upgrades or failover.

1.5.3.2 Virtual Router Redundancy Protocol (VRRP)—Allows groups of two routers to dynamically back each other up to create highly available routed environments.

1.5.3.3 Unidirectional Link Detection (UDLD)—Monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.

1.5.3.4 IEEE 802.3ad LACP—Supports up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm.

1.5.3.5 Redundant power supplies—Provides N+1 high reliability with hot swappable, redundant power supplies.

1.5.3.6 Redundant and load-sharing fans, and power supplies—Increases total performance and power availability while providing hitless, stateful failover.

1.5.3.7 Hot-swappable power supply and fan modules—Allows replacement of modules without any operational impact on other modules.

1.5.3.8 Separate data and control paths—Separates control from services and keeps service processing isolated; increases security and performance.

1.5.3.9 Rapid Per-VLAN spanning tree plus (RPVST+)

1.5.3.10 Support Ethernet Ring Protection Switching (ERPS), Supports rapid protection and recovery in a ring topology.

1.5.3.11 Support IEEE 802.3ad LACP supports up to 54 LAGs and 16 member per LAG with user-selectable L1 to L4 hashing algorithm

1.5.4 Performance

1.5.4.1 High-speed fully distributed architecture—Provides minimum 3.6 Tbps for switching and 2,000 MPPS for forwarding. All switching and routing are wire-speed to meet the demands of bandwidth-intensive applications today and in the future.

1.5.4.2 Scalable system design—Provides investment protection to support future technologies and higher-speed connectivity

1.5.5 Connectivity

1.5.5.1 Jumbo frames—Supports high-performance backups and disaster recovery systems; provides a maximum frame size of 9 K bytes.

1.5.5.2 Loopback – Supports internal loopback testing for maintenance purposes and an increase in availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.

1.5.5.3 Packet storm protection—Protects against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds.

1.5.6 Management

1.5.6.1 Management interface control—Enables or disables these interfaces depending on
security preferences: console port or reset button.

1.5.6.2 Industry-standard CLI with a hierarchical structure – Reduces training time and
expenses, and increases productivity in multivendor installations.

1.5.6.3 Management security—Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide SNMP access; and local and remote Syslog capabilities allow logging of all access.

1.5.6.4 SNMP v2c/v3—Provides SNMP read and trap support of the industry standard Management Information Base (MIB) and private extensions.

1.5.6.5 IPSLA—Monitor the network for degradation of various services, including monitoring voice. Monitoring is enabled via the NAE for history and for automated gathering of additional information when anomalies are detected.

1.5.6.6 sFlow (RFC 3176)—Increases total performance and power availability while providing hitless, stateful failover.

1.5.6.7 Remote monitoring (RMON) – Uses standard SNMP to monitor essential network functions and supports events, alarms, history, and statistics groups, as well as a private alarm extension group.

1.5.6.8 TFTP and SFTP support—Offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security.

1.5.6.9 Debug and sampler utility—Supports ping and traceroute for IPv4 and IPv6.

1.5.6.10 Network Time Protocol (NTP)—Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network. Can serve as the NTP server in the network.

1.5.6.11 IEEE 802.1AB Link Layer Discovery Protocol (LLDP)—Advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

1.5.6.12 Dual flash images – Provides independent primary and secondary operating system files for backup while upgrading.

1.5.6.13 Multiple configuration files – Easily stores the flash image.

1.5.6.14 Built-in programmable and easy-to-use REST API interface

1.5.6.15 Multiple configuration files can be stored to a flash image and allows rollback of any of these configurations without requires reboot

1.5.6.16 Support Secure Sockets Layer (SSL) which encrypts traffic, allowing secure access to the browser-based management GUI in the switch

1.5.6.17 ASIC-based wire speed network monitoring and accounting RFC 3176 sFlow

1.5.7 Layer 2 Switching

1.5.7.1 VLAN—Supports up to 4,040 port-based or IEEE 802.1Q-based VLANs.

1.5.7.2 VXLAN—Supports static VXLAN. Allows to connect two or more VXLAN tunnel endpoints (VTEP).

1.5.7.3 Port mirroring—Duplicates port traffic (ingress and egress) to a local or remote monitoring port; supports four mirroring groups with an unlimited number of ports per group.

1.5.7.4 STP—Supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

1.5.7.5 Internet Group Management Protocol (IGMP)—Controls and manages the flooding of multicast packets in a Layer 2 network.

1.5.7.6 Rapid Per-VLAN spanning tree plus (RPVST+)—Allows each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs.

1.5.8 Layer 3 Services and Routing

1.5.8.1 Address Resolution Protocol (ARP) – Determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network.

1.5.8.2 Dynamic Host Configuration Protocol (DHCP)—DHCP services are offered within a client network to simplify network management. DHCP relay enables DHCP operation across subnets.

1.5.8.3 Domain Name System (DNS) – Provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

1.5.8.4 Policy Based Routing (PBR)—Enables using a classifier to select traffic that can be forwarded based on a policy set by network administrator.

1.5.8.5 Static IPv4 routing – Provides simple manually configured IPv4 routing.

1.5.8.6 Open shortest path first (OSPF)—Delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and a graceful restart for faster failure recovery.

1.5.8.7 Border Gateway Protocol 4 (BGP-4)—Delivers an implementation of the Exterior Gateway Protocol (EGP), utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; and scales to very large networks.

1.5.8.8 6in4 tunnels—Supports the tunneling of IPv6 traffic in an IPv4 network.

1.5.8.9 IP performance optimization – Provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters,

1.5.8.10 Static IPv6 routing – Provides simple manually configured IPv6 routing.

1.5.8.11 Dual IP stack—Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

1.5.8.12 OSPFv3—Provides OSPF support for IPv6.

1.5.8.13 Equal-Cost Multipath (ECMP) – Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.

1.5.9 Security

1.5.9.1 Access control list (ACL) Features—Supports powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices such as IP addresses. For instance, IT management devices could be grouped in this way. ACLs can also protect control plane services, such as SSH, SNMP, NTP, or web servers.

1.5.9.2 Remote Authentication Dial-In User Service (RADIUS)—Eases security access administration by using a password authentication server.

1.5.9.3 Terminal Access Controller Access-Control System (TACACS+) – Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security.

1.5.9.4 Management access security—provides for both on-box as well as off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can provide user authorization services.

1.5.9.5 Secure shell (SSHv2)—Uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers.

1.5.9.6 Support Remote Authentication Dial-In User Service (RADIUS)

1.5.9.7 Support Terminal Access Controller Access-Control System (TACACS+)

1.5.9.8 Support RadSec , RadSec enables RADIUS authentication and accounting data to be passed safely and reliably across insecure networks

1.5.10 Multicast

1.5.10.1 Internet Group Management Protocol (IGMP)—Enables establishing multicast group memberships in IPv4 networks; supports IGMPv1, v2, and v3.

1.5.10.2 Multicast Listener Discovery (MLD)—Enable discovery of IPv6 multicast listeners; supports MLDv1 and v2.

1.5.10.3 IGMP/MLD Snooping—Prevent flooding of multicast traffic to non-listening ports.

1.5.10.4 Protocol Independent Multicast (PIM) – Supports one-to-many and many-to-many media casting use cases, such as IPTV over IPv4 and IPv6 networks; support for PIM Spare Mode (PIM-SM, IPv4, and IPv6).

1.5.11 Analytic

1.5.11.1 The switch should have an Analytic engine to monitors and analyzes events that can impact network health

1.5.11.2 Easy access to all network state information allows visibility and analytics

1.5.11.3 REST APIs and Python scripting for fine-grained programmability of network tasks

1.5.11.4 Continuous telemetry data with WebSocket subscriptions for event driven automation

1.5.11.5 Allows downloading of Analytic Agent from the manufacturer to extend the function and features of the switches in terms on visibility, analytic and automation.

2. WIRELESS LAN (WLAN)

2.1 General Wireless Requirements

2.1.1 The Tender shall propose an overlay wireless solution that provides centralized or distributed architecture with application control at the edge and seamless scalability.

2.1.2 Flexibility to configure wireless policy, management, or security settings at any time through centralized provisioning and management.

2.1.3 Allows backup controllers to automatically synchronized with existing primary controller, without requiring a separate network management server

2.1.4 Network-wide quality of service (QoS) for voice and video across wired and wireless networks.

2.1.5 Capability to create a self-healing and self-optimizing wireless network.

2.1.6 Traffic between the Wireless APs and WLAN controllers will be tunneled over the existing LAN infrastructure.

2.1.7 Redundancy should be built into the architecture where there is no single point of failure.

2.1.8 Supports chassis and box N+1 redundancy with under 20 seconds failover time.

2.1.9 Supports chassis and box 1+1 fast failover redundancy with sub-second failover time.

2.1.10 Traffic between the WLAN end hosts, and the Wireless access points (APs) should be secured and encrypted.

2.1.11 The proposed wireless solution must support flexible licensing options that provide license portability that enables SCCC to seamless migration of existing licenses/features while making future hardware refresh

2.1.12 The proposed wireless solution must also enable SCCC to benefit from future product feature innovations without having to purchase additional RTU licenses.

2.1.13 The proposed wireless solution must support integration with existing wifi analytic tool (Kiana), BLE or similar technology to provide indoor wayfinding and personalized visitors engagement through apps integration.

2.1.14 The tenderer shall propose the types, quantities, and locations of access points to provide the required coverage.

2.1.15 The tenderer shall show that the proposed access points and their locations will satisfy the required wireless coverage with a wireless heat map simulation or other similar analytical tool. The tenderer shall include the results of such simulation or analysis in the proposal submission.

2.1.16 The proposed wireless deployment must be able to support future deployments of location services without the need to deploy additional access points.

2.1.17 Access point locations and installation methods will be subject to SCCC's approval.

2.1.18 The tenderer shall submit heatmaps of WLAN coverage before and after deployment to SCCC using either AirMagnet or Ekahau tool.

2.2 Wireless Coverage Reference

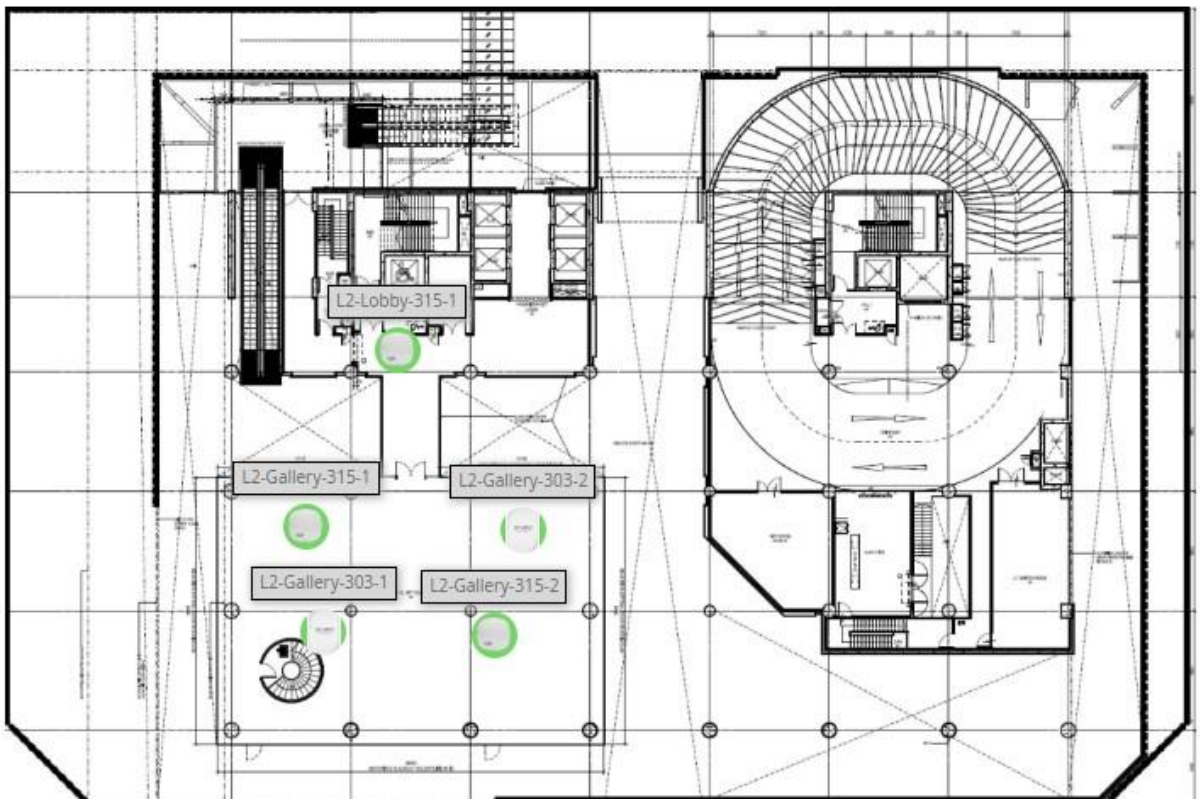
2.2.1 The tenderer shall propose a wireless solution for SCCC Level 1 that provides similar or better coverage. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location:

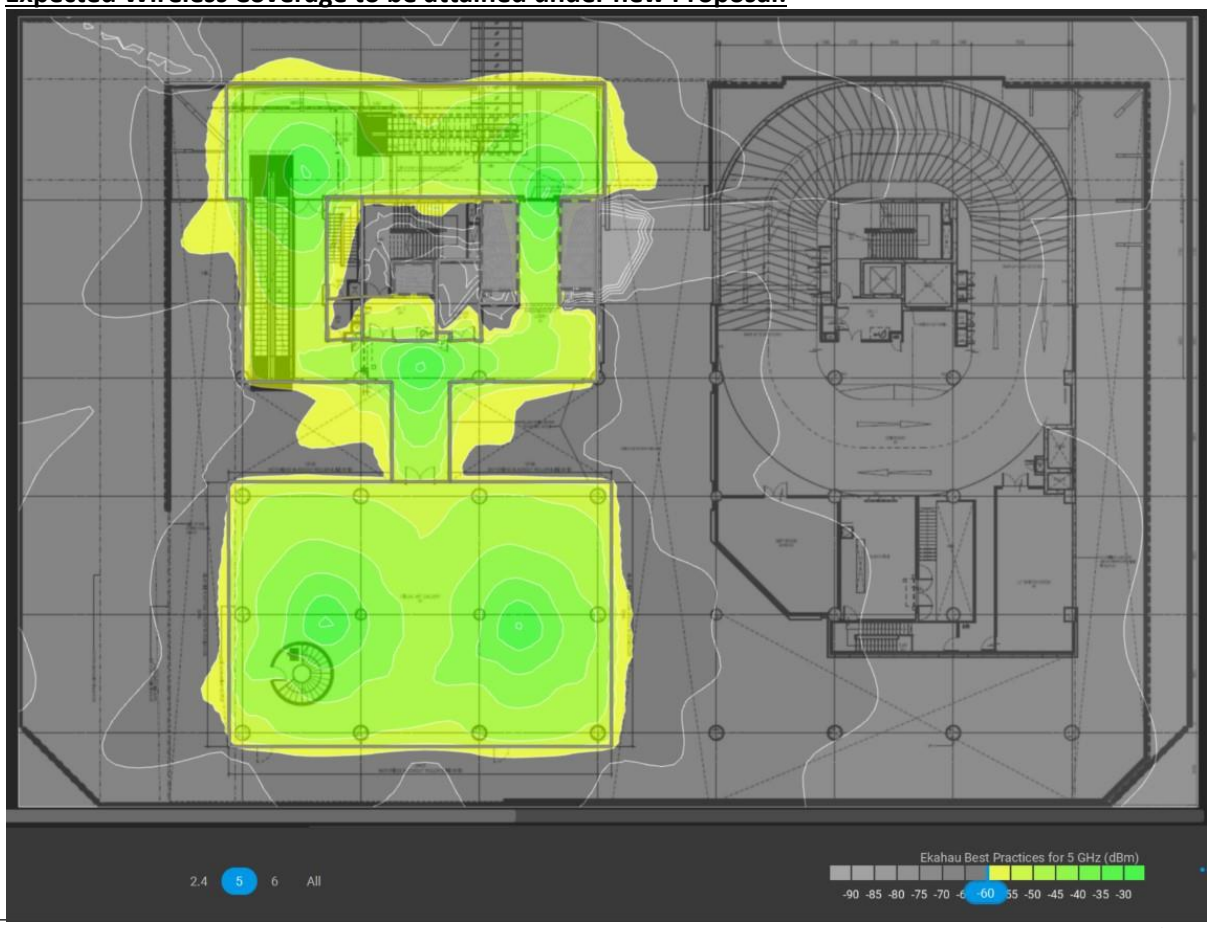
Expected Wireless Coverage to be attained under new Proposal:

2.2.2 The tenderer shall propose a wireless solution for SCCC Level 2 that provides similar or better coverage. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location:

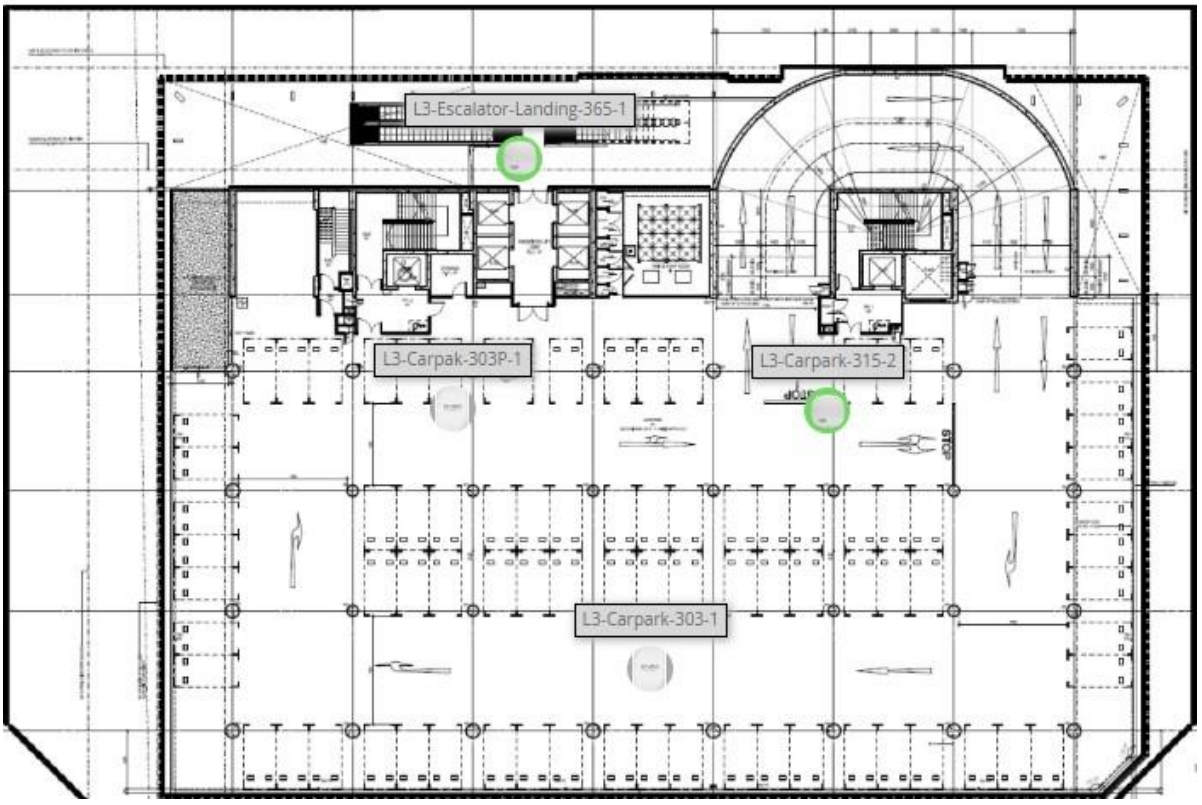


Expected Wireless Coverage to be attained under new Proposal:

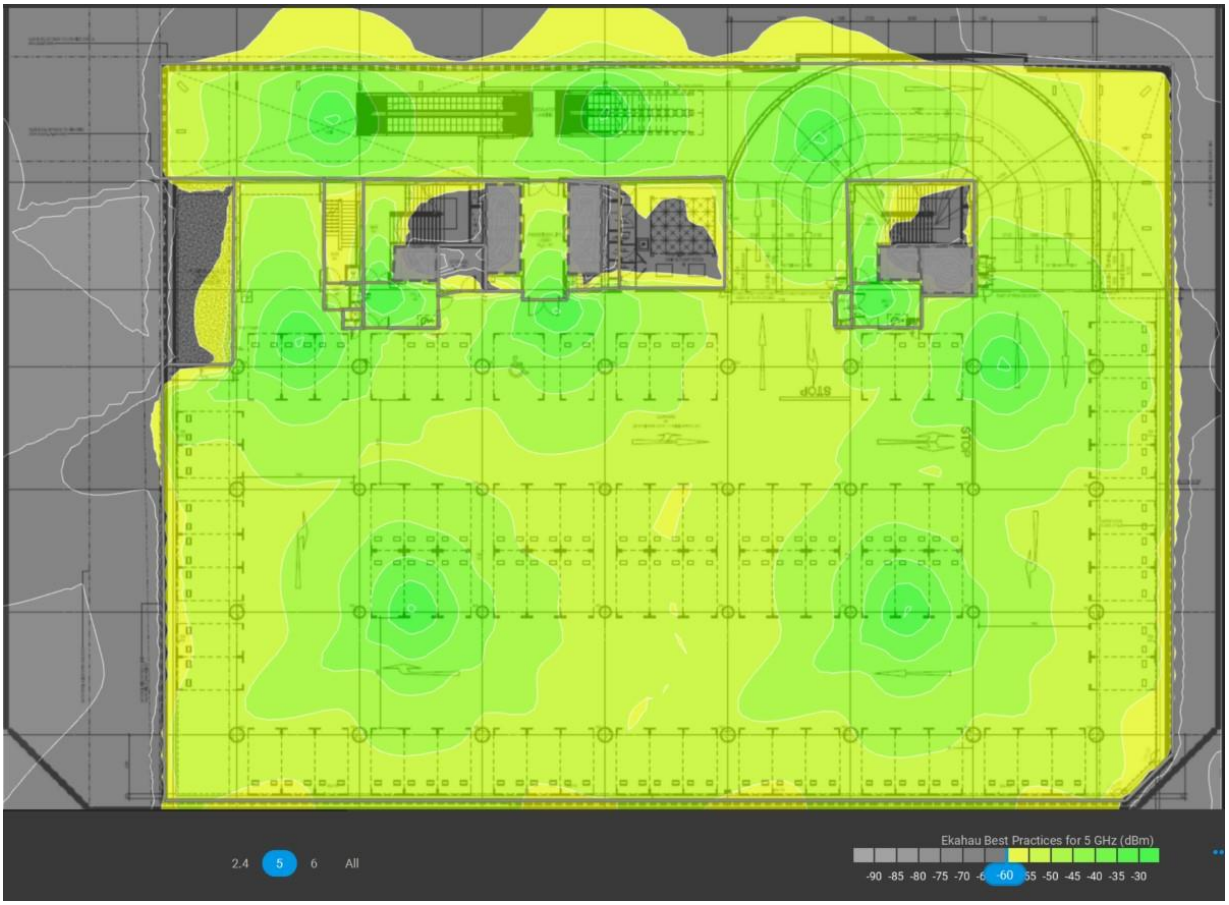


2.2.3 The tenderer shall propose a wireless solution for SCCC Level 3 that provide similar or better coverage. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

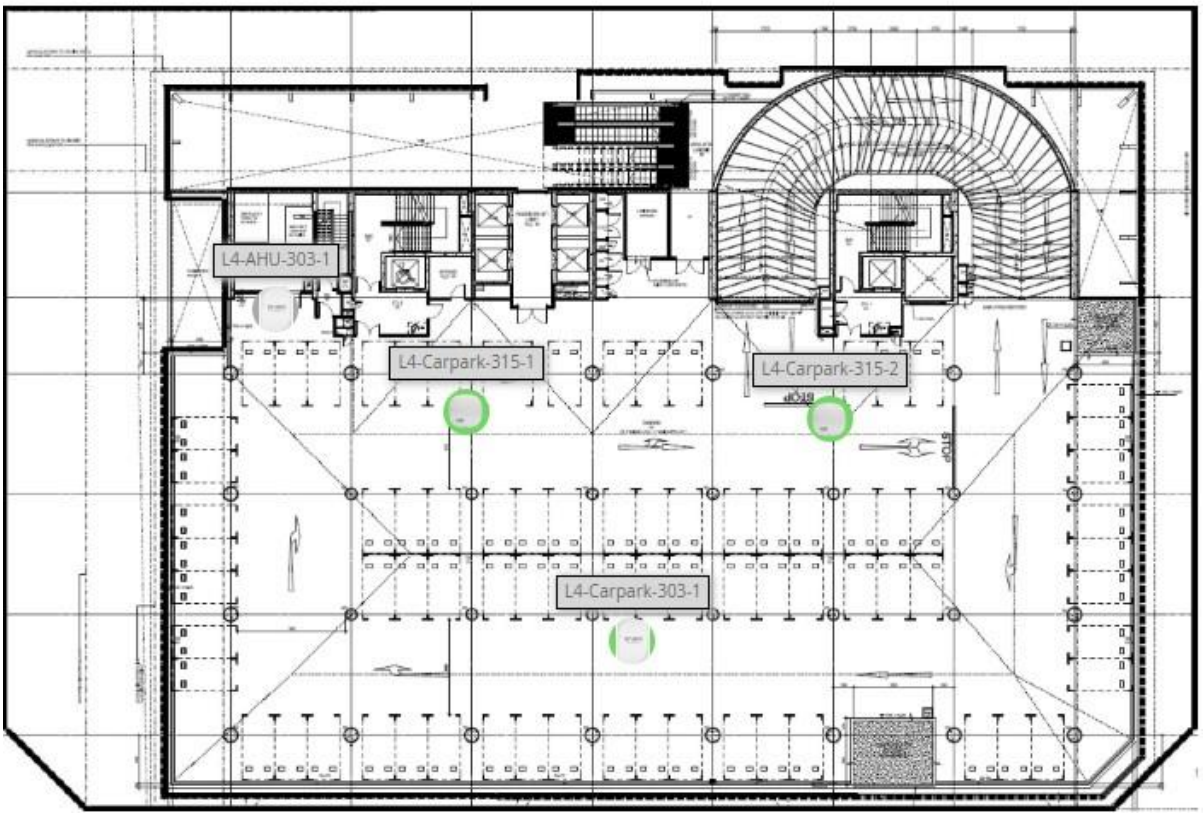


Expected Wireless Coverage to be attained under new Proposal:



2.2.4 The tenderer shall propose a wireless solution for SCCC Level 4 that provide similar or better coverage. BLE or similar beacon technology must be supported in proposed solutions.

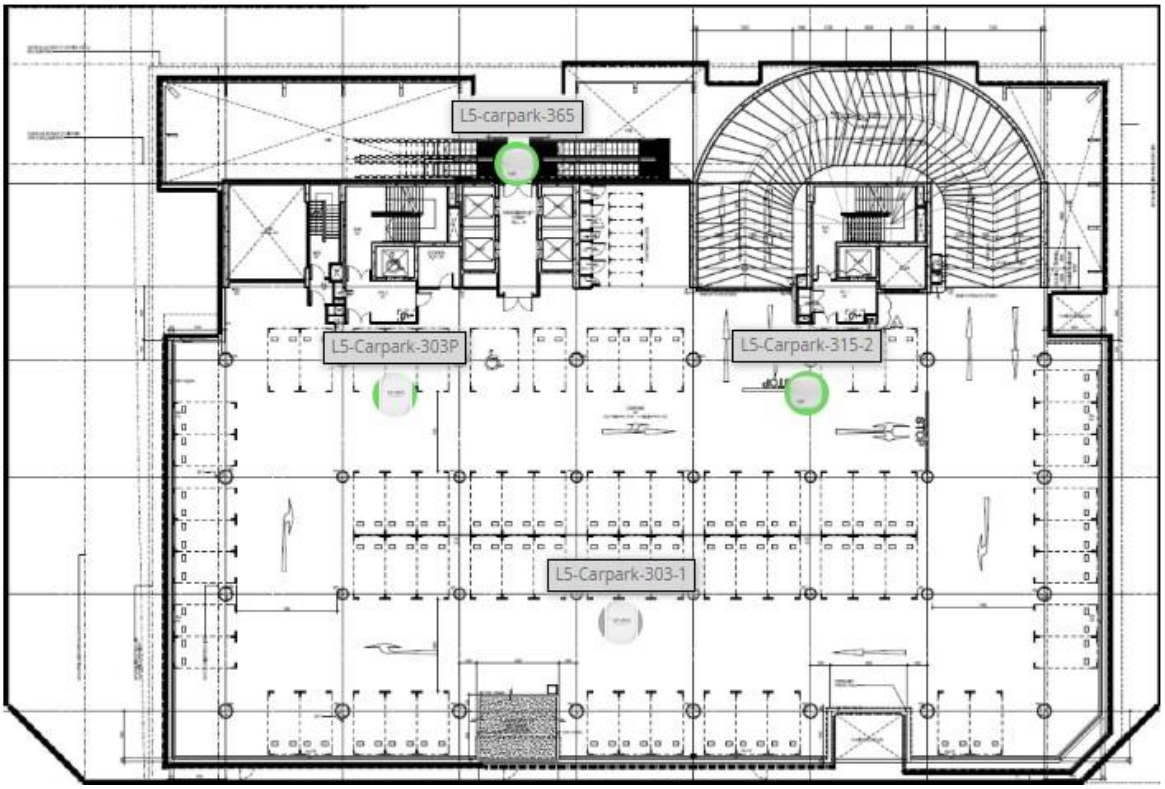
Current APs location :



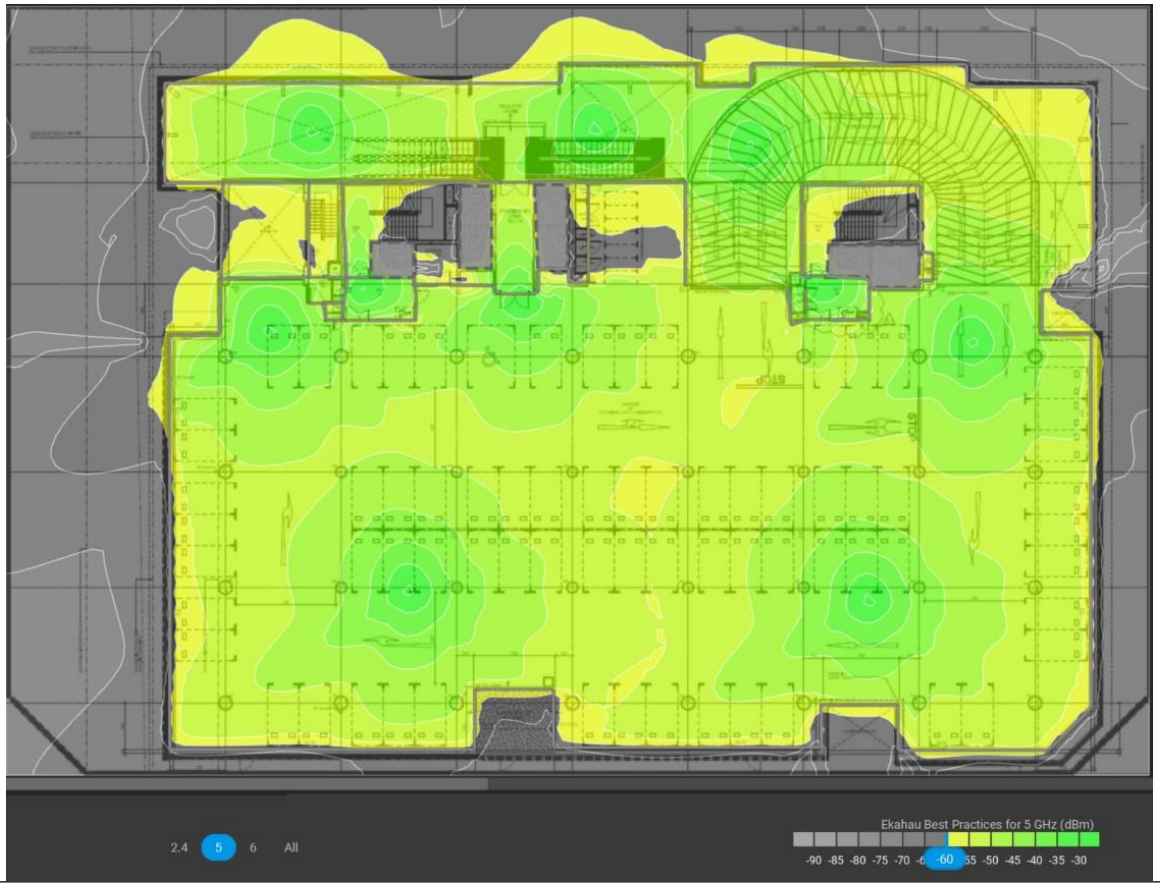
Expected Wireless Coverage to be attained under new Proposal:

2.2.5 The tenderer shall propose a wireless solution for SCCC Level 5 that provide similar or better coverage. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

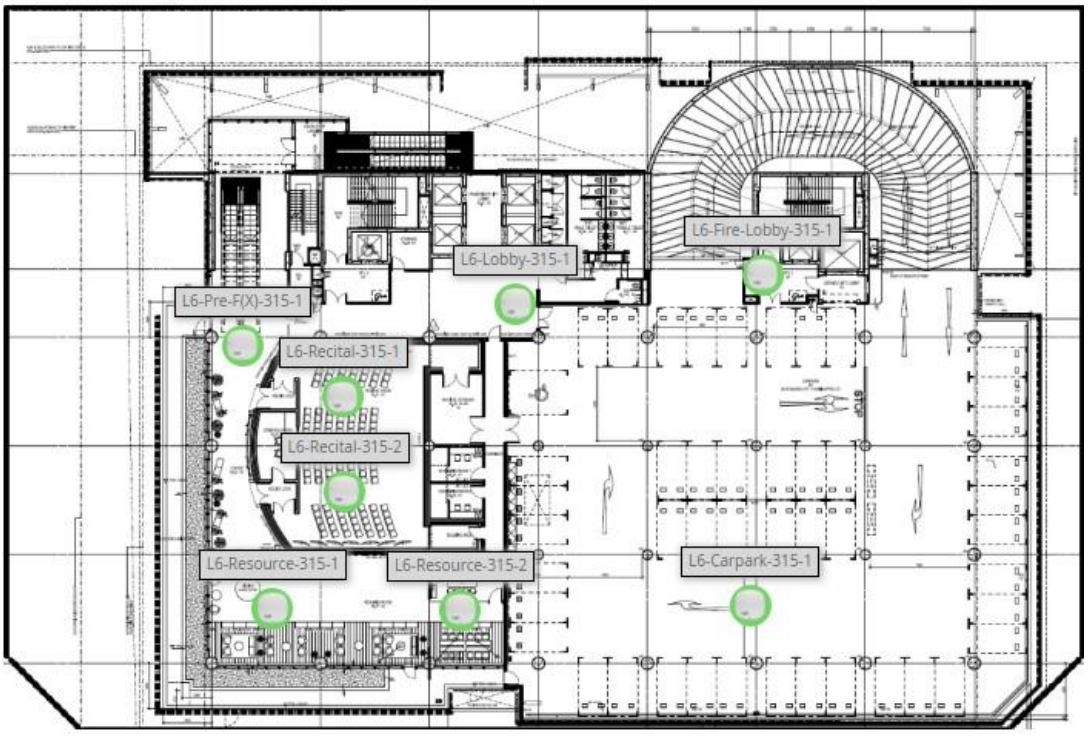


Expected Wireless Coverage to be attained under new Proposal:

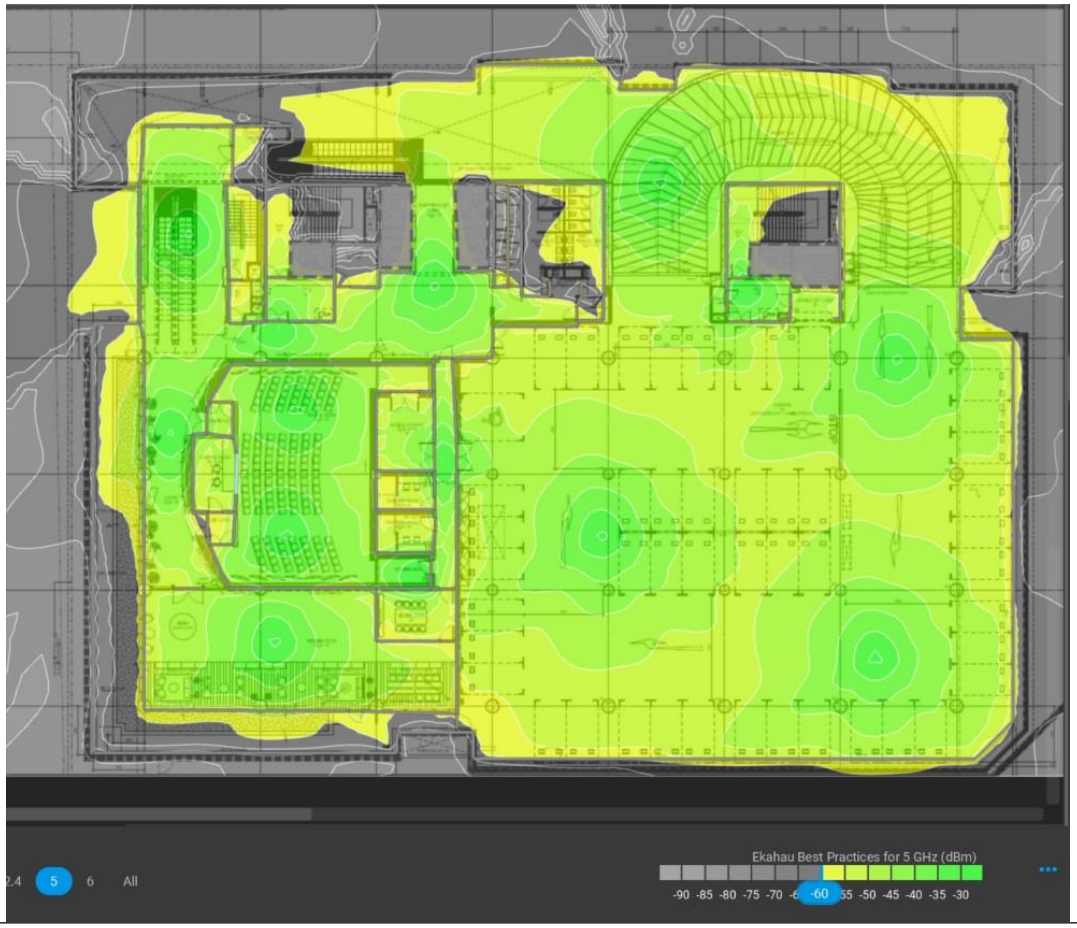


2.2.6 The tenderer shall propose a wireless solution for SCCC Level 6 that provide similar or better coverage. Tenderers may consider the use of directional antennas within Recital Room. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

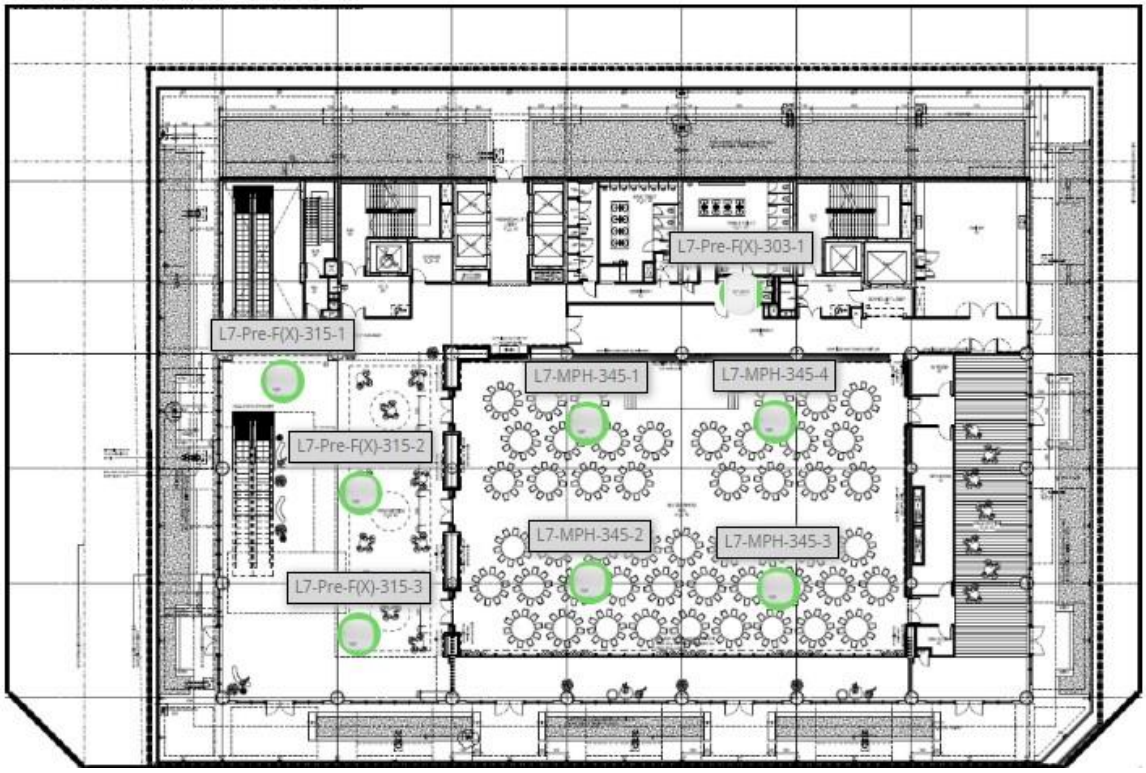


Expected Wireless Coverage to be attained under new Proposal:

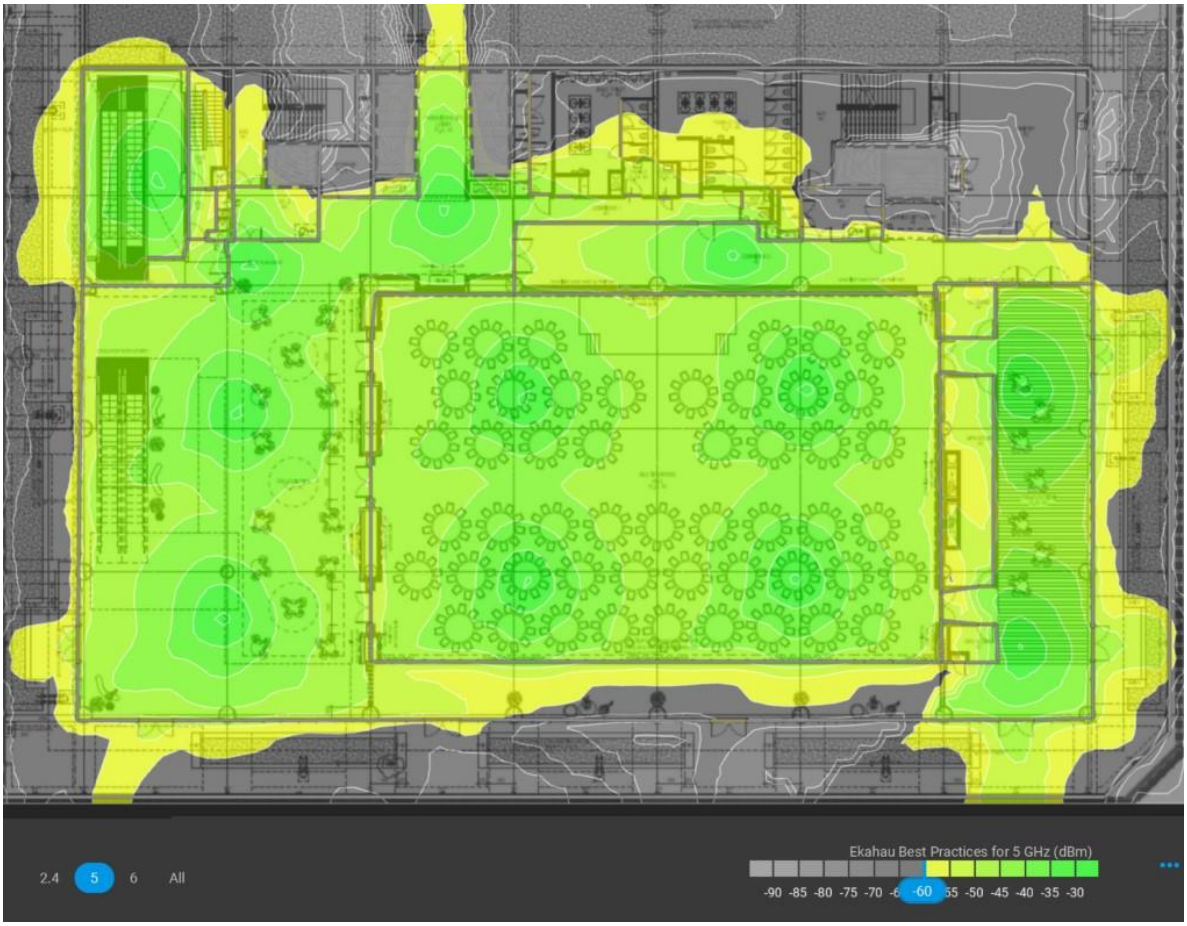


2.2.7 The tenderer shall propose a wireless solution for SCCC Level 7 that provides similar or better coverage. Tenderers should consider a high-density WLAN deployment for multi-Purpose Hall. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

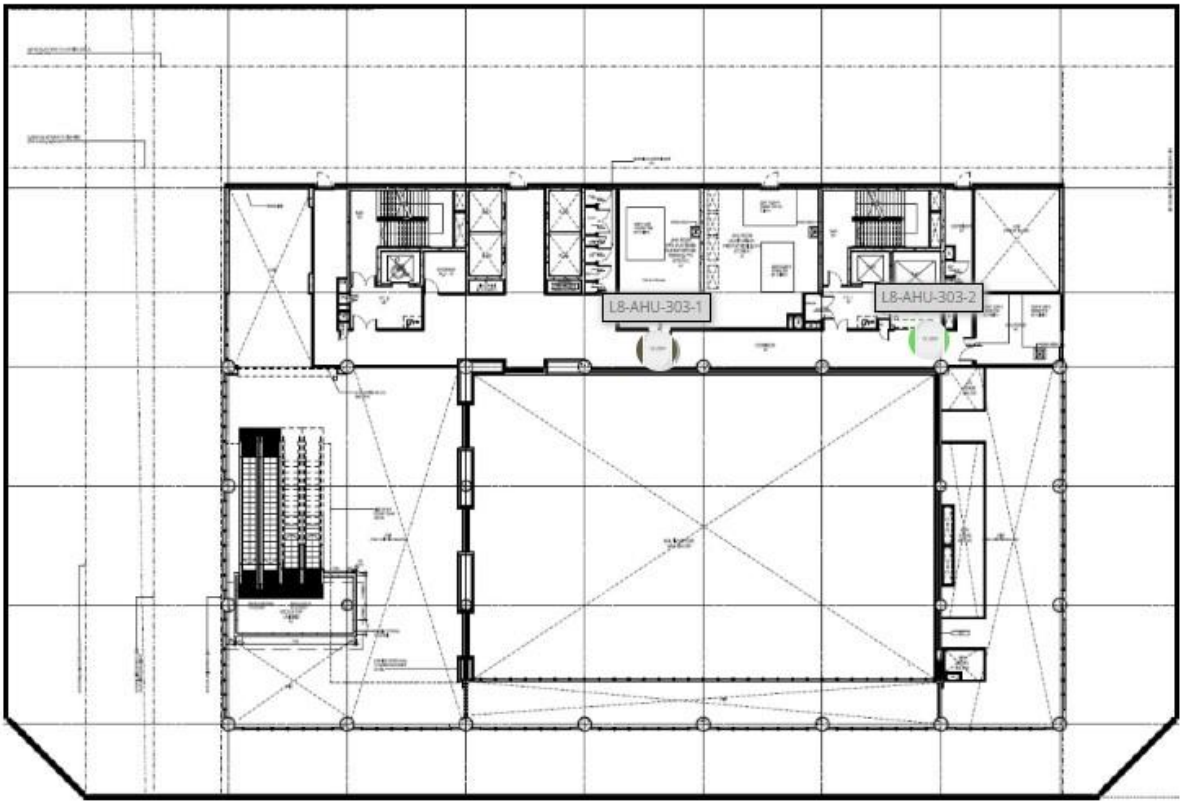


Expected Wireless Coverage to be attained under new Proposal :

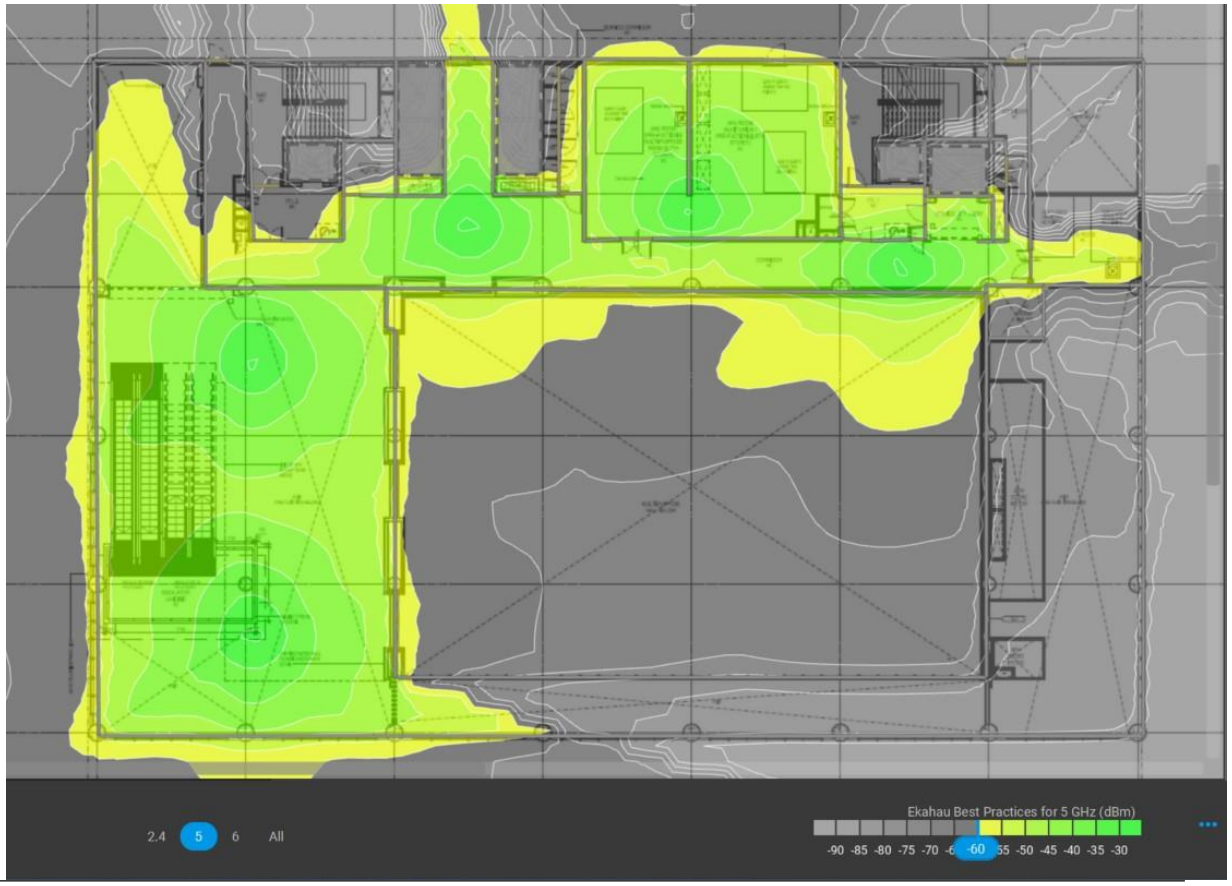


2.2.8 The tenderer shall propose a wireless solution for SCCC Level 8 that provide similar or better coverage. (Due to the layout of the building, wireless coverage for Level 8 may be supplied thru Level 7) BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

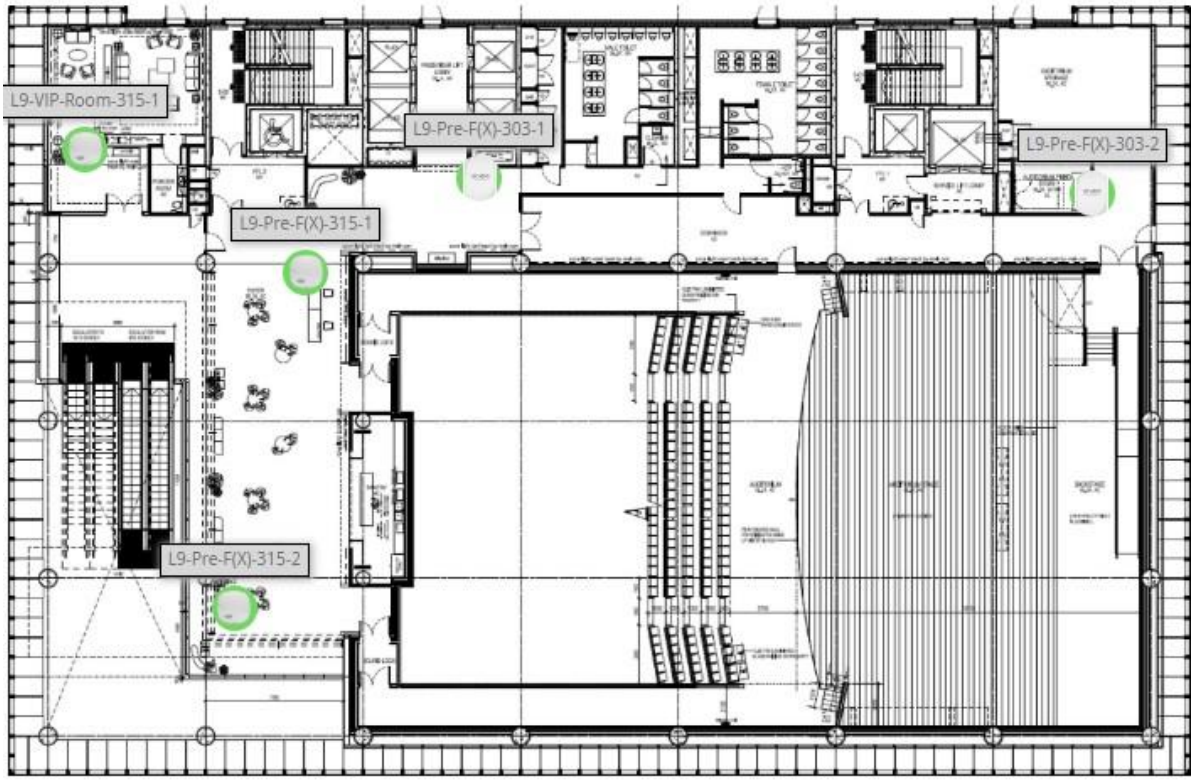


Expected Wireless Coverage to be attained under new Proposal:

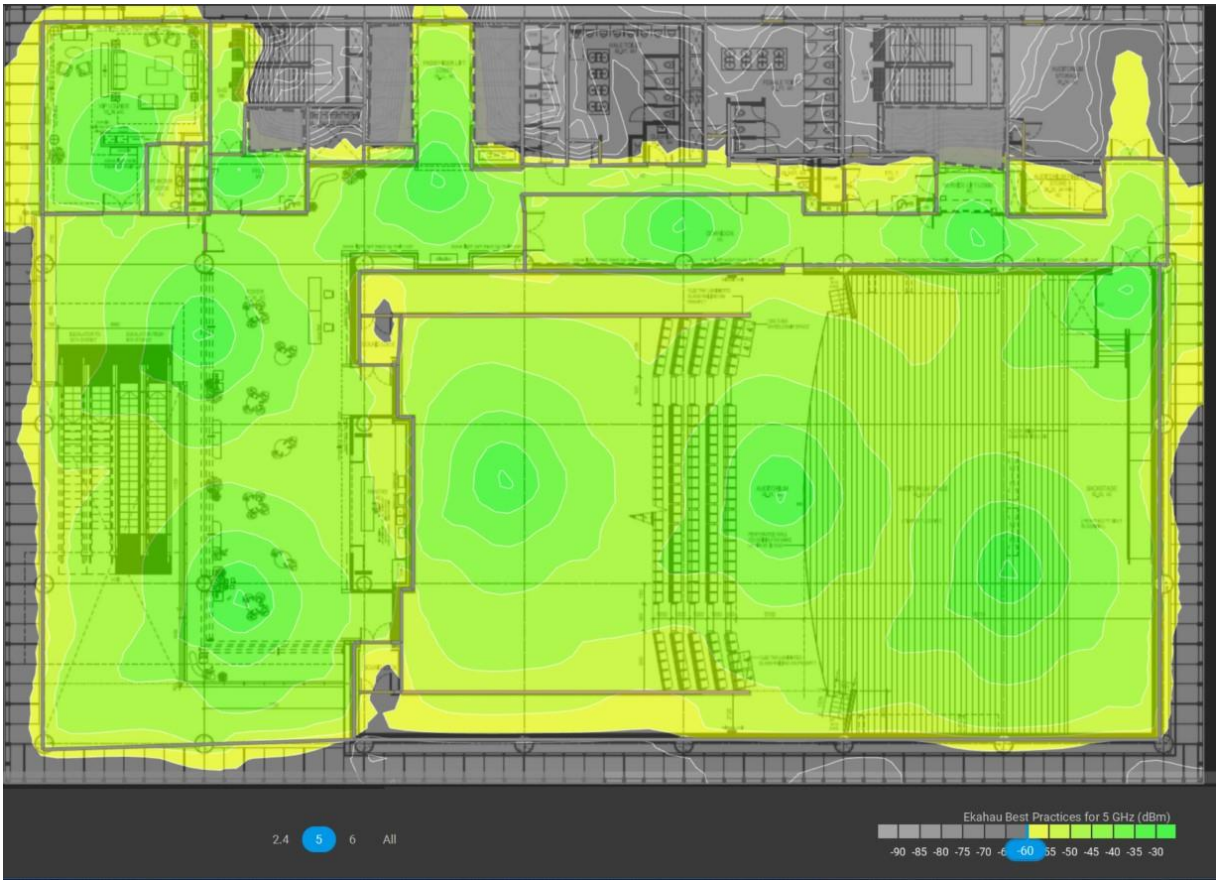


2.2.9 The tenderer shall propose a wireless solution for SCCC Level 9 that provide similar or better coverage. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

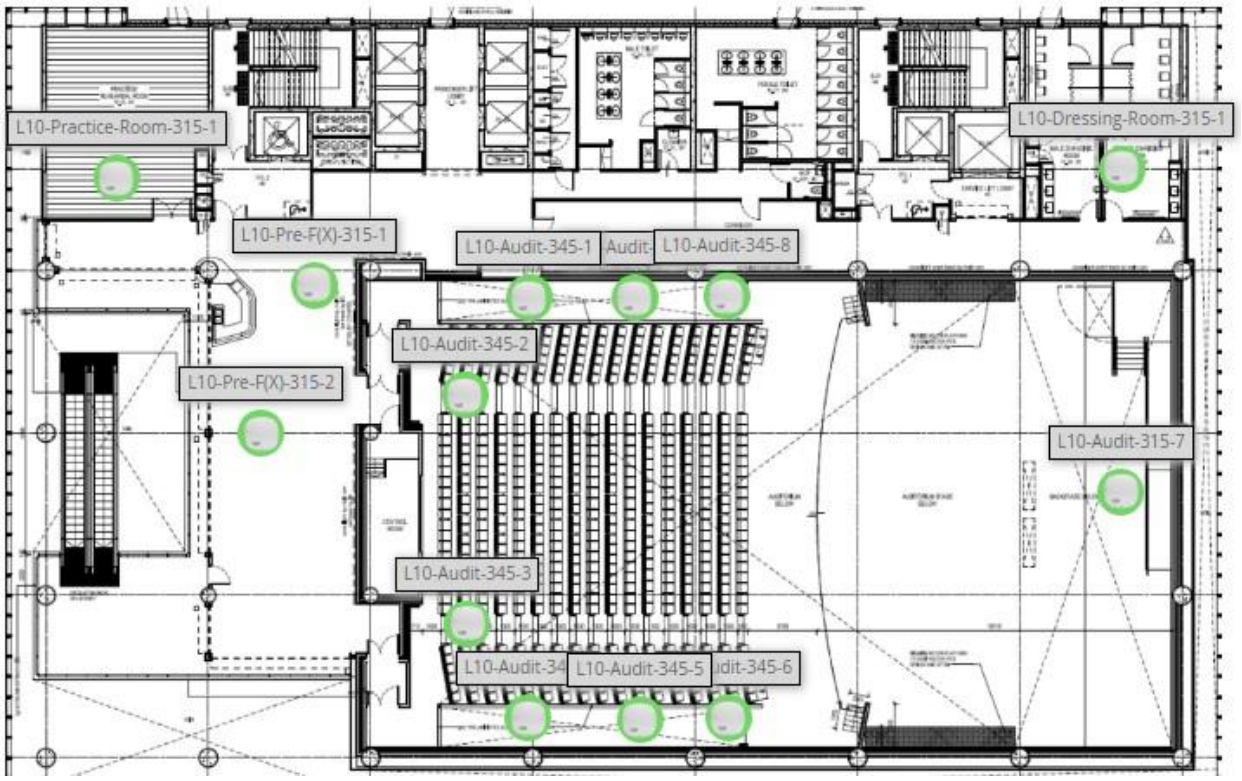


Expected Wireless Coverage to be attained under new Proposal:

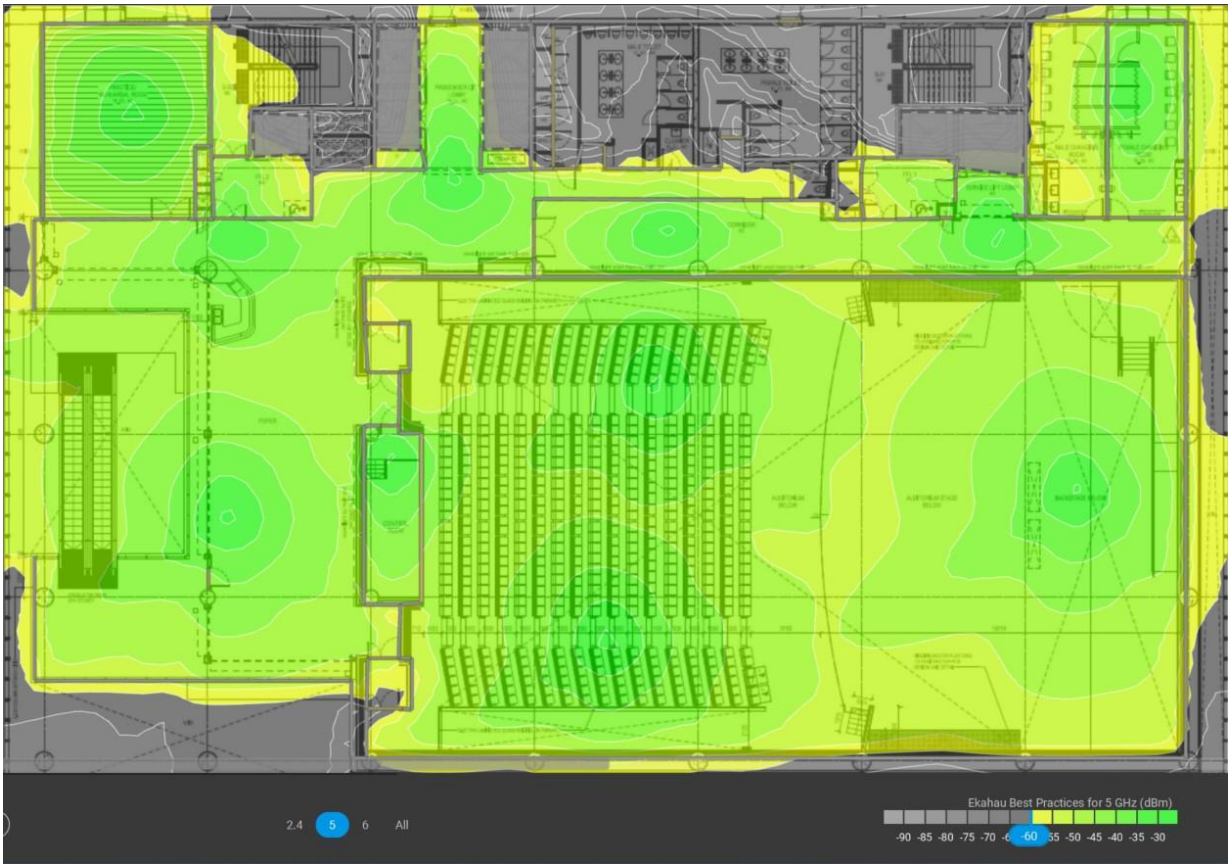


2.2.10 The tenderer shall propose a wireless solution for SCCC Level 10 that provides similar or better coverage. Tenderers should consider a high-density WLAN deployment for multi-Purpose Hall. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

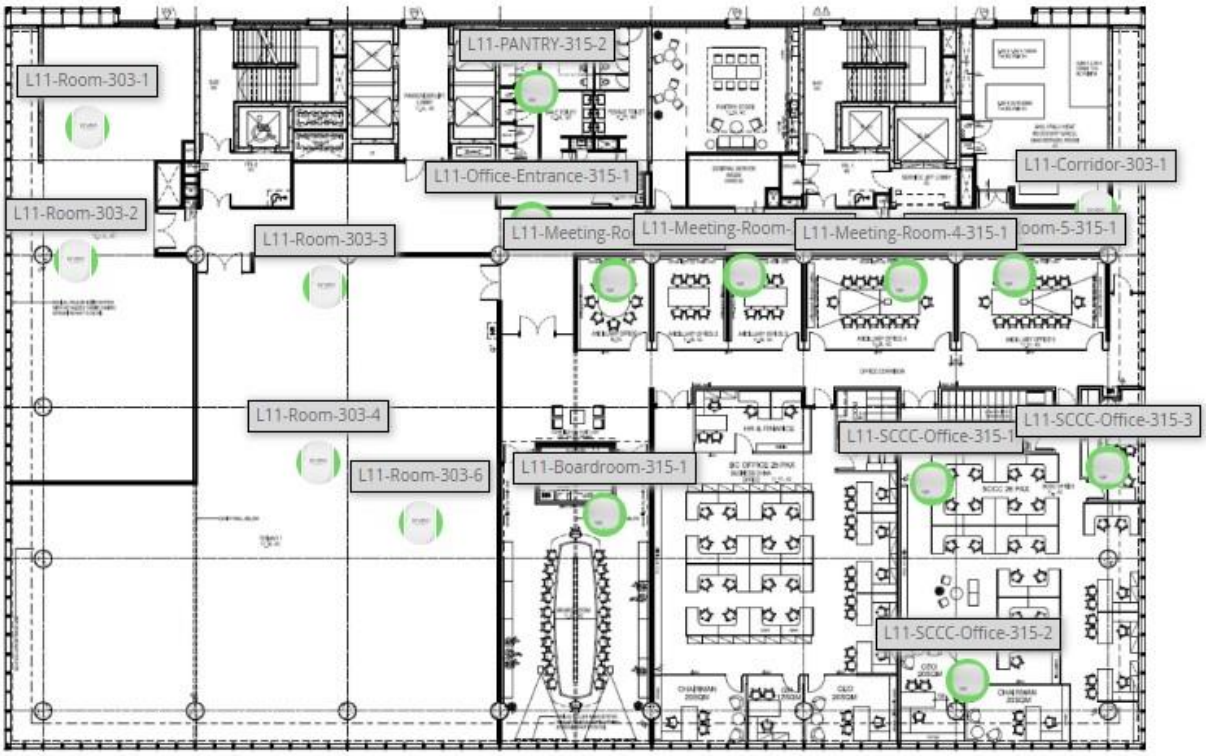


Expected Wireless Coverage to be attained under new Proposal:



2.2.11 The tenderer shall propose a wireless solution for SCCC Level 11 that provides similar or better coverage. Tenderers should consider deploying a high-speed, high-capacity WLAN deployment capable of supporting PHY rates of up to 5.2Gbps. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

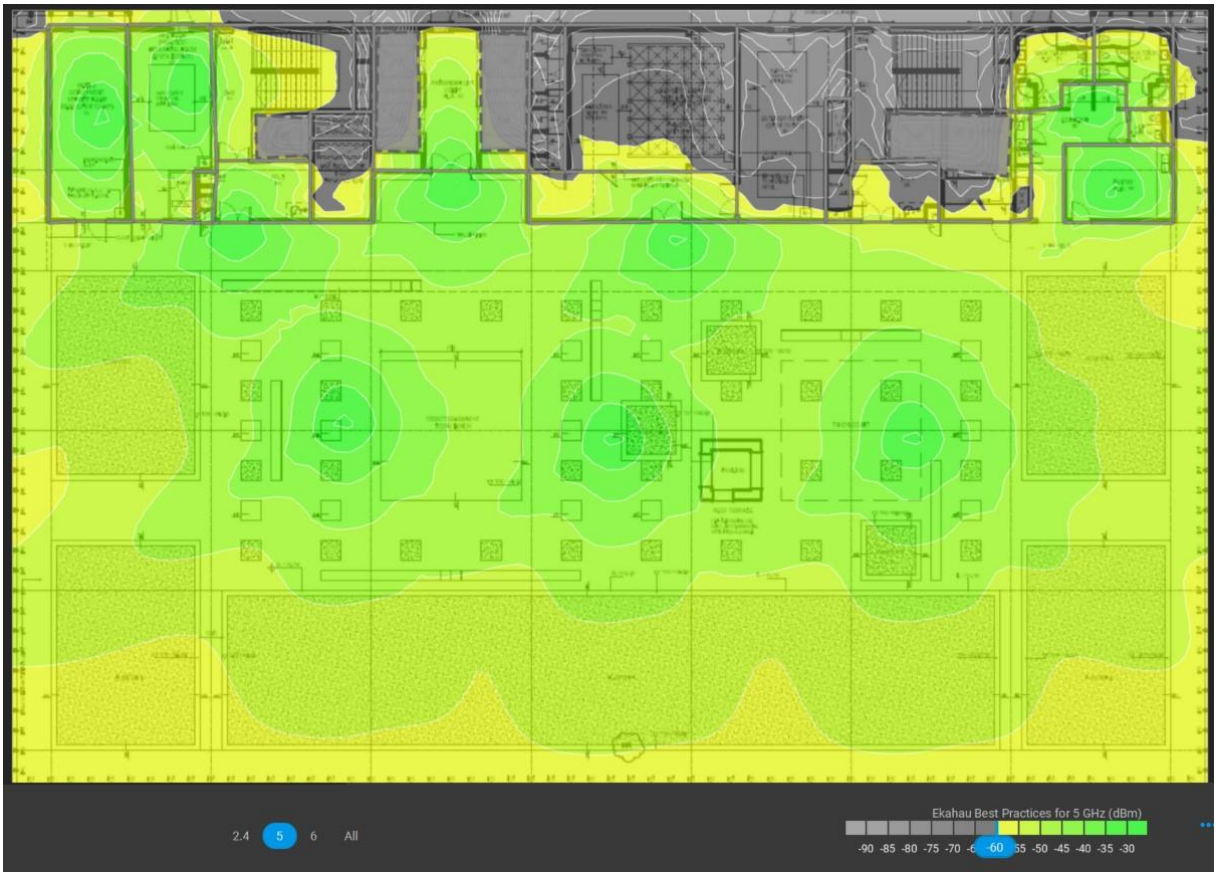


Expected Wireless Coverage to be attained under new Proposal:

2.2.12 The tenderer shall propose an outdoor 802.11ac Wave 2 wireless solution for SCCC Level 12 that provides similar or better coverage. BLE or similar beacon technology must be supported in proposed solutions.

Current APs location :

Expected Wireless Coverage to be attained under new Proposal:



2.3 Features:

2.3.1 The wireless LAN controller must be able to scale up to support at least at least 300 APs and up to 3,000 concurrent wireless clients with an aggregated throughput of no less than 12Gbps.

2.3.2 The wireless LAN controller must support at least 2 x 10Gbase-X (SFP+) ports and/or 4 x 1G Combo (Copper and Fiber).

2.3.3 The wireless LAN controller must also have the option to encrypt data path traffic between the AP and the controller using DTLS or equivalent protocols.

2.3.4 The wireless LAN controller must support high availability features to minimize downtime in the unlikely event of a controller failure, with the following deployment models and features:

2.3.5 Active/active (1:1) – each wireless LAN controller typically serves 50% of its rated capacity. The first acts as a standby for APs served by the second controller and vice-versa. If a controller fails, its APs failover to the other controller, ensuring high availability to all APs.

2.3.6 N+1 – multiple active wireless LAN controller is backed-up by a single standby controller.

2.3.7 The wireless LAN controller must also support stateful failover by wireless client state in both Active and Standby controller such that client disassociation is avoided during failover of the primary controller, resulting in zero client service downtime and no SSID outage.

2.3.8 The system must support seamlessly connectivity with roaming handoff times of 2-3 milliseconds, delay-sensitive and persistent applications such as voice and video experience uninterrupted performance, included:

2.3.8.1 Fast roaming: 2-10 msec intra-controller, 10-30 msec inter-controller

2.3.8.2 Roaming across subnets and VLANs

2.3.8.3 Automatically establishes home agent/foreign agent relationship between controllers

2.3.8.4 Prevent clients from changing IP address while roaming

2.3.8.5 Automatically load balances clients across multiple VLANs

2.3.9 The wireless LAN controller must support facilitate inter-controller roaming by enabling context and state of client devices, WLC loading information and data traffic shared and forwarded between controllers within the same mobility group.

2.3.10 The wireless LAN controller must support secure connection (e.g. IPSEC/VPN) of APs to centralized switch over “untrusted” (e.g. public WAN) network transport, without requiring external hardware and without requiring dedicated switch/controller.

2.3.11 The wireless LAN controller must support Proactive Key Caching and/or other

methods to enable fast secure roaming.

2.3.12 Optimize overall network capacity by helping to ensure that 802.11a/b/g, 802.11n, 802.11ac and 802.11ax clients operate at the best possible rates.

2.3.13 Supports wireless intrusion prevention system (IPS) provides robust protection for the entire wireless network, including detection, location, and mitigation of security penetration and DoS threats.

2.3.14 Capability to eliminate sticky clients and optimize roaming for both 802.11k and non-802.11k clients by dynamically generating neighbor AP list that includes information about BSSID, channel, and operation details of the neighboring radios. Clients are discouraged from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

2.3.15 Supports adaptive 802.11r to allow 802.11r-capable clients to benefit from BSS Fast Transition without the need to enable 802.11r on the WLAN and losing support for non-802.11r capable clients.

2.3.16 Enterprise wireless mesh that allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network.

2.3.17 Provide both real-time and historical information about Radio Frequency (RF) interference impacting network performance across wireless LAN controller.

2.3.18 Support power assignment to optimize network coverage and performance based on changing RF conditions.

2.3.19 Support automatic assignment of channels and channel width (80MHz, 40MHz and 20MHz) to adapt to interference by intelligently understanding the available channels regardless of width, and the maximum number of non-overlapped channels.

2.3.20 Detection of radar would typically force a loss of 80MHz (11ac) or 40MHz (11n) channel and constrain usable channels for DFS, the WLC must be able to isolate radar event to 20MHz and allows the continued usage of clear channels. E.g. If radar interference is detected on a Channel 60 of 80MHz channel (52/56/60/64), the controller must automatically adapt to interference and adjust the channel usage to either remaining 3x 20MHz channels or 1x 40MHz and 1x 20MHz channel, rather than abandoning the entire affected 80MHz channel.

2.3.21 Co-channel interference management to prevent adverse effects of operating multiple APs in the same channel while in close proximity (for instance within 2.4GHz band where 3x
802.11 channels are available).

2.3.22 Dynamic load balancing to automatically distribute clients to the least loaded AP; load balancing must not require any client specific configurations or software.

2.3.23 Load balancing across bands and steering of tri-band capable clients from 2.4GHz to 5GHz or 6GHz in order to improve network performance without the use of client specific configurations or software.

2.3.24 The wireless LAN controller must support radio management techniques to handle the high density of wireless devices. It should assign fair amount of air-time to all devices

connected to the same radio, load balance clients across 802.11 channels and across 2.4GHz, 5GHz & 6GHz frequency bands.

2.3.25 Provides the ability to allocate downlink airtime entitlement per SSID, client, realm based on time, differentiated user-class SLA and availability. E.g. granting a higher percentage of airtime to employee SSIDs as opposed to guest SSIDs.

2.3.26 Support packet-rate-based bandwidth contract for individual guest users for increased control of guest traffic usage.

2.3.27 The wireless LAN controller must correlate interference data from Wi-Fi and non-Wi-Fi devices for automatic interference mitigation by accurately identifying the source, location and scope of problems caused by both interferences.

2.3.28 Time-of-day / duration-based access per guest user of increased control and security.

2.3.29 Time-of-day availability of guest SSID for increased control and security.

2.3.30 Ability to detect rogue devices or potential wireless threats, and also locates these devices. This enables system administrators to quickly assess the threat level and take immediate action to mitigate threats as required.

2.3.31 Support capacity to scale access points, simultaneously serving clients, monitoring for wireless intrusion detection system and wireless intrusion protection system (wIDS/wIPS), location, rogues, and system-wide scaling of spectrum detection, classification, and event-driven radio resource management.

2.3.32 The wireless LAN controller must have the capability to shut or block WLAN client in collaboration with wired IPS on detecting malicious client traffic.

2.3.33 Capability to segment and form virtual subgroup of access points and apply different RF configurations for different access point groups.

2.3.34 The wireless LAN controller must support the following security and encryption standards:

2.3.34.1 WPA
2.3.33.2. IEEE 802.11i
2.3.33.3. RFC 2406 IPsec
2.3.33.4. RFC 1321 MD5 Message-Digest Algorithm
2.3.33.5. RFC 1851 ESP Triple DES Transform
2.3.33.6. RFC 2104 HMAC: Keyed Hashing for Message Authentication
2.3.33.7. RFC 2451 ESP CBC-Mode Cipher Algorithms
2.3.33.8. RFC 2403 HMAC-MD5-96 within ESP and AH
2.3.33.9. RFC 2401 Security Architecture for the Internet Protocol
2.3.33.10. RFC 2404 HMAC-SHA-1-96 within ESP and AH
2.3.33.11. RFC 2408 ISAKMP
2.3.33.12. RFC 2409 IKE
2.3.33.13. RFC 2405 ESP DES-CBC cipher algorithm with explicit IV
2.3.33.14. RFC 2403 Use of HMAC-SHA1-96 with ESP and AH
2.3.33.15. RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
2.3.33.16. RFC 3748, 5247 Extensible Authentication Protocol (EAP)
2.3.33.17. RFC 2716 PPP EAP TLS Authentication Protocol
2.3.33.18. RFC 2246 TLS Protocol version 1.0
2.3.33.19. RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP
2.3.33.20. RFC 3280 Internet X.509 PKI Certificate and CRL Profile
2.3.33.21. RFC 3686 Using AES Counter Mode with IPsec ESP
2.3.33.22. RFC 4347 Datagram Transport Layer Security
2.3.33.23. RFC 4346 TLS Protocol Version 1.1

2.3.35 The wireless LAN controller must support the following Authentication Authorization, and Accounting (AAA) features:

2.3.35.1 IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS,
2.3.35.2 EAP-TTLS, EAP-FAST, EAP-SIM, EAPPOTP,
2.3.35.3 EAP-GTC, EAP-TLV, EAP-AKA, EAP Experimental, EAP-MD5)
2.3.35.4 RFC 2548 Microsoft Vendor-Specific RADIUS Attributes
2.3.35.5 RFC 2716 PPP EAP-TLS
2.3.35.6 RFC 2865 RADIUS Authentication
2.3.35.7 RFC 2866 RADIUS Accounting
2.3.35.8 RFC 2867 RADIUS Tunnel Accounting
2.3.35.9 RFC 2869 RADIUS Extensions
2.3.35.10 RFC3576 Dynamic Authorization Extensions to RADIUS
2.3.35.11 RFC 3579 RADIUS Support for EAP
2.3.35.12 RFC 3580 IEEE 802.1X RADIUS Guidelines
2.3.35.13 RFC 3748 Extensible Authentication Protocol
2.3.35.14 MAC Address authentication
2.3.35.15 Web-based captive portal authentication
2.3.35.16 TACACS support for management users

2.3.36. The wireless LAN controller must support the following management and traffic analysis features and standards:

2.3.36.1 SNMPv1, v2c, v3
2.3.36.2 RFC 854 Telnet
2.3.36.3 RFC 1155 Management Information for TCP/IP-Based Internets
2.3.36.4 RFC 1156 MIB
2.3.36.5 RFC 1157 SNMP
2.3.36.6 RFC 1213 SNMP MIB II
2.3.36.7 RFC 1350 TFTP
2.3.36.8 RFC 1643 Ethernet MIB
2.3.36.9 RFC 2030 SNTP
2.3.36.10 RFC 2616 HTTP
2.3.36.11 RFC 2665 Ethernet-Like Interface types MIB
2.3.36.12 RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions
2.3.36.13 RFC 2819 RMON MIB
2.3.36.14 RFC 2863 Interfaces Group MIB
2.3.36.15 RFC 3164 Syslog
2.3.36.16 RFC 3414 User-Based Security Model (USM) for SNMPv3
2.3.36.17 RFC 3418 MIB for SNMP
2.3.36.18 RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs

2.3.37 Support Internet Group Management Protocol (IGMP) snooping and access point should transmit multicast packets only if a client associated to the access point is subscribed to the multicast group.

2.3.38 Support battery-saving features to convert Multicast frames to Unicast to offer better sleep time for the mobile device while ensuring the benefits of wireless service discovery and announcements protocols (Bonjour, DLNA or UPnP) remains consistent.

2.3.39 Support mDNS gateway capability by listening for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint etc.) from the source/host e.g. AppleTV, responds back to Bonjour clients when a request for service is initiated.

2.3.40 mDNS services can be accessed even when the mDNS device is connected via an Ethernet cable on a network.

2.3.41 The wireless LAN controller must support location specific wireless mDNS services, such that only clients connected to the same AP as the mDNS device will have access to that service.

2.3.42 Secure FTP to securely upload/download software images to and from wireless LAN controller.

2.3.43 The wireless LAN controller must provide a secure interface for management and monitoring of on-premises WLAN network via mobile application on iOS and Android platforms.

2.3.44 The wireless LAN controller must support one-touch deployment of recommended configuration based on best practices.

2.3.45 The management dashboard of the wireless LAN controller must provide at-a-glance analytics, performance and utilization trends.

2.4 Wireless Access Control and QoS Features:

2.4.1 Ability to define rules for access rights based on any combination of time, location, user identity,
device identity, and extended attributes from the authentication database.

2.4.2 Provides security enforcement for wireless users through the use of role-based classifications that can be directly integrated with the roles defined within existing authentication servers.

2.4.3 The wireless LAN controller must be able to take action including to allow the traffic, deny the traffic, rate-limit or modify the QoS level of the traffic if the policy matches.

2.4.4 Offers bandwidth contract on a per application basis (voice, video and data)

2.4.5 Support profiling of devices based on protocols like HTTP, DHCP and to identify the end devices on the network.

2.4.6 Supports deep packet inspection capability that can classify applications, applies quality of service (QoS) setting to either drop or mark the traffic, and prioritizes business-critical applications in the network.

2.4.7 Ability to apply QoS and bandwidth policies to different users based on their role within the organization and the device type they currently use, even when these different users/devices are connected to the same SSID.

2.4.8 Ability to offers bandwidth contract on a per application basis (voice, video and data) or per AP group.

2.4.9 Support Wireless MultiMedia (WMM), also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF). WMM provides prioritization of specific traffic relative to other traffic in the network.

2.4.10 Upstream and downstream packet tagging between AP and controller/switch using standard tagging mechanisms.

2.4.11 Provide policy-based quality-of-service traffic management capability to optimize WLAN bandwidth utilization, even if the traffic is not tagged by the source.

2.4.12 Ability to rate-limit traffic bidirectionally, on either a per-SSID or per-user basis for real-time (UDP) or data (TCP) traffic.

2.4.13 Support for configuring media streams with different priority to identify specific video or voice streams for preferential quality-of-service treatment.

2.4.14 Support VoIP Call Admission Control (CAC) to ensure that when a VoWLAN call is admitted into the wireless network, there is enough voice capacity across all access points.

2.4.15 The wireless LAN controller must be able to identify over 1000+ applications, including cloud and web-based mobile apps like Lync, SharePoint, Box, GotoMeeting and Salesforce.com.

2.4.16 The wireless LAN controller must support application packs that contain set of protocols/applications signatures that can be loaded on to the controller without upgrading the firmware.

2.4.17 The wireless LAN controller must support deep insight into Layer 4-7 traffic for user for all traffic across the network to analyze information about applications usage, peak network usage times for all access points. This information must be exportable to a collector for further analysis and analytics.

2.5 Wireless Mobility Features:

2.5.1 Features onboard customizable capabilities or integration with other mobile app software platform to allow business to use the proposed Wi-Fi network to engage guests with value- added and personalized mobile user experiences.

2.5.2 The solution must offer the following features:

2.5.2.1 Presence and location detection using WiFi, BLE or similar technologies.

2.5.2.2 Visibility

2.5.2.3 Easy Wi-Fi login

2.5.2.4 Zone-based or custom splash pages based on customizable contextual information.

2.5.2.5 Provides app-based mobile engagement

2.5.2.6 Offers context-aware in-venue experiences

2.5.3 Provides real-time location details alongside historical trends, enabling greater visibility into people's movements and patterns through trending data.

2.5.4 Provides analytics to determine wireless network utilization, peak use, number and types of devices.

2.5.5 Reporting and documenting people's movements throughout facilities and using collected analytics to engage business requirements more effectively.

2.5.6 Provides the capability to display real-time information on Wi-Fi client count and dwell time. Information must include:

2.5.6.1 Number of visitors

2.5.6.2 Amount of time spent

2.5.6.3 Frequency of visits

2.5.6.4 Number of new vs. repeat visitors

2.5.7 Ability to provide zone analytics by creating logical zones within venue to understand relative utilization of different areas to identify trends such as foot traffic in different part of the facility.

2.5.8 Provides the capability to integrate with Facebook to provide free Wi-Fi after devices login to the guest portal using their Facebook account.

2.5.9 Provides the capability for API integration and notifications to allow external triggers, to export data for custom analytics and to allow external consumption of the location information.

2.6 Wireless Access Point (AP) features:

The Tender shall propose Access Points with the following features for the general areas of the facility

2.6.1 High performance tri-radio mode with 6Ghz, 5GHz and 2.4GHz radio (2x2 MIMO) 802.11ax AP with OFDMA and Multi-User MIMO (MU-MIMO) (uplink and downlink for both). Able to deliver up to 3.9 Gbps combined peak data rate.

2.6.2 Support up to seven 160 MHz channels in 6 GHz support low-latency, bandwidth-hungry applications like high-definition video and augmented reality/virtual reality applications.

2.6.3 Must Support ultra-triband filtering enables 5 GHz and 6 GHz to operate without restrictions or interference. Ultra Tri-Band (UTB) enables ultimate flexibility in 5GHz and 6GHz channel selection without performance degradation

2.6.4 Support high availability with 2.5 Gbps for hitless failover of ethernet and power. These dual uplink ports provide business continuity for mission critical applications.

2.6.5 Built in GPS receivers and intelligent software enable APs to self-locate and act as reference points for accurate indoor location measurements from client devices and other indoor APs using fine time measurements and other location technologies.

2.6.6 Support both on-perm or cloud management option.

2.6.7 To support Open Locate, an emerging standard that allows APs to share their location over the air and through cloud-based APIs, enabling mobile devices to locate themselves and applications to support network analytics.

2.6.8 Supports all mandatory and several optional 802.11ax features, which include uplink and downlink OFDMA with up to 37 resource units WiFi6 in 80MHz, uplink and downlink multi-user MIMO (MU-MIMO).

2.6.9 3.9 Gbps of maximum throughput and up to 1024 clients per radio and 2048 clients per AP. Built-in technology that resolves sticky client issues for WiFi6/6E and WiFi5 devices.

2.6.10 Ideal for high density environments, such as schools, retail branches, hotels, and

enterprise offices.

2.6.11 IOT ready Bluetooth 5, NFC and Zigbee support embedded.

2.6.12 Multi-user transmission with downlink and uplink OFDMA—OFDMA increases user data rates and also reduces latency, especially for large numbers of devices with short frames or low data-rate requirements, such as voice and IoT devices. By providing multi-user capabilities, a channel can be divided in the frequency domain, and multiple transmissions can be carried out simultaneously. OFDMA is particularly effective in raising network efficiency and capacity where there are many devices, short frames, or low data-rate streams.

2.6.13 Multiuser capability with uplink and downlink multi-user MIMO—MU MIMO is another multi-user capability, originally introduced in 802.11ac. This improves network capacity by allowing multiple devices to transmit simultaneously.

2.6.14 Support an integrated Bluetooth Low-Energy (BLE) and Zigbee radio, as well as a USB port for maximum flexibility, providing secure and reliable connectivity for IOT devices and for implementing location services

2.6.15 Unified AP support—Flexibility to deploy in either controller-based or controller-less networks or Cloud controller-based.

2.6.16 Dual Radio 802.11ax access point with OFDMA and Multi-User MIMO (MU-MIMO):

- 2.6.16.1 Up to 37 OFDMA resource units and up to 1024 simultaneous clients per radio.
- 2.6.16.2 Antenna polarization diversity for optimized RF performance.
- 2.6.16.3 802.11ax Target Wait Time (TWT) to support low power client devices.

2.6.17 2.6.17 Uplink Ethernet port (E0 and E1):

- 2.6.17.1 Auto-sensing link speed (100/1000/2500BASE-T) and MDI/MDIX.
- 2.6.17.2 Supports up to 2.5 Gbps with NBase-T and IEEE 802.3bz Ethernet compatibility.
- 2.6.17.3 Backwards compatible with 100/1000Base-T.

2.6.18 Built-in Bluetooth Low-Energy (BLE) and Zigbee radio—Enables a wide range of IOT use cases, such as asset tracking and mobile engagement.

2.6.19 Quality of service for unified communications applications: Supports priority handling and policy enforcement for unified communication applications, including MS team, Zoom, Skype for Business with encrypted videoconferencing, voice, chat, and desktop sharing.

2.6.20 Support deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories.

2.6.21 Best-in-class RF Management:

- 2.6.21.1 Integrated AirMatch technology manages the 2.4 GHz ,5 GHz and 6 GHz radio bands and actively optimizes the RF environment, including channel width, channel selection, and transmit power.
- 2.6.21.2 Adaptive Radio Management (ARM) technology provides airtime fairness and helps ensure that APs stay clear of all sources of RF interference to deliver reliable, high-performance WLANs.

2.6.18 Spectrum analysis: Capable of part-time or dedicated air monitoring, the spectrum analyzer remotely scans the 2.4 GHz 5 Ghz and 6 GHz radio bands to identify sources of RF interference from 20 MHz through 160 MHz operation.

2.6.19 Device assurance—Use of Trusted Platform Module (TPM) for secure storage of credentials and keys, as well as secure boot. APs shall not hold “hard configured” internal network information or certificates for authentication to the centralized switches unless this information is stored in a trusted platform module (TPM) integrated into the AP.

2.6.20 Integrated wireless intrusion protection offers threat protection and mitigation and eliminates the need for separate RF sensors and security appliances.

2.6.21 IP reputation and security services identify, classify, and block malicious files, URLs and IPs, providing comprehensive protection against advanced online threats.

2.6.22 SecureJack-capable for secure tunneling of wired Ethernet traffic.

2.6.23 Intelligent Power Monitoring (IPM):

2.6.21.3 AP shall support serving WIFI client using just 802.3at PoE at 30W power when using IPM

2.6.21.4 Enables the AP to continuously monitor and report its actual power consumption and optionally make autonomous decisions to disable certain capabilities based on the amount of power available to the unit.

2.6.21.5 Software-configurable to disable capabilities in specified order of priority.

2.6.23.1 The IPM feature applies when the unit is powered by an 802.3at POE source.

2.6.24 Green AP system feature to support a custom deep-sleep mode to deliver significant power and cost savings

2.6.25 AP type—Indoor, tri-radio mode with 5GHz, 6Ghz and one 2.4GHz radio, 802.11ax AP with OFDMA and Multi-User MIMO (MU-MIMO). Both downlink and uplink MU-MIMO in 6GHz and 5GHz, downlink only in 2.4GHz.

2.6.26 5 GHz radio: Two spatial stream Single User (SU) MIMO for up to 1.2 Gbps wireless data rate to individual 2SS HE80 802.11ax client devices.

2.6.27 6 GHz radio: Two spatial streams MIMO for up to 2.4Gbps wireless data rate with H160 802.11ax client devices.

2.6.28 2.4 GHz radio: Two spatial stream Single User (SU) MIMO for up to 287Mbps wireless data rate with HE20 802.11ax client devices802.11ax MU-MIMO capable client devices simultaneously (typical).

2.6.29 Support for up to 1024 associated client devices per radio and up to 16 BSSIDs per radio.

2.6.30 Supported frequency bands (country-specific restrictions apply):

2.6.30.1 - 2.400 to 2.4835GHz

2.6.30.2 - 5.150 to 5.250GHz

2.6.30.3 - 5.250 to 5.350GHz

2.6.30.4 - 5.470 to 5.725GHz

2.6.30.5 - 5.725 to 5.850GHz

2.6.30.6 - 5.850 to 5.895GHz
2.6.30.7 - 5.925 to 6.425GHz
2.6.30.8 - 6.425 to 6.525GHz
2.6.30.9 - 6.525 to 6.875GHz
2.6.30.10 - 6.875 to 7.125GHz

2.6.31 Available channels—Dependent on configured regulatory domain.

2.6.32 Dynamic frequency selection (DFS) optimizes the use of available RF spectrum in 5Ghz band. Must Support Zero-Wait DFS (ZWDFS) to accelerate channel changes.

2.6.33 Supported radio technologies:
2.6.33.1 802.11b: Direct-sequence spread-spectrum (DSSS)
2.6.33.2 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)
2.6.33.3 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to 37
2.6.33.4 resource units (for an 80 MHz channel)

2.6.34 Supported modulation types:
2.6.34.1 802.11b: BPSK, QPSK, CCK
2.6.34.2 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM (proprietary extension)
2.6.34.3 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM (proprietary extension)
2.6.34.4 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
2.6.34.5 802.11n high-throughput (HT) support: HT20/40
2.6.34.6 802.11ac very high throughput (VHT) support: VHT20/40/80/160(80+80)
2.6.34.7 802.11ax high efficiency (HE) support: HE20/40/80/160

2.6.35 Supported data rates (Mbps):
2.6.35.1 802.11b: 1, 2, 5.5, 11
2.6.35.2 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
2.6.35.3 802.11n (5 GHz): 6.5 to 600 (MCS0 to MVC31, HT20 to HT40)
2.6.35.4 802.11ac: 6.5 to 3,467 (MCS0 to MCS9, NSS = 1 to 4, VHT20 to VHT80)
2.6.35.5 802.11ax (2.4 GHz): 3.6 to 1,147 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)
2.6.35.6 802.11ax (5 GHz): 3.6 to 2,402 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE80)
2.6.35.7 802.11ax (6GHz): 3.6 to 4,804 (MCS0 to MCS11, NSS = 1 to 4,HE20 to HE160)
2.6.35.8 802.11n/ac packet aggregation: A-MPDU, A-MSDU

2.6.36 Transmit power—Configurable in increments of 0.5 dBm.

2.6.37 Maximum (aggregate, conducted total) transmit power (limited by local regulatory requirements):
2.6.37.1 2.4 GHz band: +21 dBm (18 dBm per chain)
2.6.37.2 5 GHz band: +21 dBm in tri-radio mode (18 dBm per chain)
2.6.37.3 6 GHz band: +21 dBm in tri-radio mode (18 dBm per chain)

2.6.38 Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks.
2.6.39 Maximum ratio combining (MRC) for improved receiver performance.

2.6.40 Cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance.

2.6.41 Space-time block coding (STBC) for increased range and improved reception.

2.6.46 Low-density parity check (LDPC) for high-efficiency error correction and increased

throughput.

2.6.47 Transmit beam-forming (TxBF) for increased signal reliability and range.

2.6.48 Support of 802.11ax Target Wait Time (TWT) to support low-power client devices.

2.6.49 USB 2.0 host interface (Type A connector): Capable of sourcing up to 1A/5W to an attached device

2.6.50 USB 2.0 host interface (Type A connector): Capable of sourcing up to 1A/5W to an attached device

2.6.51 Support of 802.11mc Fine Timing Measurement (FTM) for precision distance ranging.

2.6.52 Bluetooth Low Energy (BLE5.0) and Zigbee (802.15.4) radio:

2.6.52.1 BLE—Up to 5 dBm transmit power (class 1) and -100 dBm receive sensitivity (125kbps)

2.6.52.2 Zigbee—Up to 5 dBm transmit power and -97 dBm receive sensitivity (250kbps).

2.6.53 Support Integrated omnidirectional antenna with roughly 30 to 40 degrees down tilt and peak gain of 3.6dBi.

2.6.54 Visual indictors (multi-color LEDs)—For System and Radio status

2.6.55 Reset button—Factory reset, LED mode control (normal/off)

2.6.56 Serial console interface (proprietary, micro-B USB physical jack)

2.6.57 Kensington security slot

2.6.58 Mean Time between Failure (MTBF)—855,000 hours (98 years) at +25 C operating temperature.

2.6.59 Regulatory Compliance

2.6.59.1 FCC/ISED
2.6.59.2 CE Marked
2.6.59.3 RED Directive 2014/53/EU
2.6.59.4 EMC Directive 2014/30/EU
2.6.59.5 Low Voltage Directive 2014/35/EU
2.6.59.6 UL/IEC/EN 60950
2.6.59.7 IEC/EN 62368-1
2.6.59.8 EN 60601-1-1, EN60601-1-2

2.6.60 Certifications requirement;

2.6.60.1 UL2043 plenum rating • Wi-Fi Alliance (WFA):
2.6.60.2 Wi-Fi CERTIFIED a, b, g, n, ac
2.6.60.3 Wi-Fi CERTIFIED 6E (ax, 6GHz)
2.6.60.4 WPA, WPA2 and WPA3 – Enterprise with CNSA option,
2.6.60.5 Personal (SAE), Enhanced Open (OWE) - WMM, WMM-PS, W-Fi Agile Multiband - Passpoint (release 2)
2.6.60.6 Bluetooth SIG
2.6.60.7 Ethernet Alliance (POE, PD device)

2.7 Outdoor Wireless Access Point (AP)

2.7.1 Support Weatherproof and temperature-hardened, Outdoor Access Points deliver the high Wi-Fi 6 performance in outdoor and environmentally challenging locations high performance for outdoor environments dual radios 2.4GHz and 5Ghz with a maximum concurrent data rate of 1.49Gbps (HE80/HE20). Able to deliver maximum capacity and range, 2x2:2SS MU-MIMO capability. With up to two spatial streams and 80 MHz channel capacity.

2.7.2 Support of Wi-Fi 6 dual radio; 5 GHz 2x2 MIMO; and 2.4 GHz 2x2 MIMO.

2.7.3 Supports all mandatory and several optional 802.11ax features.

2.7.4 Support of Integrated BLE (Bluetooth Low Energy) to enable location services.

2.7.5 Support IP66- and IP67- rated protection from the elements.

2.7.6 Features include uplink and downlink orthogonal frequency-division multiple access (OFDMA), downlink multi-user MIMO (MU-MIMO), and cellular co-location. With up to two spatial streams and 80 MHz channel capacity.

2.7.7 Support of WPA2-MPSK

2.7.7.1 WPA2-MPSK enables simple passkey management for WPA2 devices. If the Wi-Fi password on one device or device type changes, no additional changes are needed for other devices.

2.7.8 Support of VPN Tunnels abilities

2.7.8.1 The AP enables features like Remote AP. In which AP embedded VPN uplink deployments can be used to establish a secure SSL/IPSec VPN tunnel to a main site from remote location. Without external VPN devices at remote site

2.7.9 Support dynamic frequency selection (DFS) optimizes the use of available RF spectrum.

2.7.10 Support Target Wake Time capability. To optimize support for IoTs that communicate infrequently, Target Wake Time (TWT) establishes a schedule for when clients need to communicate with an AP. This helps improve client power savings and reduces airtime contention with other clients

2.7.11 Access Points support includes an integrated Bluetooth 5 and 802.15.4 radio (for Zigbee support) to simplify deploying and managing IoT-based location services, asset tracking services, security solutions, and IoT sensors. This allows organizations to leverage Access Points as an IoT platform, which eliminates the need for an overlay infrastructure and additional IT resources.

2.7.12 Support of one these ethernet interfaces with at least one of them support:

2.7.12.1 Auto-sensing link speed (100/1000 BASE-T) and MDI/MDX

2.7.12.2 PoE-PD: 48Vdc (nominal) 802.3af/at/bt (Class 3 or higher)

2.7.12.3 802.3az Energy Efficient Ethernet (EEE)

2.7.13 Support of these additional interfaces and specification:

2.7.13.1 Bluetooth 5 and 802.15.4 radio:

2.7.13.2 2.4 GHz

2.7.13.3 Bluetooth 5: up to 8 dBm transmit power and -95 dBm receive sensitivity

2.7.13.4 Zigbee: up to 8 dBm transmit power and -97 dBm receive sensitivity

2.7.13.5 Up to 4 dBm transmit power (class 2) and -91 dBm receive sensitivity

2.7.13.6 USB-C console interface.

2.7.14 Support RF Antenna options of product configuration fo internal types of these specification;

2.7.14.1 For Built-in omni-directional antennas

2.7.14.1.1 5 GHz Antennas 5.4 dBi

2.7.14.1.2 GHz Antennas 3.2 dBi

2.7.14.2 For Built-in directional antennas

2.7.14.2.1 5 GHz Antennas 6.8 dBi

2.7.14.2.2 2.4 GHz Antennas 7.1 dBi

2.7.14.2.3 Directional angle support at 90°H x 90°V

2.7.15 For WI-FI Radio, to support these capabilities and specification;

2.7.15.1 Software-configurable dual radio supports 5 GHz (Radio 0) and 2.4 GHz (Radio 1).

2.7.15.2 5 GHz :

2.7.15.2.1 Two spatial stream Single User (SU) MIMO for up to 1.2 Gbps wireless data rate with individual 2SS HE80 802.11ax client devices, or with two 1SS HE80 802.11ax MU-MIMO capable client devices simultaneously

2.7.15.3 2.4 GHz:

2.7.15.3.1 Two spatial stream Single User (SU) MIMO for up to 57 Mbps (287 Mbps) wireless data rate with individual 2SS HE40 (HE20) 802.11ax client devices or with two 1SS HE40 (HE20) 802.11ax MU-MIMO capable client devices simultaneously

2.7.15.3.2 Support for up to 256 associated client devices per radio and up to 16 BSSIDs per radio.

2.7.16 For WIFI Radio, to support these specifications;

2.7.16.1 Dynamic frequency selection (DFS) optimizes the use of available RF spectrum.

2.7.16.2 Supported radio technologies:

2.7.16.2.1 802.11b: Direct-sequence spread-spectrum (DSSS)

2.7.16.2.2 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)

2.7.16.2.3 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to 16 resource units (RU)

2.7.16.3 Supported modulation types:

2.7.16.3.1 802.11b: BPSK, QPSK, CCK

2.7.16.3.2 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM (proprietary extension)

2.7.16.3.3 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM,1024 QAM (proprietary extension)

2.7.16.3.4 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM , 1024 QAM

2.7.16.3.5 802.11n high-throughput (HT) support: HT 20/40

2.7.16.3.6 802.11ac very high throughput (VHT) support: VHT 20/40/8

2.7.16.3.7 802.11ax high efficiency (HE) support: HE20/40/80

2.7.16.4 Supported data rates (Mbps):

2.7.16.4.1 802.11b: 1, 2, 5.5, 11

2.7.16.4.2 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 - 802.11n (2.4GHz): 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)

2.7.16.4.3 802.11n (5GHz): 6.5 to 600 (MCS0 to MCS31, HT20 to HT40)

2.7.16.4.4 802.11ac: (5 GHz): 6.5 to 3,467 (MCS0 to MCS9, NSS = 1 to 2 for VHT20 to VHT80)

2.7.16.4.5 802.11ax (2.4GHz): 3.6 to 574 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)

2.7.16.4.6 802.11ax (5GHz): 3.6 to 4803 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE80)

2.7.16.4.7 802.11n/ac packet aggregation: A-MPDU, A-MSDU

2.7.16.5 Transmit power: Configurable in increments of 0.5 dBm.

2.7.16.6 Maximum (conducted) transmit power (limited by local regulatory requirements):

2.7.16.6.1 2.4 GHz band: +23 dBm per chain, +26dBm aggregate (2x2)

2.7.16.6.2 5 GHz band: +23 dBm per chain, +26dBm aggregate (2x2)

Note that conducted transmit power levels exclude antenna gain.

2.7.17 Additional WIFI radio specification to support include:

2.7.17.1 Advanced Cellular Coexistence (ACC) minimizes interference from cellular networks.

2.7.17.2 Maximum ratio combining (MRC) for improved receiver performance.

2.7.17.3 Cyclic delay/shift diversity (CDD/CSD) to enable the use of multiple transmit

2.7.17.4 Short guard interval for 20-MHz, 40-MHz and 80-MHz channels.

2.7.17.5 Space-time block coding (STBC) for increased range and improved reception.

2.7.17.6 Low-density parity check (LDPC) for high-efficiency error correction and increased throughput.

2.7.17.7 Transmit beam-forming (TxBF) for increased signal reliability and range

2.7.18 Operating temperature: -40 degree Celsius to +55 degrees Celsius (-40 degrees F to +131 degrees F)

2.7.19 Operating humidity: 5% to 95% non-condensing. Rated for operation in all weather conditions

2.7.20 Storage and transportation temperature: -40 degrees Celsius to +70 degrees Celsius (-40 degrees F to +158 degrees F)

2.7.21 Chassis rating IP66 and IP67

2.7.22 Wind survivability: up to 165 Mph

2.7.23 Support shock and vibration: ETSI 300-19-2-4 spec

2.7.24 Support cyclic delay diversity (CDD) for improved downlink RF performance.

2.7.25 Support airtime fairness

2.7.26 Support DFS channel support to use all available RF spectrum

2.7.27 Support Advanced Cellular Filtering for co-existence with DAS

2.7.28 Support spectrum analysis

2.7.29 Support channel width configure flexibility (20/40/80Mhz)

2.7.30 Support 802.3az Energy Efficient Ethernet (EEE)

2.7.31 Console port for the ease of installation and management

2.7.32 Wi-Fi alliance certified

2.7.33 Support wall/pole mount

2.7.34 Ability to use the same AP in a controller based or controller-less deployment

2.7.35 To provide SLA-grade performance by allocating radio resources, such as time, frequency, and spatial streams, to specific traffic types. To support abilities of identify user roles and which APs then able to support dynamically allocate the bandwidth needed by roles which benefit both WiFi 6 and Non-Wi-Fi 6 clients in Wi-Fi performance.

3 FIREWALL

3.1 Tier-1 Firewall Requirements

3.1.1 The proposed NGFW shall be a hardware appliance

3.1.2 The proposed firewall must be able to work with the existing Fortinet FortiAnalyzer or any other analyser tool that the Tenderer shall so propose.

3.1.3 The NGFW principal vendor must be recognized as a Leader in the latest Gartner Magic Quadrant for Enterprise Firewalls.

3.1.4 The tenderer is to propose a holistic security solution that can effectively address security concerns such as, but not limited to:

- 3.1.4.1 Advanced persistent threats
- 3.1.4.2 Malware
- 3.1.4.3 Intrusion Protection System
- 3.1.4.4 Sandboxing
- 3.1.4.5 Application and role-based control
- 3.1.4.6 Web Filtering

3.1.5 The proposed solution must provide Next Generation proposed solution (NGFW) on an appliance platform and based on a hardened operating system.

3.1.6 The proposed solution must support Active-Active or Active-Standby high-availability

3.1.7 The proposed firewall must support alternate AC power suppliers to prevent loss of operation in the event of loss of the primary power supply.

3.1.8 The proposed solution must have the capability of supporting minimally 2.5Gbps of threat protection throughput.

3.1.9 The proposed platform must support at least 3 million concurrent connections and 280,000 new connections per second.

3.1.10 The proposed solution must have a minimum of 16 x 10/100/1000 Mbps Copper and 4 x SFP/SFP+ slots.

3.1.11 Provide protection from zero-day attacks and unknown threats.

3.1.12 Provide multiple security zones and interfaces to partition the data centre networks into more manageable highly controlled network segments.

3.1.13 Ability to create granular security policy definitions per Microsoft Active Directory user and security groups to identify, block or limit usage of applications and widgets like instant messaging, social networking, video streaming, VoIP, games, etc.

3.1.14 Provide granular application function control to identify, allow, block or limit usage of applications and features within them.

3.1.15 The NGFW must have the ability to restrict or controls user access to web resources and can be applied to firewall policies using either policy-based or profile-based NGFW mode.

3.2 Tier-2 Firewall Requirements

3.2.1 The proposed solution must not be from the same vendor as the 1st tier firewall.

3.2.2 The solution must have a minimum of 8 x 10/100/1000 Mbps Copper interfaces and 2 x SFP/SFP+ slots.

3.2.3 The proposed firewall must support the following:
3.2.3.1 At least 1.5Gbps of threat protection throughput

3.2.3.2 At least 20 Gbps IPsec VPN throughput

3.2.3.3 Up to 148,000 new sessions per second

3.2.3.4 Up to 6 million concurrent connections

3.2.4 High Availability (HA) minimally supports clustering two devices in active-active or active passive

3.2.5 Purpose-built streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators

3.2.6 Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSLVPN

3.2.7 Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group

3.2.8 Provides a full historical audit trail and status monitoring of group policy changes

3.2.9 Stateful deep packet inspection firewall, packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing.

3.2.10 Support Zone-based firewall. Full VLAN support. Zone and VLAN isolation and zone-based policy

3.2.11 Micro-segmentation and auto-isolation via Synchronization

3.2.12 Advanced Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF) with full 802.1Q VLAN support.

3.2.13 Ability to integrate with Zero Trust Network Access (ZTNA) to offer a secure and simple way for users to securely connect to important applications and data.

3.2.14 Synchronized App Control to automatically identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints and the firewall.

3.2.15 Sandboxing feature to inspect executables and documents containing executable content (including .exe, .com,and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)

4 WAN LOAD BALANCER

The WAN load balancer requires the following features:

4.1 Key Features

4.1.1 T Stateful Firewall Throughput 1Gbps
4.1.2 Minimum 3 WAN ports which can used concurrently
4.1.3 Performance Support for up to 500 users
4.1.4 bonding, WAN smoothing, WAN Hot failover
4.1.5 Cloud Management system for remote access with full web GUI interface
4.1.6 Support for Drop-in Mode
4.1.7 Support for High Availability
4.1.8 Support for LAN Bypass
4.1.9 Ability to set inbound load balancing based on WAN Connection
4.1.10 bonding, WAN smoothing, WAN Hot failover
4.1.11 Cloud Management system for remote access with full web GUI interface
4.1.12 Support for Drop-in Mode
4.1.13 Support for High Availability
4.1.14 Support for LAN Bypass
4.1.15 Ability to set inbound load balancing based on WAN Connection
4.1.16 Supports up to 50 PPTP/L2TP/OpenVPN users
4.1.17 Supports up to 5 GRE tunnels
4.1.18 RJ-45 Console Port
4.1.19 Dual USB-A Port

4.2 Quality of Service (QoS)

4.2.1 Powerful QoS feature—Supports bandwidth monitoring, QoS for VOIP and E-commerce, User
Group Bandwidth control and Web Blocking

4.3 Resiliency and High Availability

4.3.1 Virtual Router Redundancy Protocol (VRRP)—Allows groups of two routers to dynamically back
each other up to create highly available routed environments.
4.3.2 IEEE 802.3ad LACP – NIC bonding

4.4 Performance

4.4.1 Support up to 30 VPN peers

4.5 Connectivity

4.5.1 Jumbo frames—Supports high-performance backups and provides a maximum frame size of 9 K bytes.
4.5.2 Connection methods – Static IP, DHCP, PPPOE, L2TP, GRE
4.5.3 Connectivity health checks via PING, DNS lookup, HTTP

4.6 Management

4.6.1 Management interface control—Enables or disables these interfaces depending on security preferences or console port
4.6.2 SNMP v1, v2c and v3 — Provides SNMP read and trap support of the industry standard Management Information Base (MIB) and private extensions.
4.6.3 Local Authentication Method via Local, Radius or TACACS+

4.6.4 Enable CLI SSH and Console

4.6.5 Debug and sampler utility—Supports ping, traceroute, wake-on-LAN and WAN analysis

4.6.6 Support Secure Sockets Layer (SSL) which encrypts traffic, allowing secure access to the browser-based management GUI in the switch

4.7 Layer 3 Services and Routing

4.7.1 Dynamic Host Configuration Protocol (DHCP)—DHCP services are offered within a client network to simplify network management. DHCP relay enables DHCP operation across subnets.

4.7.2 Domain Name System (DNS) – Provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

4.7.3 Policy Based Routing (PBR)—Enables using Protocol to select traffic that can be forwarded based on a policy set by network administrator via Source IP.

4.7.4 Static IPv4 routing – Provides simple manually configured IPv4 routing.

4.8 Security

4.8.1 NDAA Compliance—Is a NDAA-compliant product; No ties to the companies mentioned in NDAA

4.8.2 Access control list (ACL) Features—Supports powerful ACLs for IP. Supports creation of object groups representing sets of devices such as IP addresses based upon source and destination.

4.8.3 Ability to set Inbound, outbound and internal Network Firewall rules, example : based upon Protocol selection: TCP, UDP, ICMP, IP

4.8.4 Terminal Access Controller Access-Control System (TACACS+) – Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security.

4.8.5 Management access security— Web admin access via LAN only or web admin port (flexible)

4.9 General Performance Requirements

4.9.1 The load balancer must be able to support 50 up to 500 users.

4.9.2 The load balancer must be capable of providing at least 1Gbps throughput.

4.10 General WAN Requirements

4.10.1 Must have at least 2 WAN ports, convertible into LAN ports

4.10.2 Must support PPPoE, Static IP, DHCP WAN configuration.

4.10.3 Must be able to perform WAN Link Health Check.

4.10.4 Must be able to allot bandwidth allowance monitor.

4.10.5 Must be able to support IPv4 and IPv6 addressing.

4.10.6 Must have at least 1 USB 4G LTS/3G modem support.

4.11 General LAN Requirements

4.11.1 Must have at least 3 Gigabit Ethernet Ports for LAN connection

4.11.2 Must be able to support DHCP Server and DNS Proxy for LAN Clients

4.11.3 Must support DHCP Reservation functionality

4.11.4 Must be able to support VLAN capability

4.12 General DNS Requirements

4.12.1 The load balancer shall have built-in Authoritative DNS and support for:

4.12.1.1 A

4.12.1.2 CNAME

4.12.1.3 NS

4.12.1.4 MX

4.12.1.5 PTR

4.12.1.6 SOA
4.12.1.7 SRV
4.12.1.8 TXT Records

4.13 General Load-Balancing Requirements

4.13.1 The device must provide intelligent failover.
4.13.2 The device must be able to provide inbound load balancing.
4.13.3 The Device must support multiple load balancing algorithms, such as:
4.13.4 Session Persistence
4.13.5 Per-service load distribution

4.14 General High Availability Requirements

4.14.1 The device must have High Availability capability for redundancy purposes.

4.15 General VPN Requirements

4.15.1 The device should be able to bond affordable DSL, cable, cellular, and other WAN links into a single secure and fast VPN tunnel.
4.15.2 The device should be able to establish a VPN tunnel with at least 2 Peers with a minimum of 80Mbps throughput.
4.15.3 The device must be able to support 256-bit AES Encryption and pre-shared key authentication.
4.15.4 The device is capable of bandwidth aggregation and intelligent failover.
4.15.5 The device can act as PPTP VPN Server and must support Radius and LDAP authentication.
4.15.6 The device must be able to support IPsec VPN.

4.16 General Networking Requirements

4.16.1 The device must support the following NAT and IP Forwarding capabilities:
4.16.1.1 Port forwarding
4.16.1.2 Many to One, One to One NAT and NAT Pool
4.16.1.3 UPnP, NAT-PMP

4.16.2 The device must be able to support Static Routes, OSPFv2 and RIPv2.

4.17 General Captive Portal Requirements

4.17.1 The device must support wired and wireless LAN clients.
4.17.2 The device should be able to apply time and usage quotas.
4.17.3 The device must support built-in customizable splash page.

4.18 General Security Requirements

4.18.1 The device must support built-in DoS prevention.
4.18.2 The device should also be able to act as a stateful firewall.
4.18.3 The device must support web blocking and web filtering/blacklisting.

5 COMPUTE AND STORAGE SYSTEM

5.1 Compute and Storage Requirements (for Production Environment)

5.1.1 The proposed solution should be hyperconverged and able to support all major x86 vendor hardware.

5.1.2 The proposed solution should be based on a scale-out architecture with all nodes actively load balancing writes and reads.

5.1.3 The proposed solution should support multiple server virtualization technologies, such as VMWare ESX, Microsoft Hyper-V and other equivalent hypervisor platforms.

5.1.4 The proposed solution should consolidate the compute (server) tier and the storage tier into a single, integrated appliance that supports virtualization.

5.1.5 The proposed solution should support the intermix of different hardware configurations and models within the same cluster. Server models need not be of a similar resource configuration from a storage, memory and CPU perspective.

5.1.6 The proposed solution should support predictive failure analytics.

5.1.7 The proposed solution should support firmware updates without downtime.

5.1.8 The proposed solution should consist of local direct attached storage, which will eliminate the need for network-based storage architecture, such as a storage area network (SAN) or network-attached storage (NAS).

5.1.9 The proposed solution should consist of flash-based storage for performance, and local spinning hard disk storage for cost efficiency. It should also support intelligent distributed data tiering, which will intelligently place data in the optimal storage tier (flash or HDD) to yield the fastest possible performance.

5.1.10 The proposed solution should also be able to support all-flash variations of storage if required and also be able to support mixing both all-flash and flash+HDD variations in the same cluster.

5.1.11 The proposed solution should support fault resiliency, to ensure all VM and I/O requests are automatically failed over to another server until the faulty server becomes available again.

5.1.12 The proposed solution should leverage a completely software-based solution so that all intelligence of managing the hardware is based on the software. This will help to eliminate dependency on hardware-based solution leveraging specific hardware components so potentially different hardware models can be mixed in the same cluster/pool.

5.1.13 The proposed solution should support independent scaling of compute and storage resources when needed. If necessary, the proposed solution shall support scaling storage or compute only workloads via storage-only nodes or compute-only nodes.

5.1.14 The proposed solution should enable ease of use so that upgrades of the software and hypervisor are completely handled through the same console and leverage only a few clicks to manage. Upgrades should also be completely seamless and incur zero downtime by leveraging the concept of “auto rolling upgrade mechanism” whereby the upgrade software will upgrade one physical server at any time by automatically moving all workloads to the remaining servers and perform the upgrade one at a time automatically.

5.1.15 In the event of failure of a physical node, the proposed solution should support data rebuild and re-localization process must start within seconds.

5.1.16 The proposed solution should support common storage optimization technologies for both hybrid disk systems (SSD + HDD) and all-flash disk systems (SSD only) like Compression, Deduplication and Erasure Coding.

5.1.17 The proposed solution should support storage replication between different sites/clusters/pools that can leverage either asynchronous or synchronous models so various RPO SLAs can be achieved.

5.1.18 The proposed solution must not be dependent on hardware RAID for data protection or

data stripping.

5.1.19 The proposed solution should support a HTML5 management console that is not dependent on any software installed console nor flash-based console.

5.1.20 The proposed solution should support automated discovery of new servers/nodes via GUI as well as automatic mounting of storage volume to the hypervisor for ease of expansion in future.

5.1.21 The proposed solution should provide native integrated VM snapshots and enable configuration of automated VM snapshots backup via a user defined schedule.

5.1.22 The proposed solution should have the ability to provide VM data locality for localized performance at storage layer, such that IO requests from VMs should be processed on the same host where the VM resides as much as possible.

5.1.23 The proposed solution must allow for on-demand pinning/unpinning of VMs in Flash/SSD storage tier.

5.1.24 The proposed solution should be able to provide full details on the security baseline addressing various vulnerability assessments and lock downs done on components within the technology.

5.1.25 The proposed solution should provide for capacity planning for predicting runway for resources, with the ability to model future workloads/resources.

5.1.26 The proposed solution must offer native (no additional software required) VM-Anomaly detection, such as a sudden drop in CPU use for a VM (below the expected/observed typical value).

5.1.27 The proposed solution must be able to automate daily infrastructure tasks (eg. Scale-up CPU/Memory/Storage) via a GUI-like approach so alerts can be configured to trigger the automation of these infrastructure tasks.

5.1.28 The proposed solution should support performance optimizer insights and recommendations.

5.1.29 The proposed hyperconverged solutions should have minimum available resources as follow:

5.1.29.1 96 vCPU

5.1.29.2 384 GB RAM

5.1.29.3 22.7 TB usable capacity

5.1.30 The proposed storage for backup should satisfy the following requirements:

5.1.30.1 at least 20 TB of usable capacity

5.1.30.2 comes with 1 Gbps NIC and 10 Gbps NIC

5.2 Compute and Storage Requirements (for DR Environment)

5.2.1 The proposed solution should be a stand-alone server and able to support all major x86 vendor hardware.

5.2.2 The proposed solution should support multiple server virtualization technologies,

such as VMWare ESX, Microsoft Hyper-V and other equivalent hypervisor platforms.

5.2.3 The proposed solution should come with built-in Intelligent Platform Management Interface (IPMI) for server control and monitoring

5.2.4 The proposed solution should have minimum available resources as follow:

5.2.4.1 64 vCPU

5.2.4.2 96 GB RAM

5.2.4.3 8 TB usable capacity

5.2.4.4 comes with 1 Gbps and 10 Gbps NIC

5.3 Management Requirements

5.3.1 Embedded management capability comes with no license fee or host agents.

5.3.2 Supports industry-standard protocols, including Intelligent Platform Monitoring Interface Version and Simple Network Management Protocol, and an open XML API and a command-line interface (CLI).

5.3.3 Support web user interface for server management: remote keyboard, video and mouse (KVM); virtual media and administration.

5.3.4 Provide a unified view of the health of servers and profiles across multiple virtual and physical appliances.

5.3.5 Support administrators to perform following server management tasks with role-based access that can be defined on a per-user basis:

5.3.5.1 Power on, power off, power cycle, reset, and shut down the server
5.3.5.2 Manage server BIOS settings
5.3.5.3 Configure the server boot order
5.3.5.4 View server properties and sensors
5.3.5.5 Create and manage local user accounts and connect to external authentication and authorization systems, including Microsoft Active Directory
5.3.5.6 Configure network-related settings, including network interface card (NIC) properties, IPv4, VLANs, and network security
5.3.5.7 Configure communication services, including HTTP, SSH, and IPMI over LAN
5.3.5.8 Specify events to trigger platform event traps
5.3.5.9 Manage certificates
5.3.5.10 Update system firmware
5.3.5.11 Monitor faults, alarms, and server status remotely
5.3.5.12 Monitor server health and performance with advanced power and thermal control
5.3.5.13 Ability to automatically report hardware failures with hardware vendor support to speed problem resolution and accelerate parts or service technician dispatch.

5.3.6 Flexibility to be managed as standalone server or as part of management system that can manage various form factors including racks and blades.

5.4 Security Requirements

5.4.1 The proposed solution should support capability to restrict interactive shell access.

5.4.2 The proposed solution should support hardening of platform.

5.4.3 The proposed solution should support data-at-rest encryption with self-encrypting drives (SEDs), software-only encryption, and software encryption with SEDs.

5.4.4 The proposed solution should support native built-in Key Management Server or integration with 3rd party Key Management providers.

5.4.5 The proposed solution must offer native (without additional software) micro-segmentation for VM-level security (at the vNIC).

5.4.6 The proposed solution should support audit logs of access/modification.

5.5 General Backup Requirements

5.5.1 Ability to back up in virtualized environment.

5.5.2 Ability to have different backup target (Local storage (direct attached), NFS/CIFS, NAS, SAN, Tape and Cloud).

5.5.3 Ability to have Incremental backup.

5.5.4 Supports built-in replication.

5.5.5 Ability to have Storage snapshot integration.

5.5.6 Supports a minimum of 256 Bit encryption.

5.5.7 Ability to support instant VM recovery.

5.5.8 Ability to support vMotion on IVMR.

5.5.9 Ability to do single file restore.

5.5.10 Ability to do backup to tape.

5.6 File Server Requirements

5.6.1 The proposed solution must be able to integrate with the existing Active Directory.

5.6.2 The proposed solution should support minimum SMB v2.

5.6.3 The proposed solution should support setting of soft or hard limit quota on either user or shares.

5.6.4 The proposed solution should support blocking of creation and modification of specific file types on the file server.

5.6.5 The proposed solution should support cloning of file server from a specific snapshot.

5.6.6 The proposed solution should support recovery of a file server from a specific point in time snapshot.

5.6.7 The proposed solution should support Access-based enumeration (ABE) feature. ABE restricts user-access by only letting user view the files and folders with read access when browsing content on a file server.

5.6.8 The proposed solution should provide native block services through iSCSI protocol as part of the platform to support technologies like Microsoft Clustering together with the base hyperconverged platform.

5.6.9 The proposed solution should support built-in file server data replication to its existing

secondary file server at the DR site and vice-versa.

5.6.10 The proposed solution should support seamless switch over to the secondary file server at the DR site in the event of the primary file server becoming inaccessible.

5.6.11 The proposed solution should support seamless switch back to the primary file server at the Production site once it becomes accessible again.

6 NETWORK MANAGEMENT

6.1 Overall Solution

6.1.1 The solution should offer key functionality such as orchestration, control, optimization, and security wherever located.

6.1.2 The solution shall support Microservices framework - designed to deliver fault tolerance and flexibility that enable existing and new services to easily be updated or added without effecting core functionality.

6.1.3 The solution should support Per User Analytics.

6.1.4 The solution must support Wi-Fi 6/6E certified APs and will dynamically allocate the bandwidth needed through PEF and Layer 7 DPI to identify user roles and applications.

6.1.5 The solution must support not just only for Wi-Fi management but need to be able to manage switches, SD-WAN.

6.1.6 The solution should provide common Data Lake – a single unified data repository for all cross-domain events and information enables seamless event correlation and rapid information gathering and issue resolution.

6.1.7 The solution should support AIOps that identifies issues which are virtually impossible to find by humans and provides root cause and prescriptive recommendations for troubleshooting and correction.

6.1.8 The solution should be stable, able to be 24/7 Anywhere Access – perform management, monitoring and control from any device, any location and at any time.

6.2 Deployment

6.2.1 The solution supports zero-touch provisioning/plug-n-play for new deployments and services.

6.2.2 The solution shall allow preconfiguring APs in the cloud by using intelligent grouping parameters so that in many cases all that needs to be done is name a group for the new site and import the standard configuration stored.

6.2.3 The Centralized management solution installed must provide a single, unified platform for network service provisioning, monitoring and assurance, change and compliance management.

6.2.4 The solution must be able to provision licenses, upgrade or downgrade licenses without any interruptions.

6.2.5 The solution must provide guided workflows for deployment and management of wireless infrastructure.

6.2.6 The solution must support dashboard for end-to-end real-time flow visualization for the application paths for identifying issues and taking corrective actions.

6.3 Management, Monitoring and Troubleshooting

6.3.1 The management platform must support Group for configuration and Sites for statistics & baseline. The config template should be able to apply to multiple sites for simplify the configuration and monitoring efforts.

6.3.2 The management platform must support end-to-end visibility from the user to network devices.

6.3.3 The management platform must support a firmware schedule upgrade and do not need to upload the firmware manually to the management platform.

6.3.4 The management platform must support up to 90 days of historical data.

6.3.5 The management platform must support the monitoring by Sites, AP, Clients, Applications.

6.3.6 The management platform must support live view in the Management Platform for any particular AP for real time statistics including Noise, Frame, Channel Quality information.

6.3.7 The management platform must support live view in the Management Platform for any particular client for real time statistics including Throughput and Signal to Noise Ratio (SNR).

6.3.8 The management platform must support at least 500+ application visibility for better usage monitoring and troubleshooting.

6.3.9 The management platform must be able to connect particular AP console for in-depth troubleshooting.

6.3.10 The management platform must support Wireless IDS functionality for detecting Interfering and Rogue AP.

6.3.11 The management platform must support REST-API, Streaming API to allow a 3rd party system integration.

6.4 AI Optimization

6.4.1 The solution must support the Artificial Intelligence to help an IT-Operation to optimize and troubleshoot an issue automatically.

6.4.2 The solution shall have a capability to get the root cause and resolve known issues quickly where the AIOps identifies issues, such as connectivity and authentication, using AI to determine root cause and provide prescriptive recommendations to improve troubleshooting efficiency.

6.4.3 The solution shall have a capability to Continuously optimize performance with little effort where AIOps provides peer-based optimization recommendations, regardless of the size or type of your business by collecting data from tens of thousands of existing customer deployments.

6.4.4 The solution shall support collecting the relevant logs and open the TAC automatically.

6.4.5 The system shall have the AI Search capability to allow administrators to use natural language to search for and quickly find relevant information.

6.4.6 The solution shall be able to provide user and IoT device application assurance and rapid troubleshooting through easy-to-deploy sensors by simulating end-user activity in real time.

6.4.7 The AI insight must include both Peer and Local Baseline compared.

6.4.8 The AI insight should include the below :

- 6.4.8.1 High CPU & memory usage of AP
- 6.4.8.2 Excessive channel or transmit power changes of AP
- 6.4.8.3 Tx power config recommendation
- 6.4.8.4 Missing telemetry & Excessive reboots of AP
- 6.4.8.5 Low SNR links of clients
- 6.4.8.6 Excessive 2.4 Ghz dwell by a dual band client
- 6.4.8.7 High airtime utilization of AP
- 6.4.8.8 High WPA handshake failures
- 6.4.8.9 High mac auth failures
- 6.4.8.10 High captive portal auth failures

6.5 Security

6.5.1 Multi-factor authentications for Management GUI.

6.5.2 The solution must be able to configure the stateful firewall function on the APs to allow for network isolation.

6.5.3 The solution must be able to configure the WIPS/IDS function on the wireless access points.

6.5.4 The solution must support Cloud identity provider for users onboarding.

6.5.5 The solution must support devices profiling by using static finger printing, ie. DHCP option, MAC-OIU etc. and dynamic flow attribute.

6.5.6 The solution must support multi-PSK for IoT devices.

6.5.7 The solution must support guest captive portal with self-registration and the solution must provide a SMS gateway for guest self-registration over phone.

7 IDENTITY AND POLICY MANAGEMENT

7.1 Servers / Appliance

7.1.1 Single platform approach that combines AAA, NAC, BYOD, MAM and Guest Access by incorporating identity, health, physical/device information, and conditional elements into one set of policies.

7.1.2 Must have ability to scale up to 10,000 devices per appliance or virtual appliance (Both VMware and Hyper V).

7.1.3 Solution must be Agnostic to existing wired, wireless and VPN network in place today.

7.1.4 Appliance must be pre-built and ready to be imported (ovf) into VMware virtualization environment (building from ISO not acceptable).

7.1.5 Shell protected by CLI providing configuration for base appliance settings.

7.1.6 Appliance must provide disk or file encryption.

7.1.7 Ability to mix and match virtual and hardware appliances in one deployment.

7.1.8 Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model.

7.1.9 Flexibility to operate all features/functions on any appliance in the cluster.

7.1.10 Hardware platform must be running on a hardened operating system.

7.2 Functionality

7.2.1 Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.

7.2.2 Support any vendor type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).

7.2.3 Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures (endpoint health).

7.2.4 Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.

7.2.5 Solution must have fully integrated support for Microsoft NAP allowing health and posture checks on Windows endpoints without the need to install an agent.

7.2.6 All external facing interfaces are programmable, which means APIs are available to extend the system to support different authentication protocols, identity stores, health evaluation engines and port and vulnerability scanning engines.

7.2.7 The solution Must be an easy-to-deploy hardware or virtual appliance platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:

- 7.2.7.1 Full AAA server – RADIUS and TACACS+
- 7.2.7.2 Automatic device profiling and the ability to use profiled information for access authorization
- 7.2.7.3 Built-in guest management and device/user onboarding
- 7.2.7.4 Web based management interface with Dashboard
- 7.2.7.5 Reporting and analysis with custom data filters
- 7.2.7.6 Data repository for user, device, transaction information
- 7.2.7.7 Rich policies using identity, device, health, or conditional elements
- 7.2.7.8 Deployment and implementation tools.
- 7.2.7.9 Support SSO SAML for GUI and Guest portal integration.
- 7.2.7.10 Integration with leading MDM provider such as MobileIron, AirWatch, Maas360, ZenPrise, SOTI to extract endpoint information
- 7.2.7.11 Integration with Palo Alto Networks Firewall to provide context base information.

7.2.8 Must support flexible license model based on either perpetual or subscription based

licensing on required functionality (i.e. Onboard, Posture, Guest Access).

7.2.9 Correlation of user, device, and authentication information for easier troubleshooting, tracking etc.

7.2.10 AAA framework must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against an external SQL database.

7.2.11 Should support multiple methods for device identification and profiling such as:

7.2.11.1 Integrated, network based, device profiler utilizing collection via SNMP, DHCP, HTTP,
AD, ActiveSync, IF-MAP

7.2.11.2 Endpoint audit via NESSUS or NMAP scanning.

7.2.12 Policy creation tools:

7.2.12.1 Pre-configured templates

7.2.12.2 Wizard based interface

7.2.12.3 LDAP browser for quick look-up of AD attributes

7.2.12.4 Policy simulation engine for testing policy integrity

7.2.12.5 Policy model should support incorporation of several contextual elements
including identity, endpoint health, device, authentication method & types, and
conditions such as location, time, day, etc.

7.2.13 Support the following enforcement methods:

7.2.13.1 VLAN steering via RADIUS IETF attributes and VSAs

7.2.13.2 VLAN steering and port bouncing via SNMP

7.2.13.3 Access control lists – both statically defined filter-ID based enforcement, as well as
dynamically downloaded ACLs.

7.2.13.4 Roles or any other vendor-specific RADIUS attribute supported by the network
device.

7.2.13.5 Agent-based enforcement – bouncing a managed interface and sending custom
messages.

7.2.14 Must be able to join multiple Active Directory belonging to separate forest with no trust relation to facilitate any form of authentication or authorization request.

7.2.15 Must have the ability to create multiple CA Servers (either as a Root CA or Subordinate CA)
within the appliance. Device provision by such CA must allow to roam across multiple network cluster if required.

7.2.16 Must support complex PKI deployment where TLS authentication requires validating client
certificate from multiple CA trust chain. Must also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.

7.2.17 Must support importing of 3rd party vendor Radius Dictionary.

7.2.18 Must be able to join multiple Active Directory belonging to separate forest with no trust relation to facilitate any form of authentication or authorization request.

7.2.19 Support for Automatic Sign On (ASO), which captures the user's initial 802.1X, credentials and
uses these to automatically sign the user into their SAML supported applications.

7.2.20 Support for SAML capabilities, which will allow the appliance to act as an identity provider (IDP) for the principal user.

7.2.21 Profiling capabilities included in base licensing to offer full visibility of the devices present on the network.

7.2.22 Support Restful API capability to interact with leading MDM vendors within the base license.

7.2.23 Must support multiple AD domains and AD forest queries seamlessly.

7.2.24 Support intuitive policy configuration templates and visibility troubleshooting tools.

7.2.25 Supports multiple authentication/authorization sources (AD, LDAP, SQL dB) within one service.

7.2.26 Self-service device onboarding with built-in certificate authority (CA) for BYOD.

7.2.27 Support single sign-on (SSO) and Auto Sign-On support via SAML v2.0.

7.2.28 Supports NAC and EMM/MDM integration for mobile device assessments.

7.2.29 Comprehensive integration with third party systems such as SIEM, Internet security and EMM/MDM.

7.2.30 Support automatic cluster upgrade.

7.2.31 Support the following identity stores:
- 7.2.31.1 Microsoft Active Directory
- 7.2.31.1 RADIUS
- 7.2.31.3 Any LDAP compliant directory
- 7.2.31.4 Any ODBC-compliant SQL server
- 7.2.31.5 Token servers
- 7.2.31.6 Built-in SQL store, static hosts list
- 7.2.31.7 Kerberos

7.2.32 Support the following RFC standards: 2246, 2248, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3576, 3579, 3580, 3748, 4017, 4137, 4849, 4851, 5216, 528, 7030.

7.2.33 Support information assurance validations FIPS 140-2 – Certificate #2577.

7.2.34 Support the following profiling methods: DHCP, TCP, MAC OUI, ClearPass Onboard, SNMP, Cisco device sensor.

7.2.35 Support the following frameworks and protocols:
- 7.2.35.1 RADIUS, RADIUS CoA, TACACS+, web authentication, SAML v2.0
- 7.2.35.2 EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- 7.2.35.3 PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
- 7.2.35.4 TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
- 7.2.35.5 EAP-TLS
- 7.2.35.6 PAP, CHAP, MSCHAPv1 and 2, EAP-MD5

7.2.35.7 NAC, Microsoft NAP
7.2.35.8 Windows machine authentication
7.2.35.9 MAC auth
7.2.35.10 Audit (rules based on port and vulnerability scans)
7.2.35.11 Online Certificate Status Protocol (OCSP)
7.2.35.12 SNMP generic MIB, SNMP private MIB
7.2.35.13 Common Event Format (CEF), Log Event Extended Format (LEEF)
7.2.35.14 TLS 1.2

7.3 Reliability / Performance

7.3.1 Appliances have the ability to be clustered in any combination via local and remote network connections providing unlimited scale, redundancy, and access load balancing.

7.3.2 Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model.

7.3.3 Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.

7.3.4 Must support several deployment modes including centralized, distributed, or mixed.

7.3.5 Must support Virtual IP to allow seamless failover for Web-based services such as Guest portal without a need for external load balancer.

7.3.6 Ability to scale up to 1 million unique endpoint authentications.

7.4 Bring Your Own Devices (BYOD)

7.4.1 Self-service workflow built on an industry leading platform. Supports popular smart devices as well as traditional computing platforms.

7.4.2 Unique portal pages based on devices type – iOS, Android.

7.4.3 Ability to support revocation of devices.

7.4.4 Correlation of user, device, and authentication information for easier troubleshooting, tracking etc. – provides high level of visibility into what devices are on the network and associated with what users are.

7.4.5 Automated onboarding of devices to enable secure access via self-serve portal allowing for the configuration of 802.1x supplicants, device enrolment and provisioning.

7.4.6 Ability to integrate with Active Directory so users that are approved for BYOD may be authenticated via identity and/or device attributes.

7.4.7 OPTIONAL Cloud based, endpoint configuration tool for streamlining the configuration of 802.1X supplicants for laptops or handheld devices (smartphones, pads, etc.) and guiding the end-user onto the network for the first time.

7.4.8 Support for Windows, Mac, iOS (iPhones, iPads, etc.) and Android devices.

7.5 Guest Access

7.5.1 Solution must be capable of providing sponsored and self-provisioned Guest Access.

7.5.2 Ability to provide free or billable Guest Access with built in payment solution that can

integrate with payment solution providers.

7.5.3 Must be able to provide custom branding.

7.5.4 Ability to send automated SMS or email credentials to the Guest User.

7.5.5 Ability to set Account Details including Time Frame, Bandwidth Contract etc. Once account timeframe expires the User Account becomes inactive automatically.

7.5.6 Solution must be capable of providing Advertising Services (Play Video before Access, offer current Promotions, Advise of Health Alerts).

7.5.7 Guest solution should manage the individual guest credentials in a partitioned database and not pollute the user store with account credentials for guest users.

7.5.8 Ability to perform caching of MAC address post guest authentication to avoid the need for guest to re-authenticate during the period of their visit (3G like user experience after first authentication via captive portal).

7.5.9 Auto-login for self-registration workflow – no need for the guest to retrieve account credentials from email or SMS for initial login.

7.5.10 Anonymous login support with per device policy still applied.

7.5.11 Access token login support for single credential login to guest network – event management, scratch cards etc.

7.5.12 Bulk import of guest accounts with ability to trigger notification of credentials via email.

7.5.13 Bulk import of NAS devices for large scale deployments.

7.5.14 Sponsored approval workflow for guest self-registration where open SSID registration can be protected by requiring internal staff to approve the creation of guest account.

7.5.15 Prevent employees from accessing the guest network on the corporate laptop.

7.5.16 Apple Captive Network Assistant bypass for managing end to end guest workflow. For example post login welcome page display on iOS and Mac OS Lion and above devices.

7.5.17 Post login session statistics page displayed to users so they can monitor usage or quota assigned.

7.5.18 Support URL persistence so users originally requested webpage can be displayed post login.

7.5.19 Location based captive portal – display different landing pages based on where guest is connecting to the network.

7.5.20 Support guest access across multi-vendor access networks.

7.5.21 Fully customizable self-registration or guest creation pages with user interface controls such as drop down, check list, radio button.

7.5.22 Authenticated self-registration for partner / joint venture account provisioning.

7.5.23 Published API’s to allow 3rd party system to manage guest accounts.

7.5.24 NAC health checking should support agent and agentless methods and be available as a permanent or dissolvable health agent for Windows, Linux, and Macintosh endpoint platforms. In addition to authenticating the user, the solution must gather granular information about the

endpoint device, perform advanced health checks on Windows platforms (services, processes, peer-to-peer apps, registry keys, USB device usage, Windows Hot fixes, patch management agents), and perform standard health checks on Linux and Mac platforms (Anti-virus, Anti-spyware, Firewall).

7.5.25 Support persistent agent, dissolvable agent, Microsoft NAP agent.

7.5.26 Support Windows, Apple, Linux Operating System.

7.5.27 Gather granular information about the endpoint device.

7.5.28 Perform advanced health checks on Windows platforms (services, processes, peer-to-peer apps, registry keys, USB device usage, Windows Hot fixes, patch management agents), and perform standard health checks on Linux and Mac platforms (Anti-virus, Anti-spyware, Firewall).

8 NETWORK MONITORING SENSOR

8.1 General

8.1.1 The tenderer shall propose a network monitoring sensor solution which enables IT to proactively simulate real-world user and client experiences, so as to provide a consistent level of reliability and performance.

8.1.2 Continuously monitor network connectivity and the performance of wireless and Ethernet connections in critical, high-value locations.

8.1.3 Customizable test scripts and easy to deploy sensors provide application and network insights for any vendor-agnostic wireless and wired network dealing with the influx of mobile and IoT devices.

8.1.4 Simple to deploy, cloud-based data processing and an easy-to-use web-based administrative dashboard that can be accessed from anywhere.

8.1.5 Sensors can be placed within any area where users or IoT devices are located to reduce the time to identify and resolve application responsiveness and user experience issues.

8.1.6 Tests can be set up for LAN and WLAN connectivity, DHCP, DNS, authentication, captive portal response, cloud and internal applications.

8.1.7 Sensor to support these powering options:

8.1.7.1 802.3af Power over Ethernet (PoE)

8.1.7.2 Optional AC power adapter

8.1.8 Sensor to not exceed power consumption of 13W.

8.1.9 Sensor shall have these network interfaces:

8.1.9.1 802.11a/b/g/n/ac/ax 2.4GHz & 5GHz with two spatial streams

8.1.9.2 1 x Gigabit Ethernet 10/100/1,000

8.1.9.3 Bluetooth Low Energy (BLE5.1) radio

8.1.10 Sensor shall support the MTBF: minimum 867 khrs at +25° C operating temperature.

8.1.11 Sensor shall have these regulatory certifications;
- 8.1.11.1 CE Marked
- 8.1.11.2 RED Directive 2014/53/EU
- 8.1.11.3 EMC Directive 2014/30/EU
- 8.1.11.4 Low Voltage Directive 2014/35/EU UL/ IEC/EN 62368

8.2 Key Features

8.2.1 Simple to use network and app-performance dashboard and diagnostics visibility

8.2.2 Cloud-based analytics and insights engine, AI powered DEM (Digital Experience Monitoring)

8.2.3 Vendor-agnostic sensor for continuous Wi-Fi and Ethernet service assessment

8.2.4 Optionally support cellular connectivity for onboarding and troubleshooting

8.2.5 Extensive test suite for Wi-Fi, LAN, DHCP, DNS, authentication, captive portals, cloud applications, and internal applications

8.2.6 Customizable alerts and integration with email, SMS, and Slack

8.2.7 Scales to any number of sensors

8.2.8 Supports testing of multiple SSIDs

8.2.9 Optional support for LTE connection for onboarding with full managed SIM and service

8.2.10 Sensor shall support testing suite:
- 8.2.10.1 WiFi: Scan, Association, Packet capture, Measure KPIs (RSSI, Util, etc.)
- 8.2.10.2 Network: Authentication, Gateway, DNS, DHCP, Iperf3, Ping/Hping, HTTPGet / Curl, Telnet.
- 8.2.10.3 Applications: Box, Chromium (script), Captive Portal, Google: Gmail, Drive, Docs, Jira, Dropbox (API), YouTube download, VOIP MOS (Skype, BlueJeans), Salesforce, Slack, Create-Your-Own.

8.2.11 Support Web Application Testing: Sensor shall be able to test web applications from an end user perspective by easily customizing test cases to mimic end users. Thus, to enables user to test end to end workflow like hopping on to a website, logging in, clicking a button, and logging out of the web application.

8.2.12 Support for IPv6: Sensor must provide precise visibility and in-depth network performance in an IPv6 environment to show DHCPv6, DNS64/NAT64, and SLAAC configurations, and applications performance over the network.

8.2.13 Support Data Push Destination: allow user to create custom reports by configuring it to send network and application monitoring test results to a destination (data analysis platform) that businesses manage. Must support AWS S3, Google Big Query, Elasticsearch, Splunk (Beta), or a generic HTTP endpoint to receive this data. Using generic http endpoint, businesses can analyze the data in ServiceNow, PowerBI, Sumo logic, Mode analytics, PagerDuty, etc.

8.2.14 Sensor solution shall have these network security and privacy feature:

8.2.14.1 Data encryption at rest and in motion, and all communication using TLS

8.2.14.2 Hashing to conceal network access credentials use for monitoring

8.2.14.3 No SSID bridging nor externally accessible logic ports (SSH and in-bound Telnet are disallowed)

8.2.14.4 Security validation by independent vulnerability and penetration assessments

9 Privileged Access Management (PAM) As a Service (SaaS) Requirements - OPTIONAL

9.1 The PAM brand proposed must be recognized as a Leader in the latest Leaders Gartner® Magic Quadrant.

9.2 To propose PAM as a service for 15 users.

9.3 The PAM solution provides robust authentication mechanisms, including multi-factor authentication (MFA).

9.4 The PAM solution supports various authentication methods, such as smart cards, and token-based authentication.

9.5 The PAM solution enables fine-grained access control policies.

9.6 The PAM solution supports role-based access control (RBAC) to restrict privileges based on roles.

9.7 Access control policies are customisable and granular, allowing for the restriction of access to specific resources and actions.

9.8 The PAM solution must facilitate the elevation of privileges on-demand.

9.9 The PAM solution allows users to request elevated privileges, when necessary, subject to approval workflows.

9.10 The PAM solution enables privilege elevation to be time-limited and audited.

9.11 The PAM solution provides real-time session monitoring and recording capabilities.

9.11.1 The session recordings enable us to capture all user actions for auditing purposes.

9.11.2 The recordings are tamper-proof and easily retrievable.

9.12 The PAM solution includes a robust password management system.

9.13 The PAM solution enforces strong password policies.

9.14 The PAM solution enables passwords to be stored securely, utilizing encryption and hashing.

9.15 The PAM solution supports comprehensive auditing and reporting.

9.16 The PAM solution provides detailed logs of all privileged access activities.

9.17 The PAM solution provides compliance reports that can be generated automatically to meet regulatory requirements.

9.18 The PAM solution provides seamless integration with common identity and access management (IAM) systems.

9.19 The PAM solution is compatible with a wide range of operating systems, applications, and infrastructure components.

9.20 The PAM solution provides scalability to accommodate the organisation's growing needs.

9.21 The PAM solution is able to handle a large number of concurrent privileged sessions without performance degradation.

9.22 The PAM solution provides high availability features to ensure uninterrupted access control.

9.22.1 High Availability configurations includes failover mechanisms and redundancy.

9.23 The PAM solution prioritises security, utilizing encryption for data in transit and at rest.

9.24 The PAM solution offers secure remote access options without the need for VPN.

9.25 The PAM solution has an intuitive and user-friendly interface.

9.26 The PAM solution enables users to request privileges and access resources easily.

9.27 The PAM solution manages privileged accounts efficiently and effectively.

9.28 The PAM solution provides manual or automatic password rotation features for privileged accounts on a regular or scheduled basis.

9.29 The PAM solution offers customizable80 reporting and alerting features.

9.30 The alerts in the PAM solution can be triggered based on suspicious activities and policy violations.

9.31 The PAM solution complies with relevant industry standards and regulations, such as ISO 27001, NIST, and GDPR.

9.32 The PAM solution's vendor provides reliable support and regular updates for the PAM solution.

9.33 The PAM solution is equipped with a straightforward and minimally disruptive maintenance and patching processes.

9.34 The PAM solution's vendor offers comprehensive training resources and documentation to help both administrators and users to understand and effectively use the solution.

10 Email Security Requirements - OPTIONAL

10.1 The Supplier shall supply and deliver cloud-based solution and the requirements for the Email Security service for 100 mailboxes.

10.2 The solution must provide three modes of protection for email via API integration - Detect, Detect and Remediate, and Prevent (Inline).

10.3 The Solution integrates via API with Office 365 with no change on current architecture and MX of email service.

10.4 Solution relies on a cloud-based delivery model.

10.5 Solution should not disable any native security of customer Email Cloud Service Provider and will act as additional layer of security.

10.6 The Solution shall support Deployment without the need to change DNS MX records.

10.7 The Email Security solution should be inline and should be invisible for any attack reconnaissance.

10.8 The Solution should prevent mail borne threats and should be block/prevent before it reaches user inbox.

10.9 The Solution shall provide a sandbox environment to detect malicious/unknown and new attacks with attachments and URLS.

10.10 The sandbox shall cover file types commonly used in attacks (e.g. , zip, wsf, js, macros, python, exe, sh, bat, ps1).

10.11 The Solution can connect to other Office 365 SaaS applications to scan for malicious files being stored.

10.12 The Solution shall provide CDR (Content Disarm and Reconstruction) capabilities to remove malware and exploits from attachments.

10.13 The Solution shall have real time threat intelligence on the cloud with real time threat prevention.

10.14 The Email Security Scan shall integrate with email provider with reports of phishing and malware.

10.15 The Solution shall be able to detect business email compromise (BEC).

10.16 The Solution shall detect calendar invite attacks (CIAs) - calendar invite attacks are disguised as ICS files.

10.17 The solution should allow administrators to block compromised users or reset their password as an immediate step after the incident is detected.

10.18 The Solution shall allow administrator to view, re-route, or release messages in the quarantine.

10.19 The Solution shall have the ability for administrators to preview quarantined messages to determine further actions to be taken.

10.20 The Solution shall support granular policies for Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain Message Authentication Reporting & Conformance (DMARC).

10.21 The Solution shall be managed and monitored in a single dashboard for both built-in Cloud Email security and the Vendor Email Security.

10.22 The Solution's audit logs shall capture all administrator & user activities, including the following but not limited to:

10.22.1 Login/logoff;
10.22.2 Configuration changes made by administrators;
10.22.3 Action performed by administrators (e.g. release email from quarantine); and
10.22.4 Action performed by users (e.g. release email from quarantine).

10.23 All access is controlled using Role based access Control models.

10.24 The solution should have the ability to restore emails quarantined by Microsoft Office 365.

10.25 The Solution shall provide reports related to phishing, emails, malicious content (e.g. attachment, URL, malware).

11 Security Monitoring Requirements - OPTIONAL

11.1 The Solution Provider shall provide 24x7x365 SOC services to monitor events that are related to cyber threats, web defacement monitoring, dark web monitoring, web identity impersonation, compliance, and security best practices.

11.2 The Solution Provider must operate a 24x7 Security Operations Centre (SOC) based or located in Singapore with ISO27001 certification.

11.3 The solution provider must provide 3 shifts of Level 1, 2 and 3 Security Analysts.

11.4 The solution provider must provide a dedicated Customer Advisor.

11.5 The Solution Provider shall provide, manage, and maintain the SIEM and associated tools, technologies, and resources.

11.6 The Solution Provider shall provide Threat Detection services carried out by OSCP and GCIH certified Analysts.

11.7 The SIEM service must provide support for various log ingestion methods

11.7.1 File Event Sources (SFTP)
11.7.2 Windows Event Sources (HTTP/HTTPS)
11.7.3 ODBC Event Sources (ODBC)
11.7.4 Netflows
11.7.5 SNMP Event Sources (SNMP)
11.7.6 AWS
11.7.7 Azure
11.7.8 Logstash Plugin

11.8 The Solution Provider shall provide a Customer Advisor as a point of contact.

11.9 The SIEM service must have the capability to standardize logs originating from different sources, including custom systems or applications that are not natively supported by the SIEM.

11.10 The SIEM service must have the flexibility to deploy either virtualized on-premises log collectors or cloud-based log collectors (or a hybrid model) based on customer requirements.

11.11 The Service Provider must provide virtualized log collectors at no extra cost and the data transport between the log collector and SIEM must be encrypted and compressed.

11.12 The SIEM service must allow free-form text search and/or a combination of logical regular expressions to query for logs stored.

11.13 The service should provide pre-defined analytic rules for diverse use cases and advanced correlation capabilities for threat detection.

11.14 The service should allow customization of incidents for prioritization, alerting, and reporting purposes.

11.15 The SIEM used must have the ability to preserve raw logs for 1 year.

11.16 The provider must have a dedicated research team to directly input threat intelligence into the analytics platform.

11.17 The SIEM service should support integration with threat feeds, geolocation databases and custom watchlists.

11.18 The Solution Provider shall provide monthly, incident and threat Intel reports

11.18.1 Threat Intel report to include security ratings. Rating categories must include – Application Security, DNS Health, Endpoint Security, Hacker Chatter, IP Reputation, Information Leak, Network Security, Patching Cadence and Social Engineering.

11.8.2 Incident report to be sent every hourly during incident response.

11.19 The Solution Provider's SOC security analysts shall minimally use MITRE ATT&CK Framework as guidance to identify security incidents.

11.20 The Solution Provider shall perform periodic review and tuning and enhancement of the SIEM policies at no additional cost.

11.21 The Solution Provider shall configure and implement rules, recommend modifications to procedures to detect possible cyber-attacks. These changes must be made at no additional cost.

11.22 The Solution Provider must be a Singapore Registered Company with a local office and have at least three (3) years of SOC experience and have at least three (3) customers with more than 300 employees.

11.23 The Solution Provider must possess necessary licenses from Cybersecurity Agency in Singapore.

11.24 Provide Syslog service for 6 months retention, for the equipment in tender's proposed solution and existing environment.

11.25 Service Level Agreement

11.25.1 Response times

Severity Code	Response
1	1 hour
2	4 hours
3	8 hours

11.25.2 Security code

Severity Code	Severity Level	Definition	Coverage
1	**Critical**	Failure on the monitored device or the collector made normal day-to-day business and monitoring service not possible Activity that poses immediate threat to SCCC's infrastructure or critical assets	24 X 7
2	**Potential Risk**	Error that significantly affects the ability of the collector to operate normally and prevents normal day-to-day operation Activity that poses a potential future risk for compromise or loss of service	8 x 5
3	**Information**	A non-critical error that needs improvement but does not affect normal day-to-day business Activity or detected trends that should be investigated by the client but do not represent a direct severity threat to the environment	8 X 5

11.26 Below are the list of network devices, physical servers and virtual machines hosted at the data centre:

S/No	Equipment	Qty
1	Tier-1 F/W	2
2	Tier-2 F/W	2
3	Core Switches	2
4	Mobility Controller	2
5	WAN switches	2
6	WAN Load Balancer	1
7	Network Access Control	2
8	FortiAnalyzer	1
9	WAN Routers	2
10	Physical Server	2
11	Virtual Machines (Windows Server 2016 & 2019 OS)	8

12. Cloud Based Secure Access Service Edge (SASE) Solution – OPTIONAL

12.1 General

12.1.1 The SASE platform must be cloud based subscription based.

12.1.2 The solution need to support Geolocation -- which means user can always automatically connect with the nearest POP.

12.1.3 The solution should provide the following services:

12.1.3.1 Remote user securely access corportate resource (ZTNA)

12.1.3.2 User secure access Internet resources (SWG)

12.1.3.3 Security policy enforcement points, placed between users and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed (CASB).

12.1.4 The solution should have the single platform to allow users to control ZTNA, SWG and CASB.

12.1.5 The solution should support multi-tenancy

12.1.6 The solution should support 3rd party IDP integration with:

12.1.6.1 Security Assertion Markup Language (SAML)

12.1.6.2 System for Cross-domain Identity Management (SCIM)

12.1.6.3 Azure Active Directory

12.1.6.4 Okta

12.1.6.5 PingFederate

12.1.6.6 Google Workspace

12.1.7 The Agent softwware should support windows, MAcOS, Linux, IOS, Andriod

12.1.8 The solution should be able to perform device posture:

12.1.8.1 Client OS version

12.1.8.2 Firewall status

12.1.8.3 Anti-Virus status

12.1.8.4 Disk Encryption

12.2 Zero Trust Network Access (ZTNA)

12.2.1 The solution must come with the software client, and support device with client software(agent), and device without software client(agentless).

12.2.2 The corporate network should not allow the incoming traffic (traffic initiated from Internet), it can allow outgoing connection (traffic initated from corporate network) for remote user accessing corporate network resources user with agent software can access corporate network with the following protocol:

12.2.3 Any Port, Any Protocol

12.2.4 VOIP / UDP

12.2.5 Push patching / Server initiated flows

12.2.6 Wireguard Protocol

12.2.7 Users without agent software can access corporate network with the following protocol:

12.2.7.1 Web HTTP + HTTPS

12.2.7.2 Native SSH

12.2.7.3 Native RDP

12.2.7.4 RDP over Web

12.2.7.5 SSH over Web

12.2.7.6 SSH Lateral Movement Control

12.2.7.7 RDP to a single App / path

12.2.7.8 Git Protocol

12.2.7.9 Database (SQL, etc.)

12.2.7.10 RDP + SSH Self Service

12.2.7.11 Any Browser Support

12.2.7.12 RDP Session Recording

12.2.7.13 RDP Controls (File Transfer, Print, Copy/Paste)

12.2.7.14 Web URL-Rewrite Engine

12.3 Secured WAN Gateway (SWG)

12.3.1 The solution should support for IPsec Tunnels (inside out)

12.3.2 The solution should support DNS Filtering

12.3.3 The solution should support URL Filtering

12.3.4 The solution should support Reputation Intelligence (Axis = BrightCloud/Webroot)

12.3.5 The solution should support SSL Inspection

12.3.6 The solution should support SSL Exclusions

12.3.7 The solution should support Malware Scanning

12.3.8 The solution should support Customizable Categories

12.3.9 The solution should support VirusTotal Integration

12.4 Cloud Access Security Broker (CASB) – Optional

12.4.1 The solution should support Tenant Identification (block personal dropbox)

12.4.2 The solution should support App Identification

12.4.3 The solution should support App Discovery

12.4.4 The solution should support App Controls (login, post, like, share etc)

12.4.5 The solution should support Upload / Download Control

12.4.6 The solution should support Data Matchers (i.e. executable, spreadsheet, .jpg, etc)

12.4.7 The solution should support SAML Chain for SaaS (SAML Proxy i.e. agent installed)

12.5 Monitoring and Reporting

12.5.1 The solution should provide the reporting of User Device Latency

12.5.2 The solution should provide the reporting of User Device CPU

12.5.3 The solution should provide the reporting of User Device Memory

12.5.4 The solution should provide the reporting of User Device Disk Usage

12.5.5 The solution should provide the reporting of Hop by hop performance metrics

13. Managed Services

Requirements

13.1 The Tenderer shall propose a comprehensive technical, hardware and software support option for:

13.1.1 A period of 3 years, starting from date of acceptance.

13.1.2 A period of 5 years, starting from date of acceptance.

13.2 Provide Singapore Chinese Cultural Centre (SCCC) with remote helpdesk/call center, onsite desktop support services and IT Infrastructure support.

13.3 Provide 24x7 operations Service Desk as the single point of contact for any fault related IT services and service requests.

13.4 Provide service management system to record all incidents and service requests raised and ability to provide monthly report.

13.5 The scope of services shall include:

13.5.1 Managed Centralised Service Desk

13.5.2 Ticketing System, Service Fulfilment and Incident Management

13.5.3 Onsite IT Support Services

13.5.4 System and Application Account Administration and Support

13.6 Provide 1 engineer onsite full time to do Level 1 support on incidents related to users' workstations and peripherals, network connections, printer related issues, and Microsoft Office business applications during Office hour Mon - Fri (9 -6pm).

13.7 Replacement engineer must be provided if onsite engineer is away more than 1 working day or any pre-notified leave.

13.8 The Project, Service Desk and Support Team's Key personnel supporting the scope of service shall have minimum 3 year of full-time experience in delivery the managed services and customer fronting roles. To submit the curriculum vitae (CV) and particulars of the project and support team members including name, designation, appointment, qualification like industry certifications, relevant experience and track records and ensure they possess the relevant technical knowledge to carry out their role and function Knowledge of Microsoft Windows and Microsoft Office Suite applications is essential.

13.9 Capability to support the products below :

13.9.1 Fortinet Firewall

13.9.2 Peplink Load Balancer

13.9.3 Aruba WIFI, Access switches

13.9.4 Aruba core switches

13.9.5 Aruba Clearpass

13.9.6 Veeam Backup Solution

13.10 Shall provide an organisation chart for the project, showing names, reporting lines and responsibilities.

13.11 The details shall also include a schedule of the key personnel indicating duties to be performed.

13.12 The organisation chart shall include the project team members as specified in the organization.

13.13 Onsite engineer to perform routine backup work such as the administering of the daily backup jobs and restoration of backup data.

13 .14 Tenderer must have the ability to provide Level 2 IT infrastructure support (servers, storage, network, security and phone system).

13.15 Tenderer must be experienced in providing help-desk operations and services to enterprise customers

13.16 SCCC reserves the right to request for change of personnel after award of tender if the personnel is unable to perform the role to the required service level.

13.17 Service Provider shall not change the personnel in the project and/or support team without approval from SCCC appointed representative.

13.18 Service Provider shall provide full-time contract/permanent staff, there shall be no part time staff in the team.

13.19 All personnel will need to sign a non-disclosure agreement with SCCC. By signing the agreement, the Recipient agrees to keep secret and confidential and not to copy, reproduce, disseminate, transmit, distribute, publish or otherwise disclose to any third parties, whether before or after the completion of the purpose described, any Confidential Information except in accordance with the terms of this Agreement. The Recipient shall only be permitted to use the Confidential Information exclusively for the Purpose. Any disclosure of the Confidential Information must be strictly limited to those employees, agents, advisers and sub-contractors who reasonably have a need to know such Confidential Information to enable them to carry out their duties in SCCC.

13.20 The hand over from the SCCC incumbent IT Helpdesk services vendor will be implemented and completed within four (4) weeks max upon award.

13.21 Service Provider to submit a detailed transition plan to showcase how they can take over from existing IT vendor within 4 weeks from the day of award.

13.22 Service Provider shall provide to the Company an appointed Service Delivery Manager in a supervisory role to the Service Desk Agents, Onsite engineer and SLA requirement throughout the term of the Agreement. The Service Desk Agents consist of Agents Level 1 and Remote Resolution Expert as Level 2.

13.23 Service Provider shall provide Unified Service Desk Number and services for all the Company.

13.24 Service Provider shall provide IT Service Management Tool that is in the Leaders Gartner® Magic Quadrant.

13.25 Service Provider shall be familiar with the usage of the tool to deliver Service Desk Services and be able to perform activities such as, but not limited to, scripting, generating a report, opening or closing tickets, etc.

13.26 Service Provider shall provide highly trained, educated and excellent English-speaking Service Desk Agents.

13.27 Service Provider shall ensure that the Service Desk Agents communicate and make themselves clear when explaining the solutions to the users.

13.28 All SLA shall be calculated based on per requirement stated in the tender.

13.29 Priority 1 Cases - Total Network (Wireless / Lan)/ System Service Disruption, Wireless Network Service/ Lan Network Disruption during live events or live streaming, IT Security Incidents (such as virus attack or hacking).

13.30 Priority 2 Cases - VVIP Users, More than 50% of Network (Wireless / Lan)/System Service Disruption.

13.31 Priority 3 Cases - Network (Wireless / Lan)/ System Service Disruption but there is temporary workaround solution, Support to All Users.

13.32 SLA :

13.32.1 Service Provider must resolve Priority 1 case within 6 hours (100%).

13.32.2 Service Provider must resolve Priority 2 issues within 10 hours (100%).

13.32.3 Service Provider must resolve Priority 3 issues within 3 working days. (90%).

13.32.4 Service Provider is required to pick up 90% of users call within 15 seconds or 5 rings.

13.32.5 Service Provider is required to acknowledge users' emails within 1 hour.

13.32.6 Service Provider is required to respond onsite to users within 2 hours (90%) if issue unable to resolve remotely.

13.32.7 Service Provider shall work seamlessly with any Third-Party Vendor that has been awarded by the Company to deliver or provide services to run the business.

13.32.8 Service Provider's responsibilities shall include, but not be limited to, the following:

13.32.8.1 Service Provider shall provide the first point of contact for any fault, queries or issues relating to IT Services for SCCC including, but not limited to voice calls, mobile, voice mails, virtual and incident remarks received.

13.32.8.2 Service Provider shall be the SPOC to log, solve, escalate, track, and follow up till closure (end to end) any IT problems reported by SCCC's end users.

13.32.8.3 Service Provider shall receive, log and dispatch or transfer calls, as appropriate.

13.32.8.4 Service Provider shall open a call record to document calls. A call record shall include, but not be limited to, the following information:

13.32.8.4.1 End user information (e.g., phone numbers, email, department, etc.);

13.32.8.4.2 Call record numbers;

13.32.8.4.3 Date and tome Call record opened;

13.32.8.4.4 Service Request description;

13.32.8.4.5 Incident description;

13.32.8.4.6 Problem descriptions or symptoms;

13.32.8.4.7 First level problem determination, and if possible, problem resolution;

13.32.8.4.8 Call duration;
13.32.8.4.9 Incident classification;
13.32.8.4.10 Severity;
13.32.8.4.11 Ticket categorization;
13.32.8.4.12 Owner Group;
13.32.8.4.13 Ticket ID;
13.32.8.4.14 Service Request ID;
13.32.8.4.15 Name of Service Desk Agent;
13.32.8.4.16 Owner Name;
13.32.8.4.17 Call Source (e.g., phone calls, virtual chat);
13.32.8.4.18 Resolution Summary;
13.32.8.4.19 Ticket Summary;
13.32.8.4.20 Call assignment (for example, level 2, level 3);
13.32.8.4.21 Date and time of assignment;
13.32.8.4.22 Date and time of arrival;
13.32.8.4.23 Date and time rescheduled;
13.32.8.4.24 Call status;
13.32.8.4.25 Date and time resolved;
13.32.8.4.26 User acknowledgement on service resumption and availability;
13.32.8.4.27 Call resolution and closure information;
13.32.8.4.28 Structured reason for not meeting First Call Resolution FCR).

13.32.9 Service Provider shall prioritize calls in accordance with the service categories and personas categorization, severity of the call and operational impact.

13.32.10 Service Provider shall perform validation that includes the verification of the accuracy of the Configuration Item, System record, etc., assessment and problem analysis, including identification of the source of the problem during real-time engagement via Omni-Channel communication (e.g., phone call, chat, SMS).

13.32.11 Service Provider's Service Desk shall understand the underlying cause, symptoms and impact to perform the basic analysis on problem determination.

13.32.12 Service Provider shall provide a system to gather the end users' feedback at the point of service after an incident/call is closed through email or SMS for end users with email or mobile phone.

13.32.13 Expedited handling of high priority problems; and

13.32.14 Resolution coordination.

13.32.15 Service Desk Contact Centre System.

13.32.16 Annual end user customer satisfaction survey; and

13.32.17 Point of service customer satisfaction survey.

13.32.18 Agent Support

13.32.19 ADID Password Reset;

13.32.20 ADID Locked out; and

13.32.21 Application Password Reset;

13.32.22 Onsite End Users Desktop Support

13.32.22.1 Provide 1st Level Network, System and Cybersecurity, Infrastructure Support

13.32.22.2 Support for 3rd party Applications such as Wifi Human and Asset Tracking Solution, Wifi End User Experience Solution and any other solutions SCCC deployed during the contract period.

13.32.22.3 Manage and coordinate Server and System Patch Management.

13.32.22.4 Perform Periodic housekeeping of IT Policies and SOP documents.

13.32.22.5 Manage and track Licenses' Subscription.

13.32.22.6 Manage and coordinate Monthly Trainings and Phishing Campaigns.

13.32.22.7 Inventory Tracking & Management.

13.32.22.8 Daily & Monthly Reports generation.

13.32.22.9 Manage and coordinate with Third-Party vendors for adhoc projects/maintenance jobs/events.

13.32.22.10 Attend Weekly, Monthly and adhoc meetings.

13.32.22.11 Manage Phone Systems.

13.32.22.12 Manage and coordinate DR and BCP exercises.

13.32.22.13 Manage IT audits.

13.32.23 Service Provider shall perform validation that includes the verification of the accuracy of the Configuration Item, System record, etc., assessment and problem analysis, including identification of the source of the problem during real-time engagement via Omni-Channel communication (e.g., phone call, chat, SMS).

13.32.24 Service Provider shall understand the underlying cause, symptoms and impact to perform the basic analysis on problem determination.

13.32.25 Service Provider shall provide a system to gather the end users' feedback at the point of service after an incident/call is closed through email or SMS for end users with email or mobile phone.

13.32.26 Service Provider shall provide summary reports on the end users' feedback, including feedback analysis and follow-up action to be implemented as part of the improvement process, with reporting frequencies as agreed with the Company and/or In-Scope Institutions.

13.32.27 Service Provider shall escalate to support staff such as, but not limited to, Onsite Deskside Support, Network Enginners, Server Enginners, Remote Resolution Expert, CyberSecurity Enginners and the Company's support staff, and/or Third-Party Vendors, according to the escalation or notification procedures manual.

13.32.28 Service Provider shall notify SCCC of systems or equipment failures, or of an emergency, according to the escalation or notification procedures manual. The Service Provider shall establish processes to obtain notification and provide a TWENTY-FOUR (24) by SEVEN (7) Service desk to receive notifications from the various support parties.

13.32.29 Service Provider shall interface with and coordinate with SCCC and/or Third-Party ervice providers to obtain up-to-date status of incidents/problems.

13.32.30 Service Provider shall monitor incident/problem status to facilitate problem closure within the defined Service Level criteria or escalate in accordance with the
escalation procedures in the procedure manuals.

13.32.31 Service Provider shall establish and maintain call prioritization guidelines and escalation procedures.

13.32.32 Service Provider shall develop a Service Desk centre and Incident/Problem Management, operational processes and procedures the In-Scope Institutions for distribution.

13.32.33 Service Provider shall handle queries on IT Services and the procedures for accessing such IT Services.

13.32.34 Service Provider shall provide summary and detailed daily, weekly, monthly reports to the Company and/or In-Scope Institutions on the calls (by status code) received and handled by the Service Desk centre for the prior day, week and month.

13.32.35 Using the information contained in the daily, weekly and monthly reports, the Service Provider shall provide information to SCCC on call and ticket/case trend analysis, make recommendations (e.g. additional end user training requirements) and follow up on the recommendation, where appropriate.

13.32.36 Service Provider's responsibilities shall include, but not be limited to, the following:

13.32.36.1 Service Provider shall ensure that the Service Desk Agents have the business domain knowledge and are customer centric.

13.32.36.2 Service Provider shall ensure that the Service Desk Agents have strong
computer IT hardware and software, LAN/WAN skills and knowledge.

13.32.36.3 Service Provider shall ensure that the Service Desk Agents make every effort to resolve technical issues by using the remote access tool provided by the Service Provider. This will allow the Service Desk Agents to access SCCC' end users' desktops/notebooks remotely for the purpose of expediting the first call resolution.

13.32.36.4 Service Provider shall ensure that the Service Desk Agents have strong
problem-solving skills over the phone or online (via remote access tool)
and the right decision-making ability.

13.32.36.5 Service Provider shall ensure that the Service Desk Agents have the
ability to verify the identity of the callers.

13.32.36.6 Service Provider shall ensure that the Service Desk Agents have the
necessary "soft skills" and shall be continually assessed to achieve the best interpersonal and strong communication and

listening skills in handling the SCCC' end users.

13.32.36.7 Service Provider shall ensure that Service Desk Agents have access to the SCCC asset inventory to be able to understand the type of equipment and software that the SCCC end user's call relates to.

13.32.36.8 Service Provider shall effectively use and implement the capability for the SCCC end users to submit calls or report a problem/incident via electronic mail and/or the End User Self-Help Portal and shall continuously educate the SCCC end users on the use of such media.

13.32.36.9 Service Provider shall provide and continuously update a list of frequently asked questions and problem determination list (FAQs and PD Lists) regarding services applicable within the SCCC environment.

13.32.36.10 Service Provider shall conduct point of service surveys of the SCCC end users immediately after they have used the Service Desk.

13.32.37 Service Provider shall calculate statistics and publish reports monthly on the number of calls with, but not limited to, the following fields:

13.32.37.1 Sources of calls;

13.32.37.2 Frequency regarding the types or categories of calls;

13.32.37.3 Length of open tickets;

13.32.37.4 Number of calls resolved upon first contact;

13.32.37.5 Abandoned rate;

13.32.37.6 Status follow up from calls;

13.32.37.7 Other pertinent information regarding calls and problem resolution including identification of problematic assets/equipment/applications based on the call pattern;

13.32.37.8 Mean Time To Resolution (MTTR);

13.32.37.9 Ageing ticket report; and

13.32.37.10 First call resolution report.

13.32.37.11 Service Provider shall ensure that all case/tickets are routed to the correct party or parties for resolution at all times with warm transfers.

13.32.37.12 Service Provider shall ensure that all case/tickets have institution, department and username information for proper charging purposes to the In-Scope Institutions.

13.32.37.13 Service Provider shall ensure that all case/tickets are followed up until closure in a timely manner.

13.32.37.14 Service Provider shall ensure that all cases logged are followed up and responded to in a timely manner. All the pending cases logged must be responded to over the weekend/Public Holidays if needed.

13.32.38 Service Provider shall ensure that all complaints and feedback are followed up and responded to in a timely manner.

13.32.39 LEVEL 2 SUPPORT

13.32.39.1 Service Provider shall provide a 24 x 7 Remote Resolution Expert improve Mean Time to Resolution (MTTR).

13.32.39.2 Service Desk Level 1 shall perform a warm handover through Remote Resolution Expert after Service Desk tries to resolve the incident and concluded that it is out of its scope.

13.32.39.3 Service Desk Level 2 shall confirm that the issue is in-scope and assist the users via remote session to resolve the incident.

13.32.39.4 Service Desk Level 2 shall be trained in multiple domains including but not limited to the following:

13.32.39.4.1 Windows,

13.32.39.4.2 EUC application,

13.32.39.4.3 Monitoring,

13.32.39.4.4 MS office,

13.32.39.4.5 Mobility,

13.32.39.4.6 Firmware & Software patching.

13.32.39.5 The scope of support includes, but is not limited to:

13.32.39.5.1 Windows Operating System;

13.32.39.5.2 Firmware, Software Patching;

13.32.39.5.3 Mobility;

13.32.39.5.4 Microsoft Office;

13.32.39.5.5 Monitoring;

13.32.39.5.6 End-User-Computing Application

13.32.39.6 Service Provider shall work with the Company to conduct internal quality checks on procedures and processes such as, but not limited to:

13.32.39.6.1 SOP crafted addresses an In-Scope Institution's Operation requirements.

13.32.39.6.2 Provide and maintain SLD diagram

13.32.39.6.3 Service reports

13.32.40 Service Provider shall provide excellent customer service to the users of the Company s IT Services, Systems, network and facilities, through timely delivery of information and follow-up actions.

13.32.41 Service Provider shall recommend IT Services improvements and streamline the existing IT operations processes, procedures and instructions, as well as develop the processes, procedures, jobs and schedules required for the streamlining.

13.32.42 Service Provider shall achieve and meet the IT security requirements of SCCC.

13.32.43 Escalate incidents and service requests to relevant parties – Technology Support Vendor – if the incident is unresolvable at the 2nd Level.

13.32.44 Incident Management

13.32.44.1 All incidents, BCP workflow, IT IMP workflow and SOP are to be logged in the Contractor’s ITSM tool.

13.32.45 Certifications :

13.32.45.1 BizSafe Level Star or above

13.32.45.2 ISO 9001 Certification

13.32.45.3 ISO 45001 Certification

13.32.45.4 CyberSecurity Act 2018 - Penetration Test Service License

13.32.45.5 CyberSecurity Act 2018 - Managed Security Operations (SOC)
Monitoring Service License

14 Structure Cabling and UPS Requirements

14.1 Tenderer shall possess below certifications :

- 14.1.1 Work At Height Safety
- 14.1.2 Licensed Boom Lift and Scissor Lift Operator
- 14.1.3 Licensed Electrical Worker
- 14.1.4 Certified Cable Installer

14.2 Supply & install CAT 6A cabling with proper termination for new network points and submit test report for each point and update existing AutoCad documentation.

14.3 Supply & install CAT6A UTP patch panels where necessary

14.4 Supply & install CAT6A cabling for any additional AP & relocation of existing data points. To submit test report and update existing AutoCad documentation.

14.5 Uninterruptible Power Supply (UPS) system to support the proposal IT infrastructure for hold time of up to 15mins :

- 14.5.1 3 x 3kVA with optional UPS Network Management Card
- 14.5.2 2 x 3kVA with optional UPS Network Management Card
- 14.5.3 4 x 5kVA with optional UPS Network Management Card
- 14.5.4 Any additional units as deemed necessary.

14.6 Quoted UPS must be integrated into existing APC Data Center Expert Monitoring Solution.

14.7 Tenderer to provide necessary Professional Service to integrate all quoted UPS into existing APC Data Center Expert Monitoring Solution.

15. SCHEDULE OF RATE

Please refer to the following table for the Schedule of Rate (SOR). Below quantity is based on current infrastructure environment, tenders to propose any additional equipment accordingly. Failure to indicate any additional equipment needed during submission based on tender specifications, tenderer to bear the costs.

Campus Core Switch			
Description	Quantity	Amount	Remarks
layer 3 switch with minimum 24 SFP+, 24 10GBase-T and 4 QSFP+ ports and with redundant power supplies & stacking kits	2		Tenderer to indicate the model
Transceivers	1 Lot		Tenderer to indicate the model and quantity

Access Switch			
Description	Quantity	Amount	Remarks
48 ports switch according with PoE+ ports, minimum 2 SFP+ ports and redundant power supplies	6		Tenderer to indicate the model
Transceivers and stacking kits	1 Lot		Tenderer to indicate the model and quantity

Access Switch			
Description	Quantity	Amount	Remarks
24 ports switch according with PoE+ ports, minimum 2 SFP+ ports and redundant power supplies	4		Tenderer to indicate the model
Transceivers and stacking kits	1 Lot		Tenderer to indicate the model and quantity
24 ports non PoE switch, minimum 2 SFP+ ports and redundant power supplies	2		Tenderer to indicate the model
Transceivers and stacking kits	1 Lot		Tenderer to indicate the model and quantity
12 ports switch, minimum 2 SFP+ ports	2		Tenderer to indicate the model
Transceivers and stacking kits	1 Lot		Tenderer to indicate the model and quantity

Server Farm Infrastructure			
Description	Quantity	Amount	Remarks
Layer 3 switch with 48 ports and minimum 4 SFP+ ports and redundant power supplies	2		Tenderer to indicate the model
Transceivers and stacking kits	1 Lot		Tenderer to indicate the model and quantity

Wireless AP			
Description	Quantity	Amount	Remarks
Dual 2x2:2 MU-MIMO Radio Internal Antennas indoor AP and mounting bracket	61		Tenderer to indicate the model
Dual 4x4:4 MU-MIMO Radio Internal Antennas 1G/2.5G indoor AP and mounting bracket	16		Tenderer to indicate the model
Dual 2x2:2 MU-MIMO Radio Internal Antennas outdoor AP and mounting bracket	2		Tenderer to indicate the model
Dual 2x2:2 / 4x4:4 Radio Internal Omni Antenna outdoor AP and mounting bracket	2		Tenderer to indicate the model

1st and 2nd Tier Firewall			
Description	Quantity	Amount	Remarks
1st Tier (Perimeter) NGFW with 2.5 Gbps Threat Prevention throughput 280k new connections Min 16 x 10/100/1000 mbps and 4xSFP/SFP+ slots with necessary licenses and redundant power supplies	2		Tenderer to indicate the model
Transceivers	1 Lot		Tenderer to indicate the model and quantity
2nd Tier (Server Farm) NGFW with 1.5 Gbps Threat Prevention Throughput 148K new connections Min 8 x 10/100/1000 mbps and 2xSFP/SFP+ slots with necessary licenses and redundant power supplies	2		Tenderer to indicate the model
Transceivers	1 Lot		Tenderer to indicate the model and quantity

Identity and Policy Management			
Description	Quantity	Amount	Remarks
Policy management appliance/VM with necessary licenses	2		Tenderer to indicate the model and quantity

Compute, Storage and Backup			
Description	Quantity	Amount	Remarks
Production Environment			
Hyperconverged System Solutions	3		Tenderer to indicate the model and detailed BOM
Hypervisor Core License	36		Tenderer to indicate the model and detailed BOM
Backup Storage Hardware	1		Tenderer to indicate the model and detailed BOM
16-Core Windows Server Datacenter Edition License	3		Tenderer to indicate the model and detailed BOM
Backup Software License (up to 20 VMs)	1		Tenderer to indicate the model and detailed BOM
DR Environment			
Server Solutions	1		Tenderer to indicate the model and detailed BOM
16-core Windows Server Standard Edition License	1		Tenderer to indicate the model and detailed BOM

Structure Cabling and UPS			
Description	Quantity	Amount	Remarks
CAT6A cabling with proper termination for network points inclusive of 2 units of Cat6A copper patch cord	1 Lot		Tenderer to indicate description and quantity accordingly
CAT6A UTP patch panels	1 Lot		Tenderer to indicate description and quantity accordingly

Maintenance Charges			
Description	Quantity	Amount	Remarks
Software	3 & 5 Years Options		Tenderer to indicate description and quantity accordingly
Hardware	3 & 5 Years Options		Tenderer to indicate description and quantity accordingly
Licenses	3 & 5 Years Options		Tenderer to indicate description and quantity accordingly

Managed Services			
Description	Quantity	Amount	Remarks
Managed Services 3 Years	1 Lot		Tenderer to indicate description
Managed Services 5 Years	1 Lot		Tenderer to indicate description

Privileged Access Management (PAM) Solution As a Service - Optional			
Description	Quantity	Amount	Remarks
Privileged Access Management Solution as a service	1 Lot		Tenderer to indicate description and quantity accordingly
Subscription / Licenses for 3 years and 5 years options	1 Lot		Tenderer to indicate description and quantity accordingly

Cloud Based Email Security Solution - Optional			
Description	Quantity	Amount	Remarks
Cloud Based Email Security Solution	1 Lot		Tenderer to indicate description and quantity accordingly
Subscription / Licenses for 3 years and 5 years options	1 Lot		Tenderer to indicate description and quantity accordingly

Security Operations Center (SOC) with SIEM as a Service - Optional			
Description	Quantity	Amount	Remarks
Security Operations Center (SOC) with SIEM as a Service	1 Lot		Tenderer to indicate description and quantity accordingly
Subscription / Licenses for 3 years and 5 years options	1 Lot		Tenderer to indicate description and quantity accordingly

Cloud Based Security Secure Access Service Edge (SASE) Solution – Optional			
Description	Quantity	Amount	Remarks
Cloud Based Security Secure Access Service Edge (SASE) Solution with ZTNA and SWG	1 Lot		Tenderer to indicate description and quantity accordingly
Subscription / Licenses for 3 years and 5 years options	1 Lot		Tenderer to indicate description and quantity accordingly
Cloud Access Security Broker (CASB)	1 Lot		Tenderer to indicate description and quantity accordingly
Subscription / Licenses for 3 years and 5 years options	1 Lot		Tenderer to indicate description and quantity accordingly

16. LIQUIDATED DAMAGE

a. The contractor shall be liable to pay the LD at the rate of 5% per week should the project fail to complete within the specified time.

b. LD for Managed Services/ Onsite Engineer

The following amount shall be provided to Singapore Chinese Cultural Centre in the form of credit note for respective non-compliance or loss of item:

S/N	Description	Amount will be provided
1	Late for duty without approval	$0.50 for every minute
2	Early demise from duty without approval	$0.50 for every minute
3	Left Building during duty hours without approval	$0.50 for every minute
4	Absenteeism	$150 plus prorated amount based on the Tender sum rates
5	Loss of key	$100 per key
6	Unauthorised duplication of key	$200 per key
7	Loss or mishandling of access card	$50 per card
8	Late submission of monthly report	$50 per day

17. ENGINEER ON-SITE DEPLOYMENT AND MANAGED SERVICE REQUIREMENTS

Location: SCCC building, 1 Straits Boulevard, Singapore 018906

Composition	Qty	Schedule	Timings
Engineer On-site	01	Monday to Friday	0900hrs to 1800hrs

The Technical support team shall be responsible for all the operation and maintenance technical matters such as day-to-day monitoring and troubleshooting of technical problems. The technical support tram members shall comprise of the personnel with the following skillsets and experience:

a) At least TWO (2) years of IT onsite support experience;

b) Experience in troubleshooting software, hardware and network issues of similar scope;

c) Experience in technical support and in-depth knowledge of IEEE 802.11 family of WiFi technologies and products, and optimization of WiFi signal coverage including LBS calibrations and verifications

d) Experience in networking protocols and hardware such as routers, switches, firewalls, access points and wireless LAN controllers;

e) In-depth knowledge and experience in application and architecture deployment, monitoring and management of compute resources, storage and security to ensure the availability, scalability and reliability of the cloud environment;

f) Sound knowledge and experience of data communication wiring;

g) Initiative worker with excellent working attitude, strong written and communication skills, and good customer service orientation; and

h) Able to be on 24/7 standby for critical emergency incidents

i) To submit IT monthly report on the 10th of every month

18. EVALUATION CRITERIA

SCCC shall evaluate the tender proposal based on the following criteria:

a) Ability to meet tender specs & requirements specified

b) Ability to effect all deliverables within the stated schedule deadlines

c) The Tenderer shall be able to provide Singapore local support for the System throughout the installation and maintenance period.

d) The manpower deployed for this project must have attained the highest certification awarded by the equipment principal, and possess the relevant hands-on experience. Please submit engineers certifications.

e) Price competitiveness

f) Completeness of submission of the tender

g) Any other certification such as BizSAFE, ISO 9001 etc

h) Any other valued-added services for the smooth management of the IT infrastructure Management, including but not limited to Business Continuity Services/Workplace Recovery

19. KEY MANDATORY REQUIREMENTS

Tenders shall fully comply with the following Mandatory Criteria:

I. Government Supplier Registration (GSR) Requirements of EPU/CMP/10 Service (Computer related hardware, software, and services), S7; (Tendering capacity of up to $5,000,000)

II. The tender proposal shall meet the specified project delivery schedule.

III. At least five (5) years of experience in providing Computer Support Services and have provided at least two (2) similar Computer Support Services for Office buildings with performance Venue and occupancy of at least 1,000 occupants within that period;

IV. BizSafe Level 3 and above;

V. Meet the requirements as specified in Part 1, and 2 of the tender guide lines;

VI. The quoted networking brand (LAN, Wireless & NAC) must be an approved brand under GovTech NetworkTender – GVT(T) 22003.

VII. The proposed wireless network must meet minimum -60% signal strength illustrated in heat map.

VIII. The tenderer shall provide own staging or scissor lift for areas beyond MOM approved ladder height during installation or maintenance of APs.

IX. Attended Compulsory Site Briefing.

Tenderer's failing to meet the above-mentioned Mandatory Criteria will be excluded from subsequent evaluation.

20. QUERIES

All queries pertaining to this tender are to be directed to:

Mr. Phua Ann Chuan
Senior Assistant Director, Operations
Operations Department
Tel : 6812 7608
Email : estates@singaporeccc.org.sg

Ms Chua Wen Lin
Senior Executive Officer, Operations (Facilities)
Tel : 6812 7600
Email : estates@singaporeccc.org.sg

The Centre reserves the right not to entertain queries which it considers to be irrelevant, spurious or prejudiced to one tenderer.

TENDERER'S OFFER		**FORM A**
To: Singapore Chinese Cultural Centre 1 Straits Boulevard, #11-01, Singapore 018906	**Tender No:**	**SCCC/EST/2023/002**
Name of Tenderer:		
Tenderer Address & Telephone No:		

We,_____(name in block letters) hereby offer and undertake on the acceptance of this tender to supply, deliver, install, test, commission and maintain all the works and items as mentioned in the Technical Specifications and subject to the Conditions of Contract.

Our tender is made to subject to the Conditions of Tender and we agree that our tender remains open for consideration for a period of **180 days** commencing on the closing date for the submission of tenders i.e., on **29 December 2023, 2.00pm.**

We understand that you are not bound to accept the lowest or any tender you may receive and that you reserve the right to and we agree that you may accept our tender in whole or in part in accordance with of Tender Guidelines.

Unless and until a formal agreement is executed, as may be required by you in the Tender Guidelines, our offer with any authorised Variations and your written acceptance thereof shall constitute a binding agreement between us.

We agree that as and when requested by SCCC, we shall extend the validity of this offer for one or more periods not exceeding in total_____calendar months.

Our price (herein referred to as the "Contract Price") for the equipment and services to be supplied, installed and provided by us is: **S$**_____, excluding GST.

A breakdown of the Contract Price for the equipment and services is given in the Priced Schedule attached hereto.

We further undertake to give you any further information, which you may require.

Dated this_____day of_____, 2023.

Tenderer's Company or Business Registration No:	Tenderer's official Stamp:
Authorised Signature:	
Name:	Telephone/Handphone No: Fax:
Designation:	Email:

NOTICE: This Form must be duly completed and signed. Any change to its wordings may render the Tender liable to DISQUALIFICATION.

TENDERER'S PROFILE	**FORM B**
Company's Name:	
Address:	
Country of Incorporation:	
Year of Establishment:	
Ownership:	
GSR/BCA/NPA No. *(State Financial Category)*	
GST Registration No.	
Total Paid-up Capital:	

Please attach copy of the following:

- *Organisation Chart*
- *Latest Audited Balance Sheet and P&L Statement*
- *List of Reference Customers*

PRICE SCHEDULE OF TENDERER'S OFFER							**FORM C**
Item No.	***Name/Model of item***	***Quantity (No. of units) (a)***	***Tender Quotation Per Unit (Including Freight, Delivery and Installation (b)***	***Tender Quotation Per Item (a) x (b) = (c)***	***Discount (d)***	***Net Tender Quotation (c) – (d) = (e)***	***Any other Relevant Remarks***
Total Value							

TENDERER'S PROPOSAL – EQUIPMENT SPECIFICATION		**FORM D**
Item Name & Description	***Compliance with Technical Specifications (Yes/No)***	***Information & Specifications***
NOTE : Fill in column for Item Name & Description as specified under " Technical Specifications"		

TENDERER'S PROPOSAL - EQUIPMENT SUPPORT AND MAINTENANCE	**FORM E**

1. Please provide detailed information / description including the following:

   a) Number and qualifications of engineers directly responsible for maintenance

   b) Preventive maintenance policy

   c) Response time for unscheduled maintenance

   d) Availability of parts and limits to price escalation

   e) Maximum length of downtime before replacement equipment is supplied

   f) Please state the Key Performance Indicator (KPI), Key Result Area (KRA) and Return Time Objective (RTO), etc for the proposal

2.1 Please state the Warranty Period for all equipment and services supplied in the contract.

2.2 Please state in detail the maintenance services that are free of charge during the period of warranty stated in para 2.1 above.

3. Please state the annual maintenance charges including managed services and hardware for the subsequent three (3) years & five (5) years

TENDERER'S PROPOSAL – SOFTWARE SUPPORT	**FORM F**

1. Please provide detailed information / description including the following:

   a) Number and qualifications of software personnel directly responsible for servicing the system

   b) Details of local software support operations

   c) List current clients that will substantiate software support claims

   d) Response time of unscheduled software maintenance

   e) Policy for distribution of software new releases, enhancements and accompanying documents

   f) Availability of software personnel for occasional consultation

2.1 Please state the Warranty Period for all software and licenses supplied in the contract

2.2 Please state in detail the maintenance services that are free of charge during the period of warranty stated in para 2.1 above.

3. Please state the annual maintenance charges for software and licenses for the subsequent three (3) years and five (5) years.

TENDERER'S PROPOSAL – TRAINING	**FORM G**

1. Please provide detailed information / description of the training you intend to provide, including the following:

   a) Type

   b) Frequency and duration

   c) Venue

   d) Cost

   e) Training documents

   f) Number of attendance if free of charge

2. Please propose the detail of the courses/seminars that will familiarize the user with the equipment and services proposed.

MAJOR PROJECTS COMPLETED BY TENDERER'S COMPANY WITHIN THE LAST 3 YEARS					**FORM H**
Govt Bodies/Stat Boards/Other Clients	***Title***	***Description of Project***	***Contract Value***	***Start Date***	***End Date***

CURRENT PROJECTS UNDERTAKEN BY TENDERER'S COMPANY						**FORM I**
Govt Bodies/Stat Boards/Other Clients	***Title***	***Description of Project***	***Contract Value***	***Start Date***	***End Date***	***Percentage now completed***

PROFILE OF TENDERER'S PROJECT TEAM					**FORM J**
(Please complete below and state clearly the qualifications and experience of the staff in your team who would be assigned to this project, if awarded.)					
Name	***Designation***	***Yrs of experience***	***Qualification***	***Experience (Past & current projects)***	***Awards***
					NA
					NA

STATEMENT OF COMPLIANCE

The Tenderer shall fill in the **FORM K** with the following responses:

"Compliance" or "C"	Able to fully comply with the requirements. The Tenderer shall not add comments against the clause that vary the meaning of full compliance to the clause. However, comments indicating references to literature to substantiate the response is permissible. Any other comments which will vary the meaning of full compliance will be ignored. For statements that do not call for the Tenderer to meet a specific requirement but merely informs the Tenderer of a fact, the Tenderer's response shall state "C".
"Non-Compliance" or "NC"	Unable to comply with the requirements at all. Explanatory notes must be provided under the column "Remarks" for cases where the compliance is "NC".
"Not Applicable" or "NA"	If the items are not relevant to the Tender Offer, use "NA" to indicate not applicable. However, if "NA" is used against clauses/paragraphs requiring responses other than "NA", it will be assumed that the Tenderer has indicated "C".

The Tenderer shall take note of the language used in the Tender documents.

Must, Shall, Will or Mandatory	The item mentioned is an absolute requirement.
Should, Where Possible or Recommended	The item mentioned should be followed. Exceptions must be documented and approved by the Government. Compensating controls must be in place.
May or Optional	The item mentioned is truly optional. It may be followed as a suggestion.

It is imperative that all information requested be supplied accurately and concisely. Failure to supply such information may render the proposal disqualified for further consideration. Late submission of such information after the close of the deadline for submission of proposal shall not be entertained.

TENDERER COMPLIANCE LIST		FORM K
S/N	Compliance (C/NC/NA)	Reference
1	LAN	
1.1	General Network Requirements	
1.1.1		
1.1.2		
1.1.3		
1.1.3.1		
1.1.3.2		
1.1.3.3		
1.1.3.4		
1.1.3.5		
1.1.3.6		
1.1.3.7		
1.1.3.8		
1.1.4		
1.1.5		
1.1.6		
1.1.7		
1.1.8		
1.1.9		
1.2	Campus Core Switch	
1.2.1		
1.2.2		
1.2.2.1		
1.2.2.2		
1.2.2.3		
1.2.2.4		
1.2.2.5		

S/N	Compliance (C/NC/NA)	Reference
1.2.2.6		
1.2.2.7		
1.2.2.8		
1.2.2.9		
1.2.2.10		
1.2.2.11		
1.2.2.12		
1.2.2.13		
1.2.2.14		
1.2.2.15		
1.2.2.16		
1.2.2.17		
1.2.2.18		
1.2.3	Resiliency and High Availability	
1.2.3.1		
1.2.3.2		
1.2.3.3		
1.2.3.4		
1.2.3.5		
1.2.3.6		
1.2.3.7		
1.2.3.8		
1.2.3.9		
1.2.3.10		
1.2.3.11		

S/N	Compliance (C/NC/NA)	Reference
1.2.4	Performance	
1.2.4.1		
1.2.4.2		
1.2.5	Connectivity	
1.2.5.1		
1.2.5.2		
1.2.5.3		
1.2.5.4		
1.2.6	Management	
1.2.6.1		
1.2.6.2		
1.2.6.3		
1.2.6.4		
1.2.6.5		
1.2.6.6		
1.2.6.7		
1.2.6.8		
1.2.6.9		
1.2.6.10		
1.2.6.11		
1.2.6.12		
1.2.6.13		
1.2.6.14		
1.2.6.15		
1.2.6.16		
1.2.6.17		

S/N	Compliance (C/NC/NA)	Reference
1.2.7	Layer 2 Switching	
1.2.7.1		
1.2.7.2		
1.2.7.3		
1.2.7.4		
1.2.7.5		
1.2.7.6		
1.2.8	Layer 3 Services and Routing	
1.2.8.1		
1.2.8.2		
1.2.8.3		
1.2.8.4		
1.2.8.5		
1.2.8.6		
1.2.8.7		
1.2.8.8		
1.2.8.9		
1.2.8.10		
1.2.8.11		
1.2.8.12		
1.2.8.13		
1.2.8.14		

S/N	Compliance (C/NC/NA)	Reference
1.2.9	Security	
1.2.9.1		
1.2.9.2		
1.2.9.3		
1.2.9.4		
1.2.9.5		
1.2.9.6		
1.2.9.7		
1.2.9.8		
1.2.10	Multicast	
1.2.10.1		
1.2.10.2		
1.2.10.3		
1.2.10.4		
1.2.11	Analytic	
1.2.11.1		
1.2.11.2		
1.2.11.3		
1.2.11.4		
1.2.11.5		
1.3	Access Switch	
1.3.1		
1.3.1.1		
1.3.1.2		
1.3.1.3		
1.3.1.4		
1.3.1.5		
1.3.1.6		
1.3.1.7		

S/N	Compliance (C/NC/NA)	Reference
1.3.1.8		
1.3.1.9		
1.3.1.10		
1.3.1.11		
1.3.1.12		
1.3.1.13		
1.3.1.14		
1.3.1.15		
1.3.1.16		
1.3.1.17		
1.3.1.18		
1.3.1.19		
1.3.2	Quality of Service (QoS)	
1.3.2.1		
1.3.2.2		
1.3.2.3		
1.3.2.4		
1.3.2.5		
1.3.2.6		
1.3.2.7		
1.3.2.8		
1.3.3	Resiliency and High Availability	
1.3.3.1		
1.3.3.2		
1.3.3.3		
1.3.3.4		
1.3.3.5		
1.3.3.6		

S/N	Compliance (C/NC/NA)	Reference
1.3.4	Scale and Simplicity	
1.3.4.1		
1.3.4.2		
1.3.4.3		
1.3.4.4		
1.3.4.5		
1.3.4.6		
1.3.5	Connectivity	
1.3.5.1		
1.3.5.1.1		
1.3.5.1.2		
1.3.5.1.3		
1.3.5.2		
1.3.5.3		
1.3.5.4		
1.3.6	Management	
1.3.6.1		
1.3.6.2		
1.3.6.3		
1.3.6.4		
1.3.6.5		
1.3.6.6		
1.3.6.7		
1.3.6.8		
1.3.6.9		
1.3.6.10		
1.3.6.11		
1.3.6.12		
1.3.6.13		

S/N	Compliance (C/NC/NA)	Reference
1.3.6.14		
1.3.6.15		
1.3.6.16		
1.3.6.17		
1.3.7	Layer 2 Switching	
1.3.7.1		
1.3.7.2		
1.3.7.3		
1.3.7.4		
1.3.7.5		
1.3.7.6		
1.3.7.7		
1.3.8	Layer 3 Services and Routing	
1.3.8.1		
1.3.8.2		
1.3.8.3		
1.3.8.4		
1.3.8.5		
1.3.8.6		
1.3.8.7		
1.3.8.8		
1.3.8.9		
1.3.8.10		
1.3.8.11		
1.3.8.12		
1.3.8.13		
1.3.8.14		
1.3.8.15		
1.3.8.16		

1.3.8.17		

S/N	Compliance (C/NC/NA)	Reference
1.3.9	Security	
1.3.9.1		
1.3.9.2		
1.3.9.3		
1.3.9.4		
1.3.9.5		
1.3.9.6		
1.3.9.7		
1.3.9.8		
1.3.9.9		
1.3.10	Multicast	
1.3.10.1		
1.3.10.2		
1.3.10.3		
1.3.10.4		
1.3.10.5		
1.3.11	Convergence	
1.3.11.1		
1.3.11.2		
1.3.11.3		
1.3.11.4		
1.3.12	Analytic	
1.3.12.1		
1.3.12.2		
1.3.12.3		
1.3.12.4		
1.3.12.5		

S/N	Compliance (C/NC/NA)	Reference
1.4	Compact Access Switch (12 ports)	
1.4.1	Connectivity, performance and standards	
1.4.1.1		
1.4.1.2		
1.4.1.3		
1.4.1.4		
1.4.1.4.1		
1.4.1.4.2		
1.4.1.5		
1.4.1.6		
1.4.1.7		
1.4.1.8		
1.4.1.9		
1.4.1.9.1		
1.4.1.9.2		
1.4.1.9.3		
1.4.1.9.4		
1.4.1.9.5		
1.4.1.9.6		
1.4.1.9.7		
1.4.1.10		
1.4.1.11		
1.4.1.12		
1.4.2	High Availability and Resiliency	
1.4.2.1		
1.4.2.2		
1.4.2.3		

S/N	Compliance (C/NC/NA)	Reference
1.4.3	Quality of Service (QoS)	
1.4.3.1		
1.4.3.2		
1.4.3.3		
1.4.3.4		
1.4.3.5		
1.4.3.6		
1.4.3.7		
1.4.4	Management	
1.4.4.1		
1.4.4.2		
1.4.4.3		
1.4.4.4		
1.4.4.5		
1.4.4.6		
1.4.4.7		
1.4.5	Layer 3 Features	
1.4.5.1		
1.4.5.2		
1.4.6	Layer 2 switching	
1.4.6.1		
1.4.6.2		
1.4.6.3		
1.4.7	Multicast	
1.4.7.1		
1.4.7.2		
1.4.7.3		

S/N	Compliance (C/NC/NA)	Reference
1.4.8	Security	
1.4.8.1		
1.4.8.2		
1.4.8.3		
1.4.8.4		
1.4.8.5		
1.4.8.6		
1.4.8.7		
1.4.8.8		
1.4.8.9		
1.4.8.10		
1.4.9	Convergence	
1.4.9.1		
1.4.9.2		
1.4.9.3		
1.4.9.4		
1.4.10	Analytic	
1.4.10.1		
1.4.10.2		
1.4.10.3		
1.4.10.4		
1.4.10.5		

S/N	Compliance (C/NC/NA)	Reference
1.5	Datacenter Core Switch (Server Farm Switch)	
1.5.1	Key Features	
1.5.1.1		
1.5.1.2		
1.5.1.3		
1.5.1.4		
1.5.1.5		
1.5.1.6		
1.5.1.7		
1.5.1.8		
1.5.1.9		
1.5.1.10		
1.5.1.11		
1.5.1.12		
1.5.1.13		
1.5.1.14		
1.5.1.15		
1.5.1.16		
1.5.2	Quality of Service (QoS)	
1.5.2.1		
1.5.3	Resiliency	
1.5.3.1		
1.5.3.2		
1.5.3.3		
1.5.3.4		
1.5.3.5		
1.5.3.6		
1.5.3.7		
1.5.3.8		

S/N	Compliance (C/NC/NA)	Reference
1.5.3.9		
1.5.3.10		
1.5.3.11		
1.5.4	Performance	
1.5.4.1		
1.5.4.2		
1.5.5	Connectivity	
1.5.5.1		
1.5.5.2		
1.5.5.3		
1.5.6	Management	
1.5.6.1		
1.5.6.2		
1.5.6.3		
1.5.6.4		
1.5.6.5		
1.5.6.6		
1.5.6.7		
1.5.6.8		
1.5.6.9		
1.5.6.10		
1.5.6.11		
1.5.6.12		
1.5.6.13		
1.5.6.14		
1.5.6.15		
1.5.6.16		
1.5.6.17		

S/N	Compliance (C/NC/NA)	Reference
1.5.7	Layer 2 Switching	
1.5.7.1		
1.5.7.2		
1.5.7.3		
1.5.7.4		
1.5.7.5		
1.5.7.6		
1.5.8	Layer 3 Services and Routing	
1.5.8.1		
1.5.8.2		
1.5.8.3		
1.5.8.4		
1.5.8.5		
1.5.8.6		
1.5.8.7		
1.5.8.8		
1.5.8.9		
1.5.8.9		
1.5.8.10		
1.5.8.11		
1.5.8.12		
1.5.8.13		

S/N	Compliance (C/NC/NA)	Reference
1.5.9	Security	
1.5.9.1		
1.5.9.2		
1.5.9.3		
1.5.9.4		
1.5.9.5		
1.5.9.6		
1.5.9.7		
1.5.9.8		
1.5.10	Multicast	
1.5.10.1		
1.5.10.2		
1.5.10.3		
1.5.10.4		
1.5.11	Analytic	
1.5.11.1		
1.5.11.2		
1.5.11.3		
1.5.11.4		
1.5.11.5		

S/N	Compliance (C/NC/NA)	Reference
2	Wireless LAN (WLAN)	
2.1	General Wireless Requirements	
2.1.1		
2.1.2		
2.1.3		
2.1.4		
2.1.5		
2.1.6		
2.1.7		
2.1.8		
2.1.9		
2.1.10		
2.1.11		
2.1.12		
2.1.13		
2.1.14		
2.1.15		
2.1.16		
2.1.17		
2.1.18		

S/N	Compliance (C/NC/NA)	Reference
2.2	Wireless Coverage Reference	
2.2.1		
2.2.2		
2.2.3		
2.2.4		
2.2.5		
2.2.6		
2.2.7		
2.2.8		
2.2.9		
2.2.10		
2.2.11		
2.2.12		
2.3	Centralized Wireless LAN Controller Features	
2.3.1		
2.3.2		
2.3.3		
2.3.4		
2.3.5		
2.3.6		
2.3.7		
2.3.8		
2.3.8.1		
2.3.8.2		
2.3.8.3		
2.3.8.4		
2.3.8.5		

S/N	Compliance (C/NC/NA)	Reference
2.3.9		
2.3.10		
2.3.11		
2.3.12		
2.3.13		
2.3.14		
2.3.15		
2.3.16		
2.3.17		
2.3.18		
2.3.19		
2.3.20		
2.3.21		
2.3.22		
2.3.23		
2.3.24		
2.3.25		
2.3.26		
2.3.27		
2.3.28		
2.3.29		
2.3.30		
2.3.31		
2.3.32		
2.3.33		

S/N	Compliance (C/NC/NA)	Reference
2.3.34		
2.3.34.1		
2.3.34.2		
2.3.34.3		
2.3.34.4		
2.3.34.5		
2.3.34.6		
2.3.34.7		
2.3.34.8		
2.3.34.9		
2.3.34.10		
2.3.34.12		
2.3.34.13		
2.3.34.14		
2.3.34.15		
2.3.34.16		
2.3.34.17		
2.3.34.18		
2.3.34.19		
2.3.34.20		
2.3.34.21		
2.3.34.22		
2.3.34.23		

S/N	Compliance (C/NC/NA)	Reference
2.3.35		
2.3.35.1		
2.3.35.2		
2.3.35.3		
2.3.35.4		
2.3.35.5		
2.3.35.6		
2.3.35.7		
2.3.35.8		
2.3.35.9		
2.3.35.10		
2.3.35.11		
2.3.35.12		
2.3.35.13		
2.3.35.14		
2.3.35.15		
2.3.35.16		
2.3.36		
2.3.36.1		
2.3.36.2		
2.3.36.3		
2.3.36.4		
2.3.36.5		
2.3.36.6		
2.3.36.7		
2.3.36.8		
2.3.36.9		

S/N	Compliance (C/NC/NA)	Reference
2.3.36.10		
2.3.36.11		
2.3.36.12		
2.3.36.13		
2.3.36.14		
2.3.36.15		
2.3.36.16		
2.3.36.17		
2.3.36.18		
2.3.37		
2.3.38		
2.3.39		
2.3.40		
2.3.41		
2.3.42		
2.3.43		
2.3.44		
2.3.45		
2.4	Wireless Access Control and QoS Features	
2.4.1		
2.4.2		
2.4.3		
2.4.4		
2.4.5		
2.4.6		
2.4.7		
2.4.8		
2.4.9		
2.4.10		

S/N	Compliance (C/NC/NA)	Reference
2.4.11		
2.4.12		
2.4.13		
2.4.14		
2.4.15		
2.4.16		
2.4.17		
2.5	Wireless Mobility Features	
2.5.1		
2.5.2		
2.5.2.1		
2.5.2.2		
2.5.2.3		
2.5.2.4		
2.5.2.5		
2.5.2.6		
2.5.3		
2.5.4		
2.5.5		
2.5.6		
2.5.6.1		
2.5.6.2		
2.5.6.3		
2.5.6.4		
2.5.7		
2.5.8		
2.5.9		

S/N	Compliance (C/NC/NA)	Reference
2.6	Wireless Access Point (AP) Features	
2.6.1		
2.6.2		
2.6.3		
2.6.4		
2.6.5		
2.6.6		
2.6.7		
2.6.8		
2.6.9		
2.6.10		
2.6.11		
2.6.12		
2.6.13		
2.6.14		
2.6.15		
2.6.16		
2.6.16.1		
2.6.16.2		
2.6.16.3		
2.6.17		
2.6.17.1		
2.6.17.2		
2.6.17.3		
2.6.18		
2.6.19		
2.6.20		

S/N	Compliance (C/NC/NA)	Reference
2.6.21		
2.6.21.1		
2.6.21.2		
2.6.22		
2.6.23		
2.6.24		
2.6.25		
2.6.26		
2.6.27		
2.6.27.1		
2.6.27.2		
2.6.27.3		
2.6.27.4		
2.6.28		
2.6.29		
2.6.30		
2.6.31		
2.6.32		
2.6.33		
2.6.34		
2.6.34.1		
2.6.34.2		
2.6.34.3		
2.6.34.4		
2.6.34.5		
2.6.34.6		
2.6.34.7		
2.6.34.8		

S/N	Compliance (C/NC/NA)	Reference
2.6.34.9		
2.6.34.10		
2.6.35		
2.6.36		
2.6.37		
2.6.37.1		
2.6.37.2		
2.6.37.3		
2.6.37.4		
2.6.38		
2.6.38.1		
2.6.38.2		
2.6.38.3		
2.6.38.4		
2.6.38.5		
2.6.38.6		
2.6.38.7		
2.6.39		
2.6.39.1		
2.6.39.2		
2.6.39.3		
2.6.39.4		
2.6.39.5		
2.6.39.6		
2.6.39.7		
2.6.39.8		
2.6.40		

S/N	Compliance (C/NC/NA)	Reference
2.6.41		
2.6.41.1		
2.6.41.2		
2.6.41.3		
2.6.42		
2.6.43		
2.6.44		
2.6.45		
2.6.46		
2.6.47		
2.6.48		
2.6.49		
2.6.50		
2.6.51		
2.6.52		
2.6.52.1		
2.6.52.2		
2.6.53		
2.6.54		
2.6.55		
2.6.56		
2.6.57		
2.6.58		
2.6.59		
2.6.59.1		
2.6.59.2		
2.6.59.3		
2.6.59.4		

S/N	Compliance (C/NC/NA)	Reference
2.6.59.5		
2.6.59.6		
2.6.59.7		
2.6.59.8		
2.6.60		
2.6.60.1		
2.6.60.2		
2.6.60.3		
2.6.60.4		
2.6.60.5		
2.6.60.6		
2.6.60.7		
2.7	Outdoor Wireless Access Point (AP)	
2.7.1		
2.7.2		
2.7.3		
2.7.4		
2.7.5		
2.7.6		
2.7.7		
2.7.7.1		
2.7.8		
2.7.8.1		
2.7.9		
2.7.10		
2.7.11		

S/N	Compliance (C/NC/NA)	Reference
2.7.12		
2.7.12.1		
2.7.12.2		
2.7.12.3		
2.7.13		
2.7.13.1		
2.7.13.1.1		
2.7.13.1.2		
2.7.13.1.3		
2.7.13.1.4		
2.7.13.2		
2.7.14		
2.7.14.1		
2.7.14.1.1		
2.7.14.1.2		
2.7.14.2		
2.7.14.2.1		
2.7.14.2.2		
2.7.14.2.3		
2.7.15		
2.7.15.1		
2.7.15.2		
2.7.15.2.1		
2.7.15.3		
2.7.15.3.1		
2.7.15.3.2		

S/N	Compliance (C/NC/NA)	Reference
2.7.16		
2.7.16.1		
2.7.16.2		
2.7.16.2.1		
2.7.16.2.2		
2.7.16.2.3		
2.7.16.3		
2.7.16.3.1		
2.7.16.3.2		
2.7.16.3.3		
2.7.16.3.4		
2.7.16.3.5		
2.7.16.3.6		
2.7.16.3.7		
2.7.16.4		
2.7.16.4.1		
2.7.16.4.2		
2.7.16.4.3		
2.7.16.4.4		
2.7.16.4.5		
2.7.16.4.6		
2.7.16.4.7		
2.7.16.5		
2.7.16.6		
2.7.16.6.1		
2.7.16.6.2		

S/N	Compliance (C/NC/NA)	Reference
2.7.17		
2.7.17.1		
2.7.17.2		
2.7.17.3		
2.7.17.4		
2.7.17.5		
2.7.17.6		
2.7.17.7		
2.7.18		
2.7.19		
2.7.20		
2.7.21		
2.7.22		
2.7.23		
2.7.24		
2.7.25		
2.7.26		
2.7.27		
2.7.28		
2.7.29		
2.7.30		
2.7.31		
2.7.32		
2.7.33		
2.7.34		
2.7.35		

S/N	Compliance (C/NC/NA)	Reference
3	Firewall	
3.1	Tier-1 Firewall Requirements	
3.1.1		
3.1.2		
3.1.3		
3.1.4		
3.1.4.1		
3.1.4.2		
3.1.4.3		
3.1.4.4		
3.1.4.5		
3.1.4.6		
3.1.5		
3.1.6		
3.1.7		
3.1.8		
3.1.9		
3.1.10		
3.1.11		
3.1.12		
3.1.13		
3.1.14		
3.1.15		

S/N	Compliance (C/NC/NA)	Reference
3.2	Tier-2 Firewall Requirements	
3.2.1		
3.2.2		
3.2.3		
3.2.3.1		
3.2.3.2		
3.2.3.3		
3.2.3.4		
3.2.4		
3.2.5		
3.2.6		
3.2.7		
3.2.8		
3.2.9		
3.2.10		
3.2.11		
3.2.12		
3.2.13		
3.2.14		
3.2.15		

S/N	Compliance (C/NC/NA)	Reference
4	WAN Load Balancer	
4.1	Key features	
4.1.1		
4.1.2		
4.1.3		
4.1.4		
4.1.5		
4.1.6		
4.1.7		
4.1.8		
4.1.9		
4.1.10		
4.1.11		
4.1.12		
4.1.13		
4.1.14		
4.1.15		
4.1.16		
4.1.17		
4.1.18		
4.1.19		
4.2	Quality of Service (QoS)	
4.2.1		
4.3	Resiliency and High Availability	
4.3.1		
4.3.2		

S/N	Compliance (C/NC/NA)	Reference
4.4	Performance	
4.4.1		
4.5	Connectivity	
4.5.1		
4.5.2		
4.5.3		
4.6	Management	
4.6.1		
4.6.2		
4.6.3		
4.6.4		
4.6.5		
4.6.6		
4.7	Layer 3 Services and Routing	
4.7.1		
4.7.2		
4.7.3		
4.7.4		
4.8	Security	
4.8.1		
4.8.2		
4.8.3		
4.8.4		
4.8.5		

S/N	Compliance (C/NC/NA)	Reference
4.9	General Performance Requirements	
4.9.1		
4.9.2		
4.10	General WAN Requirements	
4.10.1		
4.10.2		
4.10.3		
4.10.4		
4.10.5		
4.10.6		
4.11	General LAN Requirements	
4.11.1		
4.11.2		
4.11.3		
4.11.4		
4.12	General DNS Requirements	
4.12.1		
4.12.1.1		
4.12.1.2		
4.12.1.3		
4.12.1.4		
4.12.1.5		
4.12.1.6		
4.12.1.7		
4.12.1.8		

S/N	Compliance (C/NC/NA)	Reference
4.13	General Load-Balancing Requirements	
4.13.1		
4.13.2		
4.13.3		
4.13.4		
4.13.5		
4.14	General High Availability Requirements	
4.14.1		
4.15	General VPN Requirements	
4.15.1		
4.15.2		
4.15.3		
4.15.4		
4.15.5		
4.15.6		
4.16	General Networking Requirements	
4.16.1		
4.16.1.1		
4.16.1.2		
4.16.1.3		
4.16.2		
4.17	General Captive Portal requirements	
4.17.1		
4.17.2		
4.17.3		
4.18	General Security Requirements	
4.18.1		
4.18.2		
4.18.3		

S/N	Compliance (C/NC/NA)	Reference
5	Compute and Storage System	
5.1	Compute and Storage Requirements (for Production environment)	
5.1.1		
5.1.2		
5.1.3		
5.1.4		
5.1.5		
5.1.6		
5.1.7		
5.1.8		
5.1.9		
5.1.10		
5.1.11		
5.1.12		
5.1.13		
5.1.14		
5.1.15		
5.1.16		
5.1.17		
5.1.18		
5.1.19		
5.1.20		
5.1.21		
5.1.22		
5.1.23		
5.1.24		
5.1.25		
5.1.26		

S/N	Compliance (C/NC/NA)	Reference
5.1.27		
5.1.28		
5.1.29		
5.1.29.1		
5.1.29.2		
5.1.29.3		
5.1.30		
5.1.30.1		
5.1.30.2		
5.2	Compute and Storage Requirements (for DR environment)	
5.2.1		
5.2.2		
5.2.3		
5.2.4		
5.2.4.1		
5.2.4.2		
5.2.4.3		
5.2.4.4		
5.3	Management Requirements	
5.3.1		
5.3.2		
5.3.3		
5.3.4		
5.3.5		
5.3.5.1		
5.3.5.2		
5.3.5.3		

S/N	Compliance (C/NC/NA)	Reference
5.3.5.4		
5.3.5.5		
5.3.5.6		
5.3.5.7		
5.3.5.8		
5.3.5.9		
5.3.5.10		
5.3.5.11		
5.3.5.12		
5.3.513		
5.3.6		
5.4	Security Requirements	
5.4.1		
5.4.2		
5.4.3		
5.4.4		
5.4.5		
5.4.6		
5.5	General Backup Requirements	
5.5.1		
5.5.2		
5.5.3		
5.5.4		
5.5.5		
5.5.6		
5.5.7		
5.5.8		
5.5.9		
5.5.10		

S/N	Compliance (C/NC/NA)	Reference
5.6	File Server Requirements	
5.6.1		
5.6.2		
5.6.3		
5.6.4		
5.6.5		
5.6.6		
5.6.7		
5.6.8		
5.6.9		
5.6.10		
5.6.11		
6	Network Management	
6.1	Overall Solution	
6.1.1		
6.1.2		
6.1.3		
6.1.4		
6.1.5		
6.1.6		
6.1.7		
6.1.8		
6.2	Deployment	
6.2.1		
6.2.2		
6.2.3		
6.2.4		
6.2.5		
6.2.6		

S/N	Compliance (C/NC/NA)	Reference
6.3	Management, Monitoring and Troubleshooting	
6.3.1		
6.3.2		
6.3.3		
6.3.4		
6.3.5		
6.3.6		
6.3.7		
6.3.8		
6.3.9		
6.3.10		
6.3.11		
6.4	AI Optimization	
6.4.1		
6.4.2		
6.4.3		
6.4.4		
6.4.5		
6.4.6		
6.4.7		
6.4.8		
6.4.8.1		
6.4.8.2		
6.4.8.3		
6.4.8.4		
6.4.8.5		
6.4.8.6		

S/N	Compliance (C/NC/NA)	Reference
6.4.8.7		
6.4.8.8		
6.4.8.9		
6.4.8.10		
6.5	Security	
6.5.1		
6.5.2		
6.5.3		
6.5.4		
6.5.5		
6.5.6		
6.5.7		
7	Identity and Policy Management	
7.1	Servers and Appliance	
7.1.1		
7.1.2		
7.1.3		
7.1.4		
7.1.5		
7.1.6		
7.1.7		
7.1.8		
7.1.9		
7.1.10		

S/N	Compliance (C/NC/NA)	Reference
7.2	Functionality	
7.2.1		
7.2.2		
7.2.3		
7.2.4		
7.2.5		
7.2.6		
7.2.7		
7.2.7.1		
7.2.7.2		
7.2.7.3		
7.2.7.4		
7.2.7.5		
7.2.7.6		
7.2.7.7		
7.2.7.8		
7.2.7.9		
7.2.7.10		
7.2.7.11		
7.2.8		
7.2.9		
7.2.10		
7.2.11		
7.2.11.1		
7.2.11.2		

S/N	Compliance (C/NC/NA)	Reference
7.2.12		
7.2.12.1		
7.2.12.2		
7.2.12.3		
7.2.12.4		
7.2.12.5		
7.2.13		
7.2.13.1		
7.2.13.2		
7.2.13.3		
7.2.13.4		
7.2.13.5		
7.2.14		
7.2.15		
7.2.16		
7.2.17		
7.2.18		
7.2.19		
7.2.20		
7.2.21		
7.2.22		
7.2.23		
7.2.24		
7.2.25		
7.2.26		
7.2.27		
7.2.28		
7.2.29		
7.2.30		

S/N	Compliance (C/NC/NA)	Reference
7.2.31		
7.2.31.1		
7.2.31.2		
7.2.31.3		
7.2.31.4		
7.2.31.5		
7.2.31.6		
7.2.31.7		
7.2.32		
7.2.33		
7.2.34		
7.2.35		
7.2.35.1		
7.2.35.2		
7.2.35.3		
7.2.35.4		
7.2.35.5		
7.2.35.6		
7.2.35.7		
7.2.35.9		
7.2.35.10		
7.2.35.12		
7.2.35.13		
7.2.35.14		

S/N	Compliance (C/NC/NA)	Reference
7.3	Reliability / Performance	
7.3.1		
7.3.2		
7.3.3		
7.3.4		
7.3.5		
7.3.6		
7.4	Bring Your Own Devices (BYOD)	
7.4.1		
7.4.2		
7.4.3		
7.4.4		
7.4.5		
7.4.6		
7.4.7		
7.4.8		
7.5	Guest Access	
7.5.1		
7.5.2		
7.5.3		
7.5.4		
7.5.5		
7.5.6		
7.5.7		
7.5.8		
7.5.9		
7.5.10		

S/N	Compliance (C/NC/NA)	Reference
7.5.11		
7.5.12		
7.5.13		
7.5.14		
7.5.15		
7.5.16		
7.5.17		
7.5.18		
7.5.19		
7.5.20		
7.5.21		
7.5.22		
7.5.23		
7.5.24		
7.5.25		
7.5.26		
7.5.27		
7.5.28		

S/N	Compliance (C/NC/NA)	Reference
8	Network Monitoring Sensor	
8.1	General Requirements	
8.1.1		
8.1.2		
8.1.3		
8.1.4		
8.1.5		
8.1.6		
8.1.7		
8.1.7.1		
8.1.7.2		
8.1.8		
8.1.9		
8.1.9.1		
8.1.9.2		
8.1.9.3		
8.1.10		
8.1.11		
8.1.11.1		
8.1.11.2		
8.1.11.3		
8.1.11.4		

S/N	Compliance (C/NC/NA)	Reference
8.2	Key Features	
8.2.1		
8.2.2		
8.2.3		
8.2.4		
8.2.5		
8.2.6		
8.2.7		
8.2.8		
8.2.9		
8.2.10		
8.2.10.1		
8.2.10.2		
8.2.10.3		
8.2.11		
8.2.12		
8.2.13		
8.2.14		
8.2.14.1		
8.2.14.2		
8.2.14.3		
8.2.14.4		

S/N	Compliance (C/NC/NA)	Reference
9	Privileged Access Management (PAM) As a Service (SaaS) Requirements - OPTIONAL	
9.1		
9.2		
9.3		
9.4		
9.5		
9.6		
9.7		
9.8		
9.9		
9.10		
9.11		
9.11.1		
9.11.2		
9.13		
9.14		
9.15		
9.16		
9.17		
9.18		
9.19		
9.20		
9.21		
9.22		
9.22.1		
9.23		
9.24		

S/N	Compliance (C/NC/NA)	Reference
9.25		
9.26		
9.27		
9.28		
9.29		
9.30		
9.31		
9.32		
9.33		
9.34		
10	Email Security Requirements - OPTIONAL	
10.1		
10.2		
10.3		
10.4		
10.5		
10.6		
10.7		
10.8		
10.9		
10.10		
10.11		
10.12		
10.13		
10.14		
10.15		
10.16		

S/N	Compliance (C/NC/NA)	Reference
10.17		
10.18		
10.19		
10.20		
10.21		
10.22		
10.23		
10.24		
10.25		
11	Security Monitoring Requirements - OPTIONAL	
11.1		
11.2		
11.3		
11.4		
11.5		
11.6		
11.7		
11.7.1		
11.7.2		
11.7.3		
11.7.4		
11.7.5		
11.7.6		
11.7.7		
11.7.8		
11.8		
11.9		
11.10		

S/N	Compliance (C/NC/NA)	Reference
11.11		
11.12		
11.13		
11.14		
11.15		
11.16		
11.17		
11.18		
11.18.1		
11.18.2		
11.19		
11.20		
11.21		
11.22		
11.23		
11.24		
11.25		
11.25.1		
11.25.2		
11.26		

S/N	Compliance (C/NC/NA)	Reference
12	Cloud Based Secure Access Service Edge (SASE) Solution - OPTIONAL	
12.1	General Requirements	
12.1.1		
12.1.2		
12.1.3		
12.1.3.1		
12.1.3.2		
12.1.3.3		
12.1.4		
12.1.5		
12.1.6		
12.1.6.1		
12.1.6.2		
12.1.6.3		
12.1.6.4		
12.1.6.5		
12.1.6.6		
12.1.7		
12.1.8		
12.1.8.1		
12.1.8.2		
12.1.8.3		
12.1.8.4		

S/N	Compliance (C/NC/NA)	Reference
12.2	Zero Trust Network Access (ZTNA)	
12.2.1		
12.2.2		
12.2.3		
12.2.4		
12.2.5		
12.2.6		
12.2.7		
12.2.7.1		
12.2.7.2		
12.2.7.3		
12.2.7.4		
12.2.7.5		
12.2.7.6		
12.2.7.7		
12.2.7.8		
12.2.7.9		
12.2.7.10		
12.2.7.11		
12.2.7.12		
12.2.7.13		
12.2.7.14		

S/N	Compliance (C/NC/NA)	Reference
12.3	Secured WAN Gateway (SWG)	
12.3.1		
12.3.2		
12.3.3		
12.3.4		
12.3.5		
12.3.6		
12.3.7		
12.3.8		
12.3.9		
12.4	Cloud Access Security Broker (CASB) - OPTIONAL	
12.4.1		
12.4.2		
12.4.3		
12.4.4		
12.4.5		
12.4.6		
12.4.7		
12.5	Monitoring and Reporting	
12.5.1		
12.5.2		
12.5.3		
12.5.4		
12.5.5		

S/N	Compliance (C/NC/NA)	Reference
13	Managed Services	
13.1		
13.1.1		
13.1.2		
13.2		
13.3		
13.4		
13.5		
13.5.1		
13.5.2		
13.5.3		
13.5.4		
13.6		
13.7		
13.8		
13.9		
13.9.1		
13.9.2		
13.9.3		
13.9.4		
13.9.5		
13.9.6		
13.10		
13.11		
13.12		
13.13		
13.14		
13.15		

S/N	Compliance (C/NC/NA)	Reference
13.16		
13.18		
13.19		
13.20		
13.21		
13.22		
13.23		
13.24		
13.25		
13.26		
13.27		
13.28		
13.29		
13.30		
13.31		
13.32		
13.32.1		
13.32.2		
13.32.3		
13.32.4		
13.32.5		
13.32.6		
13.32.7		
13.32.8		
13.32.8.1		
13.32.8.2		
13.32.8.3		

S/N	Compliance (C/NC/NA)	Reference
13.32.8.4		
13.32.8.4.1		
13.32.8.4.2		
13.32.8.4.3		
13.32.8.4.4		
13.32.8.4.5		
13.32.8.4.6		
13.32.8.4.7		
13.32.8.4.8		
13.32.8.4.1		
13.32.8.4.10		
13.32.8.4.11		
13.32.8.4.12		
13.32.8.4.13		
13.32.8.4.14		
13.32.8.4.15		
13.32.8.4.16		
13.32.8.4.17		
13.32.8.4.18		
13.32.8.4.19		
13.32.8.4.20		
13.32.8.4.21		
13.32.8.4.22		
13.32.8.4.23		
13.32.8.4.24		
13.32.8.4.25		
13.32.8.4.26		
13.32.8.4.27		
13.32.8.4.28		

S/N	Compliance (C/NC/NA)	Reference
13.32.9		
13.32.10		
13.32.11		
13.32.12		
13.32.13		
13.32.14		
13.32.15		
13.32.16		
13.32.17		
13.32.18		
13.32.19		
13.32.20		
13.32.21		
13.32.22		
13.32.22.1		
13.32.22.2		
13.32.22.3		
13.32.22.4		
13.32.22.5		
13.32.22.6		
13.32.22.7		
13.32.22.8		
13.32.22.9		
13.32.22.10		
13.32.22.11		
13.32.22.12		
13.32.22.13		

S/N	Compliance (C/NC/NA)	Reference
13.32.23		
13.32.24		
13.32.25		
13.32.26		
13.32.27		
13.32.28		
13.32.29		
13.32.30		
13.32.31		
13.32.32		
13.32.33		
13.32.34		
13.32.35		
13.32.36		
13.32.36.1		
13.32.36.2		
13.32.36.3		
13.32.36.4		
13.32.36.5		
13.32.36.6		
13.32.36.7		
13.32.36.8		
13.32.36.9		
13.32.36.10		

S/N	Compliance (C/NC/NA)	Reference
13.32.37		
13.32.37.1		
13.32.37.2		
13.32.37.3		
13.32.37.4		
13.32.37.5		
13.32.37.1		
13.32.37.7		
13.32.37.8		
13.32.37.9		
13.32.37.10		
13.32.37.11		
13.32.37.12		
13.32.37.13		
13.32.37.14		
13.32.38		
13.32.39		
13.32.39.1		
13.32.39.2		
13.32.39.3		
13.32.39.4		
13.32.39.5		
13.32.39.5.1		
13.32.39.5.2		
13.32.39.5.3		
13.32.39.5.4		
13.32.39.5.5		

S/N	Compliance (C/NC/NA)	Reference
13.32.39.5.6		
13.32.39.5.6.1		
13.32.39.5.6.2		
13.32.39.5.6.3		
13.32.40		
13.32.41		
13.32.42		
13.32.43		
13.32.44		
13.32.44.1		
13.32.45		
13.32.45.1		
13.32.45.2		
13.32.45.3		
13.32.45.4		
13.32.45.5		

S/N	Compliance (C/NC/NA)	Reference
14	Structured Cabling and UPS Requirements	
14.1		
14.1.1		
14.1.2		
14.1.3		
14.1.4		
14.2		
14.3		
14.4		
14.5		
14.5.1		
14.5.2		
14.5.3		
14.5.4		
14.6		
14.7		