

PART 2

REQUIREMENT SPECIFICATIONS

ALL RIGHTS RESERVED. THIS DOCUMENT SHOULD NOT BE REPRODUCED IN ANY FORM OR BY ANY MEANS WITHOUT THE PRIOR PERMISSION OF THE SINGAPORE SPORTS SCHOOL LTD.

THE INFORMATION GIVEN IN THIS DOCUMENT IS NOT TO BE COMMUNICATED, EITHER DIRECTLY OR INDIRECTLY, TO THE PRESS OR TO ANY PERSON NOT AUTHORISED TO RECEIVE IT.

Contents

1	INTRODUCTION	4
2	SCOPE OF TENDER	4
3	SCOPE OF WORK.....	7
4	SYSTEM REQUIREMENTS.....	9
5	Comprehensive Network Security Penetration Testing Requirement	83
6	MAINTENANCE AND SUPPORT SERVICES	86
7	PROJECT IMPLEMENTATION SCHEDULE	87

1 INTRODUCTION

Background

- 1.1 The Singapore Sports School Ltd (hereinafter referred to as the “School”) is a Specialised Independent School that offers selected youths an integrated academic and sports programme in a world-class environment. It is located at 1 Champions Way Singapore 737913 (Primary Site) and 5 Stadium Lane 397773 (Secondary Site) with staff strength of around 230 staff and has a student-athlete population close to 600.

Purpose

- 1.2 The purpose of this Tender is to invite Tenderers to submit a proposal for the design, supply, delivery, installation, testing and commissioning of a new network infrastructure (henceforth known as the “System”) for the School, including provision of software support and hardware maintenance for the System and the list of the School’s existing network equipment under **Annex B of Part 2 Requirement Specifications**.

2 SCOPE OF TENDER

- 2.1 The Scope of Tender shall include the following:
- 2.1.1 Design, supply, deliver, install, test and commission a fully operational new Network Infrastructure System in the Primary Site to meet all the requirements in the Requirement Specifications;
 - 2.1.2 Provide software support and hardware maintenance for the following items:
 - (a) The System as listed in the Contractor’s submitted 1st Schedule (pursuant to Clause 17.1 of **Part 1, Section C**), for a period of THREE (3) years with an option of TWO (2) yearss extensions. The maintenance services shall come into effect on Commissioning Date for Acceptance; and
 - (b) The School’s existing List of Network Equipment: Firewall and Uninterrupted Power Supply, based on the stipulated period(s) in **Annex B of Part 2 Requirement Specifications**.
 - 2.1.3 Decommission, dismantle and disposal of the existing network infrastructure equipment in the Primary Site. The Tenderer is to quote the **price payable to the School**, for the scrape/ trade-in value of the removed equipment under **Part 3, Annex E – Price Schedule**. A brief summary of the existing list of network equipment is found in **Annex A of Part 2 Requirement Specifications**.

- 2.2 The Tenderer shall submit a proposal for the above tender scope that meets all the requirements in **Part 2, Requirement Specifications** and a proposed Acceptance Test Plan to ensure compliance with the requirements. Any partially complete proposal shall be considered invalid.
- 2.3 The proposed System shall take into account the following considerations:
- 2.3.1 The System is designed with high availability and redundancy capability. Where necessary, the connections between network devices, servers and firewalls shall be reinforced using resilient links, link aggregation and multi-point aggregation technologies. There shall be no single point of failure in the infrastructure; automatic fail-over and recovery capabilities shall exist should any component in the System fail;
 - 2.3.2 Be responsible for performing sizing exercises to ensure the proposed System adequately fits the School's operational requirements and is scalable and evolvable to meet the future and changing needs of the School;
 - 2.3.3 Ensure that all the proposed hardware and software have sufficient capacity to be upgraded for future expansion. For example, there will be expansion slots for processors, memory, ports, hard disks;
 - 2.3.4 Shall describe the amount of spare capacity design for the proposed hardware and equipment. For example, a modular or chassis-based switch comes with a spare capacity of two work module slots.
 - 2.3.5 Ensure the proposed System is fully compatible with the School's existing three Internet Access Links.
 - 2.3.6 Provide options to increase the school's wireless coverage and capacity by deploying additional access points throughout the Contract Period. The tenderer must include the optional charges for the additional equipment and services under **Part 3, Annex E—Price Schedule**.
 - 2.3.7 Provide options to extend the wireless coverage and density in outdoor environments using either ruggedised outdoor access points or directional antenna connected to indoor access points with necessary connectivity and mounting provision. All such implementations shall be safe and secured;
 - 2.3.8 Propose network monitoring and the respective management tools that will fully support the proposed implementation of the System;
 - 2.3.9 The following products, equipment and services (including but not limited to):

No	Description	Clause	Quantity
1	Core Network Switch (48-port)	4.3	2
2	Server Farm Switch (24-port)	4.4	2
3	Demilitarised Zone Switch (24-port)	4.4	2

No	Description	Clause	Quantity
4	Power over Ethernet (POE) Layer 3 Intelligent Network Switch (48-port)	4.5	33
5	Layer 3 Intelligent Network Switch (48-port)	4.6	32
6	Transit Switch (24-port)	4.7	4
7	Wireless Network Architecture	4.8	1 lot
	- Network Management Solution (SaaS)	4.8.24	
	- Wireless Intrusion Prevention System	4.8.123	
8	Wireless Access Point (Indoor)	4.9	300
9	Wireless Access Point with External Antenna (Outdoor)	4.10	7
10	Identity and Policy Management System	4.11	2
11	Next Generation Enterprise Firewalls and Management Tools	4.12	4
12	Application Delivery Controller	4.13	1 lot
13	Server and network racks with installation services	4.14	10
14	Maintenance and Support for existing Equipment: Firewall and Uninterrupted Power Supply	4.15	Refer to Annex B
15	Cabling Requirement	4.16	1 lot
16	Comprehensive Network Security Penetration Testing	4.17	1 lot
17	All other software, hardware, product and equipment, and maintenance and support services necessary for the successful deployment and implementation of the System.		1 lot

2.3.10 The Tender Proposal shall include a detailed write-up of the following:

- (a) Design of the new network infrastructure showing the different devices and interconnectivity;
- (b) A transition plan that will describe in detail the seamless cutover from the existing network infrastructure to the new System without affecting the School's operation;
- (c) A comprehensive change management plan that includes communication, deployment and training of the new System and related procedures to users before, during and after the System rollout;
- (d) A deployment plan and user acceptance test plan which addresses functional, stress and load performance testing to validate that the proposed System meets all the requirements in this Tender; and
- (e) A network security Vulnerability Assessment and Penetration Test (VAPT) plan to describe how the proposed network infrastructure design addresses any security threats with respect to the confidentiality, integrity and availability of the School's information assets.

- 2.3.11 The Tenderer shall clearly state in the proposal other components, facilities, resources, or value-added services that may be made available to the School to ensure the successful management of this project and implementation of the System.
- 2.3.12 The Tenderer shall provide itemised costing details for the proposed solution, including all products, equipment and services to be rendered, in **Part 3, Annex E – Price Schedule** of this Tender. The prices shall be all inclusive and no further charges shall be incurred for the successful implementation and commissioning of the System.
- 2.3.13 The Tenderer shall supply the Schedule of Rates (SOR) in **Part 3, Annex E – Price Schedule** of this Tender for all the products and equipment to be purchased at the discretion of the School using the fixed prices quoted which shall remain valid throughout the lifespan of this Contract. The SOR shall be all-inclusive, including but not limited to professional services and cabling works required.

3 SCOPE OF WORK

- 3.1 The Contractor shall be wholly responsible for the timely provision of the System in accordance with the requirements and contractual terms in this Tender during the entire contractual period. The scope of work shall cover, but not limited to, the following:
- (a) Project initiation;
 - (b) Conduct a thorough assessment of the existing network infrastructure and understand its architecture, components, and performance. Identify any limitations, bottlenecks, or areas for improvement in the current setup, ensure new network infrastructure addresses the identified limitations and meets the future needs of the School;
 - (c) Design of the new network infrastructure and finalisation of design/technical specifications;
 - (d) Dismantling and removal of the existing network infrastructure equipment;
 - (e) Delivery of the proposed product and equipment and implementation of the new network infrastructure;
 - (f) Execution of deployment plan and change management activities;
 - (g) Execution of acceptance tests comprising of user acceptance and network security penetration tests;
 - (h) Training to the School's assigned staff;
 - (i) Documentation;
 - (j) Providing maintenance and support services for the System based on its submitted list in **Schedule 1 of Part 1, Section C**; and the School's existing list of network equipment: Firewall and Uninterrupted Power Supply listed in **Annex B of Part 2** of this Invitation to Tender; and

- (k) Undertaking service requests.
- 3.2 The Contractor shall ensure all installation works do not cause disturbance or inconvenience to staff, students and visitors of SSP. Any work that may cause disruption, disturbance or inconvenience shall be done after office hours after permission is granted by SSP, and without additional charges to SSP.
- 3.3 The Contractor shall ensure that any works that may cause disruption of the existing IT services can only be carried out on weekends (Saturdays and Sundays) or weekdays after 9pm, subject to SSP's approval. This shall be done at no additional charge to SSP.
- 3.4 The Contractor shall work closely and share all relevant information with other appointed Contractors and personnel of SSP, when required, to ensure the successful implementation and support of the System, including integration with the organization's existing IT infrastructure.
- 3.5 The Contractor shall ensure the implementation of the System will not affect the normal operation of the organization's existing IT infrastructure. The Contractor shall make good any damage to the existing IT infrastructure to the satisfaction of SSP.
- 3.6 The Contractor shall take all necessary precautions not to damage and disturb all the School's properties, including but not limited to cables, equipment, pipes, roads, completed works, etc., throughout the contract period. Any damage to the properties shall be made good at the Contractor's expense.
- 3.7 As part of the acceptance test, the Contractor shall submit the report on the findings of the network security penetration test on the proposed System, which shall include, but not be limited to, the following:
- (a) An executive summary of the results of the network security penetration test;
 - (b) List of risks/vulnerabilities identified and severity ratings;
 - (c) Root causes of the risks/vulnerabilities and their recommended rectifications;
 - (d) Implications for not addressing the risks/vulnerabilities identified; and
 - (e) Implications for implementing the recommended rectifications.
- 3.8 The Contractor shall not, without the prior written consent of the School, publish or release, allow publication or release of, in any media, any news item, article, publication, advertisement, prepared speech or any other information or material pertaining to any part of the obligations to be performed, or any information received, obtained, compiled, derived or generated including any reference to, mention of, or the Tenderer's association or purported association with the School.
- 3.9 The Contractor shall be the authorised reseller of the principal products, devices and equipment proposed in this Tender. All technical installations shall be carried out by trained personnel certified by the principal supplier of the product, device or equipment.

4 SYSTEM REQUIREMENTS

4.1 General Requirements

- 4.1.1 The System proposed by the Tenderer shall show all the interconnections of network devices and equipment, servers, storage and workstations.
- 4.1.2 The proposed System shall be highly robust and reliable, and take the following into consideration in the design:
 - (a) Availability of 99.9% ;
 - (b) Resiliency;
 - (c) Fit-for-Purpose;
 - (d) Security;
 - (e) Performance;
 - (f) Cost Effectiveness; and
 - (g) Able to support Ethernet network bandwidth up to 40G.
- 4.1.3 The proposed System should be able to separate the servers' network traffic from that of end-users. It shall also have a network Demilitarised Zone (DMZ) and a two (2) tier firewall architecture to safeguard the School's network from attacks initiated externally and internally.
- 4.1.4 The proposed System must be capable of having programmable overlays that allow network virtualisation across SSP and underlays that support end-to-end connectivity using standard routing protocols.
- 4.1.5 The proposed system shall include the network virtualisation feature, which allows multiple tenancies through virtualisation, with shared common infrastructure but segregated data and control plane.
- 4.1.6 Overlapping IP addresses or VLANs shall be supported across different virtual networks.
- 4.1.7 Wireless traffic shall be isolated by dedicated VLANs at the controller and dynamically assigned by 802.1x authentication. Wireless endpoints shall be mapped using VLAN to their virtual networks.
- 4.1.8 The proposed System shall allow segmentation by software and policy enforcement based on user identity and group membership, using tags to control role-based access across the School's network.
- 4.1.9 The overlay packets must go through stateful inspection via a set of firewalls (active/active or active/standby) before access to common shared services (e.g. DNS, DHCP, NTP, AAA & Active Directory) and access to other virtual networks is allowed to provide an additional layer of security and monitoring of traffic.

- 4.1.10 All the proposed equipment and switches shall support Syslog logging.
- 4.1.11 There shall be encryption at Layer 2 using IEEE 802.1AE to prevent data modification by malicious attackers.
- 4.1.12 The proposed network infrastructure shall be IPv6 ready and it shall support the co-existence of IPv4 and IPv6.
- 4.1.13 All the proposed network switches shall support, but not limited to, the following switch management and operation features:
 - (a) SSH (at least version 1 and 2);
 - (b) Telnet;
 - (c) Console;
 - (d) FTP;
 - (e) SFTP;
 - (f) HTTPS;
 - (g) Remote Monitoring (REMON - RFC 1757) and (RMON – RFC 2819); and
 - (h) Simple Network Management Protocol (SNMP) Version 1, 2c and 3
- 4.1.14 The proposed network infrastructure shall support security, the Internet of Things (IoTs), Bring-Your-Own Devices (BYODs), cloud services, table scale (MAC/router/Access Control List), and buffering for enterprise applications.
- 4.1.15 The proposed network infrastructure shall be capable of providing Bonjour Services for Apple devices.

4.2 General Switch Requirements

- 4.2.1 General switch requirements apply to the Core Switch, Server Farm switch, Demilitarised switch, Access switch, and Transit switch.
- 4.2.2 The network switch shall come with the following enhanced switch access authentication security features:
 - (a) Authorised User Configuration Mode;
 - (b) Integrity Check for Firmware images;
 - (c) Integrity Check for Configuration File;
 - (d) Integrity Check for Critical Software;
 - (e) Display Upgrade Information;
 - (f) Stored Password with Salt;
 - (g) Restricts access to the switch only for specific IP addresses (configured as management station);
 - (h) Bans those IP addresses permanently from further access on invalid authentication attempts reaching the threshold limit;
 - (i) Provides options to configure privileges for all access types and align IP services dynamically with AAA authentication configuration;
 - (j) Restricts only one session per user;

- (k) Option for password obscuring to prohibit disclosure while entering the password;
- (l) Option to configure user passwords with SHA-224/256 (SHA-2) or SHA-2+AES encryption;
- (m) SSH/SSL Pub Key hashed with SHA2;
- (n) Separate user password for SNMPv3 frame authentication/encryption;
- (o) Supports both DSA 1024 and RSA 2048 public key algorithms for SSH private and SSH public keys;
- (p) Provides the option to verify the integrity of the images in each directory matches with the SHA-2 (SHA256 or 512 key) shared along with the image file;
- (q) Process Self-Test functional commands to view the major hardware and software process status;
- (r) Support of TLS 1.2 version for TLS connections; and
- (s) Valid ASA credentials need to be provided to access SWLOG content.

- 4.2.3 The proposed switch must support a built-in cloud agent, which will perform a call home and be managed by the cloud management server. The same switch must also be able to be managed by an on-premises management server in the event the cloud is not available.
- 4.2.4 The proposed switch must support Intelligent Fabric Technology that can self-configure, self-attach, and self-heal the network through Auto-Fabric, eliminating many manual tasks and human errors during deployment.
- 4.2.5 The proposed switch must be capable of propagating switch configurations, such as user profiles or device profiling signatures, across the network to other switches. This feature leverages the broker/client relationship, community names, and topics to publish configuration information between switches.
- 4.2.6 The proposed switch must support the FIPS 140-2 standard, which provides strong cryptographic algorithms. Devices using FIPS 140-2 compliant encryption use it in various management interfaces, such as SFTP, HTTP, SSH, and SSL.
- 4.2.7 The proposed switch must be able to work in the “thin switch” mode, where it will fetch the configuration and software image from a centralised on-premise or cloud management platform when boot up. Configuration changes will only be made on this centralised management platform.
- 4.2.8 The proposed switch must support secure boot, which ensures that a device boots using only software trusted by the Original Equipment Manufacturer (OEM).

4.3 Core Network Switch Requirements

The Core Switch:

- 4.3.1 Must be designed for highly scalable 1GE/10GE/25GE/40GE/100GE Gigabit Ethernet networks.
- 4.3.2 Shall have at least 48 ports of 1GE/10GE/25GE SFP+ with 8 ports of 100GE QSFP28.
- 4.3.3 Must be in a 1 rack unit (RU) form factor without additional power tray accessories requirement.
- 4.3.4 It shall have redundant and hot-swappable slide-in power supplies, which will come with 5 + 1 individual variable-speed fan module for redundancy purposes and be hot-swappable.
- 4.3.5 Shall have a front-to-back or back-to-front cooling mechanism for Hot/Cold aisle deployment.
- 4.3.6 Shall support the following network virtualisation technologies:
 - (a) must be capable of creating a low latency, virtualisation-ready fabric architecture that scales to 3Tbps throughput;
 - (b) support up to 6 switches to be virtualised into a single virtual switch unit;
 - (c) split-chassis mechanism to ensure if the two switches fail to communicate with each other for some reason, the master switch will inform the slave switch to shut down all the interfaces on the slave switch to prevent disturbance to the network; and
 - (d) The switch must support MAC Retention, which allows a system of stackable switches to retain the MAC address of the primary switch for a fixed or indefinite time, even after multiple takeovers. This minimises the recalculation of protocols, such as Spanning Tree and Link Aggregation.
- 4.3.7 Must support the following simplified management features:
 - (a) Fully programmable RESTful web services interface with XML and JSON support. The API enables access to Command Line Interface (CLI) and individual management information base (MIB) objects;
 - (b) Intuitive CLI in a scriptable Python and Bash environment through the console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6;
 - (c) Powerful WebView Graphical Web Interface through HTTP and HTTPS over IPv4/IPv6;
 - (d) Full configuration and reporting using Simple Network Management Protocol (SNMP) v1/2/3 to facilitate third-party network management over IPv4/IPv6;
 - (e) File upload using USB, Trivial File Transfer Protocol (TFTP), FTP, SFTP or secure copy (SCP) over IPv4/IPv6;

- (f) Multiple microcode image support with fallback recovery; and
- (g) Local (on the flash) and remote server logging (Syslog) for events and commands

4.3.8 Must support the following high-resiliency and availability features:

- (a) Unified management, control and fabric-mesh virtual chassis technology;
- (b) Virtual chassis 1+N redundant supervisor manager;
- (c) Virtual chassis In-Service Software Upgrade (ISSU);
- (d) Smart continuous switching technology;
- (e) ITU-T G.8032/Y1344 2010: Ethernet Ring Protection;
- (f) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1D Spanning Tree Protocol (STP) and IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), Per-VLAN spanning tree (PVST+) and 1x1 STP mode;
- (g) IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP) and static LAG groups across modules;
- (h) Virtual Router Redundancy Protocol (VRRP) with tracking capabilities;
- (i) IEEE protocol auto-discovery;
- (j) Bidirectional Forwarding Detection (BFD);
- (k) Redundant and hot-swappable power supplies;
- (l) Redundant fans;
- (m) Hot-swappable fan tray; and
- (n) Built-in CPU protection against malicious attacks

4.3.9 Must support the following L3 protocols and features:

- (a) Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains (up to 128 instances) on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information;
- (b) Routing Information Protocol v1, v2, RIPng;
- (c) Open Shortest Path First Protocol V2, V3;
- (d) Border Gateway Protocol V4;
- (e) Virtual Routing Redundancy Protocol V2, V3;
- (f) Policy Based Routing;
- (g) DHCP relay;
- (h) Internet Control Message Protocol V6;
- (i) Network Discovery Protocol (NDP);
- (j) Internet Group Management Protocol (IGMP) v1/v2/v3 snooping;
- (k) Protocol Independent Multicast – Sparse-Mode (PIM-SM), Source Specific Multicast (PIM-SSM);
- (l) Protocol Independent Multicast – Dense-Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir);
- (m) Distance Vector Multicast Routing Protocol (DVMRP);
- (n) Multicast Listener Discovery (MLD) v1/v2 snooping; and

- (o) IPv4/IPv6 security ACL

4.3.10 Shall support the following Layer 2 protocols and features:

- (a) Ethernet – IEEE 802.3i 10BASE-T;
- (b) Fast Ethernet – IEEE 802.3u 100BASE-TX;
- (c) Gigabit Ethernet – IEEE 802.3z 1000BASE-X and IEEE 802.3ab 1000BASE-T;
- (d) 10G Ethernet - IEEE 802.3ae;
- (e) 25G Ethernet - IEEE 802.3by;
- (f) 40G Ethernet - IEEE 802.3ba;
- (g) 100G Ethernet – IEEE 802.3bm;
- (h) IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports;
- (i) IEEE 802.1ak (Multiple VLAN Registration Protocol MVRP);
- (j) Shortest Path Bridging (SPB) to provide mesh connection with all links active - IEEE 802.1aq;
- (k) Link Layer Discovery Protocol (LLDP) for exchanging information with neighbor – 802.1AB;
- (l) 4,094 VLAN IDs per switch;
- (m) VLAN trunking and tunneling – IEEE 802.1Q (VLAN) and IEEE 802.3Q tunneling (Q-in-Q);
- (n) Link aggregation – IEEE 802.3ad;
- (o) Spanning Tree Protocol (STP) – IEEE 802.1D;
- (p) Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1w;
- (q) Multiple Spanning Tree Protocol (MST) – IEEE 802.1s;
- (r) Per-VLAN Spanning Tree Plus (PVST+) and Per-VLAN Rapid Spanning Tree (PVRST);
- (s) Spanning-Tree Protocol Port Fast Forwarding;
- (t) Spanning-Tree Root Guard (STRG), which prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes;
- (u) User Port mechanism, which drops the packets or shuts down the port when it detects control packets like BGP, BPDU, RIP, OSPF, VRRP, DVMRP, PIM, ISIS, DHCP Server and DNS-REPLY;
- (v) Jumbo frames of 9,216 bytes;
- (w) Automatic media-dependent interface crossover (MDIX), which automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed; and
- (x) Unidirectional Link Detection Protocol (UDLD) allows unidirectional links caused by incorrect fibre-optic wiring or port faults to be detected and disabled on fibre-optic interfaces.

4.3.11 Shall support the following security features:

- (a) Per-port broadcast, multicast, and unicast storm control, which prevents faulty end stations from degrading overall systems performance;

- (b) Build in a mechanism which rate limits the traffic to the switching processor CPU, thereby ensuring stability, availability and predictable network performance;
 - (c) TACACS or RADIUS authentication to facilitate centralised control of the switch and restrict unauthorised users from altering the configuration; and
 - (d) Controls communication between peer users so that each session comprises a set of user ports and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate through network ports.
- 4.3.12 Early ARP discard - ARP packets destined for other hosts are discarded to reduce processing overhead and exposure to ARP DoS attacks.
- 4.3.13 Prevent IP address spoofing using the user port mechanism, which can either drop the packets or shut down the port.
- 4.3.14 Shall support the following Quality of Service (QoS) features:
- (a) Standard 802.1p CoS and DSCP field classification provided, using marking and reclassification on a per-packet basis by source and destination IP address, source and destination MAC address, or Layer 4 TCP or UDP port number;
 - (b) Automatic QoS that simplifies QoS configuration in voice-over IP (VoIP) networks by issuing interface and global switch commands to detect IP phones, classify traffic, and help enable egress queue configuration;
 - (c) Control-plane and data-plane QoS ACLs on all ports help ensure proper marking on a per-packet basis;
 - (d) Strict priority queuing to ensure that the highest-priority packets (such as voice or other mission-critical packets) are serviced ahead of all other traffic;
 - (e) Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps;
 - (f) Ingress policing and egress shaping to provide asynchronous data flows upstream and downstream from the end station;
 - (g) Support for end-to-end head-of-line (E2E-HOL) blocking prevention, IEEE 802.1Qbb Priority-based Flow Control (PFC) and IEEE 802.3x Flow Control (FC) for congestion avoidance; and
 - (h) Eight egress queues per port help enable differentiated management of different traffic types across the stack.
- 4.3.15 Must support multipath Ethernet technologies (SPB) that combine the reliability and scalability benefits of Layer 3 routing with the flexibility of Layer 2 networks to enable the ability to extend Layer 2 (VLANs) across multiple datacenters using open standard protocols

- 4.3.16 Shall support the following performance and scalability numbers:
- (a) Switching fabric capacity of at least 4Tbps;
 - (b) At least 2900Mpps forwarding rate;
 - (c) Hardware-based multicasting replication;
 - (d) At least 228,000 unicast MAC addresses under VLAN;
 - (e) wire-rate performance on every single port;
 - (f) Mean time between failure of at least 208,000hrs; and
 - (g) Data buffer of at least 32MB.
- 4.3.17 Shall support out-of-band management and monitoring capability that bypasses the network modules and offers remote management to the management module directly
- 4.3.18 Shall support high-availability hardware Virtual Extensible LAN (VXLAN) Virtual Tunnel End Point (VTEP) gateways to support layer 2 overlay networks, which segment and tunnel device traffic through a data center or cloud network infrastructure.
- 4.3.19 Shall support Virtual eXtensible LAN (VXLAN) Snooping feature, which attempts to detect and identify VXLAN traffic by sampling packets to determine if they are VXLAN encapsulated packets.
- 4.3.20 Shall support a built-in DHCP server providing IPv4 and IPv6 addresses to end devices.

4.4 Server Farm Switch and Demilitarised Switch Requirements

- 4.4.1 Must be designed for highly scalable 1GE/10GE/25GE/40GE/100GE Gigabit Ethernet networks.
- 4.4.2 Must be in a one-rack unit (RU) form factor without the requirement of additional power tray accessories.
- 4.4.3 Must support redundant and hot-swappable slide-in power supplies.
- 4.4.4 Must come with a 4 + 1 individual variable-speed fan module for redundancy purposes and is hot-swappable.
- 4.4.5 For data center applications, the switch must support front-to-back or back-to-front cooling for Hot/Cold aisle deployment.
- 4.4.6 Shall meet the requirements stated in Clause 4.2.5 to Clause 4.2.9.
- 4.4.7 Shall support the following Layer 2 protocols and features:
- (a) Gigabit Ethernet – IEEE 802.3z 1000BASE-X and IEEE 802.3ab 1000BASE-T;
 - (b) 10G Ethernet - IEEE 802.3ae;
 - (c) 25G Ethernet - IEEE 802.3by;

- (d) 40G Ethernet - IEEE 802.3ba;
- (e) 100G Ethernet – IEEE 802.3bm;
- (f) IEEE 802.3x full duplex on 1000BASE-T ports;
- (g) IEEE 802.1ak (Multiple VLAN Registration Protocol MVRP)
- (h) Shortest Path Bridging (SPB) to provide mesh connection with all links active - IEEE 802.1aq;
- (i) Link Layer Discovery Protocol (LLDP) for exchanging information with neighbor – 802.1AB;
- (j) 4,094 VLAN IDs per switch;
- (k) VLAN trunking and tunneling – IEEE 802.1Q (VLAN) and IEEE 802.3Q tunneling (Q-in-Q);
- (l) Link aggregation – IEEE 802.3ad;
- (m) Spanning Tree Protocol (STP) – IEEE 802.1D;
- (n) Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1w;
- (o) Multiple Spanning Tree Protocol (MST) – IEEE 802.1s;
- (p) Per-VLAN Spanning Tree Plus (PVST+) and Per-VLAN Rapid Spanning Tree (PVRST);
- (q) Spanning-Tree Protocol Port Fast Forwarding;
- (r) Spanning-Tree Root Guard (STRG) which prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes;
- (s) User Port mechanism which drop the packets or shuts down the port when it detect control packets like BGP, BPDU, RIP, OSPF, VRRP, DVMRP, PIM, ISIS, DHCPSEVER and DNS-REPLY;
- (t) Jumbo frames of 9,216 bytes;
- (u) Automatic media-dependent interface crossover (MDIX) which automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed; and
- (v) Unidirectional Link Detection Protocol (UDLD) that allows unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.

4.4.8 Shall support the following Multicast protocols and features:

- (a) IGMPv1/v2/v3 snooping and Multicast Listener Discovery (MLD) v1/v2 for fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors;
- (b) Up to 40K multicast flow per stack; and
- (c) Multicast VLAN Registration (MVR) continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.

4.4.9 Shall support the following security features:

- (a) Per-port broadcast, multicast, and unicast storm control, which prevents faulty end stations from degrading overall systems performance;

- (b) Build in a mechanism which rates limit the traffic to the switching processor CPU thereby ensuring stability, availability and predictable network performance;
 - (c) TACACS or RADIUS authentication to facilitate centralized control of the switch and restrict unauthorized users from altering the configuration; and
 - (d) Controls communication between peer users in a way that each session comprises of a set of user ports and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate through network ports.
- 4.4.10 Shall support out-of-band management and monitoring capability that bypasses the network modules and offers remote management to the management module directly
- 4.4.11 Shall support the Virtual eXtensible LAN (VXLAN) Snooping feature, which attempts to detect and identify VXLAN traffic by sampling packets to determine if they are VXLAN-encapsulated packets.
- 4.4.12 The switch will attempt to detect and identify remote applications by scanning IP packets and comparing the packets to pre-defined bit patterns (application signatures). Once an application is identified, the switch collects and stores information about the application flow in a database on the local switch
- 4.4.13 Shall support a built-in DHCP server providing IPv4 and IPv6 addresses to end devices.
- 4.4.14 Server Farm Switch shall have at least 48 ports of 1GE/10GE BaseT with 6 ports of 100GE QSFP28.
- 4.4.15 The Server Farm Switch shall support the following performance and scalability numbers:
- (a) Switching fabric capacity of at least 2.16Tbps;
 - (b) At least 1600Mpps forwarding rate;
 - (c) Hardware-based multicasting replication;
 - (d) At least 228,000 unicast MAC addresses under VLAN;
 - (e) wire-rate performance on every single port;
 - (f) Data buffer of at least 32MB.
- 4.4.16 The Demilitarised Switch shall have at least 24 ports of 1GE/10GE BaseT, 2 ports of 1GE/10GE SFP+ with 2 ports of 100GE QSFP28.
- 4.4.17 The Demilitarised switch shall support the following performance and scalability numbers:
- (a) Switching fabric capacity of at least 920Gbps;
 - (b) At least 684Mpps forwarding rate;
 - (c) Hardware-based multicasting replication;

- (d) At least 228,000 unicast MAC addresses under VLAN;
- (e) wire-rate performance on every single port;
- (f) Data buffer of at least 32MB.

4.5 Layer 3 Power over Ethernet (POE) Network Access Switch Requirements

The Layer 3 Power over Ethernet (POE) Network Access Switch:

- 4.5.1 The proposed switch should be a fixed-configuration chassis in a 1U form factor with 48 100M/1G/2.5G/5G multigigabit 95W of POE ports, two 100G/200G QSFP56 VFL/stacking ports, USB, RJ45 console, EMP and one uplink module expansion slot.
- 4.5.2 Should be able to come with 600W, 1200W, or 2000W, three different types of power supply to cater to different POE needs.
- 4.5.3 Must support the QSFP28 VFL/Stacking ports to be uplinked in a non-VC configuration.
- 4.5.4 Should have all the RJ-45 and fibre ports supporting 256-bit MACsec.
- 4.5.5 Should support a 1+1 hot-swappable redundant power supply, in which both the primary and backup power supply units are internal (slot-in) and removable to allow for easier maintenance and replacement.
- 4.5.6 The proposed switch supports balanced and unbalanced load sharing for PoE. Any supported PoE PSU can be mixed to fulfil the PoE budget while providing system redundancy.
- 4.5.7 Shall support virtual chassis technology such as:
 - (a) The switch must support virtual chassis technology that creates a highly resilient single unified system of up to 8 switches;
 - (b) The switch must provide a unified data plane, unified configuration, and single IP address management for a group of stacked switches;
 - (c) Each switch must be able to operate as both a master controller and fording processor in a virtual chassis environment. The virtual chassis must provide 1:N master redundancy allowing each stack member to serve as a master to provide the highest level of redundancy for data forwarding;
 - (d) The switch must support seamless failover of the virtual chassis master with no downtime during the VC master failover to ensure continuous operation and no user interruption;
 - (e) The switch must support an aggregate of at least 1.6Tbps virtual chassis interconnect that allows customers to build a unified, highly resilient switching system, one switch at a time;
 - (f) The virtual chassis must support redundant fabric interconnect links in the form of a loop to maintain virtual chassis integrity in case of intermediate switch failure;

- (g) The switch must support virtual chassis master configuration management and ensure that all switches are automatically upgraded when the master switch receives a new software version;
- (h) Automatic software version checking and updating must be supported to ensure that all virtual chassis members have the same software version;
- (i) The switch must support synchronization of configuration between the switches in the same virtual chassis topology;
- (j) The switch must support establishing a virtual chassis topology with other switches located geographically apart;
- (k) The switch must support the establishment of a virtual chassis topology with different switch variants within the product class;
- (l) The switch in a virtual chassis configuration must support In Service Software Upgrade, which allows the upgrade of individual switch firmware one at a time without rebooting the entire virtual chassis. During the software upgrade, network traffic should have a minimum interruption;
- (m) The switch must support a distributed switching and routing architecture that allows switching and routing functions to be distributed to individual switches in the virtual chassis to avoid performance bottlenecks at the central processor and
- (n) The switch must support MAC Retention, which allows a system of stackable switches to retain the MAC address of the primary switch for a fixed or indefinite time, even after multiple takeovers. This minimises the recalculation of protocols, such as Spanning Tree and Link Aggregation

4.5.8 Shall support Power over Ethernet (PoE) technology such as

- (a) IEEE 802.3af PoE up to 15.4 watts of power per port;
- (b) IEEE 802.3at PoE+ up to 30 watts of power per port;
- (c) IEEE 802.3bt type 4 compliant PoE with up to 95W of PoE per port;
- (d) POE power must be able to be provided to all 48 ports concurrently; and
- (e) The switch must be able to assign disconnect priority to PoE powered device. In the event of an inadequate PoE budget in the system, the switch should be capable of shutting down low-priority PoE devices to ensure critical PoE-powered devices are operational.

4.5.9 Shall support the following Layer 3 protocols and features:

- (a) Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains (up to 8 instances) on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information;
- (b) Routing Information Protocol v1, v2, RIPng;
- (c) Open Shortest Path First Protocol V2, V3;
- (d) Border Gateway Protocol V4;

- (e) Virtual Routing Redundancy Protocol V2, V3;
- (f) Policy Based Routing;
- (g) DHCP relay;
- (h) Internet Control Message Protocol V6;
- (i) Network Discovery Protocol (NDP);
- (j) Internet Group Management Protocol (IGMP) v1/v2/v3 snooping;
- (k) Protocol Independent Multicast – Sparse-Mode (PIM-SM), Source Specific Multicast (PIM-SSM);
- (l) Protocol Independent Multicast – Dense-Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir);
- (m) Distance Vector Multicast Routing Protocol (DVMRP);
- (n) Multicast Listener Discovery (MLD) v1/v2 snooping; and
- (o) IPv4/IPv6 security ACL.

4.5.10 Shall support the following Layer 2 protocols and features:

- (a) Ethernet - IEEE 802.3i 10BASE-T;
- (b) Fast Ethernet - IEEE 802.3u 100BASE-TX;
- (c) Gigabit Ethernet - IEEE 802.3z 1000BASE-X and IEEE 802.3ab 1000BASE-T;
- (d) MultiGig Ethernet - IEEE 802.3bz 2.5/5 GigE;
- (e) 10 Gigabit Ethernet – IEEE 802.3ae;
- (f) IEEE 802.3by 25 GigE;
- (g) IEEE 802.3ba 40GBASE-X;
- (h) IEEE 802.3bm 100 GigE;
- (i) IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports;
- (j) 4,000 VLAN IDs with up to 1,000 active VLANs;
- (k) VLAN trunking and tunneling – IEEE 802.1Q (VLAN) and IEEE 802.3Q tunneling (Q-in-Q);
- (l) Energy Efficient Ethernet – IEEE 802.3az (EEE);
- (m) Link aggregation – IEEE 802.3ad;
- (n) Ethernet Ring Protection (ERPV2) – ITU-T G.8032/Y.1344 2010;
- (o) Spanning Tree Protocol (STP) – IEEE 802.1D;
- (p) Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1w;
- (q) Multiple Spanning Tree Protocol (MST) – IEEE 802.1s;
- (r) Per-VLAN Spanning Tree Plus (PVST+) and Per-VLAN Rapid Spanning Tree (PVRST);
- (s) Spanning-Tree Protocol Port Fast Forwarding;
- (t) Spanning-Tree Root Guard (STRG), which prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes;
- (u) Port mechanism to shut down the port when it detects control packets like BPDU, Spoofing, RIP, DHCP-server and DHCP-reply;
- (v) Loopback detection, which automatically detects and prevents the L2 forwarding loop even when the port is connected to a hub and a physical loop is formed at the hub;

- (w) Jumbo frames of 9,216 bytes;
 - (x) Automatic media-dependent interface crossover (MDIX), which automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed; and
 - (y) Unidirectional Link Detection Protocol (UDLD) allows unidirectional links caused by incorrect fibre-optic wiring or port faults to be detected and disabled on fibre-optic interfaces.
- 4.5.11 Shall provide the following 802.1x user access and their related authentication features:
- (a) If AAA server(s) is inaccessible, the switch shall support inaccessible authentication bypass such that it provides a configurable alternative on the switch to grant critical port network access in a locally specified VLAN;
 - (b) 802.1x Unidirectional Controlled Port, which allows the Wake-on-LAN (WoL) magic packets to reach a workstation attached to an unauthorized 802.1x switch port;
 - (c) For IP devices without 802.1x supplicant, the switch shall proxy an 802.1x authentication request based on the device's MAC address;
 - (d) Multiple Authentication, which allows an IP phone with an IEEE 802.1x supplicant and a single host behind the IP phone to authenticate into the network independently;
 - (e) Flexible authentication that supports multiple authentication mechanisms, including 802.1X, MAC Authentication Bypass and web authentication using a single, consistent configuration; and
 - (f) Allow MAC-address authentication to be executed before IEEE 802.1x authentication. This is to ensure that the blacklisted device cannot gain access to the network via IEEE 802.1x authentication.
- 4.5.12 Shall support Intuitive CLI in a scriptable Python and Bash environment through the console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6
- 4.5.13 Must support mDNS bridging or proxy services to allow mDNS services provided by wired mDNS to be consumed by wireless user devices.
- 4.5.14 Must support 802.1aq Shortest Path Bridging to create a fully meshed architecture with an optimised network path and support for cloud services.
- 4.5.15 Must support application analytics and monitoring capability to allow a comprehensive view of more than 2000 applications running on the network. Visibility can be used to optimise the network's performance and apply application-level control.
- 4.5.16 Must support deep packet inspection (DPI) technology to allow real-time classification of flows at the application level, enabling monitoring and QoS treatment for priority and bandwidth to selected applications.

- 4.5.17 Shall support the following performance and scalability numbers:
- (a) Switching fabric capacity of at least 1880Gbps;
 - (b) At least 1398Mpps forwarding rate ;
 - (c) Full wire-rate capability on all interfaces;
 - (d) Hardware-based multicasting replication;
 - (e) At least 1,000 IGMP groups and 1,000 multicast routes;
 - (f) At least 128,000 unicast MAC addresses under VLAN;
 - (g) At least 116K IPv4 routes;
 - (h) At least 58K IPv6 routes;
 - (i) At least 64K ARP entries; and
 - (j) Front to Back airflow supporting Data Center deployment.
- 4.5.18 Provides extensive debug diagnostic commands and system health checks within the switch. These include (1) the ability to capture and store hardware failure and environmental information into nonvolatile memory and (2) boot-time and runtime diagnostics that perform hardware-specific fault-detection tests and take appropriate corrective action in response to diagnostics test results
- 4.5.19 Must be able to provide dynamic IP addresses on lease for client interfaces on a network. It manages a pool of IP addresses and information about client configuration parameters. The DHCP server obtains an IP address request from the client interfaces. After receiving the requests, the DHCP server assigns an IP address, a lease period, and other IP configuration parameters, such as the subnet mask and the default gateway.

4.6 Layer 3 Intelligent Network Access Switch Requirements

- 4.6.1 The proposed switch should be a Gigabit Ethernet L3 fixed configuration chassis in a 1U form factor with 48 RJ-45 10/100/1000 Base-T ports, two 40/100G QSFP28 VFL/stacking ports, four SFP28 (1G/10G/25G) ports, USB, RJ45 console and EMP.
- 4.6.2 Must support the QSFP28 VFL/Stacking ports to be uplinked in a non-VC configuration.
- 4.6.3 Should have all the RJ-45 and SFP28 ports support 256-bit MACsec.
- 4.6.4 Should support a 1+1 hot-swappable redundant power supply, in which both the primary and backup power supply units are internal (slot-in) and removable to allow for easier maintenance and replacement.
- 4.6.5 Shall support virtual chassis technology such as:
- (a) The switch must support virtual chassis technology that creates a highly resilient single unified system of up to 8 switches;

- (b) The switch must provide a unified data plane, unified configuration, and single IP address management for a group of stacked switches;
- (c) Each switch must be able to operate as both a master controller and forwarding processor in a virtual chassis environment. The virtual chassis must provide 1:N master redundancy, allowing each stack member to serve as a master to provide the highest level of redundancy for data forwarding;
- (d) The switch must support seamless failover of the virtual chassis master with no downtime during the VC master failover to ensure continuous operation and no user interruption;
- (e) The switch must support an aggregate of at least 1.6Tbps virtual chassis interconnect that allows customers to build a unified, highly resilient switching system, one switch at a time;
- (f) The virtual chassis must support redundant fabric interconnect links in the form of a loop to maintain virtual chassis integrity in case of intermediate switch failure;
- (g) The switch must support virtual chassis master configuration management and ensure all switches are automatically upgraded when the master switch receives a new software version.
- (h) Automatic software version checking and updating must be supported to ensure that all virtual chassis members have the same software version;
- (i) The switch must support synchronisation of configuration between the switches in the same virtual chassis topology;
- (j) The switch must support the establishment of a virtual chassis topology with other switches located geographically up to 10km away;
- (k) The switch must support the establishment of a virtual chassis topology with different switch variants within the product class;
- (l) The switch in a virtual chassis configuration must support In Service Software Upgrade, which allows the upgrade of individual switch firmware one at a time without rebooting the entire virtual chassis. During the software upgrade, network traffic should have a minimum interruption;
- (m) The switch must support a distributed switching and routing architecture that allows switching and routing functions to be distributed to individual switches in the virtual chassis to avoid performance bottlenecks at the central processor; and
- (n) The switch must support MAC Retention, which allows a stackable switch system to retain the primary switch's MAC address for a fixed or indefinite time, even after multiple takeovers. This minimises the recalculation of protocols, such as Spanning Tree and Link Aggregation.

4.6.6 Shall support the following Layer 3 protocols and features:

- (a) Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains (up to 8 instances) on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information.
- (b) Routing Information Protocol v1, v2, RIPng.
- (c) Open Shortest Path First Protocol V2, V3
- (d) Border Gateway Protocol V4
- (e) Virtual Routing Redundancy Protocol V2, V3
- (f) Policy Based Routing
- (g) DHCP relay
- (h) Internet Control Message Protocol V6
- (i) Network Discovery Protocol (NDP)
- (j) Internet Group Management Protocol (IGMP) v1/v2/v3 snooping
- (k) Protocol Independent Multicast – Sparse-Mode (PIM-SM), Source-Specific Multicast (PIM-SSM),
- (l) Protocol Independent Multicast – Dense-Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir)
- (m) Distance Vector Multicast Routing Protocol (DVMRP)
- (n) Multicast Listener Discovery (MLD) v1/v2 snooping
- (o) IPv4/IPv6 security ACL

4.6.7 Shall support the following Layer 2 protocols and features:

- (a) Ethernet - IEEE 802.3i 10BASE-T;
- (b) Fast Ethernet - IEEE 802.3u 100BASE-TX;
- (c) Gigabit Ethernet - IEEE 802.3z 1000BASE-X and IEEE 802.3ab 1000BASE-T;
- (d) MultiGig Ethernet - IEEE 802.3bz 2.5/5 GigE;
- (e) 10 Gigabit Ethernet – IEEE 802.3ae;
- (f) IEEE 802.3by 25 GigE;
- (g) IEEE 802.3ba 40GBASE-X;
- (h) IEEE 802.3bm 100 GigE;
- (i) IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports;
- (j) 4,000 VLAN IDs with up to 1,000 active VLANs;
- (k) VLAN trunking and tunneling – IEEE 802.1Q (VLAN) and IEEE 802.3Q tunneling (Q-in-Q);
- (l) Energy Efficient Ethernet – IEEE 802.3az (EEE);
- (m) Link aggregation – IEEE 802.3ad;
- (n) Ethernet Ring Protection (ERPV2) – ITU-T G.8032/Y.1344 2010;
- (o) Spanning Tree Protocol (STP) – IEEE 802.1D;
- (p) Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1w;
- (q) Multiple Spanning Tree Protocol (MST) – IEEE 802.1s;
- (r) Per-VLAN Spanning Tree Plus (PVST+) and Per-VLAN Rapid Spanning Tree (PVRST);
- (s) Spanning-Tree Protocol Port Fast Forwarding;

- (t) Spanning-Tree Root Guard (STRG) which prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes;
- (u) Port mechanism to shut down the port when it detects control packets like BPDU, Spoofing, RIP, dhcp-server and dhcp-reply;
- (v) Loopback detection, which automatically detects and prevents the L2 forwarding loop even when the port is connected to a hub and physical loop is formed at the hub;
- (w) Jumbo frames of 9,216 bytes;
- (x) Automatic media-dependent interface crossover (MDIX), which automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed; and
- (y) Unidirectional Link Detection Protocol (UDLD) that allows unidirectional links caused by incorrect fibre-optic wiring or port faults to be detected and disabled on fibre-optic interfaces

4.6.8 Shall provide the following 802.1x user access and their related authentication features:

- (a) If the AAA server(s) is inaccessible, the switch shall support inaccessible authentication bypass such that it provides a configurable alternative on the switch to grant critical port network access in a locally specified VLAN;
- (b) 802.1x Unidirectional Controlled Port, which allows the Wake-on-LAN (WoL) magic packets to reach a workstation attached to an unauthorised 802.1x switch port;
- (c) For IP devices without 802.1x supplicant, the switch shall proxy an 802.1x authentication request based on the device's MAC address;
- (d) Multiple Authentication, which allows an IP phone with an IEEE 802.1x supplicant and a single host behind the IP phone to authenticate into the network independently;
- (e) Flexible authentication that supports multiple authentication mechanisms, including 802.1X, MAC Authentication Bypass and web authentication using a single, consistent configuration; and
- (f) Allow MAC-address authentication to be executed before IEEE 802.1x authentication. This is to ensure that blacklisted device cannot gain access to the network via IEEE 802.1x authentication

4.6.9 Shall support Intuitive CLI in a scriptable Python and Bash environment through the console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6

4.6.10 Must support mDNS bridging or proxy services to allow mDNS services provided by wired mDNS to be consumed by wireless user devices.

4.6.11 Must support 802.1aq Shortest Path Bridging to create a fully meshed architecture with an optimised network path and support for cloud services.

- 4.6.12 Must support application analytics and monitoring capability to allow a comprehensive view of more than 2000 applications running on the network. This visibility can be used to optimise the network's performance and apply application-level control.
- 4.6.13 Must support deep packet inspection (DPI) technology to allow real-time classification of flows at the application level, enabling monitoring and QoS treatment to prioritise and bandwidth to selected applications.
- 4.6.14 Shall support the following performance and scalability numbers:
- (a) Switching fabric capacity of at least 696Gbps ;
 - (b) At least 517Mpps forwarding rate;
 - (c) Full wire-rate capability on all interfaces;
 - (d) Hardware-based multicasting replication;
 - (e) At least 1,000 IGMP groups and 1,000 multicast routes;
 - (f) At least 128,000 unicast MAC addresses under VLAN;
 - (g) At least 116K IPv4 routes;
 - (h) At least 58K IPv6 routes;
 - (i) At least 64K ARP entries; and
 - (j) Front-to-back airflow supporting Data Center deployment.
- 4.6.15 Provides extensive debug diagnostic commands and system health checks within the switch. These include (1) the ability to capture and store hardware failure and environmental information into nonvolatile memory and (2) boot-time and runtime diagnostics that perform hardware-specific fault-detection tests and take appropriate corrective action in response to diagnostics test results
- 4.6.16 Must be able to provide dynamic IP addresses on lease for client interfaces on a network. It manages a pool of IP addresses and information about client configuration parameters. The DHCP server obtains an IP address request from the client interfaces. After receiving the requests, the DHCP server assigns an IP address, a lease period, and other IP configuration parameters, such as the subnet mask and the default gateway.

4.7 Transit Switch Requirements

- 4.7.1 The proposed switch should be a Gigabit Ethernet L3 fixed configuration chassis in a 1U form factor with 24 RJ-45 10/100/1000 Base-T ports, two 40/100G QSFP28 VFL/stacking ports, four SFP28 (1G/10G/25G) uplink ports, USB, RJ45 console and EMP.
- 4.7.2 Must support the QSFP28 VFL/Stacking ports to be uplinked in a non-VC configuration.
- 4.7.3 Should have all the RJ-45 and SFP28 ports support 256-bit MACsec.

- 4.7.4 Should support a 1+1 hot-swappable redundant power supply, in which both the primary and backup power supply units are internal (slot-in) and removable to allow for easier maintenance and replacement.
- 4.7.5 Shall support virtual chassis technology such as:
- (a) The switch must support virtual chassis technology that creates a highly resilient single unified system of up to 8 switches;
 - (b) The switch must provide a unified data plane, unified configuration, and single IP address management for a group of stacked switches;
 - (c) Each switch must be able to operate as both a master controller and forwarding processor in a virtual chassis environment. The virtual chassis must provide 1:N master redundancy, allowing each stack member to serve as a master to provide the highest level of redundancy for data forwarding;
 - (d) The switch must support seamless failover of the virtual chassis master with no downtime during the VC master failover to ensure continuous operation and no user interruption;
 - (e) The switch must support an aggregate of at least 1.6Tbps virtual chassis interconnect that allows customers to build a unified, highly resilient switching system, one switch at a time;
 - (f) The virtual chassis must support redundant fabric interconnect links in the form of a loop to maintain virtual chassis integrity in the case of intermediate switch failure;
 - (g) The switch must support virtual chassis master configuration management and ensure that all switches are automatically upgraded when the master switch receives a new software version;
 - (h) Automatic software version checking and updating must be supported to ensure that all virtual chassis members have the same software version;
 - (i) The switch must support synchronisation of configuration between the switches in the same virtual chassis topology;
 - (j) The switch must support the establishment of a virtual chassis topology with other switches located geographically up to 10km away;
 - (k) The switch must support the establishment of a virtual chassis topology with different switch variants within the product class;
 - (l) The switch in a virtual chassis configuration must support In Service Software Upgrade, which allows the upgrade of individual switch firmware one at a time without rebooting the entire virtual chassis. During the software upgrade, network traffic should have a minimum interruption;
 - (m) The switch must support a distributed switching and routing architecture that allows switching and routing functions to be distributed to individual switches in the virtual chassis to avoid performance bottlenecks at the central processor; and

- (n) The switch must support MAC Retention, which allows a stackable switch system to retain the primary switch's MAC address for a fixed or indefinite time, even after multiple takeovers. This minimises the recalculation of protocols, such as Spanning Tree and Link Aggregation.

4.7.6 Shall support the following Layer 3 protocols and features:

- (a) Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains (up to 8 instances) on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information;
- (b) Routing Information Protocol v1, v2, RIPv2;
- (c) Open Shortest Path First Protocol V2, V3;
- (d) Border Gateway Protocol V4;
- (e) Virtual Routing Redundancy Protocol V2, V3;
- (f) Policy Based Routing;
- (g) DHCP relay;
- (h) Internet Control Message Protocol V6;
- (i) Network Discovery Protocol (NDP);
- (j) Internet Group Management Protocol (IGMP) v1/v2/v3 snooping;
- (k) Protocol Independent Multicast – Sparse-Mode (PIM-SM), Source-Specific Multicast (PIM-SSM);
- (l) Protocol Independent Multicast – Dense-Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-Bidir);
- (m) Distance Vector Multicast Routing Protocol (DVMRP);
- (n) Multicast Listener Discovery (MLD) v1/v2 snooping; and
- (o) IPv4/IPv6 security ACL.

4.7.7 Shall support the following Layer 2 protocols and features:

- (a) Ethernet - IEEE 802.3i 10BASE-T;
- (b) Fast Ethernet - IEEE 802.3u 100BASE-TX;
- (c) Gigabit Ethernet - IEEE 802.3z 1000BASE-X and IEEE 802.3ab 1000BASE-T;
- (d) MultiGig Ethernet - IEEE 802.3bz 2.5/5 GigE;
- (e) 10 Gigabit Ethernet – IEEE 802.3ae;
- (f) IEEE 802.3by 25 GigE;
- (g) IEEE 802.3ba 40GBASE-X;
- (h) IEEE 802.3bm 100 GigE;
- (i) IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports;
- (j) 4,000 VLAN IDs with up to 1,000 active VLANs;
- (k) VLAN trunking and tunneling – IEEE 802.1Q (VLAN) and IEEE 802.3Q tunneling (Q-in-Q);
- (l) Energy Efficient Ethernet – IEEE 802.3az (EEE);
- (m) Link aggregation – IEEE 802.3ad;
- (n) Ethernet Ring Protection (ERPV2) – ITU-T G.8032/Y.1344 2010;

- (o) Spanning Tree Protocol (STP) – IEEE 802.1D;
- (p) Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1w;
- (q) Multiple Spanning Tree Protocol (MST) – IEEE 802.1s;
- (r) Per-VLAN Spanning Tree Plus (PVST+) and Per-VLAN Rapid Spanning Tree (PVRST);
- (s) Spanning-Tree Protocol Port Fast Forwarding;
- (t) Spanning-Tree Root Guard (STRG), which prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes;
- (u) Port mechanism to shut down the port when it detects control packets like BPDU, Spoofing, RIP, dhcp-server and dhcp-reply;
- (v) Loopback detection, which automatically detects and prevents L2 forwarding loops even when the port is connected to a hub and a physical loop is formed at the hub;
- (w) Jumbo frames of 9,216 bytes;
- (x) Automatic media-dependent interface crossover (MDIX), which automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed; and
- (y) Unidirectional Link Detection Protocol (UDLD) that allows unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces

4.7.8 Shall provide the following 802.1x user access and their related authentication features:

- (a) If the AAA server(s) is inaccessible, the switch shall support inaccessible authentication bypass such that it provides a configurable alternative on the switch to grant critical port network access in a locally specified VLAN;
- (b) 802.1x Unidirectional Controlled Port, which allows the Wake-on-LAN (WoL) magic packets to reach a workstation attached to an unauthorised 802.1x switch port;
- (c) For IP devices without 802.1x supplicant, the switch shall proxy an 802.1x authentication request based on the device's MAC address;
- (d) Multiple Authentication, which allows an IP phone with an IEEE 802.1x supplicant and a single host behind the IP phone to authenticate into the network independently;
- (e) Flexible authentication supports multiple authentication mechanisms, including 802.1X, MAC Authentication Bypass and web authentication using a single, consistent configuration; and
- (f) Allow MAC-address authentication to be executed before IEEE 802.1x authentication. This is to ensure that the blacklisted device cannot gain access to the network via IEEE 802.1x authentication.

4.7.9 Shall support Intuitive CLI in a scriptable Python and Bash environment through the console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6

- 4.7.10 Must support mDNS bridging or proxy services to allow mDNS services provided by wired mDNS to be consumed by wireless user devices.
- 4.7.11 Must support 802.1aq Shortest Path Bridging to create a fully meshed architecture with optimized network path and cloud services support.
- 4.7.12 Must support application analytics and monitoring capability to allow a comprehensive view of more than 2000 applications running on the network. Visibility can be used to optimize the network's performance and apply application-level control.
- 4.7.13 Must support deep packet inspection (DPI) technology to allow real-time classification of flows at the application level, enabling monitoring and QoS treatment to prioritise and bandwidth to selected applications.
- 4.7.14 Shall support the following performance and scalability numbers:
 - (a) Switching fabric capacity of at least 648Gbps;
 - (b) At least 482Mpps forwarding rate;
 - (c) Full wire-rate capability on all interfaces;
 - (d) Hardware-based multicasting replication;
 - (e) At least 1,000 IGMP groups and 1,000 multicast routes;
 - (f) At least 128,000 unicast MAC addresses under VLAN;
 - (g) At least 116K IPv4 routes;
 - (h) At least 58K IPv6 routes;
 - (i) At least 64K ARP entries; and
 - (j) Front-to-back airflow supporting Data Center deployment.
- 4.7.15 Provides extensive debug diagnostic commands and system health checks within the switch. These include (1) the ability to capture and store hardware failure and environmental information into nonvolatile memory and (2) boot-time and runtime diagnostics that perform hardware-specific fault-detection tests and take appropriate corrective action in response to diagnostics test results.
- 4.7.16 Must be able to provide dynamic IP addresses on lease for client interfaces on a network. It manages a pool of IP addresses and information about client configuration parameters. The DHCP server obtains an IP address request from the client interfaces. After obtaining the requests, the DHCP server assigns an IP address, a lease period, and other IP configuration parameters, such as the subnet mask and the default gateway.

4.8 Wireless Network Solution Requirements

General Requirement

- 4.8.1 The WLAN solution shall cater for at least three (3) wireless users, namely staff/teacher, student, and guest/visitor, with varied access levels.

- 4.8.2 Shall ensure the traffic between wireless end hosts and wireless access points is secured and encrypted.
- 4.8.3 Shall provide optimum wireless coverage and optimum wireless capacity in classrooms, including density and throughput, to support the conduct of seasonal e-Exams to allow concurrent downloads and uploads of exam materials to/from computing devices used for e-Exams.
- 4.8.4 Shall have the wireless capacity for one full level of students (120 users) at the School's Auditorium, Dinning Hall (Arena), Function Room and Audio Visual Aided Room.
- 4.8.5 Shall support network-wide Policy Based QoS traffic management capability to optimise wireless network bandwidth utilization
- 4.8.6 Shall have network-wide centralised security policies across wired and wireless networks.
- 4.8.7 Shall have the capability to eliminate sticky clients so as to steer each wireless client device to the best wireless access point on the wireless network to achieve optimal wireless performance.
- 4.8.8 Shall have Wireless Intrusion Prevention System (WIPS) to provide robust protection for the entire wireless network, including detection, location, and mitigation of security penetration and Denial of Service (DoS) threats.
- 4.8.9 Shall have the flexibility to configure wireless policy, management, or security settings at any time through centralised provisioning and management. The WLAN solution shall rely on a distributed data plane.
- 4.8.10 Shall have network-wide quality of services (QoS) for voice and video, across wired and wireless networks

Architecture Overview

- 4.8.11 The Wireless LAN (WLAN) solution shall be based on IEEE 802.11 and shall be Wi-Fi Alliance certified for Data and Voice.
- 4.8.12 Shall propose a distributed control function (no centralised controller) with native support for redundancy, eliminating traffic bottlenecks, and lowering latency.
- 4.8.13 Shall rely on a distributed data plane.
- 4.8.14 Shall allow two types of deployment with Centralised Management:
 - (a) "Large deployment" for a multi-site deployment with Access Points spread over multiple management VLANs that may operate in a different RF environment.

- (b) “Cloud deployment” is for any deployment (single or multi-site) with centralised management in the cloud.

The solution shall offer advanced features like Intrusion Detection/Prevention or a Captive Portal to manage guests’ or BYOD connections without additional third-party components for both deployment types. The solution shall also support advanced wireless services, using Bluetooth LE and ZigBee technologies or advanced servers included in the solution. This is without the addition of third-party components.

- 4.8.15 Shall propose a centralised management function, irrespective of the deployment model.
- 4.8.16 Shall propose a centralised management function based on an embedded and secure WEB GUI, irrespective of the deployment model.
- 4.8.17 In addition to a centralised management function, all Access Points of the WLAN solution shall propose a dedicated web interface to monitor and configure a single AP in the global infrastructure, irrespective of the deployment model.
- 4.8.18 The centralised management function shall be able to handle wired equipment (switches) management for a “unified management” approach.
- 4.8.19 The WLAN solution should rely on a simple licensing model: one license per AP, including all functions (basic or advanced) handled by the AP.
- 4.8.20 The centralised management function shall ensure the integrity of the WLAN solution by supporting optimal monitoring, management, and security features.
- 4.8.21 The centralised management function shall allow access to all Wireless Intrusion Prevention System (wIPS) and Wireless Intrusion Detection System (wIDS) features.
- 4.8.22 The centralised management function shall provide insight at the application layer (e.g. facebook.com, youtube.com, salesforce.com...) based on an application signature file, even when the applications operate over HTTP or HTTPS protocols. It shall also enable control of those applications.
- 4.8.23 The centralised management function shall be collocated with the Guest and BYOD management applications.
- 4.8.24 Moving from the Wi-Fi Express option (255 APs) shall allow easy migration to a “Large deployment” (4096 APs) when needed.
- 4.8.25 Shall have been designed with scalability in mind to allow the 4096 APs limit without requiring new equipment or deployment design change.

- 4.8.26 Shall allow the connection of two distant sites over a wireless point-to-point link.
- 4.8.27 Shall allow the connection of multiple distant sites over wireless (Mesh Network).
- 4.8.28 Shall allow easier deployment of Mesh Networks.
- 4.8.29 Shall support IPv6 for wireless clients.
- 4.8.30 Shall support L2GRE tunnelling with a highly flexible architecture.
- 4.8.31 Shall support RAP functionality, allowing an AP to secure traffic sent over an untrusted network like the Internet. It should use the latest security standards, such as WireGuard.
- 4.8.32 Shall provide RAP functionality as a complete multi-site solution to support different office extensions and provide equivalent network functionality to that managed in the main office. The WLAN solution shall provide the equivalent RAP level of service to operators that support different remote WLAN configurations for different customers.

Network Management Solution (SaaS)

- 4.8.33 The WLAN solution shall support MAC-based authentication provided by a SaaS Network Management Solution cloud included in the WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party Network Management Solution (NMS) component.
- 4.8.34 The WLAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication.
- 4.8.35 The built-in RADIUS server shall be able to interface with an external authentication server (Radius, LDAP, Active Directory, Microsoft Azure AD): Free Radius, Microsoft NPS Radius Server, Microsoft AD, Open LDAP, etc..
- 4.8.36 The built-in RADIUS server shall support the following EAP types: EAP-MD5, EAP-TLS, EAP-AKA, EAP-PEAP, EAP-FAST, EAP-SIM, EAP-TTLS, and EAP-GTC.
- 4.8.37 Shall be able to utilise RADIUS attributes to assign each authenticated user/device to a specific ROLE. A role defines a VLAN and enforces security and QoS using role-based ACLs and QoS policies that can be directly integrated with the roles defined within existing authentication servers.

- 4.8.38 Shall include and handle a flexible and adaptive RADIUS attributes dictionary, allowing the addition of an IETF or any vendor-specific RADIUS attribute.
- 4.8.39 If the built-in RADIUS server interfaces with an external RADIUS server, then it shall be able to interface with multiple and distinct RADIUS servers depending on specific access conditions (SSID name, Access Point IP address, the identity of the connecting user..., etc.).
- 4.8.40 Shall support following link layer encryption standards: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP, WPA3_PSK_SAE_AES, WPA3_SAE_AES.
- 4.8.41 Shall support the latest WPA3 encryption standard.
- 4.8.42 Shall support the OWE encryption standard with open Wi-Fi networks.
- 4.8.43 Shall support the following 802.1x supplicants: Windows 11 (and more), MAC OS, IOS, Android, and Chromebook .
- 4.8.44 Shall support time-based policy access to an SSID.
- 4.8.45 Shall propose a “Guest” management solution based on an embedded and built-in Captive Portal providing web-based authentication for guests and visitors.
- 4.8.46 The Guests Captive Portal included in the WLAN solution shall allow a customisable look & feel.
- 4.8.47 The Guest management solution shall at least allow the following authentication methods:
- (a) Username & Password;
 - (b) Access Code; and
 - (c) Simple Term & Condition acceptance
- 4.8.48 The Guest management solution shall allow guests to authenticate using their favorite social network account (supported social networks shall be listed).
- 4.8.49 The WLAN solution shall offer the possibility to build a walled garden environment (with configured domain names) for guest users before they authenticate.
- 4.8.50 The Guest management solution shall allow non-IT staff (e.g., a receptionist) to create temporary guest accounts.
- 4.8.51 The WLAN solution shall allow guest self-registration and employee-sponsored access.

- 4.8.52 Shall allow guest accounts to be provisioned in bulk by importing a file containing guest account information and shall propose a template import file.
- 4.8.53 Shall allow the School to create a batch of guest accounts by specifying a guest prefix and the number of accounts to be created.
- 4.8.54 Will allow the School to define networking SLAs (security, QoS) for guest network connections.
- 4.8.55 Shall allow the definition and application of “data quotas” to guests to limit access based on the total traffic consumed.
- 4.8.56 Shall allow guests to receive SMS notifications.
- 4.8.57 Shall allow guests to receive Email notifications.
- 4.8.58 Shall offer the possibility to interface with a third-party external Captive Portal for guest authentication without forcing traffic through any server or appliance.
- 4.8.59 The Guest management solution shall allow setting a validity period for an authenticated device so that credentials are not entered each time a guest accesses the network.
- 4.8.60 Shall implement strict Guest traffic isolation.
- 4.8.61 Shall allow data retention on user sessions when providing Guest Wi-Fi.
- 4.8.62 Shall support BYOD and provide simple device onboarding.
- 4.8.63 The onboarding process of employee devices shall be based on employee corporate accounts.
- 4.8.64 The BYOD application shall allow the device's validity period and the maximum number of devices per account to be set.
- 4.8.65 Shall support DSSSK to allow the simultaneous use of different Pre-Shared Keys (PSK) for the WPA2 encryption standard in the identical SSID.
- 4.8.66 Shall support the European Commission’s (EU) WIFI4EU initiative. That includes support for Hotspot 2.0 (Passpoint® release 3Wi-Fi Alliance certification program).
- 4.8.67 Shall allow automatic and/or manual RF management (channel and power).
- 4.8.68 Shall support the IEEE 802.11d standard to adapt channel and power levels to specific geographical regions and countries' regulations.

- 4.8.69 Shall support the IEEE 802.11h standard to adapt to regulatory constraints related to using the 5GHz frequency band.
- 4.8.70 Shall support large width for sparse AP deployment .
- 4.8.71 Shall support the most recent modulations for the latest Dual-band clients.
- 4.8.72 Shall support power-saving functions for battery-consuming clients or clients with specific data transmission requirements.
- 4.8.73 Shall minimise airtime consumption in highly dense environments where cell overlap is significant.
- 4.8.74 Must be compatible with previous 802.11ac (Wi-Fi 5) and 802.11b/g/n (Wi-Fi 4) standards and remain compatible if clients do not fully support the latest standards.
- 4.8.75 Shall support Short Guard Interval.
- 4.8.76 Shall support Long Guard Interval and Long symbol duration.
- 4.8.77 Shall be smart enough to guide a new client to the optimal band/channel (2.4GHz/5GHz and 6GHz) considering, at a given time, both the number of associated clients on each band and the medium utilisation.
- 4.8.78 If no channel (2.4GHz/5GHz/6GHz) is overloaded (high, medium utilisation) or crowded (high client count), an AP shall, by default, guide a new client to the 5GHz/6GHz band.
- 4.8.79 Even if the 5GHz/6GHz band is not overloaded but crowded (high client count), an AP shall guide a new client to the 2.4GHz band.
- 4.8.80 If a channel (2.4GHz/5GHz/6GHz) is overloaded (high, medium utilisation), even if it is not crowded, an AP shall guide a new client to the less-loaded band/channel.
- 4.8.81 If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilisation) and no band/channel is crowded, an AP shall guide a new client to the 5GHz/6GHz band.
- 4.8.82 If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilisation) and the 5GHz band is crowded, an AP shall guide a new client to the 2.4GHz band..
- 4.8.83 Shall be able to guide a new client to the appropriate channel (5GHz/6GHz) when connecting to access points operating in the 6GHz band, considering the client's capability to connect to these frequency bands.

- 4.8.84 When a new client discovers multiple APs to associate with, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.
- 4.8.85 Shall force clients to the 5GHz (or 6GHz) only when they are dual-band capable and to the 6GHz only when they are Wi-Fi 6E capable.
- 4.8.86 Shall deny connection to an AP when the client's signal becomes too weak and disconnect a client to force it to roam when the signal becomes too weak.
- 4.8.87 Shall support the IEEE 802.11v and 802.11k standards to facilitate network-guided roaming.
- 4.8.88 Should support data rate control to encourage clients to roam at higher rates.
- 4.8.89 Shall propose APs that can scan the air to provide interfering/rogue APs and wireless attack detection and shall not rely on external scanning equipment.
- 4.8.90 The scanning function of the APs shall not impact active voice or video calls (SIP and H.323). The scanning function of the APs shall not impact active voice or audio/video calls (SIP, H.323 or proprietary).
- 4.8.91 At least for the 5GHz/6GHz band, the WLAN solution shall allow the definition of the list of channels that can participate in dynamic configuration.
- 4.8.92 Shall allow the definition of a range of transmit power per band (min & max) even if power settings are configured for automatic and dynamic assignments.
- 4.8.93 Shall propose Access Points which can all be configured and deployed in a dedicated scanning mode.
- 4.8.94 Shall propose Access Points with wireless packet capture capabilities.
- 4.8.95 Shall simplify reviewing the roaming history for a given client device..
- 4.8.96 Shall allow long interval background scanning.
- 4.8.97 The WLAN solution has wIDS/wIPS capabilities with no additional and dedicated equipment or additional license.
- 4.8.98 Shall be able to identify Interfering APs.
- 4.8.99 Shall be able to identify and contain Rogue APs .
- 4.8.100 Shall allow the definition of flexible policies to classify an AP as a Rogue AP.

- 4.8.101 Shall allow the definition of flexible AP attack detection policies.
- 4.8.102 Shall allow the definition of flexible client attack detection policies.
- 4.8.103 Shall be able to blacklist a WLAN client, either manually or automatically, after a client attack has been detected.
- 4.8.104 Shall allow the School to configure a blacklist duration.
- 4.8.105 Shall allow the configuration of an authentication failure times threshold.
- 4.8.106 Shall offer WLAN Access Points that shall support fine-tuned Quality of Service (QoS), allowing the following actions based on the identity of the connecting user:
 - (a) ACL-based (source/destination IP address and TCP/UDP ports) permit/deny decision
 - (b) QoS priority marking and queuing
- 4.8.107 Shall comply with the 802.11e WMM standard and shall allow for a custom QoS tag (802.1p/DSCP) to WMM queue mapping.
- 4.8.108 Shall have traffic L7 Application fingerprinting (aka Deep Packet Inspection (DPI) capabilities allowing an administrator to take control of applications (even if they all run on top of the HTTP or HTTPS protocols), including not only blocking applications but also allowing to prioritise and rate-limit applications.
- 4.8.109 Shall be able to define and guarantee bandwidth based on an SSID and a user/device role.
- 4.8.110 Shall allow the setting of the maximum number of clients per band/radio and AP for a specific SSID.
- 4.8.111 Shall propose broadcast traffic optimisation mechanisms (including Broadcast filtering and Broadcast/Multicast Key rotation).
- 4.8.112 Shall be able to optimise multicast traffic by converting multicast traffic to unicast traffic, leveraging its IGMP snooping capabilities.
- 4.8.113 Multicast optimisation shall stop on high load.
- 4.8.114 Shall propose the WMM Automatic Power Save Delivery (APSD) feature to allow clients to conserve battery life.
- 4.8.115 Shall, by default, identify Voice and Audio/Video calls and provide appropriate treatment.
- 4.8.116 Shall support Layer 2 roaming capabilities across APs with no special client-side software required.

- 4.8.117 Shall support Layer 3 roaming across APs with no special client-side software required.
- 4.8.118 Shall support 802.11r Fast Roaming and OKC—Opportunistic Key Caching.
- 4.8.119 Shall comply with the 802.11k Radio Resource Management standard.
- 4.8.120 Shall comply with the 802.11v BSS Transition Management standard.
- 4.8.121 Shall inform the wired side of the network about roaming across APs..
- 4.8.122 Shall support advanced location-based services provided by Cloud services included in the solution, as well as Bluetooth LE wireless with dedicated Asset Tracking applications.
- 4.8.123 Shall support RTLS service provided by an RTLS application if it exists in the network or by an RTLS Cloud service included in the solution, using WLAN radio only for location-based service.
- 4.8.124 Shall offer secure onboarding for IoT devices that are as simple as possible without requiring additional third-party components.
- 4.8.125 Shall support advanced analytics services provided by the SaaS NMS cloud solution, which is included in the WLAN solution, as well as services dedicated to statistical and analytical tasks for different XL/Multi-tenant deployments.
- 4.8.126 Shall support advanced management services provided by the SaaS NMS cloud solution included in the solution, services dedicated to different sites, the management of WLAN devices for each site, and the management of wireless itself for XL deployments.

Wireless Intrusion Prevention System

- 4.8.127 The proposed wireless solution should come with wireless Intrusion Detection and Prevention (wIDS/wIPS) capabilities and reduce deployment and management costs by using Access Points to serve clients and contain wireless threats simultaneously.
- 4.8.128 The proposed wireless solution with integrated wIDS/wIPS capabilities should better protect the WLAN by analysing and correlating 802.11 frames inline. It can monitor the wireless radio spectrum for unsafe Access Points or unsafe clients, and countermeasures can be taken to mitigate the impact of foreign intrusions.
- 4.8.129 The proposed wireless solution with embedded wIDS/wIPS capabilities does not require additional licenses to protect the wireless network. Each access point comes with a dedicated antenna for dedicated scanning capabilities.

- 4.8.130 The proposed wireless solution allows for the creation of flexible policies to detect and react to AP wireless attacks. When an attack is detected based on the policy, the detected AP is displayed with details for review and action. An AP Attack Detection Policy detects multiple attacks originating from foreign APs.
- 4.8.131 Should come with the following detection methods:
- (a) AP Spoofing;
 - (b) AP Impersonation;
 - (c) Broadcast De-authentication;
 - (d) Broadcast Disassociation;
 - (e) Adhoc networks using a valid SSID;
 - (f) Long SSID;
 - (g) Adhoc Networks;
 - (h) Wireless Bridge;
 - (i) Null Probe Response;
 - (j) Invalid Address Combination;
 - (k) Reason Code Invalid of De-authentication; and
 - (l) Reason Code Invalid of Disassociation.
- 4.8.132 The proposed wireless solution allows the creation of flexible policies to detect and react to client wireless attacks. When an attack is detected based on the policy, the detected client is displayed and can be automatically blacklisted (its MAC address is not allowed to associate to any AP of the WLAN).
- 4.8.133 Should come with the following detection methods:
- (a) Valid Station Misassociation;
 - (b) Omerta Attack;
 - (c) Unencrypted Valid Client;
 - (d) 802.11 40Mhz Intolerance setting;
 - (e) Active 802.11n Greenfield Mode;
 - (f) DHCP Client ID;
 - (g) DHCP Conflict;
 - (h) DHCP Name Change;
 - (i) Malformed Frame Association Request;
 - (j) Sticky Client;
 - (k) Detect Long SSID in Client detection; and
 - (l) Detect Reason Code Invalid
- 4.8.134 Should allow to blacklist a client manually or automatically. If a wireless attack has been detected, the intruder identified (MAC address) by the wIDS/wIPS application is prevented from associating with the network.

4.9 Wireless Access Point (Indoor)

- 4.9.1 Should come with integrated omnidirectional antennas, with a maximum antenna gain of 4.6dBi in 2.4GHz, 5.8dBi in 5GHz, and 6.4dBi in 6GHz.
- 4.9.2 Should include a third dedicated full-band antenna for scanning the air, improving network security and Wi-Fi quality.
- 4.9.3 Should support Tri radio and Tri-band with the following maximum data rates.
 - (a) 6 GHz: 2x2:2 up to 5.76Gbps wireless data rate to individual 2SS EHT320 802.11be client devices;
 - (b) 5 GHz: 4x4:4 up to 5.76Gbps wireless data rate to individual 2SS EHT160 802.11be client devices; and
 - (c) 2.4 GHz: 2x2:2 up to 688Mbps wireless data rate to individual 2SS EHT40 802.11be client devices.
- 4.9.4 Should have one full-band radio dedicated to scanning, which inherently improves network security and Wi-Fi quality.
- 4.9.5 Should have an integrated Bluetooth 5.4/Zigbee radio, enabling location and building automation services.
 - (a) Bluetooth 5.4: up to 6dBm transmit power (class 1) and -93dBm receive sensitivity; and
 - (b) Zigbee: up to 6dBm transmit power (class 1) and -93dBm receive sensitivity
- 4.9.6 Should support the following frequency bands:
 - (a) 2.400 to 2.4835 GHz;
 - (b) 5.150 to 5.250 GHz;
 - (c) 5.250 to 5.350 GHz;
 - (d) 5.470 to 5.725 GHz;
 - (e) 5.725 to 5.850 GHz;
 - (f) 5.925 to 6.425 GHz;
 - (g) 6.425 to 6.525 GHz;
 - (h) 6.525 to 6.875 GHz; and
 - (i) 6.875 to 7.125 GHz
- 4.9.7 Should support the following:
 - (a) Short guard interval for 20-MHz, 40-MHz, 80-MHz, 160MHz and 320-MHz channels
 - (b) Transmit beamforming (TxBF) for increased signal reliability and range
 - (c) 802.11n/ac packet aggregation:
 - i. Aggregated Mac Protocol Data Unit (A-MPDU)
 - ii. Aggregated Mac Service Data Unit (A-MSDU)
 - (d) Supported data rates (Mb/s):
 - i. 802.11b: 1, 2, 5.5, 11
 - ii. 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54

- iii. 802.11n(2.4GHz): 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)
 - iv. 802.11n(5GHz): 6.5 to 600 (MCS0 to MCS31, HT20 to HT40)
 - v. 802.11ac(2.4GHz): 6.5 to 400
(MCS0 to MCS9, NSS=1 to 2, VHT20 to VHT40)
 - vi. 802.11ac(5GHz): 6.5 to 1733
(MCS0 to MCS9, NSS = 1 to 2, VHT20 to VHT80)
 - vii. 802.11ax(2.4GHz): 3.6 to 574
(MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)
 - viii. 802.11ax(5GHz): 3.6 to 4804
(MCS0 to MCS11, NSS = 1 to 4, HE20 to HE160)
 - ix. 802.11ax(6GHz): 3.6 to 2402
(MCS0 to MCS11, NSS = 1 to 2, HE20 to HE160)
 - x. 802.11be(2.4GHz): 3.6 to 688
(MCS0 to MCS13, NSS = 1 to 2, EHT20 to EHT40)
 - xi. 802.11be(5GHz): 3.6 to 5765
(MCS0 to MCS13, NSS = 1 to 4, EHT20 to EHT160)
 - xii. 802.11be(6GHz): 3.6 to 5765
(MCS0 to MCS13, NSS = 1 to 2, EHT20 to EHT320)
- (e) Supported modulation types:
- i. 802.11b: BPSK, QPSK, CCK
 - ii. 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
 - iii. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
 - iv. 802.11be: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM, 4096-QAM
 - v. 802.11n high-throughput (HT) support: HT 20/40
 - vi. 802.11ac very high throughput (VHT) support: VHT 20/40/80
 - vii. 802.11ax high efficiency (HE) support: HE 20/40/80/160
 - viii. 802.11be Extreme High Throughput (EHT) support: EHT20/40/80/160/320
- (f) Advanced Cellular Coexistence (ACC)
- (g) Minimizes interference from 3G/4G cellular networks, distributed antenna systems, and commercial small cell/femtocell equipment
- 4.9.8 Shall come with the following interfaces:
- (a) 1 x multi-gigabit 1/2.5/5/10GE autosensing RJ-45 uplink port Eth0 with Power over Ethernet (PoE) 802.3bt compliant.
 - (b) 1 x 1GE RJ45 port, Eth1
 - (c) 1x USB 2.0 Type C (5V, 1A)
 - (d) 1 x USB Type C Console
 - (e) Reset button: Factory reset
- 4.9.9 Shall come with the following Visual Indicators (Tri-color LED) for system and radio status, example below:
- (a) Red flashing: System abnormal, link down;
 - (b) Red light: System startup;

- (c) Red and blue rotate flashing: System running, OS upgrading;
 - (d) Blue light: System running, dual bands working;
 - (e) Green flashing: System running, no SSID created;
 - (f) Green light: System running, single band working; and
 - (g) Red, blue and green rotate flashing: System running, use for location of an AP
- 4.9.10 Shall come with the following security features:
- (a) Integrated Trusted Platform Module (TPM 2.0) for secure storage of credentials and keys;
 - (b) 802.11i, WPA2, WPA3, Enterprise with CNSA Option, Personal (SAE);
 - (c) 802.1X;
 - (d) WEP, Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP);
 - (e) Firewall: ACL, wIPS/wIDS and DPI application policy enforcement; and
 - (f) Portal page authentication
- 4.9.11 Shall support direct DC power and Power over Ethernet (PoE). When both power sources are available, DC power takes priority over PoE.
- 4.9.12 Shall be able to support an 802.3bt compliance source. The AP shall work in unrestricted functionalities with an 802.3bt POE.
- 4.9.13 Shall be able to operate at a temperature of 0°C to 45°C and humidity of 5% to 95% non-condensing.
- 4.9.14 Shall support up to 16 SSID per radio and support up to 1280 associated client devices.
- 4.9.15 Should support enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with Unified Access, and built-in application intelligence and analytics. This makes it ideal for enterprises of all sizes that demand a simple, secure, and scalable wireless solution.
- 4.9.16 Should be able to deploy as a standalone cluster for up to 255 AP per cluster for simplified plug-and-play deployment with an AP acting as a virtual controller, be managed by its on-premise Network Management System for large enterprise deployment, or be managed from the cloud.
- 4.9.17 DPI technology must be built-in, providing real-time flow classification at the application level. The network administrator can obtain a comprehensive view of applications running in the network and apply adequate control to optimise the network's performance for business-critical applications.

- 4.9.18 Should support role-based management access in the cluster deployment, which includes Admin, Viewer, and GuestOperator access. GuestOperator access simplifies guest account creation and management and can be used by any non-IT person, such as a front desk worker or receptionist.
- 4.9.19 Shall support a built-in customisable captive portal that enables customers to offer unique guest access.
- 4.9.20 Should support fine-tuned quality of service (QoS) parameters to differentiate and provide appropriate QoS for each application, such as voice, video, and desktop sharing.
- 4.9.21 Should support Application-aware RF scanning to avoid interruption of real-time applications.
- 4.9.22 Should support Radio Dynamic Adjustment (RDA) technology, which automatically assigns channels and power settings, provides DFS/TPC, and ensures that access points stay clear of all radio frequency interference (RFI) sources to deliver reliable, high-performance wireless LANs.
- 4.9.23 Should be able to provide dedicated air monitoring for spectrum analysis and wireless intrusion protection.
- 4.9.24 It will be based on a controller-less architecture, whereby every AP is capable of processing control and data traffic instead of having a centralised controller to manage them.
- 4.9.25 Must support a built-in cloud agent that will perform a call home and be managed by the management server in the cloud. The same access point must also be able to be managed by an on-premises management server in the event that the cloud is not available.
- 4.9.26 Shall be able to log all user activities, such as login, logout, TCP, UDP, and URL access, into a log file stored locally in the AP. At the same time, it can automatically SFTP to an external log server for safekeeping.
- 4.9.27 Should come with stainless steel mounting kits to prevent damage from the AP's high temperature.

4.10 Wireless Access Point with External Antenna (Outdoor)

- 4.10.1 Should come with a built-in integrated directional antenna.
- 4.10.2 The proposed access point should support dual radio with 5 GHz 802.11ax 4x4:4 MU-MIMO and 2.4 GHz 802.11ax 2x2:2 MU-MIMO with an Integrated directional antenna (H80 x V80) and a peak gain of 7.5dBi in 2.4G and 7.4dBi in 5G.

- 4.10.3 Should include a third dedicated full-band antenna for scanning the air, improving network security and Wi-Fi quality.
- 4.10.4 Should have an integrated Bluetooth 5.1/Zigbee radio, enabling location and building automation services.
- (a) Bluetooth 5: up to 18dBm transmit power (class 1) and *-93dBm* receive sensitivity;
 - (b) Zigbee: up to 18dBm transmit power and -102dBm receive sensitivity ; and
 - (c) Integrated vertically polarised omnidirectional antenna with a peak gain of 3.3dBi.
- 4.10.5 Should support the following frequency bands:
- (a) 2.400 to 2.4835 GHz;
 - (b) 5.150 to 5.250 GHz;
 - (c) 5.250 to 5.350 GHz;
 - (d) 5.470 to 5.725 GHz; and
 - (e) 5.725 to 5.850 GHz
- 4.10.6 Should support the following:
- (a) short guard interval for 20 MHz, 40 MHz, 80 MHz and 160(80+80)MHz channels;
 - (b) Transmit beam forming (TxBF) for increased signal reliability and range;
 - (c) 802.11n/ac packet aggregation:
 - a. Aggregated Mac Protocol Data Unit (A-MPDU)
 - b. Aggregated Mac Service Data Unit (A-MSDU)
 - (d) supported data rates (Mb/s):
 - a. 802.11b: 1, 2, 5.5, 11
 - b. 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
 - c. 802.11n(2.4GHz): 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)
 - d. 802.11n(5GHz): 6.5 to 600 (MCS0 to MCS31, HT20 to HT40)
 - e. 802.11ax(2.4GHz): 3.6 to 573 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)
 - f. 802.11ac: 6.5 to 1733 (MCS0 to MCS9, NSS = 1 to 4, VHT20 to VHT80; NSS=2, VHT160(80+80))
 - g. 802.11ax(5GHz): 3.6 to 2,402 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE80; NSS=2, VHT160(80+80))
 - (e) Supported modulation types:
 - a. 802.11b: BPSK, QPSK, CCK
 - b. 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
 - c. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
 - (f) 802.11n high-throughput (HT) support: HT 20/40;

- (g) 802.11ac very high throughput (VHT) support: VHT 20/40/80/160(80+80); and
 - (h) 802.11ax high efficiency (HE) support: HE 20/40/80/160(80+80)
 - (i) Advanced Cellular Coexistence (ACC) Minimizes interference from 3G/4G cellular networks, distributed antenna systems, and commercial small cell/femtocell equipment
- 4.10.7 Shall come with the following interfaces:
- (a) 1x 10/100/1000/2500 Mbps IEEE 802.3 compliant autosensing (RJ-45) uplink port, ENET0, Power over Ethernet (PoE) 802.3at/bt compliant;
 - (b) 1x 10/100/1000 Mbps IEEE 802.3 compliant auto-sensing (RJ-45) downlink port, ENET1, PoE PSE output up to 802.3at power dependent on input PoE ;
 - (c) 1x SFP port ;
 - (d) 1x USB 2.0 Type C (5V, 1A); and
 - (e) Reset button: Factory reset
- 4.10.8 Shall come with the following Visual Indicators for system and radio status:
- (a) SYS ON: Power on and system running ;
 - (b) SYS Flashing: Bootloader-OS loading or upgrading ;
 - (c) 2.4G ON: 2.4GHz SSID created and running ;
 - (d) 5G ON: 5GHz SSID created and running ;
 - (e) ENET0 ON: Ethernet0 link UP ;
 - (f) ENET1 ON: Ethernet1 link UP ;
 - (g) SFP ON: SFP link UP ; and
 - (h) PSE ON: PSE Enabled
- 4.10.9 Shall come with the following security features:
- (a) Integrated Trusted Platform Module (TPM 2.0) for secure storage of credentials and keys ;
 - (b) 802.11i, WPA2, WPA3, Enterprise with CNSA Option, Personal (SAE), Enhanced Open (OWE) ;
 - (c) 802.1X ;
 - (d) WEP, Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP) ;
 - (e) Firewall: ACL, wIPS/wIDS and DPI application policy enforcement with OmniVista™ ; and
 - (f) Portal page authentication
- 4.10.10 Shall be able to support either 802.3at or 802.3bt compliance source with the following application:
- (a) Maximum (worst case) power consumption:
 - a. 64W (802.3bt Type4 PoE in) with ENET1 802.3at PSE enabled.

- b. 46W (802.3bt Type3 PoE) with ENET1 802.3af PSE enabled.
24W (802.3at) with disabled ENET1 PSE, USB.
 - (b) Maximum power consumption in idle mode: 10W; and
 - (c) Power over Ethernet (PoE): 48 V DC (nominal) 802.3bt/at compatible source
- 4.10.11 Shall be able to operate at a temperature of -40°C to 65°C and humidity of 10% to 90% non-condensing.
- 4.10.12 Should have a Mean Time Between Failure (MTBF) of not less than 1,003,257 hr at +25°C operating temperature.
- 4.10.13 Shall support up to 16 SSID per radio (total 32 SSID) and support for up to 1024 associated client devices per AP.
- 4.10.14 Should support 802.11ax, having a maximum concurrent data rate of 3 Gb/s (2.4Gb/s in 5 GHz and 573 Mb/s in 2.4 GHz).
- 4.10.15 Should support enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with unified access and built-in application intelligence and analytics so that it is ideal for enterprises of all sizes demanding a simple, secure and scalable wireless solution.
- 4.10.16 Should be able to deploy as a standalone cluster for up to 256 units per cluster for simplified plug-and-play deployment with an Access Point acting as a virtual controller or be managed by its Network Management System for large enterprise deployment up to 4K Access Points, or be able to manage from the cloud up to 4K Access Points.
- 4.10.17 DPI technology must be built in, providing real-time classification of flows at the application level. The network administrator can obtain a comprehensive view of applications running in the network and apply adequate control to optimize the network's performance for business-critical applications.
- 4.10.18 Should support role-based management access in the cluster deployment, including Admin, Viewer, and Guest Operator access. Guest Operator access simplifies guest account creation and management and can be used by any non-IT person, such as a front desk worker or receptionist.
- 4.10.19 Shall support a built-in customisable captive portal which enables customers to offer unique guest access.
- 4.10.20 Should support fine-tuned quality of service (QoS) parameters to differentiate and provide appropriate QoS for each application, such as voice, video, and desktop sharing.

- 4.10.21 Should support Application-aware RF scanning to avoid interrupting real-time applications.
- 4.10.22 Should support Radio Dynamic Adjustment (RDA) technology, which automatically assigns channels and power settings, provides DFS/TPC and ensures that access points stay clear of all radio frequency interference (RFI) sources to deliver reliable, high-performance wireless LANs.
- 4.10.23 Should be able to provide dedicated air monitoring for spectrum analysis and wireless intrusion protection.
- 4.10.24 Shall be based on a controller-less architecture, whereby each AP is capable of processing control and data traffic instead of having a centralised controller to manage them.
- 4.10.25 Must support a built-in cloud agent, which will perform a call home and be managed by the cloud management server. The same access point must also be able to be managed by an on-premises management server if the cloud is not available.
- 4.10.26 Shall be able to log all user activities, such as login, logout, TCP, UDP, and URL access, into a log file stored locally in the AP. At the same time, it can automatically SFTP to an external log server for safekeeping.
- 4.10.27 Should come with stainless steel mounting kits to prevent damage from the AP's high temperature.

4.11 Identity and Policy Management System

Server/Appliance

- 4.11.1 Shall support a single platform that combines AAA, Network Access Control (NAC), Bring Your Own Device (BYOD), Mobile Application Management (MAM) and Guest Access by incorporating identity, health, physical/device information and conditional elements into one set of policies.
- 4.11.2 Must be able to scale to up to 5,000 devices per appliance or virtual appliance (Both VMware and Hyper V).
- 4.11.3 The solution must be agnostic to existing wired, wireless and VPN networks in place today.
- 4.11.4 The appliance must be pre-built and ready to be imported (ovf) into the VMware virtualisation environment (building from ISO is not acceptable).
- 4.11.5 Shell is protected by CLI, which provides configuration for base appliance settings.

- 4.11.6 Appliance must provide disk or file encryption.
- 4.11.7 Ability to mix and match virtual and hardware appliances in one deployment.
- 4.11.8 Platform must be deployable in an out-of-band model and support clustering with N+1 redundancy model.
- 4.11.9 Flexibility to operate all features/functions on any appliance in the cluster.
- 4.11.10 The hardware platform must be running on a hardened operating system.

Functionality

- 4.11.11 Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.
- 4.11.12 Support any vendor type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).
- 4.11.13 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).
- 4.11.14 Must incorporate a complete set of reporting, analysis, and troubleshooting tools. Data from access transactions can be organised by customisable data elements and used to generate graphs, tables, and reports. Must correlate and organise user, authentication, and device information together.
- 4.11.15 The solution must fully integrate support for Microsoft NAP, allowing health and posture checks on Windows endpoints without installing an agent.
- 4.11.16 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.
- 4.11.17 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:
 - (a) Full AAA server – RADIUS and TACACS+;
 - (b) Automatic device profiling and the ability to use profiled information for access authorization ;
 - (c) Built-in guest management and device/user onboarding;
 - (d) Web based management interface with Dashboard;
 - (e) Reporting and analysis with custom data filters;
 - (f) Data repository for user, device, transaction information ;

- (g) Rich policies using identity, device, health, or conditional elements
 - (h) Deployment and implementation tools;
 - (i) Support SSO SAML for GUI and Guest portal integration;
 - (j) Integration with leading MDM/EMM (Enterprise Mobility Management) provider such as Ivanti (Formerly MobileIron), VMware AirWatch, to extract endpoint information; and
 - (k) Integration with Palo Alto Networks Firewall to provide context base information
- 4.11.18 Must support flexible license model based on either perpetual or subscription-based licensing on required functionality (i.e. Access, Onboard, Posture).
- 4.11.19 Correlation of user, device, and authentication information for easier troubleshooting, tracking, etc.
- 4.11.20 The Authentication, Authorisation, and Accounting (AAA) framework must allow for the complete separation of Authentication and Authorization sources. For example, authentication is against Active Directory, but authorisation is against an external SQL database.
- 4.11.21 Should support multiple methods for device identification and profiling, such as:
- (a) Integrated, network-based, device profiler utilising collection via SNMP, DHCP, HTTP, AD, ActiveSync, IF-MAP; and
 - (b) Endpoint audit via NESSUS or NMAP scanning
- 4.11.22 Policy creation tools:
- (a) Pre-configured templates;
 - (b) Wizard-based interface;
 - (c) LDAP browser for quick look-up of AD attributes;
 - (d) Policy simulation engine for testing policy integrity; and
 - (e) The policy model should support the incorporation of several contextual elements, including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.
- 4.11.23 Support the following enforcement methods:
- (a) VLAN steering via RADIUS IETF attributes and VSAs;
 - (b) VLAN steering and port bouncing via SNMP;
 - (c) Access control lists – both statically defined filter-ID-based enforcement, as well as dynamically downloaded ACLs;
 - (d) Roles or any other vendor-specific RADIUS attribute supported by the network device; and
 - (e) Agent-based enforcement – bouncing a managed interface and sending custom messages.
- 4.11.24 Must be able to join multiple Active Directory belonging to separate

forests with no trust relation to facilitate any form of authentication or authorisation request.

- 4.11.25 Must be able to create multiple Certificate Authority (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 clusters if required
- 4.11.26 Must support complex PKI deployment where TLS authentication requires validating client certificates from multiple CA trust chains. Must also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.
- 4.11.27 Must support importing of 3rd party vendor Radius Dictionary.
- 4.11.28 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 Security Assertion Markup Language (SAML) supported applications.
- 4.11.29 Support for SAML capabilities will allow the appliance to act as an identity provider (IDP) for the principal user.
- 4.11.30 Profiling capabilities included in base licensing to offer full visibility of the devices present on the network.
- 4.11.31 Support Single sign-on (SSO) support works with Ping, Okta and other identity management tools to improve user experience with SAML 2.0-based applications.
- 4.11.32 Support Restful API capability to interact with leading MDM vendors within the base license.
- 4.11.33 Must support multiple AD domains and AD forest queries seamlessly.
- 4.11.34 Support intuitive policy configuration templates and visibility troubleshooting tools.
- 4.11.35 Supports multiple authentication/authorisation sources (AD, LDAP, SQL dB) within one service.
- 4.11.36 Self-service device onboarding with a built-in certificate authority (CA) for BYOD
- 4.11.37 Supports NAC and EMM/MDM integration for mobile device assessments.
- 4.11.38 Comprehensive integration with third-party systems such as SIEM, Internet security and EMM/MDM.
- 4.11.39 Support automatic cluster upgrade.

- 4.11.40 Support the following identity stores:
- (a) Microsoft Active Directory;
 - (b) RADIUS;
 - (c) Any LDAP compliant directory;
 - (d) Any ODBC-compliant SQL server;
 - (e) Token servers;
 - (f) Built-in SQL store, static hosts list;
 - (g) Kerberos;
 - (h) Microsoft Azure Active Directory; and
 - (i) Google Suite.
- 4.11.41 Support the following Request For Comments (RFC) standards: 2246, 2248, 2407, 2408, 2409, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3579, 3580, 3748, 3779, 4017, 4137, 4301, 4302, 4303, 4308, 4346, 4514, 4518, 4809, 4849, 4851, 4945, 5176, 5216, 5246, 5280, 5281, 5282, 5424, 5755, 5759, 6614, 6818, 6960, 7030, 7170, 7296, 7321, 7468, 7748, 7815, 8031, 8032, 8247, 8446, 8709, 8894, 8908
- 4.11.42 Support information assurance validations Federal Information Processing Standards (FIPS) 140-2 – Certificate #4473A
- 4.11.43 Support the following profiling methods: DHCP, TCP, MAC OUI, ClearPass Onboard, SNMP, and Cisco device sensor.
- 4.11.44 Support the following frameworks and protocols:
- (a) RADIUS, RADIUS CoA, TACACS+, web authentication, SAML v2.0;
 - (b) RadSec (TLS encoded RADIUS);
 - (c) 802.1X-2010, 802.1X-2020;
 - (d) TEAP (Tunneled EAP);
 - (e) EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);
 - (f) PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD);
 - (g) TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);
 - (h) EAP-TLS;
 - (i) PAP, CHAP, MSCHAPv1 and 2, EAP-MD5;
 - (j) OAuth2;
 - (k) WPA3;
 - (l) NAC, Microsoft NAP;
 - (m) Windows machine authentication;
 - (n) MAC auth;
 - (o) Online Certificate Status Protocol (OCSP);
 - (p) SNMP generic MIB, SNMP private MIB; and
 - (q) Common Event Format (CEF), Log Event Extended Format (LEEF), and RFC5424

- 4.11.45 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 Hotfixes, patch management agents), and perform standard health checks on Linux and Mac platforms (Anti-virus, Anti-spyware, Firewall).
- 4.11.46 Support persistent agent, dissolvable agent and agentless
- 4.11.47 Support health check for Windows, MacOS, and Linux Operating Systems.
- 4.11.48 Centrally view the online status of all devices from the proposed policy manager platform
- 4.11.49 Perform advanced health checks on Windows platforms (services, processes, peer-to-peer apps, registry keys, USB device usage, Windows Hotfixes, patch management agents) and perform standard health checks on Linux and Mac platforms (Anti-virus, Anti-spyware, Firewall).
- 4.11.50 Support endpoint messaging, notifications and session control. Messages can include reasons for remediation, links to helpful URLs and helpdesk contact information.

Reliability and Performance

- 4.11.51 Appliances can be clustered in any combination via local and remote network connections, providing unlimited scale, redundancy, and access load balancing.
- 4.11.52 Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model.
- 4.11.53 Failure of the master node should not impact the ability of backup appliances to continue servicing authentication traffic.
- 4.11.54 Must support several deployment modes, including centralised, distributed, or mixed.

Bring Your Own Devices (BYOD)

- 4.11.55 Self-service workflow built on an industry-leading platform. Supports popular smart devices as well as traditional computing platforms.
- 4.11.56 Unique portal pages based on device type – iOS, Android.
- 4.11.57 Ability to support revocation of devices.

- 4.11.58 Correlation of user, device, and authentication information for easier troubleshooting, tracking, etc. It provides a high level of visibility into what devices are on the network and what users are associated with them.
- 4.11.59 Automated device onboarding enables secure access via a self-serve portal, configuring 802.1x supplicants, device enrolment, and provisioning.
- 4.11.60 Ability to integrate with Active Directory so users approved for BYOD may be authenticated via identity and/or device attributes.
- 4.11.61 Support for Windows, Mac, iOS (iPhones, iPads, etc.) and Android devices.

Guest Access

- 4.11.62 The solution must be capable of providing sponsored and self-provisioned Guest Access.
- 4.11.63 Must be able to provide custom branding.
- 4.11.64 Option to send automated SMS (through integration with SMS Gateway) or email credentials to the Guest User.
- 4.11.65 Ability to set Account Details, including Time Frame, Bandwidth Contract, etc. Once the account timeframe expires, the User Account becomes inactive automatically.
- 4.11.66 Must be capable of providing Advertising Services (Play Video before Access, offer current Promotions, Advise of Health Alerts)
- 4.11.67 The guest solution should manage the individual guest credentials in a partitioned database and not pollute the user store with account credentials for guest users.
- 4.11.68 Ability to cache MAC address post-guest authentication to avoid guests needing to re-authenticate during their visit (3G-like user experience after first authentication via captive portal).
- 4.11.69 Auto-login for self-registration workflow: The guest does not need to retrieve account credentials from email or SMS for initial login.
- 4.11.70 Anonymous login support with the per-device policy still applied.
- 4.11.71 Access token login support for single credential login to guest network – event management, scratch cards, etc.
- 4.11.72 Bulk import of guest accounts with the ability to trigger notification of credentials via email.
- 4.11.73 Sponsored approval workflow for guest self-registration where open SSID

registration can be protected by requiring internal staff to approve creating a guest account.

- 4.11.74 Prevent employees from accessing the guest network on the corporate laptop.
- 4.11.75 Apple Captive Network Assistant bypass for managing end-to-end guest workflow.
- 4.11.76 Post login session statistics page displayed to users so they can monitor usage or quota assigned.
- 4.11.77 Support URL persistence so users originally requested webpage can be displayed post login.
- 4.11.78 Location-based captive portal – display different landing pages based on where guests connect to the network.
- 4.11.79 Support guest access across multi-vendor access networks.
- 4.11.80 Fully customisable self-registration or guest creation pages with user interface controls such as drop-down, checklist, and radio buttons.
- 4.11.81 Authenticated self-registration for partner / joint venture account provisioning.
- 4.11.82 Published APIs to allow 3rd party systems to manage guest accounts.

4.12 Next Generation Enterprise Firewall and Management Tools

- 4.12.1 As part of the proposed network infrastructure, the Tenderer shall propose a TWO (2) Tier Next Generation Enterprise Firewall (NGFW) Infrastructure with Threat Prevention capabilities and High Availability (HA) configuration.

General Requirements

- 4.12.1 Shall have the hardened Operating System (OS) built as a firewall appliance (i.e. not on generic server hardware) and shall handle all traffic in a single pass stream-based manner with all features turned on to deliver predictable performance (i.e. no further degradation by turning on any software/hardware modules) without compromising any security capabilities. It shall be optimised for layer seven application-level content processing and have a dedicated field-programmable gate array (FPGA) to handle signature matching and processing in a single-pass parallel processing architecture.
- 4.12.2 Shall strictly have both the Management Plane and Network Traffic Processing Plane segregated on the same hardware appliance; the management core must be allocated by default without a resource

separation process to draw from the data processing core, reducing performance.

- 4.12.3 Management functionality shall be provided via a dedicated control plane processor that drives the configuration management, logging, and reporting without touching data processing hardware. There shall be no exception to this clause, and no workaround is permitted.
- 4.12.4 The administration and management of the NGFW shall be done via the management plane on the same physical hardware only, without requiring additional external management server appliances or software installation. There shall be no exception to this clause, and no workaround is permitted.
- 4.12.5 Must not have a special inspection mode or one that offers different security capabilities. It must have a consistent inspection engine without disparity in security capabilities, regardless of the selected inspection mode. If a false claim is found, the product will be refunded, and the vendor will be penalised.

Certification

- 4.12.6 The proposed NGFW must be National Information Assurance Partnership (NIAP) Common Criteria Certified for the following Protection Profile Identifier:
 - (a) Network Device Protection Profile (NDPP) Extended Package;
 - (b) Stateful Traffic Filter Firewall;
 - (c) Protection Profile for Network Devices Version 1.1; and
 - (d) Network Device Protection Profile (NDPP) Extended Package VPN Gateway Version 1.1
- 4.12.7 The proposed NGFW must be in the Leaders Quadrant in the Gartner Magic Quadrant for Enterprise Network Firewalls.

Management

- 4.12.8 The Management Plane (handling Admin Consoles, Reporting, etc.) and the Data Processing Plane (handling Firewall Policies, IPS, Anti-Virus, Anti-Spyware Scanning, etc.) must be separated such that when the Management Plane were to hang, it could be separately restarted without disrupting the on-going traffic data processing functions.
- 4.12.9 Must be managed from a Web-based Graphical User Interface (GUI) or Command-Line Interface (CLI) as a single view to manage security policies and network configurations (e.g., routing table, interface setup), with no workaround, e.g., third-party integration or API call, allowed. In addition, this Management Port must contain a different routing table from the production traffic. Other production interfaces can be configured as management ports.

- 4.12.10 All the Firewall, IPS, Anti-Virus, Anti-Spyware, and Data Filtering logs must be automatically correlated. All these logs must contain User ID and Application information on the corresponding events without additional software/hardware/blades.
- 4.12.11 Must be able to granularly assign management functions for each management user group or individual users. The control of the management functions must include the followings:
- (a) Enable / Disable Main Tabs in the GUI (Dashboard, ACC, Monitor, Policies, Objects, Network, Device);
 - (b) Enable / Disable / Read Only specific sub-functions inside the Main Tabs listed above;
 - (c) Enable / Disable Save and Commit Function;
 - (d) Enable / Disable XML API Functions for Report, Log, Configuration, Operational Requests, Commit, User-ID Agents, Export, Import, and
 - (e) CLI access control.
- 4.12.12 Must have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) basis without the need for any additional software subscription/licenses or hardware components.
- 4.12.13 Must be able to generate reports on individual user ID with (but not limited to) the following activities & Application Usage, without the need for additional software subscription/licenses or hardware components.
- 4.12.14 Must be able to natively trigger custom alerts based on condition matching criteria [expression functions connectors, attributes, operators and values] in the form of HTTP forwarding, email, SMS, Syslog and SNMP based on any log attributes from the following log sources (e.g. traffic, threat, URL, system, configuration) without customisation. The tenderer shall demonstrate on how to achieve the following alerts based on the following conditions:-
- 4.12.15 Threat Logs: -
- (a) Source Address;
 - (b) Application;
 - (c) User;
 - (d) Destination Port;
 - (e) Threat Type ; and
 - (f) Action.
- 4.12.16 Must be able to natively auto-trigger a workflow on a third-party service that provides an HTTP-based API alert based on condition matching criteria [expression functions connectors, attributes, operators and values] on any log attributes from the following log sources (e.g. traffic, threat, URL, system, configuration) without customisation.

- 4.12.17 Must be able to natively auto-quarantine or blacklist IP addresses to existing security policies based on any log attributes from multiple log sources (traffic, threat, URL) without customisation.
- 4.12.18 The proposed NGFW Web GUI must be able to display the log details of the user ID to IP mapping information.
- (a) User-ID Log Information shall include:
 - (b) Timestamp;
 - (c) Username;
 - (d) Mapped IP Address;
 - (e) Remaining Time before expiry;
 - (f) User-ID Source; and
 - (g) User-ID Source Type.

Application Identification

- 4.12.19 Shall have a purpose-built Application Identification Engine, that make use of the following mechanisms to identify applications: -
- (a) Application signatures;
 - (b) TLS/SSL and SSH decryption;
 - (c) Application and Protocol Decoding; and
 - (d) Heuristics

The Application Identification Engine shall, for example, be able to control and distinguish SharePoint Application traffic from typical web-browsing traffic despite using the same TCP Ports natively (i.e. without any additional software blades/Subscription on the same physical hardware)

- 4.12.20 Shall be able to classify unknown applications and apply actions (e.g., Deny, Allow, Scan content, etc.) in the firewall rules. To facilitate custom application signature creation, packet captures shall be generated natively and automatically by default for network traffic that contains all unknown applications.
- 4.12.21 Shall allow the organisation to write its own customized application identification signature using its Web-based Graphic User Interface (GUI). The customised application signature can be created based on multiple parameters, such as pattern matching within the protocol-level context and payload. The signature shall be configurable and applied only to the current transaction or the full user session.
- 4.12.22 Shall natively, without additional software/hardware, allow the administrator to review any policy impact for new or modified application signatures included in a content release version. This Web GUI feature will enable the administrator to simultaneously update the security policies and install new content, allowing for a seamless shift in policy enforcement.

- 4.12.23 Shall natively, without additional software/hardware, identify all applications seen on any legacy layer 4 Security policy rule and provide an easy workflow for selecting the layer seven applications to be allowed on that rule. This simplified workflow allows the gradual and native migration of a legacy rule to an application-based one to enable applications and safely improve security posture.
- 4.12.24 Shall have visibility into and be able to control over 15,000 SaaS applications and their corresponding functions without waiting for App-ID signature development.
- 4.12.25 Shall have a Cloud Engine that can recommend Security policy rules with specific SaaS App IDs and import those recommended security policies into the Next Generation Firewall.

User Identification

- 4.12.26 Shall support all the following authentication services
- 4.12.27 Directory services: Microsoft Active Directory, Microsoft Exchange, OpenLDAP, Novell eDirectory, RADIUS, Kerberos, TACACS+, Sun ONE Directory Server.
- 4.12.28 Syslog Listeners to harvest user information from 3rd Party Vendors by using Regex or Field Identifier.
- 4.12.29 Shall support user enforcement as part of a security policy requirement via x-forwarded-for entry.
- 4.12.30 For any other User Database not supported out-of-the-box, the proposed vendor shall provide other means (e.g., API) to map the User Identification without any additional hardware/licenses/subscriptions. There shall be no exception to this clause, and any workaround is NOT permitted.
- 4.12.31 Should allow third-party PKI certificates to encrypt the user-ID communication with the appliance.

Machine Learning-Based Security Inspection

- 4.12.32 Shall support inline Machine Learning (ML)-based web security engines to prevent evasive and unknown web threats.
- 4.12.33 Shall support real-time analysis of URL filtering using the cloud-based detection modules to protect against new and unknown threats that do not currently exist in the URL database.
- 4.12.34 Shall support inspecting HTTP response data from the firewall upon receipt of a suspicious web request. The data is further analysed through

the deep learning detectors, which provide inline protection against evasive zero-day web attacks.

- 4.12.35 Shall include cloaked websites, where web page contents are surreptitiously retrieved from unknown websites. This can consist of malicious content that conventional URL databases cannot account for, such as multi-step attacks, CAPTCHA challenges, and previously unseen one-time-use URLs.
- 4.12.36 Shall support automatically updating and deploying detectors and analysers to categorise websites without requiring the administrator to download update packages.
- 4.12.37 Shall support URL Filtering local inline categorisation, which enables the firewall data plane to apply an ML model to webpages to alert users when phishing variants are detected while preventing malicious variants of JavaScript exploits from entering your network.
- 4.12.38 The proposed solution ML model must detect malicious content by evaluating file details, including decoder fields and patterns, and formulating a high probability classification and verdict.
- 4.12.39 Shall support inline ML-based protection to detect malicious PE (portable executables), ELF and MS Office files, and PowerShell and shell scripts in real-time.
- 4.12.40 The proposed solution's inline ML model must dynamically detect malicious files of a specific type by evaluating file details, including decoder fields and patterns, to formulate a high-probability file classification. This protection extends to currently unknown as well as future variants of threats.
- 4.12.41 In addition to the signature-based detection mechanism, the proposed solution shall support an inline detection system to prevent unknown and evasive C2 threats with extensible deep learning models that enable inline analysis capabilities on the firewall on a per-request basis to prevent zero-day threats from entering the network.
- 4.12.42 Shall support a cloud-delivered security service that works with your existing Threat Prevention capabilities to deliver protections for evasive command-and-control (C2) threats using real-time traffic inspection via inline deep learning detection models.
- 4.12.43 The proposed solution, cloud-delivered deep learning models, **MUST** support the analysis of C2 threats over HTTP, HTTP2, SSL, unknown-UDP, and unknown-TCP applications.

- 4.12.44 As we see Cobalt Strike tools being prevalently used, the proposed solution's cloud-delivered deep learning models should be able to block against Cobalt Strike attack profiles.
- (a) Basic Attack Scenario: the product's essential protection against the most commonly available public attack profiles attempting data exfiltration and malware delivery via HTTP.
 - (b) Random Attack Scenario: the protection when the data transform language utilised in Cobalt Strike is leveraged to generate "randomised" attack scenarios using tools that are part of the Cobalt Strike arsenal of researchers and the public.
 - (c) Custom Attack Scenario: purposely chosen and modified attacks from the Basic and Random attack scenarios. The modifications were made to previously blocked attacks to confirm whether they would be sufficient to bypass the defences. The variables that are supported for customisation were modified using data transform language.
 - (d) Non-standard ports-based Attack Scenario: confirming whether the next-generation firewalls can continue to provide protection when attacks use HTTP over a nonstandard port.
 - (e) Hostname Change Attack Scenario: confirm if the next-generation firewalls continue to provide the same level of protection when the threat actors adjust/seed/modify the hostname used by a profile to evade reputation-based protection.
- 4.12.45 The proposed solution must support inline deep learning detection engines via threat prevention cloud to analyse traffic for command injection and SQL injection vulnerabilities in real-time to protect users against zero-day threats.
- 4.12.46 The proposed solution must support inline deep learning detection engines profile for SQL injection and Command injection.
- 4.12.47 The proposed solution must support adding exceptions to the detection profile for false-positives handling.

User Authentication

- 4.12.48 Shall provide a Cloud Identity Engine as a centralised, single-source, cloud-based identity solution for user identification and authentication.
- 4.12.49 The Cloud Identity Engine shall support next-generation firewalls in on-premises, cloud-based, or hybrid network environments.
- 4.12.50 The Cloud Identity Engine shall provide read-only access to an on-premises directory (Active Directory) or a cloud-based directory (Azure Active Directory) information for user visibility and policy enforcement.

- 4.12.51 The user authentication component of the Cloud Identity Engine shall allow the configuration of a profile for a SAML 2.0-based identity provider (IdP) that authenticates users by redirecting their access requests through the IdP before granting access.
- 4.12.52 Supports redistribution of User context information, such as User-to-IP Mapping, Tags or Quarantine Lists to other firewalls or devices.

High Availability

- 4.12.53 The proposed NGFW overall solution shall be available in High Availability (HA) Configuration.
- 4.12.54 Shall have the concept of HA1 and HA2 for High Availability configuration. Dedicated HA1 and HA2 will use the management plane for HA configuration. HA1 will be a dedicated HA port for the control link, and HA2 will be a dedicated HA port for the data link.
- 4.12.55 HA1 will be used as a control link, i.e., to exchange hellos, heartbeats, and HA state information and for management plane sync for routing and user-ID information. The Next Generation Security Platform will use this link to synchronise configuration changes with its peers.
- 4.12.56 HA2 will be used for data link i.e. to synchronise sessions, forwarding tables, IPSec security associations and ARP tables between Next Generation Security platforms in an HA pair. Data flow on the HA2 link will be always unidirectional (except for the HA2 keep-alive); it flows from the active to the passive next-generation security platforms.
- 4.12.57 Shall synchronise all sessions, decryption certificates, VPN security associations, threat and application signatures, configuration changes, and Forwarding Information Base (FIB) tables without additional management server, and no workaround shall be allowed.
- 4.12.58 For Active-Active HA setup, the proposed NGFW must have a dedicated HA3 port to function as a packet forwarding link for session setup and asymmetric traffic handling.

Policy Optimiser

- 4.12.59 The proposed solution must have the capability to analyse Port-based rule usage and convert it to a Layer 7 Application-Based rule without disrupting Network Traffic. This function must be achieved directly on the NGFW without relying on external software or a reporter.
- 4.12.60 Must be able to use Machine Learning to analyse existing Traffic Logs and, in return, provide Security Rules recommendations.

Tier 1 Firewall Requirements

- 4.12.61 The Tenderer shall propose 2 units of NGFWs capable of supporting application layer visibility and enforcement (i.e., default service ports lockdown without definition) with a minimum of 7.5 Gbps of threat prevention throughput per second for all inbound and outbound traffic concurrently.
- 4.12.62 Threat prevention throughput is calculated with firewall, app-id, vulnerability protection, AV, and Anti-spyware enabled concurrently on the same physical appliance. Disabled Server Response Inspection (DSRI) is disabled to inspect both direction of all traffic. The tenderer may be asked to demonstrate this during the evaluation process.
- 4.12.63 Shall support a minimum of 1,400,000 concurrent sessions and 145,000 new sessions per second.
- 4.12.64 Shall have a minimum of 12 10/100/100 RJ45 network ports.
- 4.12.65 Shall support at least 10 SFP/SFP+ ports for network traffic. Each port can operate as SFP (1Gbps) or SFP+ (10Gbps) based on the installed transceiver.
- 4.12.66 Shall support at least 4 SFP28 (25Gbps) ports.
- 4.12.67 Shall require redundant power supplies.

File and Data Filtering

- 4.12.68 Shall be able to alert or block specified true file types over specified applications and in the specified session flow direction (inbound/outbound/both). A custom notification page shall appear when a user attempts to download the selected file type.
- 4.12.69 Shall include the ability to identify and control the transfer of sensitive data patterns, such as credit card and Social Security numbers or custom data patterns, in both application content and file attachments.
- 4.12.70 Shall unpack zippedfiles with up to 4 levels of encoding, for packet inspection. There shall be an option to block or bypass inspection for files hidden in more levels of encoding.
- 4.12.71 Shall support the following data filtering profiles:
 - (a) Predefined Data Patterns;
 - (b) Built-In Support for Azure Information Protection and Titus Data Classification; and
 - (c) Custom Data Patterns for Data Loss Prevention (DLP) Solutions
- 4.12.72 Shall support the following file types for blocking both upload and download:
 - (b) PE files (.scr, .cpl, .dll, .ocx, .pif, .exe);
 - (c) Java files (.class, .jar) ;

- (b) Help files (.chm, .hlp);
- (c) other potentially malicious file types, including .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat; and
- (d) flash, .tar, multi-level encoding, .cab, .msi, encrypted-rar, and encrypted-zip files

4.12.73 Shall allow definition of custom file blocking response pages allow admins to provide more information to users when they see a response page.

Advanced Threat Protection

- 4.12.74 Shall support extensive (i.e. all threat signatures and heuristics rated as Low, Medium, High and Critical Severity enabled.) Threat Prevention Capabilities. Threat prevention throughput is calculated with firewall, app-id, vulnerability protection, AV, Anti-spyware enabled concurrently on the same physical appliance.
- 4.12.75 The solution shall be capable of supporting and analysing network traffic regardless of ports or encryption with full visibility, including web traffic (both HTTP, HTTP/2 and SSL), all email protocols (SMTP, SMTPS, IMAP, POP), FTP and SMB traffic to detect or prevent malicious malware and activity.
- 4.12.76 Shall perform stream-based antivirus and anti-spyware and not store and forward traffic inspection.
- 4.12.77 Shall support packet capturing as part of the IPS rule of specific threats for forensic evidence or investigation.
- 4.12.78 Shall analyse all DNS queries or requests and have the capability to allow, alert, block or sinkhole DNS request or query to blacklist and Packet Capture (pcap) the malicious domains.
- 4.12.79 Shall have the capability to determine the endpoint IP address that requested the blacklisted or malicious domains even when the request is proxied through an Internal DNS Server.
- 4.12.80 Shall have the capability to sinkhole DNS requests for blacklisted or malicious Domains to a configured destination IP address.
- 4.12.81 Shall be able to define different antivirus/vulnerability protection/antispyware/apt profiles for each security policy.
- 4.12.82 Shall have the capability to either select to download the content update only or download and install the content update according to the defined schedule.

- 4.12.83 Shall have the capability to define a Threshold to indicate the minimum number of hours after an update becomes available before the firewall will download it regardless of the schedule.
- 4.12.84 Shall support an out-of-the-box IPS signature converter plugin to automatically convert rules for Snort and Suricata intrusion prevention system (IPS) software into custom Palo Alto Networks threat signatures.
- 4.12.85 Shall support auto quarantine of High-Risk hosts, including threats detected to/from a specific host
- 4.12.86 Shall, out-of-the-box, be able to protect against C2 traffic, such as Empire and Cobalt Strike, derived from hack tools.

Anti-Malware Protection

- 4.12.87 The proposed solution must automatically support and apply the following prevention features. The unknown files should be analysed in-country.
 - (a) Anti-malware signature;
 - (e) URL filtering to block callback and download of malicious payload;
 - (f) DNS domain to block malicious domain; and
 - (g) C&C signature and URL to prevent C&C callback.
- 4.12.88 The proposed unknown malware solution should be in a single appliance for web and email and able to block threats on all detected applications without performance degradation.
- 4.12.89 Shall support protection against Advanced Persistent Threat (APT) via behavioural analysis regardless of protocol or encryption, with full visibility into all applications, users, and URLs (for web traffic) within a single appliance.
- 4.12.90 Shall be able to create Anti-Malware signatures based on payload to block malicious files, as well as DNS and URL signatures to block command-and-control communications. The signatures shall be downloaded and installed automatically on the security platforms every five minutes.
- 4.12.91 Shall be able to leverage the information captured from the APT solution and update the Anti-virus, Anti-Spyware/Botnet, IPS, and URL Filtering engines for protection within the same appliance.
- 4.12.92 Shall be able to identify the infected users and the application used by the APT malware and correlate with the firewall, URL filtering, and IPS event to provide rich contextual information.
- 4.12.93 Shall be capable of applying an APT profile based on users, source/destination IP addresses, and applications in a single policy for granular controls. Exemption can also be configured based on users, source/destination IP addresses, and applications.

- 4.12.94 The APT sandbox shall support both cloud-based and on-premises solutions and have the flexibility to use both or choose either method for file analysis. The on-premises appliance shall also support clustering to ensure high availability and redundancy.
- 4.12.95 Shall be able to classify credential phishing links found in emails and determine whether it is an exploit or malware.
- 4.12.96 The APT solution shall support the use of API calls for the submission of files or links for analysis and retrieve results from the analysis from both cloud and on-premises platforms.
- 4.12.97 The APT solution shall have the capability to support bare metal analysis (i.e. detonate the malware on real hardware) to detect evasive malwares.
- 4.12.98 The APT solution shall have the capability to perform APT malware update in real-time as soon as the signatures are generated, please provide proof. If a false claim is found, the product will be refunded, and the vendor will be penalized."
- 4.12.99 The APT function shall not further degrade the performance from the original Threat Prevention (Protection) throughput. If a false claim is found, the product will be refunded, and the vendor will be penalised.
- 4.12.100 The Malware Analysis Engine must be able to support the following Operation System Emulation:
- (a) Windows Operating System;
 - (b) Mac Operating System;
 - (c) Linux; and
 - (d) Android
- Note: Supplier must be able to support all Operating Systems or else will be considered as non-compliant.
- 4.12.101 The APT function shall provide an Inline Machine Learning (ML) based capability that dynamically detects malicious files of a specific type by evaluating various file details, including decoder fields and patterns, to formulate a high probability classification of a file.
- 4.12.102 The APT function shall support the holding file sample transfer while the NGFW queries the real-time signature cloud to perform a signature lookup. When the lookup is completed, the file is released to the requesting client, based on the security policy for specific verdicts. This shall help prevent the initial transfer of known malware; in other words, reduces the likelihood of a patient-zero outbreak from occurring.
- 4.12.103 The APT function shall support cloud-based ML detection engines that provide inline analysis of PE (portable executable) files traversing the network to detect and prevent advanced malware in real time. The Inline

Cloud Analysis shall prevent files from being downloaded and potentially spreading through your network while it performs real-time analysis of the target sample.

- 4.12.104 The APT Solution should be equipped with the following detection capabilities without performance degradation:
- (a) Malware Family Fingerprinting;
 - (b) Automated Unpacking;
 - (c) Steathy Observation;
 - (d) Intelligent Runtime Memory Analysis; and
 - (e) Malware Dependency Emulation

URL Filtering

- 4.12.105 Shall support integrated URL filtering/categorisation and has the ability to automatically query a master cloud-based database for URL category information when an unknown URL is found. Lookup results are automatically inserted into the cache for future activity.
- 4.12.106 Shall provide customizable end-user notifications with the following options:
- (a) a customizable block page with the feature of having a warning page with a "Warning and Continue" button when a user accessing a page potentially violating your URL Filtering policy; and
 - (b) a page informing a user that they are violating policy can include your corporate logo, references to the username, IP address, the URL attempting to be accessed, and the category of the URL.
- 4.12.107 Shall be able to apply URL category for file upload/download (e.g. prevent upload/download of executable files from unknown sites to limit malware propagation).
- 4.12.108 Shall be able to reference URL block list(s) customized by the organization that is hosted on-premises and have the capability to provide authentication when consuming this list(s). The Enterprise Security Platform shall dynamically check the list for changes at a regular interval without any manual administrative changes to the firewall configuration.
- 4.12.109 Shall be able to apply URL filtering to QoS policies for bandwidth control, based on specific URL categories.
- 4.12.110 Should be able to apply URL categories on the SSL decryption policies for selective decryption.
- 4.12.111 Shall include an individual user activity report showing applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period without additional software and hardware

modules. There shall be no exception to this clause and any workaround is NOT permitted.

- 4.12.112 Shall support logging of HTTP fields such as User-Agent, Referrer and X-Forwarder-For and include in the URL filtering logs to facilitate troubleshooting and forensic analysis. The HTTP headers in URL filtering logs are available for custom log forwarding to a syslog server.
- 4.12.113 The proposed solution must support updates to Malware, Phishing & C2 URL categories every 5 minutes automatically without any workaround.
- 4.12.114 Shall support Security Focus URL Categories without requiring deciding what website is likely to be exposed to web threats. The categories shall include:
 - (a) High risk, medium risk, and low risk—These categories indicate the level of suspicious activity that a site display. All URLs—except those that are confirmed malware, C2, or phishing sites—now include this risk rating; and
 - (b) Newly-registered domains—This category identifies sites that were registered within the last 32 days. New domains are frequently used as tools in malicious campaigns.
- 4.12.115 Shall support up to 4 multiple URL categories that classify the content, purpose, and safety of a site, including a risk rating that indicates how likely it is that the page will be exposed to threats.
- 4.12.116 More granular URL categorisations allow moving beyond a basic block-or-allow approach to web access. Instead, control how users interact with content, especially websites that, while necessary for business, are more likely to be used as part of a cyberattack (like blogs or cloud storage services). For example, allowing users to visit high-risk websites but enforce read-only access to questionable content by blocking obfuscated JavaScript and preventing dangerous file downloads.
- 4.12.117 Shall be able to inspect the SSL/TLS handshakes of web traffic such as inspecting the Server Name Indication (SNI) field, an extension to the TLS protocol found in the Client Hello message and enforce the matching Security policy rule if the domain in the SNI field belongs to a malicious URL category.
- 4.12.118 Shall support Machine Learning to provides real time URL analysis and malware prevention then classify them into benign or malicious categories.
- 4.12.119 Shall have layers of detection capabilities to provide the most comprehensive phishing. protection including
 - (a) ML-based image analysis;
 - (b) Static and dynamic analysis;

- (c) Deep recursive analysis;
- (d) Deep learning convolutional neural networks (CNN) model;
- (e) Append attack detection;
- (f) ML-powered domain analysis;
- (g) Deobfuscating JavaScript engine;
- (h) Phishing redirection chain analysis; and
- (i) Fake CAPTCHA interaction analysis

4.12.120 Shall support inline cloud-based deep learning detectors that evaluate suspicious webpage contents in real time to protect users against zero-day threats. This includes

- (a) Cloaked websites;
- (b) Multi-step attacks;
- (c) CAPTCHA challenges; and
- (d) Previously unseen one-time-use URLs

When the firewall processes a URL request containing suspicious webpage contents, it forwards the HTTP response data to the cloud and analyses the contents of the webpage that are deemed suspicious and categorizes them accordingly. "

4.12.121 Should be able to stop SaaS Phishing attacks by analysing both the page's image and text, as well as the source code of the web.

4.12.122 Should be able to prevent MiMT (Man-in-The-Middle) phishing attacks with the following methods:

- (a) Brand/Platform Identifier
- (b) Attribution Engine
- (c) HTTP Header Analysis

4.12.123 Should be able to prevent Phishing Kits attacks with the following methods:

- (a) Webpage Source Code Analysis
- (d) Attribution Engine
- (e) Kit Directory Analysis

Virtual Private Network (VPN)

General Requirements

4.12.124 Shall provide a complete VPN infrastructure for managing the mobile workforce to enable secure access for all users, regardless of what devices they are using or where they are located.

4.12.125 Shall support 6.6 Gbps of IPSEC VPN throughput.

4.12.126 The VPN infrastructure shall be supported on both IPv4 and IPv6 networks.

- 4.12.127 Supports route-based VPN where the firewall makes routing decision based on destination addresses. The firewall shall also interoperate with third-party policy-based VPN devices.
- 4.12.128 Supports IPSec Protocol for tunnel setup and ESP for TCP/IP packet encryption.
- 4.12.129 Supports IKE v1, v2 or both.
- 4.12.130 Supports Pre-shared key or certificate-based authentication.
- 4.12.131 Supports both physical L3 or a logical tunnel interface. The tunnel interfaces must be attached to a zone, where zone-based security policies will be imposed.

VPN Remote User Access

- 4.12.132 The remote access VPN shall provide a portal for managing the VPN infrastructure. All endpoints participating in the remote access VPN network shall receive configuration information from the VPN portal, including information about available VPN gateway(s) and any client certificates that may be required to connect to the gateways.
- 4.12.133 The VPN portal shall also control the behaviour and distribution of the VPN endpoint agent software for Mac and Windows OS. Both the VPN Portal and Gateways must be available out of the box without the need for additional appliances or solutions or licenses.
- 4.12.134 The remote access VPN solution must connect the users to the VPN Gateway regardless of whether they are outside the corporate network or within the corporate network. This is to ensure a consistent security posture to be put in place, regardless of their location. As such, the gateway shall provide security enforcement for traffic from the VPN client that includes both:
 - (a) External gateway for remote access client connectivity when they are outside the corporate network.
 - (b) Internal gateway for clients when they are inside the corporate network.
- 4.12.135 The external VPN gateway shall provide security enforcement and/or virtual private network (VPN) access for remote users. The remote users shall either connect automatically to the external gateways depending on the priority you assign to the gateway, source region, and the response time or connect manually to a list of gateways.
- 4.12.136 For the remote users that connect automatically to the external VPN gateways, they shall either connect automatically to the external gateways depending on the priority you assign to the gateway, source region, and the response time, or connect manually to a list of gateways.

- 4.12.137 The internal VPN gateway shall reside on the internal network, configured as a gateway for applying security policy for access to internal resources and it shall be used in conjunction with User-ID and/or Host Information Profile (HIP) checks to provide a secure and accurate method of identifying and controlling traffic by user and/or device state. The HIP function must be available out of the box without the need for additional appliances or solutions.
- 4.12.138 An endpoint remote access VPN agent can connect to the internal VPN gateway automatically after performing internal host detection to determine the endpoint's location.
- 4.12.139 The VPN clients can also be able to select and connect to the internal gateways by either source IP address or a pre-configured list of gateways based on DHCP options obtained from a DHCP server. No additional appliances or solution is required for either options.
- 4.12.140 The remote access VPN agent must support Windows and MAC OS, Linux, iOS, Android, Windows UWP and Chromebook devices.
- 4.12.141 The remote access VPN shall strictly support all the following authentication methods:
- (a) Local: Both the user account credentials and the authentication mechanisms are local to the firewall;
 - (b) External: The user authentication functions are performed by an external LDAP, Kerberos, TACACS+, SAML, or RADIUS service (including support for Microsoft Azure Active Directory two-factor authentication, token-based authentication mechanisms, such as one-time password (OTP) authentication);
 - (c) Client certificate: use a client certificate to obtain the username and authenticate the user before granting access to the system;
 - (d) Two-Factor: authenticate a user, such as a one-time password in addition to login credentials; and
 - (e) Multi-Factor: For sensitive, non-browser-based network resources (for example, financial applications or software development applications) that may require additional authentication.
- 4.12.142 The tenderer shall work with the School to set up user access authentication via the School's Azure Active Directory credentials, ensuring a single sign-on (SSO) experience. The tenderer should provide diagrams, workflows and integration descriptions. Azure AD Multi-Factor Authentication (MFA) should be enforced for all users accessing the system.
- 4.12.143 The remote access VPN must strictly support the integration with any third-party mobile endpoint management system, such as a mobile device management (MDM) or enterprise mobility management (EMM) system,

to manage both company-provisioned and employee-owned devices (such as in a BYOD environment).

- 4.12.144 The remote access VPN shall support a Host Information Profile (HIP) that allows the collection and enforcement of the following information:
- (a) Security patches;
 - (b) Anti-virus definitions;
 - (c) Disk encryptions;
 - (d) Jail broken or rooted devices;
 - (e) Specific software versions, included custom in-house applications; and
 - (f) The HIP function must be available out of the box without the need for additional appliances or solutions.
- 4.12.145 The remote access VPN solution shall support split tunnelling based on all the following:
- (a) Destination domain;
 - (b) Client Application;
 - (c) HTTP/HTTPS video streaming application; and
 - (d) This shall provide granular control based on applications, sensitive information as well as high bandwidth consuming traffic.

DNS Security

- 4.12.146 The proposed solution shall apply predictive analytics to disrupt attacks that use DNS for command-and-control or data theft or Malicious Newly Registered Domains (NRD).
- 4.12.147 Shall automatically protect against millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence. The malicious domain database sources should include and not limited to the following:
- (a) Malware prevention service;
 - (b) URL filtering service;
 - (c) Passive DNS and device telemetry;
 - (d) Threat Research Team; and
 - (e) More than 30 third-party sources of threat intelligence
- 4.12.148 Shall predict and stop malicious domain access from Domain Generation Algorithms-based malware with instant enforcement.
- 4.12.149 Shall provide limitless protection against malicious domains with a cloud-based database for infinite scale.
- 4.12.150 Shall be able to provide the below to neutralize DNS Tunnelling security issues:
- (a) Use machine learning to detect Command-and-Control or data theft hidden in DNS tunnelling quickly;

- (b) Extend Next Generation Security Operating Platform signature-based protection to identify advanced tunnelling attempts; and
 - (c) Rapidly neutralize DNS tunnelling with automated policy action
- 4.12.151 Shall integrate with the on-premises NGFW platform to automate dynamic response to block call-backs and find infected machines without manual intervention once relevant security policies are configured in the NGFW platform.
- 4.12.152 NGFW and DNS security policies should be controlled and integrated into a single management platform. Alerts from above should be coordinated across the entire security stack, including firewall policy violations, IPS/IDS, Web security and Malware Analysis.
- 4.12.153 Shall ensure that advanced security is seamlessly applied to DNS queries in real-time with no business impact.
- 4.12.154 Shall ensure strict privacy and security controls are in place to prevent unauthorized submissions of sensitive or personally identifiable information through industry-standard best practices for security and confidentiality on potentially malicious domains.
- 4.12.155 The proposed NGFW must support identifying and blocking of DGA domain without solely relying on Signatures.
- 4.12.156 Shall support automation of detection and response workflows which can automate the process of sinkholing malicious domains on the NGFW to cut off C2, rapidly identify infected users on the network, and even isolate them.
- 4.12.157 The proposed NGFW must support DNS Protection deployment by turning on a service without having to reroute your DNS traffic to outside resolvers.
- 4.12.158 The proposed solution shall support automation of detection and response workflows, which can automate the process of sinkholing malicious domains on the NGFW to cut off C2, rapidly identify infected users on the network, and even isolate them.
- 4.12.159 The proposed NGFW must be able to define separate policy actions as well as a log severity level for a specific signature type (e.g., C2, dynamic DNS, malware, newly registered domain, phishing, grayware, parked domain, proxy avoidance and anonymizers).
- 4.12.160 The proposed solution must be able to uses ML-based analysis to identify advanced DNS-based threats. Such as Domain Generation Algorithm (DGA), DNS Tunneling, Ultra-Slow DNS Tunneling, Strategically Aged Domains, Fast Flux Domains, Dangling DNS Attacks, Wildcard DNS,

NXNS Denial-of-Service Domains, Malicious Newly Registered Domains (NRD).

- 4.12.161 The proposed solutions can identify traffic contained in DoH (DNS-over-HTTPS) requests and apply DNS Security real-time protection measures.
- 4.12.162 A The proposed solution shall support the following coverage of DNS Attack Techniques:
- (a) Predictive Detection;
 - (b) Strategically Aged Domains;
 - (c) Subdomain Reputation;
 - (d) Stockpiled Domains;
 - (e) Compromised DNS Zones;
 - (f) Wildcard DNS;
 - (g) Dangling DNS;
 - (h) NXNS Attack;
 - (i) Ultra-slow DNS Tunnelling; and
 - (j) Squatting Domains (Fraud domains impersonating popular names)

Tier 2 Firewall Requirements

- 4.12.163 The Tenderer shall propose 2 units of NGFWs with a capability of supporting application layer visibility and enforcement (i.e. default service ports lockdown without definition) with a minimum of 10 Gbps of threat prevention throughput per second for all traffic in both inbound and outbound traffic concurrently.
- 4.12.164 Threat prevention throughput is calculated with firewall, app-id, vulnerability protection, AV, and Anti-spyware enabled concurrently on the same physical appliance. Disabled Server Response Inspection (DSRI) is disabled to inspect both direction of all traffic. The tenderer may be asked to demonstrate this as part of the evaluation process.
- 4.12.165 Shall support minimum 2,200,000 concurrent sessions and 205,000 new sessions per second.
- 4.12.166 Shall have a minimum of 12 10/100/100 RJ45 network ports.
- 4.12.167 Shall support at least 10 SFP/SFP+ ports for network traffic. Each port can operate as either SFP (1Gbps) or SFP+ (10Gbps) based on the installed transceiver.
- 4.12.168 Shall support at least 4 SFP28 (25Gbps) ports.
- 4.12.169 Shall require redundant power supplies.

4.13 Application Delivery Controller

Web Application Firewall (WAF)

- 4.13.1 The WAF must be only natively cloud based. The WAF Must have at least 321 Tbps in global capacity for DDoS protection.
- 4.13.2 Must support minimum two (2) domains for application security.
- 4.13.3 The WAF platform Must be able to run every WAF/ DDoS mitigation service on every pop/nodes.
- 4.13.4 Must provide 100% uptime Service Level Agreement.
- 4.13.5 Provider must provide 100% API first features and complete coverage for infrastructure as a code via Terraform.
- 4.13.6 Must update any configuration change globally within 30 seconds
- 4.13.7 A granular role-based system for granting multi-user access must be provided for both the web-based dashboard and API.
- 4.13.8 Dashboard access should support integration with Active Directory or with external Identity Provider (through federation protocols like SAML2.0)
- 4.13.9 All security mitigations shall be managed via single console and API.
- 4.13.10 Shall support complete administration of the solution through both a web-based GUI interface, and via an API. Using the same web-based dashboard and API to control WAF, CDN, DNS services.
- 4.13.11 Must provide the ability to configure rate limiting rules by HTTP request and response header fields, computed or derived values based on vendor-managed threat intelligence and HTTP request body fields on top of HTTP methods and response codes.
- 4.13.12 Must provide the ability to perform rate limiting by counting the number of requests over a period based on: IP address, IP with NAT support, Query, Host, HTTP Headers, Cookie, ASN, Country, Path, JSON body field.
- 4.13.13 Must provide the ability to perform rate limiting based on the complexity or cost of handling requests during a given period regardless of the total number of requests sent by the client
- 4.13.14 Rate limiting must provide a maximum sampling period of 1 day.
- 4.13.15 Must provide the ability to support up to 100 rate limiting rules per domain.
- 4.13.16 Must provide the ability to stack rate limiting rules on the same endpoint.

- 4.13.17 Must provide rate limiting to prevent abusive clients. Rate limiting must provide the ability to count the number of requests by source IP address. Rate limiting must also be able to identify individual users behind a NAT.
- 4.13.18 Must provide the ability to configure rate limiting rules to identify requests by HTTP methods and response codes.
- 4.13.19 Must provide the ability to provide custom responses for blocked requests, allowing for customer to define the response type, response code and response body.
- 4.13.20 The solution must have the ability to protect against the OWASP Top 10 Web application security risks for web and API traffic.
- 4.13.21 Should support the usage of AI/ML to uncover anomalies and predict the frequency and volumes of attacks as well as abnormal sequential paths used before they hit critical mass.
- 4.13.22 Must be able to enforce blocking of any attacks in-line, without any third-party integration
- 4.13.23 Must be able to provide rate-limiting recommendations in the dashboard to block against volumetric-based attacks by using a system of adaptive rate limiting based on the API endpoint's P99, P90 and P50 request rates.
- 4.13.24 Must be able to enforce rate-limiting rules in line with a one-click action from recommendation to the setting of custom rate-limiting rules to detect and block unknown and API endpoint attacks.
- 4.13.25 Must provide a metric to help evaluate the rule's effectiveness to adjust rate limiting and custom rule criteria or action.
- 4.13.26 Must support caching on URLs for both ignoring and including any query string, and this must be exposed as a configuration option.
- 4.13.27 Must provide the capability to serve “stale” content if all origin servers are offline, even where the cached version has expired.
- 4.13.28 Must provide a dashboard feature or API to facilitate the purging of content from the cache based on URL, Hostname, Cache-Tags or Prefix. Cache purges should take effect globally in less than 10 seconds and MUST be completed in less than 1 minute.
- 4.13.29 Must provide the ability to control cache TTL by status code.
- 4.13.30 Must provide a cache analytics dashboard. Analytic must include the details of requests summary, requests by source, cache status and top content types/paths/hosts/device types/countries.

- 4.13.31 Must provide the capability to filter traffic to origin servers to remove all traffic not useful to the origin, and to eliminate known or suspected malicious traffic. Providers **MUST** demonstrate their capability to deal with large-scale DDoS attacks against the hostnames terminated on their network to ensure continued availability of web properties.
- 4.13.32 Must provide an IP Reputation Database to verify users' IPs.
- 4.13.33 Must provide a global anycast network to protect all web applications and APIs proxied behind Cloudflare from L3, 4, and 7 DDoS attacks.
- 4.13.34 Must provide a list of cloud WAF IP ranges to be whitelisted on the origin servers. This should not be frequently changed to reduce configuration changes needed. Provider must also provide timely notifications if changes are made to these IP ranges.
- 4.13.35 Must provide the ability to see where their end-users are having trouble connecting to their proxy's digital properties. The solution must be able to show which end-users' traffic has failed to connect to the cloud proxy, where it failed to connect and why.
- 4.13.36 Must provide audit logs for user actions.
- 4.13.37 Must provide an option to push the audit logs stored in 3rd party storages (Google Cloud storage, AWS, Azure, etc.)
- 4.13.38 Must have the ability to integrate with 3rd party SIEMs (e.g. Sumologic, Splunk, etc.)
- 4.13.39 Must be able to deliver all content to end users over HTTP/2, HTTP/3 over IPv6, IPv4 or any appropriate combination of these.
- 4.13.40 Must be able to redirect HTTP traffic over HTTPS, as well as ensure other resources (such as images) are also loaded over HTTPS.
- 4.13.41 Must provide Certificate Transparency Monitoring to help customers spot malicious certificates and send email whenever a certificate is issued for one of the domains.
- 4.13.42 Must provide a way to support TLS 1.3. Providers **MUST** provide a way to control the minimum version of TLS allowed.
- 4.13.43 Must provide a way to implement SSL certificates using ECDSA as cryptography. Providers **MUST** provide a way to remove non-secure cipher suites.
- 4.13.44 Must support the uploading of customer-owned certificates and ordering of certificates from the dashboard.

- 4.13.45 For certificates managed by the provider, providers must automatically manage SSL renewal upon expiry.
- 4.13.46 The WAF service shall support HTTP Strict Transport Security (HSTS), customizable max-age value, the option to include sub-domain, HSTS pre-load and HTTPS redirection.
- 4.13.47 Must provide smart tiered caching technology by using specific upper tier and lower tier data centers to propagate content, minimizing static content requests to your server, while reducing bandwidth and total costs.
- 4.13.48 Must provide machine-learning anomaly score detection capabilities to allow the WAF to detect the likelihood that the request is malicious or contains a SQLi, XSS or RCE attack and block potentially malicious requests effectively. An attack score should be assigned to each request, and administrators shall be able to utilise these scores to build custom firewall rules.
- 4.13.49 The WAF service shall enable the administrator to create custom WAF rules based on vendor-managed threat intelligence open-proxy lists to block traffic against a list of known malicious ip address.
- 4.13.50 Must provide real-time visibility into firewall events triggered on the domain protected by the provider. Analytics MUST present all mitigations across various security solutions provided (e.g. Firewall, API security, DDoS) in a single dashboard and include details of requests, bandwidth, backend response types, threats, geolocation, and firewall events by the vendor.
- 4.13.51 Must have an AI Assistant to query the dashboard for and generate time series charts based on a request formulated with natural language.
- 4.13.52 Must support instant logs to access the live stream of traffic from the dashboard or CLI.
- 4.13.53 Must provide a way to create custom WAF rules to match a HTTP request body, or form submissions. Providers must support regex in creating such rules.
- 4.13.54 Must provide a way to log a HTTP request payload for WAF matched requests. Providers must support this logging in an encrypted, secure way.
- 4.13.55 The WAF service shall/must provide automated DDoS, Health Check and Security Alerts via email.
- 4.13.56 The proposed solution must minimally have industry recognition in the following analyst reports:
 - (a) 'Leader' in the Gartner® Magic Quadrant™ for Web Application and API Protection (WAAP)

- (b) 'Leader' in The Forrester Wave for Web Application Firewall.
- (c) 'Leader' in The Forrester Wave for DDoS Mitigation Solutions.
- (d) 'Leader' in GigaOm Radar Report for DDoS Protection"

4.13.57 Shall have the following certification/ OR equivalent:

- (a) ISO 27001
- (b) SOC 2 Type II
- (c) PCI DSS 3.2.1

4.14 Server Racks

- 4.14.1 The rack solution comprises IT Racks, Environmental Management, and accessories.
- 4.14.2 The solution includes subsystem Electrical and Safety compliance and Environmental and Mechanical Specifications.
- 4.14.3 The IT rack has the following specifications:
 - (a) 42U, Width600mm x Depth1100mm;
 - (b) UL2416 & EIA-310E certified;
 - (c) Minimum Net weight of 105.2 kg;
 - (d) Maximum permissible load of 1199.75 kg;
- 4.14.4 The input cable length shall be at least 3m.
- 4.14.5 The rack PDU shall feature network management capability via Web and SNMP, providing real-time remote monitoring and power management of connected loads.
- 4.14.6 The rack PDU shall have an environmental monitoring port for external temperature/humidity monitoring.
- 4.14.7 Professional service to transfer equipment in existing server racks to the new proposed server racks, including cabling works. Each rack has up to five servers.

4.15 Maintenance and Support for Existing Palo Alto 1420 Firewall and Uninterrupted Power Supply (UPS)

- 4.15.1 Tenderer shall provide maintenance and support services for the Palo Alto 1420 firewall and Uninterrupted Power Supply listed in *Annex B List of Existing Equipment: Firewall and Uninterrupted Power Supply*.
- 4.15.2 The maintenance and support services for Palo Alto 1420 Firewall shall be in accordance with the conditions outlined in Part 1 Section C Conditions of Software and Hardware Maintenance and Support.

Requirement for Uninterrupted Power Supply

- 4.15.3 Tenderer shall quote and replace existing UPS batteries listed in Annex B List of Uninterrupted Power Supply
- 4.15.4 The Tenderer shall provide Preventive Maintenance services for the Uninterrupted Power Supply (UPS) once every 6 months for the UPS listed in Annex B List of Uninterrupted Power Supply.
- 4.15.5 The Tenderer shall provide the maintenance services at the School's designated location within Singapore. The Tenderer shall note that the UPS Hardware may be relocated to new or other existing premises within Singapore. The Tenderer's obligations shall remain unchanged regardless of where the UPS Hardware is located during the Contract Period.
- 4.15.6 The Tenderer must be an authorized partner of the original equipment manufacturer ('OEM') of the UPS Hardware and be authorized by the OEM to provide maintenance services for the UPS Hardware which include firmware and maintenance services required under this Tender.
- 4.15.7 The Tenderer shall ensure that maintenance, diagnosis, or repair on the UPS Hardware shall not cause any interruption or disruption to existing operations of the School's systems. In the event that interruption or disruption is unavoidable, the Tenderer shall seek the School's approval to shut down the Hardware before proceeding with the works. For ad-hoc urgent works, maintenance windows are subject to the School's approval.
- 4.15.8 The Tenderer shall within 24 hours of the School's notification, restore the UPS Hardware that is defective or malfunctioning, to good working condition. In doing so, the Tenderer shall:
- (a) Permanently rectify the defect or malfunction; failing which it shall
 - (d) Perform a temporary bypass solution; failing which it shall
 - (e) Provide the School with UPS Hardware which is functionally equivalent to the defective component until the failure or malfunction is rectified.
- If a temporary bypass solution is provided, it shall only be used as an interim measure while rectifying the root cause.
- 4.15.9 The Tenderer shall perform diagnostic check to ensure that the UPS Hardware is functional.
- (a) The Tenderer shall adjust the UPS Hardware and ensure that they remain in good working condition.

- (b) The Contractor shall perform diagnostic programs on the UPS Hardware and perform backups of the hardware setup and/or configuration prior to taking any action.
- (c) The Contractor shall provide and supply labour, transport, material, replacement parts, and temporary loan sets necessary at no additional costs to the School. All replacement parts provided shall be in good working condition. Any test shall be performed to ensure that the parts are in good working condition at the Contractor's site prior to carrying out the replacement at the School's site.
- (d) The Contractor shall provide a report on all Preventive Maintenance Services provided, including:
 - a. the summary of the work done;
 - b. remedial actions taken;
 - c. a review of all service support performed; and
 - d. a report on whether the service levels have been met.

Replacement of Spare Parts

- 4.15.10 In performing the remedial maintenance services, the Contractor shall source spare parts to restore the UPS Hardware to good working condition, at the Schedule of Rate to the School.
- 4.15.11 The spare parts and/or replacement provided by the Contractor shall become part of the UPS Hardware and the property of the School. All the defective parts and components removed from the UPS Hardware when they are replaced with a good workable part, and except for hard disks, such defective parts or components shall become the property of the Contractor.
- 4.15.12 In the event of an announcement of the product's end of life by the OEM, the Contractor shall ensure that he has sufficient spares available to provide the maintenance service throughout the Contract Period.

4.16 Cabling Requirement

General Requirement

- 4.16.1 The Tenderer shall supply, but not limited to, fiber Patch cords and Cat 6A Patch cords, be responsible for performing patching from the patch panels to the network switches, as part of the implementation of the System.
- 4.16.2 All the cabling products supplied under this Tender shall be genuine and RoHS-compliant products. Online resources must be available for the verification of the products proposed.
- 4.16.3 The cables, accessories, components and patch cords shall be from a single manufacturer cabling solution.

- 4.16.4 All the installed cables shall be fixed and supported in an appropriate manner to a surface. No loose or trailing cables are permitted. Trunking shall be used in ceiling voids and on walls. There shall be no exposed cable present where the cable exists in the trunking to supply an outlet.
- 4.16.5 All cables shall be supported along their entire length and tied in bundles at 3-meter intervals with nylon tie wraps.
- 4.16.6 All cables shall be a distance away and not share the same shafts or voids used by power cables and lightning conductors. The minimum separation shall be about 100mm. For high-tension power cables, a minimum separation of 500mm will be required.

The Cat6a Cable:

- 4.16.7 Shall be connected to the RJ45 Category 6a patch panel in a star topology format. The length of each run shall not exceed 90 meters and should be continuous without any joints or splices. Shall be of 4-pair unshielded twisted pair (UTP), Category 6a and Low Smoke Zero Halogen (LSZH).
- 4.16.9 Shall consist of eight 23AWG copper conductors. Copper-clad aluminium is not permitted.
- 4.16.10 Shall be round in construction, with a maximum nominal diameter of 7.24 mm.
- 4.16.11 Shall have a minimum of 29mm of bend radius for the 4-pair UTP cable under no load.
- 4.16.12 Shall not include internal or external shields, screened components or drain wires.
- 4.16.13 Shall be tested and certified by an authorised organisation.
- 4.16.14 Shall comply with ISO/IEC 11801:2010, EN 50173 Part 1 through Part 5:2010 and 2011, ANSI/TIA-568-C, IEC 0603-7-4, IEEE 802.3 applications and Singapore's Codes and Regulations in this related field.
- 4.16.15 be capable of supporting the Ethernet applications of 802.3e 1BASE5, 802.3i 10BASE-T 10 Mbit/s over twisted pair, 802.3u 100BASE-TX, 100BASE-T4, Fast Ethernet at 100 Mbit/s w/auto negotiation, 802.3y 100BASE-T2 100 Mbit/s (12.5 MB/s), 802.3z 1000BASE-X Gbit/s Ethernet over Fibre Optic at 1 Gbit/s, 802.3ab 1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s, 802.3af Power over Ethernet (12.95 W), 802.3an 10GBASE-T 10 Gbit/s Ethernet over unshielded twisted pair, 802.3at Power over Ethernet enhancements(25.5 W) and 802.3az Energy Efficient Ethernet.

5 Comprehensive Network Security Penetration Testing Requirement

- 5.1.1 The contractor shall engage an independent party to conduct comprehensive security testing on the new Network Infrastructure before the commissioning of the System. The testing shall have both white-box and black-box testing and include, but not be limited to the followings:
- (a) Rogue Access Point Test;
 - (b) Encryption Attacks;
 - (c) Client Wireless Test;
 - (d) Modern Wireless Exploitation Attacks; and
 - (e) Distributed Denial of Services (DDos) Test.
- 5.1.2 The quoted cost for the comprehensive security testing shall include all the tools, software, professional services, and any other necessary equipment required for the security testing and provided by the Contractor, or the independent party engaged by the Contractor. The security testing shall not jeopardise the availability, performance, integrity, confidentiality, and security of the SSP's systems, network, and data.

The Rogue Access Point Test:

- 5.1.4 Involve a rogue access point to be implemented within the target wireless network environment and comprises TWO (2) parts:
- (a) The rogue access point will seek to impersonate or spoof a valid access point by using the same SSID as the valid one to elicit connections from client devices and analyse connection attempts and data to obtain wireless credentials or compromise a client device; and
 - (b) A user connecting to the rogue access point will attempt to connect to a wired network using a different SSID to create a wireless environment and gain unauthorised access to the network.

The Encryption Attacks Test:

- 5.1.5 Shall attempt to exploit the encryption technologies implemented in the new Network Infrastructure using publicly available exploits/tools and conventional methods such as:
- (a) Brute force testing of the encryption key in use and
 - (b) Forge PKI certification (EAP-TLS) Shall observe wireless network traffic for over three (3) hours or more, analyzing the packets for any sensitive data or data and providing an indication of approaches to compromise the environment or end-user devices.
- 5.1.7 Simulate an access point to transmit de-authentication disassociation frames to all its clients by including the use of broadcast and multicast addresses in the source address field.

The Client Wireless Test:

5.1.8 Shall attempt session hijacking, certificate or credential theft against the new SSP Network Infrastructure.

5.1.9 Shall aim to attack client devices for weakness in the underlying wireless stack and card drivers.

The Modern Wireless Exploitation Attacks Test:

5.1.10 Attempt Man-in-the-Middle attacks in the new Network Infrastructure, particularly the component of the Wireless Network.

5.1.11 Exploits the Wireless component of the new Network Infrastructure through features available only in a modern wireless network.

The DDoS Test: Shall attempt DDoS attacks in the new Network Infrastructure, particularly the component of the Wireless Network.

5.1.13 Shall attempt to bring the new Network Infrastructure to a complete halt by overloading the access points or jamming the wireless such that legitimate users can no longer gain access to the SSP network.

6 MAINTENANCE AND SUPPORT SERVICES

6.1 During the stipulated Contract Period in this **Part 2, Requirement Specifications**, the Contractor shall render replacement parts and diagnostic services and any other works and services in accordance with the Maintenance Contract pursuant to **Part 1, Section C** in this Invitation to Tender for

6.1.1 the System, based on the Contractor's submitted 1st Schedule, pursuant to Clause 17 of **Part 1, Section C**; and

6.1.2 the list of School's existing network equipment under **Annex B of Part 2**.

Pursuant to Clause 4.3 of **Part 1, Section C**, the Tenderer is required to indicate in their Tender proposal the selected option for the Remedial Maintenance.

6.2 Where during the stipulated Contract Period for the provision of software support and hardware maintenance for the System or any part thereof is found to be:

(a) defective in either design, materials or workmanship; or

(b) not in accordance with the Contract; or

(c) having been installed, operated, stored and maintained in accordance with the written instructions of the Contractor, fails to function properly or fails to meet any performance guarantees set forth in the Contract or any additional requirements which may be mutually agreed between the School and the Contractor;

then, unless it is shown that the foregoing is caused solely by improper use or mishandling on the part of the School, the Contractor shall, at its own expense (including but not limited to transportation costs, air freight charges, costs of testing, manufacturing and examination), upon notification from the School, replace or completely repair the defective parts of the System or otherwise completely rectify the defects.

6.3 For the purpose of **Clause 6.2** above, the phrase "improper use or mishandling on the part of the School" shall include unapproved modifications to the System by the School. In this Clause, the phrase "unapproved modifications to the System by the School" means modifications made to the System by the School without the approval of the Contractor but does not include:

(a) modifications made in accordance with or pursuant to documentation provided by the Contractor;

(b) modifications to the System to enable it to meet the Requirement Specifications or such additional requirements as may be agreed between the School and the

- Contractor;
 - (c) configuration of the System;
 - (d) installation of approved System Software into the System; or
 - (e) installation of System Software or types of System Software which the System is intended to work with.
- 6.4 Maintenance and support must include all additional hardware purchased under this contract.

7 PROJECT IMPLEMENTATION SCHEDULE

- 7.1 The Contractor shall provide a detailed project schedule that can meet the milestones described in **Schedule 2 of Part 1, Section B**. The project schedule shall show details up to task level, start date, end date and the resource involved. The project schedule shall reflect possible overlaps between key activities and their interdependencies.
- 7.2 The Contractor may propose a schedule to achieve the milestones earlier.
- 7.3 The Contractor shall draw up the schedule using Microsoft Project and submit the softcopy and PDF version to the School within **TWO (2) Calendar weeks** from the Letter of Acceptance date. The schedule shall be submitted as part of the milestone for submission of the implementation plan in **Schedule 2 of Part 1, Section B**.

Annex A – List of Existing School’s Network Equipment

Annex B – List of Existing Equipment: Firewall and Uninterrupted Power Supply

(Note: The Annexes will be provided by the School after the compulsory Tender Briefing and upon the Tenderer’s submission of the duly signed off Confidentiality and Data Protection Undertaking under Schedule 5 of Part 1, Section B)