Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St. Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

# TERMS OF REFERENCE

**Supply, Delivery, Installation, and Configuration of:**

**OSG Data Center with Wide Area Network Solution & Next Generation Firewall for multi-branch setup**

**and**

**OSG Relocated Division's Data and Network Infrastructure**

## RATIONALE

The OSG Data Center Project aims to improve the organization's IT infrastructure's efficiency, security, and reliability. The organization can achieve a highly optimized and automated data center environment by implementing a hyper-converged solution using VSAN, WAN solution with a next-generation firewall deployment housed in a smart cabinet.

The hyper-converged solution using VSAN combines computing, storage, and networking resources into a single platform, eliminating the need for separate infrastructure components and reducing complexity and costs. The smart cabinet provides a self-contained and highly efficient infrastructure for hosting IT equipment, enabling the organization to reduce energy consumption, minimize space requirements, and simplify management.

The WAN solution with next-generation firewall deployment enhances network security by providing advanced threat protection, intrusion prevention, and secure remote access. The SD-WAN linking the main and branch office and co-location facility improves connectivity and enables the organization to streamline network management and reduce costs.

The OSG is also establishing a connection between a second location (Convergys One Building located at 6796 Ayala Avenue, corner Salcedo Street, Legaspi Village, Makati City) and its present local area network to increase its data and network capacity. The project will be the focal point for all data management,

processing, and archiving. The provision of access to computing and storage resources will support various OSG ICT application systems and services.

## OBJECTIVES

The OSG Data Center Project aims to create a highly available, secure, and scalable data center environment that can support the organization's mission-critical applications and services. The organization can improve operational efficiency, reduce costs, and enhance the overall user experience by leveraging advanced technologies and solutions. Additionally, the project aims to comply with industry standards and best practices for data center design and operations to ensure a highly resilient and reliable IT infrastructure.

The Relocated Division's Data and Network Infrastructure Project aims to provide the OSG with a modern, scalable, and secure data center infrastructure that will support its growing needs for data storage and processing. It also aims to implement and maintain a secure and efficient information technology infrastructure for the offsite office. The plan includes a data cabinet with a backup power supply, wireless infrastructure for all relocating legal divisions and units, a rackmount server, and storage to link the primary and off-site office spaces.

## TERMS

1. *Scope.* - Supply, delivery, installation, and configuration of: (a) OSG Data Center with wide area network solution & next generation firewall for multi-branch setup, and (2) OSG Relocation Data and Network Infrastructure.

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Seventeen Million Four Hundred and Sixty Thousand Pesos (₱17,460,000.00), inclusive of all government taxes, charges and other standard fees**.

| ITEM | QTY |
|---|---|
| **Hyper-converged Infrastructure with Single Integrated Rack Solution** | |
| – Single Integrated Rack Solution | 1 unit |

| | |
|---|---|
| – Hyper-converged Infrastructure (Server, Storage, Network Switches) | 1 lot |
| – Network Attached Storage (for Backup and Replication) | 1 unit |
| **WAN Solution with NGFW** | |
| – Wide Area Network Solution with Next Generation Firewall for multi-branch setup | 1 lot |
| **Relocation Data and Network Infrastructure** | |
| – 42RU Data Cabinet and 2KVA UPS with quick-release and reversible doors<br>– Rackmount Server with dual CPU<br>– LAN and Wireless Connectivity<br>– Network Attached Storage<br>– Next Generation Firewall | 1 lot |

3. *Payment.* - The OSG shall pay the Supplier in accordance with the following schemes/schedules:

| | Particulars | Remarks/Conditions |
|---|---|---|
| First Release | a) 15% Mobilization Payment | The amount represents the mobilization fund. The Supplier shall submit a written request within five days upon receipt of the signed and notarized Contract. |
| Second Release | b) 65% of the Total Contract Price, net of Mobilization Payment | Within fifteen days from delivery of Hyper-converged Infrastructure with Single Integrated Rack Solution and WAN Solution with NGFW. |
| Third Release | c) 30% of the Total Contract Price | Within fifteen days from completion of the scope of work, knowledge transfer for end-users (based on certification from the Case Management Service), and issuance of the |

| | | |
|---|---|---|
| | | Inspection and Acceptance Report by the OSG. |
| Fourth Release | d) Retention Fee equivalent to 5% of the Total Contract Price. | In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty security shall be required from the Supplier for one year from the issuance of the Inspection and Acceptance Report by the OSG. |

4. *Delivery*. The Supplier has thirty (30) calendar days (inclusive of Saturdays, Sundays, and holidays) from the date of receiving the Notice to Proceed (NTP) to deliver and install all equipment to the designated location and complete the scope of work. The Supplier shall follow the health and safety protocols imposed by the OSG and/or the concerned Building Administrator.

5. *Training*. The Supplier must provide the necessary comprehensive training/knowledge transfer program for the end users (IT) and other users (TWG for ICT, BAC, and BAC Secretariat) within ten days from completion of the installation and/or configuration of the equipment. The training shall be conducted by personnel certified by the provider of the solution being offered.

6. Qualifications of the Supplier:

   a. The Supplier shall have an SLCC that is at least one contract similar to the Project the value of which, adjusted to current prices using the PSA's Consumer Price Index, must be equivalent to at least fifty percent of the ABC, completed within five years prior to the deadline for the submission and receipt of bids.

      - For this purpose, similar contract shall refer to procurement contract of ICT equipment with hyper-converged infrastructure, wireless LAN infrastructure solutions for enterprises, and/or other similar contracts.

b. The Supplier must present a Client Satisfaction Rating for at least five contracts with government agencies and/or private corporations with whom the Supplier has previous or ongoing contract/s similar to this project.

c. The Supplier shall submit a valid and current Certificate of Distributorship/Dealership/ Resellership of the product being offered, issued by the principal or manufacturer of the product (if the Supplier is not the manufacturer). If not issued by the manufacturer, they must also submit a certification/document linking the Supplier to the manufacturer.

d. The Supplier shall have at least three personnel (with relevant certification) to support the solution being offered.

e. The Supplier must have a main or satellite office within 150 kilometer radium from the OSG Building or Convergys One Building.

f. The Supplier shall submit documents relevant to the project, such as but not limited to the following:

- Valid DTI or SEC Registration;
- Valid and Current Business Permit;
- Tax Clearance Certificate as finally reviewed and approved by BIR;
- Statement of contracts completed which are similar in nature to the contract to be bid; and
- Net Financial Contracting Capacity (NFCC) Computation.

7. Applicable provisions of the Government Procurement Reform Act (RA No. 9184) and its Revised Implementing Rules and Regulations (RIRR) shall form part of the Terms of Reference (TOR).

# Technical Specifications:

| HYPER-CONVERGED INFRASTRUCTURE WITH SINGLE INTEGRATED RACK SOLUTION | | |
|---|---|---|
| **Item** | **Specifications** | **Compliance** |
| **Single Integrated Rack Solution** | | |
| | The all-in-one data center solution shall include rack, containment design with cold/hot aisle, IT cooling unit, centralized monitoring & management system, UPS, power distribution unit and emergency ventilation system | |
| GENERAL | | |
| | • All-in-one single rack solution, equips with power protection, power management & distribution, IT cooling and monitoring system | |
| | • Cabinet dimension (Width x Depth x Height) 600mm × 1200mm × 2150mm | |
| | • Integrated with cold aisle and hot aisle containment design with tempered glass door. | |
| | • Front and rear door shall equip intelligent door lock. Support local door access via proximity card and key and remote door authorization via IP-based web interface. | |
| | • Rack shall have in-built tri-color intelligent lighting. Enable health indication of infrastructure. | |
| | • Shall offer at least 24RU IT usable space. | |
| | • Shall support at least 3kW IT load. | |
| | • Incoming power requirement of 50A/1P and voltage (Vac), 198Vac ~ 254Vac. | |
| STANDARD FEATURES | | |
| | • Single rack with integration of power protection, thermal management, and monitoring & management under centralized platform, provides stable operating condition for IT device. | |
| | • Fully enclosed operation and internal cooling circulation system, to ensure cleanliness of cabinets and with temperature control, prolong the life of IT equipment. | |

| | | |
|---|---|---|
| | The compact and low noise design shall suit for office area application. | |
| | • The system shall support high availability in term of cold air supply. UPS to backup cooling unit in the event of power outage. | |
| | • The system shall equip with intelligent control functions such as integrated environment monitoring, device monitoring and alarm notification, provide centralized monitoring platform for computer room management. | |
| | • 9" LCD touchscreen panel provides intermediate status of rack in term of UPS status, thermal profile, security management and alarm notification. | |
| | • The system shall have front & rear door electronic door access control. | |
| | • This electronic door access shall grant authorized user access to equipment via card authentication. | |
| | • This electronic door access shall grant access for scheduled times & selected door access (Front or rear) for each ID card configured. | |
| | • This electronic door lock shall support remote door access authorization via IP based web hosting. | |
| **RACK** | • Rack can house 19" rack mount hardware equipment which complies with the industry-standard (EIA-310-D). The whole cabinet system shall be fully enclosed during operation, to keep the system clean and dust free. | |
| **POWER MANAGEMENT UNIT (PMU)** | | |
| | • The power management unit shall manage power distribution and surge protection to the entire rack system. | |
| | • PMU shall act as centralized power management to supply and distribute power to devices, with Level C SPD protection. The power distribution of the whole unit shall meet the requirements of Level C lightning protection test. | |
| | • It shall pass the lightning protection test of L-PE and N-PE 15kA and meets the YD/T944 standard. | |

| | | |
|---|---|---|
| | • The PMU and all electrical wiring components within the integrated rack system shall be preinstalled from the factory. | |
| **RACK POWER DISTRIBUTION UNIT (rPDU) 0U TYPE** | | |
| | The system shall have dual intelligent power distribution units (PDU) setup. | |
| | • 2 x Intelligent switched PDU 16 ways 12 x C13 + 4 x C19; 16 A max allowed | |
| The intelligent PDU shall support: | | |
| | • Branch level current metering | |
| | • Remote on/off control of individual receptacles. | |
| | • Sequential start-up setting for individual receptacles. | |
| PDU shall have secure remote administration interface via the in-the-rack monitoring module. Easy and accessible integral web-based managing tool. | | |
| | • Logging of all authentications, and configuration changes. | |
| | • Real-time electrical parameters such as information display of voltage, amps, kW, power factor and kW-hr. | |
| | • E-mail and SMS notification to multiple users in case of events. | |
| | • Power switch control of individual receptacles | |
| | • Sequential start-up setting for individual receptacles | |
| **UPS SYSTEM** | | |
| | The system shall have rack mount UPS with capacity of 6kVA/6kW supporting IT load & IT cooling. UPS shall utilize double conversion online topology designed to protect electronic equipment by supplying reliable, network-grade power featuring extremely tight voltage and frequency regulation. | |
| UPS shall design as per following standards: | | |
| **UPS Input:** | • Voltage: Input/output voltage specifications of the UPS shall be | |
| | ❖ Rectifier AC Input: 220/230/240VAC, single-phase, | |

| | | |
|---|---|---|
| | two-wire-plus-ground | |
| | ❖ Bypass AC Input: 220/230/240VAC, single-phase, two-wire-plus-ground | |
| | ❖ AC Output: 220/230/240VAC, single-phase, two-wire-plus-ground | |
| | • Frequency Range: 40 - 70Hz | |
| | • UPS inrush current not to exceed 1.5 times rated input current | |
| | • Current distortion less than 5% THD at full load input current in double-conversion mode | |
| | • The UPS shall have built-in protection against surges, sags and over current from the AC source. The protection must sustain input surges of 4kV (Line to ground) without damage as per criteria listed in EN 61000-4-5: 1995 | |
| **UPS Output:** | • 100% of load rating for any load from 0.5 lagging to unity load power factor | |
| | • Voltage Tolerance: | |
| | ❖ ±1% RMS average for a balanced, three-phase load | |
| | ❖ ±2% for 100% unbalanced three-phase load | |
| | ❖ +/- 3% for parallel UPS | |
| | • Voltage Distortion: | |
| | ❖ <2% for 0-100% linear loads | |
| | ❖ <4% for 0-100% Non-linear loads • System efficiency up to 95.5% | |
| | • Phase Imbalance: | |
| | ❖ Balanced loads 120° ±1° | |
| | ❖ 100% unbalanced loads 120° ±1° | |
| | • Frequency Regulation: Synchronized to bypass: ±3.0Hz default setting | |
| | • Voltage Transients (average of all three phases) meets IEC 62040-3: 2010 Figure 2 Curve 1, Class 1 & ITIC and | |

| | | |
|---|---|---|
| | CBEMA Curve Requirements. | |
| | • Overload Capacity: | |
| | ❖ 105% - 125% of full load for 5minutes | |
| | ❖ 125% - 150% of full load for 1minute | |
| | ❖ >150% of full load for a minimum of 200 milliseconds | |
| | • Load crest factor without derating 3:1 | |
| | • Dynamic response recovery time of 60ms. | |
| **UPS Characteristics** | | |
| | • UPS form factor, 2RU. | |
| | • Battery system in-rack: sealed, non-spillage, maintenance-free lead-acid battery | |
| | • Standard 1 unit of rack mount battery, for 7 minutes runtime at 3kW load | |
| **UPS must Comply to standards:** | | |
| | • **General safety requirements:** EN62040-1/IEC62040-1 | |
| | • **EMC requirements:** EN62040-2/IEC62040-2 (Class C2) | |
| | • **Method of specifying the performance and test requirements:** EN62040-3/IEC62040-3(VFI SS 111) | |
| | • Safety of information technology equipment, including electrical business equipment: EN60950 | |
| | • Moisture, dust, and high-altitude test: GB/T 2423.21-2008 | |
| | • Energy star certified: 2011/65/EU uninterruptible power supplies version 1.0 program | |
| **COOLING SYSTEM** | | |
| | • The compressor shall come with an environment-friendly refrigerant (R410A), and inverter type arrangement with variable capacity operation of 30% to 100%. | |
| | • This cooling unit shall have an integrated condenser, | |

| | | |
|---|---|---|
| | compressor, and evaporator within the cooling housing, eliminate the need to have outdoor mechanical installation. | |
| | • Total airflow shall have at least 750 CMH | |
| | • This system shall enable eco mode function. Allow drawing ambient air into the rack intelligently to maintain other maximum operating condition of IT devices. It shall perform automatic changeover to air conditioning mode when the ambient condition exceeds threshold setting. | |
| | • UPS shall back up the cooling unit during power outage. To ensure continuous cold air supply. | |
| **FAN MODULE (EMERGENCY VENTILATION)** | | |
| | The system shall have emergency ventilation to prevent high-temperature partial buildup inside the cabinet in the event of cooling system failure. Fan module shall start up automatically when overheating happens within the cabinet, to prevent the devices from operating in at high temperatures. When the system is normalized, the emergency ventilation shall switch off to ensure an airtight environment in the system and high efficiency cooling of the air conditioner. | |
| **MONITORING** | | |
| | • All components shall pre-integrated and pre-configured from the factory. | |
| | • The centralized monitoring appliance shall pre-integrated in system | |
| | • The system shall equip environmental sensors (temperature sensor & water leak sensor) | |
| | • The monitoring appliance support USB port for wireless modem connection, for SMS capability and digital input sensor for DI input monitoring appliance. | |
| | • The system shall equip with intelligent Tri-color LED lighting. To indicate health status of cabinet. | |
| | • The system shall have front & rear door electronic door access control. | |

| | | |
|---|---|---|
| | • The monitoring system shall monitor the state of intelligent devices, record alarm events, and notify the user of the intelligent device alarms through email or SMS mode. It shall enable operating parameters setting and view device states through the embedded Web HMI, moreover, it shall send the states of the monitored intelligent devices to the network management software (NMS) through SNMP protocol mode. | |
| **Monitoring Standard Package includes features as follows:** | | |
| | • Alarm Management | |
| | • Data Log History | |
| | • Device Management | |
| | • Integration-ready for monitoring of third-party fire-suppression activation | |
| **OPERATION CONDITIONS** | | |
| The operation environment requirements are: | | |
| Installation position | The installation site needs to be level; | |
| | The height of using space should not be less than 2400mm (If the Airduct is included, the height of using space should not be less than 2700mm) | |
| Installation field | In the computer room and office area, the front door is more than 1.2m away from the wall or obstacles and the rear door is more than 1.0m away from the wall or obstacles. | |
| Ambient temperature | Indoor: 0°C ~ 40°C | |
| Ambient humidity | 80%RH | |
| Altitude | For the UPS, the altitude is required to be: < 3000m, derating is required when the altitude is above 3000m with reference to GB/T3859.2; For the air conditioner, derating is required when the altitude is above 1000m | |
| Rated Operation Voltage | Single phase, L+N+PE, 220Vac/230Vac/240Vac; 50/60Hz | |
| Storage environment | Indoor and clean | |
| Ambient humidity | Ambient humidity | |

| | | |
|---|---|---|
| ≤95%, (40°C) RH | ≤95%, (40°C) RH | |
| **Warranty** | With at least one year warranty on parts and labor, on-site, and includes 1 PM visit for 1 year. | |
| **Implementation** | Must include Installation and Start-Up Services | |
| | The Supplier must be the Reseller of the brand being offered (must provide Manufacturer or Reseller Certificate). | |
| Support Service Requirement | The Supplier must provide the following: | |
| | * Unlimited corrective maintenance/ repair services within the warranty period | |
| | * Eight hours by five days, Monday to Friday technical support and must meet the following response and resolution time: | |
| | > Within one (1) hour for phone or email support | |
| | > Within two (2) hours response time for onsite support | |
| | > Root cause analysis for all support cases filed. | |
| | * Submission of Service Report within 5 calendar days after rendering service | |
| | The Supplier must provide full documentation for Activity Plan on the installation of patches and upgrades and Root Cause Analysis for incidents encountered. | |
| | The Supplier must provide onsite support for the installation and deployment of software patches and version upgrades. | |
| | The Supplier must provide access to the Vendor portal for download of the latest product contents, patches, updates/upgrades including extensive online-self-help resources and knowledge base. Advisory to patches and fixes shall also be provided | |
| | The Supplier must provide a procedure for support and problem escalation. | |
| | The Supplier must conduct system health checks every quarter with the following scope:<br>• System/Application patches, fixes, security patches, and alerts<br>• System/Application profile | |

| | | |
|---|---|---|
| | • Resource utilization<br>• Log analysis<br>• Formal reports on the output of conducted health checks within 5 days | |
| Other Warranty and After Sales Requirements | * Immediate replacement of the equipment and/or its parts. | |
| | * The Supplier shall replace a factory defective unit with a new unit within 30 days upon delivery of the item. | |
| | The Supplier must provide a certificate for the above services as part of the technical requirements. | |
| | | |
| **Supply, delivery, and installation of Three (3) nodes pre-validated hyper-converged infrastructure (HCI) system.** | | |
| **HCI Nodes** | | |
| **Features** | | |
| Form Factor | Must be 2U Rack Server per node | |
| Processor | Must have 1 x Intel Xeon Gold 5320 20C 150W 2.3GHz Processor per node | |
| Storage | Must have 2 x 1.6TB Mainstream SAS 12Gb Hot Swap SSD per node | |
| | Must have 10 x 8TB 7.2K SAS 12Gb Hot Swap 512e HDD per node | |
| | Must have 2 x 480GB SATA 6Gbps Non-Hot Swap SSD per node | |
| Memory | Must have 8 x 32GB TruDDR4 3200 MHz (2Rx8 1.2V) RDIMM per node | |
| Network | Must have 1 x 10Gb 4-port Ethernet Adapter per node | |
| Security | Must be Trusted Platform Module 2.0, Chassis intrusion switch, Power-on password | |
| Cooling | Must have 5 x Performance Fan per node | |
| Power Supply | Must have 2 x 750W (230V/115V) Platinum Hot-Swap Redundant Power Supply per node | |

| | | |
|---|---|---|
| Software Requirement | The proposed solution must be a hyperconverged compute and storage, scale-out architecture | |
| | Must support storage thin provisioning. | |
| | Must support Per-VM snapshots and replication. | |
| | Must support native Block Services via iSCSI. | |
| | Must come with management software providing single pane of glass regardless of solution size. | |
| | Must support the latest version of MS Hyper-V or VMware vSphere | |
| | Must have Integrated or native hypervisor. | |
| | Must be ready for data-at-rest encryption solution with an upgrade of HCI license. | |
| | Must be ready for data-In-transit encryption solution with an upgrade of HCI license. | |
| | Must be ready for file services supporting SMB and NFS protocols with an upgrade of HCI license. | |
| | Must be ready for Data Persistence platform for modern stateful services with an upgrade of HCI license. | |
| | Must be ready for RAID-5/6 and Erasure Coding with an upgrade of HCI license. | |
| | Must support QoS and set IOPS Limit | |
| | Must support call home remote support. | |
| | Must include license with Three (3) Years support. | |
| | The proposed HCI Software must be among the Leaders of Gartner Magic Quadrant: Hyperconverged Infrastructure evaluation, Q3 2020 or later. | |
| **Warranty and Support** | Must be three years with a single point of global contact available 24x7 for both hardware and software support and drive retention | |
| **Switch** | Must include network top of rack switch | |
| **Key Features** | Must be Stackable Layer 3 switches with BGP, EVPN, VXLAN, VRF, and OSPF with robust security and QoS | |

| | | |
|---|---|---|
| | For enhanced visibility and troubleshooting, Network Analytics Engine (NAE) automatically monitors and analyzes events that can impact network health. Advanced telemetry and automation provide the ability to easily identify and troubleshoot network, system, application and security related issues easily, through the use of python agents, CLI-based agents, CLI-based agents, and REST APIs | |
| | Empowers IT teams to orchestrate multiple switch configuration changes for smooth end-to-end service rollouts through NetEdit that introduces automation that allows for rapid network-wide changes and ensures policy conformance post network updates. Intelligent capabilities include search, edit, validation (including conformance checking), deployment and audit features. | |
| | Flexible cloud-based or on-premises management for unified wired, WLAN, SD-WAN, and public cloud infrastructure network operations. Designed to simplify day zero through day two operations with streamlined workflows. | |
| | Supports Dynamic Segmentation that enables seamless mobility, consistent policy enforcement, and automated configurations for wired and wireless clients across networks of all sizes. | |
| | Supports an easy-to-use mobile app simplifies connecting, stacking and managing switches for unparalleled deployment convenience. | |
| **Quality of Service (QoS)** | Strict priority (SP) queuing and Deficit Weighted Round Robin (DWRR) | |
| | Traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues | |
| | Transmission rates of egressing frames can be limited on a per-queue basis using Egress Queue Shaping (EQS) | |
| | Large buffers for graceful congestion management | |
| **Resiliency and High Availability** | High performance front plane stacking for up to 10 switches in a stack via chain or ring topology | |
| | Flexibility to mix both modular and fixed switch series models within a single stack | |
| | Hot-swappable power supplies and fans | |

| | | |
|---|---|---|
| | Provides N+1 and N+N redundancy for high reliability in the event of power line or supply failures | |
| | Supports Virtual Router Redundancy Protocol (VRRP) that allows groups of two routers to dynamically back each other up to create highly available routed environments. | |
| | Supports Unidirectional Link Detection (UDLD) that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks. | |
| | Support for IEEE 802.3ad LACP to up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm. | |
| | Ethernet Ring Protection Switching (ERPS) supports rapid protection and recovery in a ring topology | |
| | IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w | |
| **Performance** | Up to 880 Gbps in non-blocking bandwidth and up to 654 Mpps for forwarding | |
| | Supports 10GbE/25GbE uplinks and large TCAM sizes ideal for mobility and IoT deployments in large campuses with several thousand clients | |
| | Switch Virtual Interfaces (dual stack) capacity up to 1,024 | |
| | MAC table capacity up to 32,768 entries. | |
| | VRF capacity up to 256. | |
| **Connectivity** | 24x 1G/10G SFP+ and 4x 1G/10G/25G SFP56 ports | |
| | • 1x USB-C Console Port<br>• 1x OOBM port<br>• 1x USB Type A Host port<br>• 1x Bluetooth dongle to be used with Mobile App | |
| | Jumbo frames allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9198 bytes | |
| | Packet storm protection against broadcast and multicast storms with user-defined thresholds | |

| | | |
|---|---|---|
| | Smart link enables simple, fast converging link redundancy and load balancing with dual uplinks avoiding Spanning Tree complexities | |
| **Management** | Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; network operators can gather a variety of network statistics and information for capacity planning and real-time network monitoring purposes. | |
| | Management interface control enables or disables each of the following depending on security preferences, console port, or reset button | |
| | Industry-standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments | |
| | Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection and local and remote syslog capabilities allow logging of all access | |
| | SNMP v2c/v3 provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions | |
| | Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms and events | |
| | TFTP and SFTP support offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security | |
| | Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time | |
| | IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network, facilitating easy mapping by | |

| | | |
|---|---|---|
| | network management applications | |
| | Dual flash images provide independent primary and secondary operating system files for backup while upgrading | |
| | Multiple configuration files can be stored to a flash image | |
| | Ingress and egress port monitoring enable more efficient network problem solving | |
| | Precision Time Protocol allows precise clock synchronization across distributed network switches as defined in IEEE 1588. Needed for time critical applications like AVB, smart grid power automation, etc. Supports transparent clock E-E | |
| **Layer 2 Switching** | VLAN support and tagging for IEEE 802.1Q (4094 VLAN IDs) | |
| | IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs | |
| | MVRP allows automatic learning and dynamic assignment of VLANs | |
| | VXLAN encapsulation (tunnelling) protocol for overlay network that enables a more scalable virtual network deployment | |
| | Bridge Protocol Data Unit (BPDU) tunnelling Transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs | |
| | Port mirroring duplicates port traffic (ingress and egress) to a monitoring port; supports 4 mirroring groups | |
| | STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) | |
| | Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network | |
| | IPv4 Multicast in VXLAN/EVPN Overlay support allows PIMSM/IGMP snooping in the VXLAN Overlay | |
| | IPv6 VXLAN/EVPN Overlay support, allows IPv6 traffic over the VXLAN overlay | |

| | | |
|---|---|---|
| | VXLAN ARP/ND suppression allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network | |
| **Layer 3 Services** | Address Resolution Protocol (ARP) determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network | |
| | Dynamic Host Configuration Protocol (DHCP) simplifies the management of large IP networks and supports client; DHCP Relay enables DHCP operation across subnets, and DHCP server centralizes and reduces the cost of IPv4 address management | |
| | Domain Name System (DNS) provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server | |
| | Supports internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility | |
| | Route maps provide more control during route redistribution; allow filtering and altering of route metrics | |
| **Layer 3 Routing** | Supports Border Gateway Protocol (BGP) that provides scalable, robust, and flexible IPv4 and IPv6 routing, and also supports BGP-4 that delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks with graceful restart capability | |
| | Supports Open shortest path first (OSPF) delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery. | |
| | Supports Policy-based routing uses a classifier to select traffic that can be forwarded based on policy set by the network administrator | |

| | | |
|---|---|---|
| | Dual IP stack maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design | |
| **Security** | Access control list (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header | |
| | ACLs also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis | |
| | Management access security for both on- and offbox authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services | |
| | Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks | |
| | Supports multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards | |
| | Supports MAC-based client authentication | |
| | Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3 | |
| | Switch CPU protection provides automatic protection against malicious network traffic trying to shut down the switch | |
| | ICMP throttling defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic | |
| | Port security allows access only to specified MAC addresses, which can be learned or specified by the administrator | |
| | MAC address lockout prevents particular configured MAC addresses from connecting to the network | |

| | | |
|---|---|---|
| | Secure Sockets Layer (SSL) encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch | |
| | MAC Pinning allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected | |
| **Accessories** | Must include compatible 6x 10GBASE-T SFP+ RJ45 transceivers | |
| **Warranty** | With at least a Lifetime Warranty on parts and include one (1) Year next business day support | |
| **Implementation** | Must include Installation and Migration Services | |
| | The Supplier must be Certified Partner of both HCI Software and Hardware components of the proposed solution (must provide Manufacturer or Reseller Certificate). | |
| Support Service | The Supplier must provide the following: | |
| | * Unlimited corrective maintenance/ repair services within the warranty period | |
| | * Twenty (24) hours by seven (7) days technical support and must meet the following response and resolution time: | |
| | > Within one (1) hour for phone or email support | |
| | > Within two (2) hours response time for onsite support | |
| | > Root cause analysis for all support cases filed. | |
| | * Submission of Service Report within 5 calendar days after rendering service | |
| | The Supplier must provide full documentation for Activity Plan on the installation of patches and upgrades and Root Cause Analysis for incidents encountered. | |
| | The Supplier must provide onsite support for the installation and deployment of software patches and version upgrades. | |
| | The Supplier must provide access to the Vendor portal for download of the latest product contents, patches, updates/upgrades including extensive online-self-help resources and knowledge base. Advisory to patches and fixes shall also be provided | |

| | | |
|---|---|---|
| | The Supplier must provide a procedure for support and problem escalation. | |
| | The Supplier must conduct system health checks every quarter with the following scope:<br>• System/Application patches, fixes, security patches, and alerts<br>• System/Application profile<br>• Resource utilization<br>• Log analysis<br>• Formal reports on the output of conducted health checks within 5 days | |
| Other Warranty and After Sales Requirements | * Immediate replacement of the equipment and/or its parts. | |
| | * The Supplier shall replace a factory defective unit with a new unit within thirty days upon delivery of the item. | |
| | The Supplier must provide a certificate for the above services as part of the technical requirements. | |
| **Network Attached Storage (for Backup and Replication) – 1 Unit** | | |
| Technical Specifications | Must be 2U 8-Bay Rackmount and must include Rail Kit | |
| | Must be 2.5" and 3.5" SATA HDD/SSD drives compatible | |
| | Must be expanded to 12 bays | |
| | Must have Unified Data Management Operating System with support for the Btrfs file system | |
| | Mut provides schedulable and near-instantaneous data protection for shared folders and LUNs | |
| | Must be capable of File and folder-level data restoration | |
| | Must be capable to detects and recovers corrupted files using mirrored metadata and RAID configurations | |
| | Must be capable of Inline compression | |
| Backup Solutions | Must have the following features: | |
| | Must be capable to protect Windows PCs and servers, VMs, other file servers, and even Google Workspace and Microsoft 365 cloud applications. | |

| | | |
|---|---|---|
| | Must be capable to consolidates backup tasks for physical and virtual environments, and enables rapid restoration of files, entire physical machines, and VMs. | |
| | Must be capable of Active Backup for Google Workspace and Microsoft 365 | |
| | Must have private cloud solution for file sharing, concurrent document editing, emails, instant messaging, and others. | |
| | Must be capable of Virtualization | |
| | Must supports local backup, network backup, and data backup to public clouds | |
| Back up Tools | • DSM configuration backup, macOS Time Machine support, Synology Drive Client desktop application<br>• Shared folder sync supports a maximum of 16 tasks | |
| Snapshot Replication | • Maximum number of snapshots for shared folders: 1,024<br>• Maximum number of replications: 32 | |
| Hardware Specifications | Must be Quad-core, 2.2 GHz Processor | |
| | Must be 4 GB DDR4 ECC SODIMM and expandable up to 32 GB Memory | |
| | Must be Hot swappable drives Compatible | |
| | Must have<br>• 2 x USB 3.2 Gen 1 ports<br>• 1 x Expansion port (eSATA) external ports | |
| | Must have 4 x 1GbE RJ-45 LAN Port | |
| | Must be Wake on LAN/WAN compatible | |
| | Must have PCI 3.0 slots:<br>• 1 x 4-lane x8 slot<br>• Supports 10GbE/25GbE network interface cards2 and M.2 NVMe SSD adapter cards for SSD cache | |
| | Must have Scheduled power on/of | |
| | Must have 2x System Fans | |

| | | |
|---|---|---|
| | Must include 6 x 12TB Enterprise SATA 6 Gb/s 7,200 rpm HDD (must be the same brand) | |
| HDD Specifications | Must be 6.0 Gb/s, 3.0 Gb/s, 1.5 Gb/s interface speed | |
| | Must be 256 MiB Buffer size | |
| | Must be 242 MiB/s Maximum sustained data transfer speed | |
| | Must be 2,500,000 hours MTTF | |
| | Must be 550 total TB transferred per year workload rating | |
| **DSM Specifications** | | |
| Networking protocols | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) | |
| File systems | • Internal: Btrfs, ext4<br>• External: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT | |
| Supported RAID types | Hybrid RAID (SHR), Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | |
| Storage management | • Maximum single volume size: 108 TB<br>• Maximum system snapshots: 65,53610<br>• Maximum internal volumes: 64 | |
| SSD cache | • Read/write cache support<br>• 2.5" SATA SSD support<br>• M.2 NVMe SSD support | |
| File sharing capabilities | • Maximum local user accounts: 2,048<br>• Maximum local groups: 256<br>• Maximum shared folders: 512<br>• Maximum concurrent SMB/NFS/AFP/FTP connections: 1,000 | |
| Privileges | Windows Access Control List (ACL), application privileges | |
| Directory services | Connects with Windows AD/LDAP servers enabling domain users to login via SMB/NFS/AFP/FTP/File Station using their<br>existing credentials | |
| Security | Firewall, shared folder encryption, SMB encryption, FTP over SSL/TLS, SFTP, rsync over SSH, login auto block, Let's Encrypt<br>support, HTTPS (customizable cipher suite) | |

| | | |
|---|---|---|
| Supported clients | Windows 7 onwards, macOS 10.12 onwards | |
| Supported browsers | Chrome, Firefox, Edge, Internet Explorer 10 onwards, Safari 10 onwards, Safari (iOS 10 onwards), Chrome (Android 6.0 onwards) on tablets | |
| **File Server & Synchronization** | | |
| Drive | Synchronizes files across Windows, macOS, Linux, Android and iOS. The built-in cross-platform portal allows access to data anytime and anywhere.<br>• Maximum number of hosted files: 1,000,000<br>• Maximum number of concurrent connections for PC clients: 550 | |
| File Station | Provides virtual drives, remote folders, Windows ACL editor, compression/extraction of archived files, bandwidth control for specific users/groups, creation of sharing links, and transfer logs. | |
| FTP Server | Supports bandwidth control for TCP connections, custom FTP passive port ranges, anonymous FTP, FTP over TLS/SSL and SFTP protocols, network booting with TFTP and PXE support, and transfer logs. | |
| Presto File Server | Enables high-speed data transfer over WAN through the exclusive SITA technology between Synology NAS and desktop. | |
| Cloud Sync | Offers one or two-way synchronization with public cloud storage providers, including Alibaba Cloud OSS, Amazon S3-compatible storage, Back blaze B2, Baidu Cloud, Box, Dropbox, Google Cloud Storage, Google Drive, hubiC, MegaDisk,<br>Microsoft OneDrive, OpenStack Swift-compatible storage, Tencent COS, WebDAV servers and Yandex Disk. | |
| Universal Search | Enables global search of applications and files. | |
| Warranty | Must be 3 Year warranty on parts and labor. | |
| Installation | Must include Installation, configuration, and setup. | |
| Support Service Requirement | The Supplier must provide the following: | |
| | * Unlimited corrective maintenance/ repair services within the warranty period | |

| | | |
|---|---|---|
| | * Twenty-four hours by seven days (Monday to Sunday) technical support and must meet the following response and resolution time: | |
| | > Within one hour for phone or email support | |
| | > Within four hours for on-site support | |
| | > For onsite support, the Supplier must attend to and repair the defective unit within two (2) business days | |
| | > In case of outside repair within the 1-year warranty period, the Supplier shall provide a service unit to the OSG within three (3) days upon pull out of the unit. The repaired hardware or replacement for the pulled-out hardware/unit must be delivered within fifteen (15) calendar days from the issuance of service unit. | |
| | The Supplier should replace a factory defective unit with a new unit within thirty days upon delivery of the item. | |
| Certification | The Supplier must be an authorized reseller of the brand being offered. | |

| WIDE AREA NETWORK SOLUTION WITH NEXT GENERATION FIREWALL FOR MULTI-BRANCH SETUP | | |
|---|---|---|
| Item | Specifications | Compliance |
| **Upgrade and Replacement of Existing Firewall – one unit** | | |
| GENERAL | | |
| Must performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.<br><br>Must be capable of proxy-less and non-buffering inspection technology that provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations and can be applied on common protocols as well as raw TCP streams. | | |
| Must have a single-pass DPI architecture that simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture. | | |
| Must have multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity. | | |
| Must identify and mitigate even the most insidious modern threats, including future Meltdown exploits. It even detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. | | |
| Must scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams. | | |
| HARDWARE | | |
| Form Factor | The system must be of one (1) unit rack mountable. | |
| Interfaces | The system's interface must include:<br><br>1 Gbe Interfaces – 24x 1 Gbe<br>10G SFP+ - 6x 10G SFP+<br>5G SFP+ - 4x 5G SFP+<br>USB 3.0 – 2x USB 3.0<br>Management interfaces - 1 GbE, 1 Console | |

| | | |
|---|---|---|
| Management | CLI, Web GUI, NSM | |
| Built-in storage | 128 GB M.2 | |
| **PERFORMANCE** | | |
| Throughput | The system must have the minimum throughput requirements (or higher):<br>Firewall Inspection Throughput - 5.5 Gbps;<br>Threat Prevention throughput - 3.5 Gbps;<br>Application inspection throughput - 4.2 Gbps;<br>IPS throughput - 3.8 Gbps;<br><br>Anti-malware inspection throughput - 3.5 Gbps;<br>TLS/SSL decryption and inspection throughput (DPI SSL) - 850 Mbps;<br>VPN throughput - 2.2 Gbps; | |
| Connections | The system must be capable of handling:<br><br>Connections per second - 22,000/sec;<br>Maximum connections (SPI) - 2,000,000;<br>Max DPI-SSL Connections - 150,000;<br>Maximum connections (DPI) - 750,000; | |
| IPsec VPN | The system must be capable of handling 50 (up to 1000 Concurrent IPSec VPN Clients) | |
| SSL-VPN | The system must be capable of handling 2 (up to 500 Concurrent SSL-VPN Clients) | |
| **INTEGRATION** | | |
| Authentication | The system must support LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC). | |
| **SOFTWARE** | | |
| Superior threat prevention and performance | The system must be qualified as a next generation firewall (NGFW) and Multi-core hardware architecture. | |
| Protection against unknown attacks | The system must have a Cloud-based multi-engine analysis that catches unknown and highly evasive advanced malware. | |
| Threat intelligence and automation for memory-based | The system must be capable of Memory inspection. This allows the system to see the instructions and sequences before they can be executed without the code. | |

| | | |
|---|---|---|
| signatures | | |
| Network control and flexibility | The system must have powerful operating system, Application Control Intelligence, Network Segmentations and VLAN's and Wireless Security. | |
| Robust Networking Capabilities | The system must have an extensive switching and routing capabilities and supports high availability. | |
| Anti-malware | The system must be capable of<br>• Stream-based malware scanning<br>• Gateway anti-virus<br>• Gateway anti-spyware<br>• Bi-directional inspection<br>• No file size limitation | |
| Secure SD-WAN | The system must have<br>• Future-proof against an ever-changing threat landscape by investing in a NGFW with multi-gigabit threat analysis performance;<br>• Provide direct and secure internet access to distributed branch offices instead of back-hauling through corporate headquarters;<br>• Allow distributed branch offices to securely access internal resources in corporate headquarters or in a public cloud, significantly improving application latency;<br>• Automatically block threats that use encrypted protocols such as TLS 1.3, securing networks from the most advanced attacks; and<br>• Reduce complexity and maximize efficiency using a central management system delivered through an intuitive single pane of glass user interface. | |
| | The system must have<br>• TLS 1.3 with enhanced security<br>• Deep packet inspection for TLS/SSL/SSH<br>• Inclusion/exclusion of objects, groups or hostnames<br>• SSL control<br>• Enhancements for DPI-SSL with CFS<br>• Granular DPI SSL controls per zone or rule<br>• Advanced threat protection<br>• Memory Inspection | |

| | | |
|---|---|---|
| TLS/SSL/SSH decryption and inspection | • Cloud-based multi-engine analysis<br>• Virtualized sandboxing<br>• Hypervisor level analysis<br>• Full system emulation<br>• Broad file type examination<br>• Automated and manual submission<br>• Real-time threat intelligence updates<br>• Block until verdict | |
| Intrusion Prevention | The system must have<br>• Signature-based scanning<br>• Automatic signature updates<br>• Bi-directional inspection<br>• Granular IPS rule capability<br>• GeoIP enforcement<br>• Botnet filtering with dynamic list<br>• Regular expression matching | |
| Firewall | The system must be capable of<br>• Stateful packet inspection<br>• reassembly-free deep packet inspection<br>• DDoS attack protection (UDP/ ICMP/SYN flood)<br>• IPv4/IPv6 support<br>• Biometric authentication for remote access<br>• DNS proxy<br>• Full API support<br>• Switch integration<br>• SD-WAN scalability<br>• SD-WAN Usability Wizard<br>• Connections scalability (SPI, DPI, DPI SSL)<br>• Enhanced dashboard<br>• Enhanced device view<br>• Top traffic and user summary<br>• Insights to threats<br>• Notification center | |
| Application Identification | The system must have<br>• Application control<br>• Application bandwidth management<br>• Custom application signature creation<br>• Data leakage prevention<br>• Application reporting over NetFlow/IPFIX<br>• Comprehensive application signature database | |

| | | |
|---|---|---|
| Virtual Private Network | The system must be capable of<br>• Secure SD-WAN<br>• Auto-provision VPN<br>• IPSec VPN for site-to-site connectivity<br>• SSL VPN and IPSec client remote access<br>• Redundant VPN gateway<br>• Mobile Client for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire<br>• Route-based VPN (OSPF, RIP, BGP) | |
| High Availability | The system must be capable of<br>• A/P high availability with state sync<br>• High availability - Active/Standby with state sync | |
| IPv6 | The system must support IPv6 | |
| **ENVIRONMENT** | | |
| Input power | The system must be capable of running at 100-240 VAC, 50-60 Hz. | |
| Power Consumption | The system must not consume more the 36.3W of power. | |
| Humidity | The system must be 5-95% non-condensing | |
| **SECURITY SERVICES** | | |
| Real-Time Updates | The system must be supported by<br>• Real-time threat intelligence updates<br>• Automatic signature updates | |
| Advanced Protection | The system has complete suite of security services for firewalls that features Gateway Security, Content Filtering Service, Anti-Spam, 24x7 Support, ATP, Memory Inspection, DNS Security, Cloud Management and Cloud based Reporting - 7 Days | |
| **IMPLEMENTATION SERVICES** | | |
| Scope of Services | Must include Configuration, Testing, Documentation and Knowledge Transfer | |
| | The engineer must be available 24x7 Monday to Sunday | |
| | The engineer must have a certification granted by the supplier/manufacturer of the brand being offered. | |

| | | |
|---|---|---|
| **SUPPORT SERVICES** | | |
| Enhanced Support | The system must include email and phone support for customers during local business hours; for two (2) years. | |
| Firmware Upgrades | The system must include firmware upgrades during its warranty period. | |
| Comprehensive Support | The system must have Global Support available 8x5 or 24x7. | |
| **ACCREDITATION** | | |
| Standards | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMPs, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | |
| Certifications (in progress) | The system must have certifications under Common Criteria NDPP Firewall with VPN and IPS | |
| Brand/Standard | The technology or brand must either be American or European for a more Global Standard compliance. | |
| Local Support | The brand must have local second level of support via its distributor that is compliant with global standard like ISO or Duns and Bradstreet to maintain a quality-of-service delivery. | |
| The local support must include the following: | | |
| | **Two Year Support Services**<br>**24x7 Monday to Sunday**. | |
| | Phone/Remote Technical Support | |
| | Onsite Technical Support with 2 to 4 hours Response Time | |
| | Corrective Maintenance for 5 Cases Per Year | |
| | The Supplier must provide full documentation for the Activity Plan on the installation of patches and upgrades and Root Cause Analysis of incidents encountered. | |
| | The Supplier must provide onsite support for the installation and deployment of software patches and version upgrades. | |
| | The Supplier must provide onsite support for the installation and deployment of software patches and version upgrades. | |

| | | |
|---|---|---|
| | Submission of Activity/Service Report within 5 calendar days after rendering service | |
| | Semi-Annual Preventive Maintenance visits during Regular Business Hours | |
| | Immediate replacement of the equipment and/or its parts. | |
| | The Supplier shall replace a factory defective unit with a new unit within 30 days upon delivery of the item. | |
| | The Supplier must provide a certificate for the above services as part of the technical requirements. | |
| Certification | Must be certified with ICSA labs Advance Threat Defense certified with 100% unknown threat detection for 7 consecutive quarters from Q1-Q4, 2021 & Q1-Q3, 2022. | |
| | The Supplier must be an authorized reseller of the brand being offered. Must provide Authorization certificate from the Manufacturer or Vendor. | |
| **Next Generation Firewall - 1 unit** | | |
| **GENERAL** | | |
| Must performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port. | | |
| Must be capable of proxy-less and non-buffering inspection technology that provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations and can be applied on common protocols as well as raw TCP streams. | | |
| Must have a single-pass DPI architecture that simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture. | | |
| Must have multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity. | | |
| Must identify and mitigate even the most insidious modern threats, including future Meltdown exploits. It even detects and blocks malware that exhibits no malicious behavior and hides its weaponry via encryption. | | |
| Must scan all inbound, outbound, and intra-zone traffic for viruses, Trojans, key loggers, and other malware in files of unlimited length and size across all ports and | | |

| | | |
|---|---|---|
| TCP streams. | | |
| **HARDWARE** | | |
| Form Factor | The system must be of one (1) unit rack mountable. | |
| Interfaces | The system's interface must include:<br><br>1 Gbe Interfaces – 16x 1 Gbe<br>10G SFP+ - 3x 10G SFP+<br>USB 3.0 – 2x USB 3.0<br>Management interfaces - 1 GbE, 1 Console | |
| Management | CLI, Web GUI, NSM | |
| Built-in storage | 64 GB M.2 | |
| **PERFORMANCE** | | |
| Throughput | The system must have the minimum throughput requirements (or higher):<br>Firewall Inspection Throughput – 5.2 Gbps;<br>Threat Prevention throughput – 3.0 Gbps;<br>Application inspection throughput – 3.6 Gbps;<br>IPS throughput – 3.4 Gbps;<br>Anti-malware inspection throughput – 2.9 Gbps;<br>TLS/SSL decryption and inspection throughput (DPI SSL) – 800 Mbps;<br>VPN throughput – 2.1 Gbps; | |
| Connections | The system must be capable of handling:<br><br>Connections per second - 21,000/sec;<br>Maximum connections (SPI) – 1,500,000;<br>Max DPI-SSL Connections – 125,000;<br>Maximum connections (DPI) – 500,000; | |
| IPsec VPN | The system must be capable of handling 50 (up to 1000 Concurrent IPSec VPN Clients) | |
| SSL-VPN | The system must be capable of handling 2 (up to 500 Concurrent SSL-VPN Clients) | |
| **INTEGRATION** | | |
| Authentication | The system must support LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC). | |

| | | |
|---|---|---|
| **SOFTWARE** | | |
| Superior threat prevention and performance | The system must be qualified as a next generation firewall (NGFW) and Multi-core hardware architecture. | |
| Protection against unknown attacks | The system must have a Cloud-based multi-engine analysis that catches unknown and highly evasive advanced malware | |
| Threat intelligence and automation for memory-based signatures | The system must be capable of Memory inspection. This allows the system to see the instructions and sequences before they can be executed without the code. | |
| Network control and flexibility | The system must have powerful operating system, Application Control Intelligence, Network Segmentations and VLAN's and Wireless Security. | |
| Robust Networking Capabilities | The system must have an extensive switching and routing capabilities and supports high availability. | |
| Anti-malware | The system must be capable of<br>• Stream-based malware scanning<br>• Gateway anti-virus<br>• Gateway anti-spyware<br>• Bi-directional inspection<br>• No file size limitation | |
| Secure SD-WAN | The system must have<br>• Future-proof against an ever-changing threat landscape by investing in an NGFW with multi-gigabit threat analysis performance;<br>• Provide direct and secure internet access to distributed branch offices instead of back-hauling through corporate headquarters.<br>• Allow distributed branch offices to securely access internal resources in corporate headquarters or in a public cloud, significantly improving application latency.<br>• Automatically block threats that use encrypted protocols such as TLS 1.3, securing networks from the most advanced attacks.<br>• Reduce complexity and maximize efficiency using a central management system delivered through an | |

| | | |
|---|---|---|
| | intuitive single pane of glass user interface. | |
| TLS/SSL/SSH decryption and inspection | The system must have<br>• TLS 1.3 with enhanced security<br>• Deep packet inspection for TLS/SSL/SSH<br>• Inclusion/exclusion of objects, groups, or hostnames<br>• SSL control<br>• Enhancements for DPI-SSL with CFS<br>• Granular DPI SSL controls per zone or rule<br>• Advanced threat protection<br>• Memory Inspection<br>• Cloud-based multi-engine analysis<br>• Virtualized sandboxing<br>• Hypervisor-level analysis<br>• Full system emulation<br>• Broad file type examination<br>• Automated and manual submission<br>• Real-time threat intelligence updates<br>• Block until verdict | |
| Intrusion Prevention | The system must have:<br>• Signature-based scanning<br>• Automatic signature updates<br>• Bi-directional inspection<br>• Granular IPS rule capability<br>• GeoIP enforcement<br>• Botnet filtering with dynamic list<br>• Regular expression matching | |
| Firewall | The system must be capable of:<br>• Stateful packet inspection<br>• reassembly-free deep packet inspection<br>• DDoS attack protection (UDP/ ICMP/SYN flood)<br>• IPv4/IPv6 support<br>• Biometric authentication for remote access<br>• DNS proxy<br>• Full API support<br>• Switch integration<br>• SD-WAN scalability<br>• SD-WAN Usability Wizard1<br>• Connections scalability (SPI, DPI, DPI SSL)<br>• Enhanced dashboard<br>• Enhanced device view | |

| | | |
|---|---|---|
| | • Top traffic and user summary<br>• Insights into threats<br>• Notification center | |
| Application Identification | The system must have:<br>• Application control<br>• Application bandwidth management<br>• Custom application signature creation<br>• Data leakage prevention<br>• Application reporting over NetFlow/IPFIX<br>• Comprehensive application signature database | |
| Virtual Private Network | The system must be capable of:<br>• Secure SD-WAN<br>• Auto-provision VPN<br>• IPSec VPN for site-to-site connectivity<br>• SSL VPN and IPSec client remote access<br>• Redundant VPN gateway<br>• Mobile Client for iOS, Mac OS X, Windows, Chrome, Android, and Kindle Fire<br>• Route-based VPN (OSPF, RIP, BGP) | |
| High Availability | The system must be capable of:<br>• A/P high availability with state sync<br>• High availability - Active/Standby with state sync | |
| IPv6 | The system must support IPv6 | |
| **ENVIRONMENT** | | |
| Input power | The system must be capable of running at 100-240 VAC, 50-60 Hz. | |
| Power Consumption | The system must not consume more the 36.3W of power. | |
| Humidity | The system must be 5-95% non-condensing | |
| **SECURITY SERVICES** | | |
| Real-Time Updates | The system must be supported by<br>• Real-time threat intelligence updates<br>• Automatic signature updates | |
| Advanced Protection | The system has a complete suite of security services for firewalls that features Gateway Security, Content Filtering Service, Anti-Spam, 24x7 Support, ATP, Memory Inspection, | |

| | | |
|---|---|---|
| | DNS Security, Cloud Management and Cloud based Reporting – 7 Days. | |
| **IMPLEMENTATION SERVICES** | | |
| Scope of Services | Must include Configuration, Testing, Documentation and Knowledge Transfer | |
| | The engineer must be available 24x7 Monday to Sunday | |
| | The engineer must have a certification granted by the supplier/manufacturer of the brand being offered. | |
| **SUPPORT SERVICES** | | |
| Enhanced Support | The system must include email and phone support for customers during local business hours; for two (2) years. | |
| Firmware Upgrades | The system must include firmware upgrades during its warranty period. | |
| Comprehensive Support | The system must have Global Support available 8x5 or 24x7. | |
| **ACCREDITATION** | | |
| Standards | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMPs, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | |
| Certifications (in progress) | The system must have certifications under Common Criteria NDPP Firewall with VPN and IPS | |
| Brand/Standard | The technology or brand must either be American or European for a more Global Standard compliance. | |
| Local Support | The brand must have local second level of support via its distributor that is compliant with global standard like ISO or Duns and Bradstreet to maintain a quality-of-service delivery. | |
| The local support must include the following: | | |
| | **2 Year Support Services**<br><br>**24x7 Monday to Sunday**. | |
| | Phone/Remote Technical Support | |
| | Onsite Technical Support with 2 to 4 hours of Response Time | |

| | | |
|---|---|---|
| | Corrective Maintenance for 5 Cases Per Year | |
| | The Supplier must provide full documentation for the Activity Plan on the installation of patches and upgrades and Root Cause Analysis of incidents encountered. | |
| | The Supplier must provide onsite support for the installation and deployment of software patches and version upgrades. | |
| | The Supplier must provide onsite support for the installation and deployment of software patches and version upgrades. | |
| | Submission of Activity/Service Report within 5 calendar days after rendering service | |
| | Semi-Annual Preventive Maintenance visits during Regular Business Hours | |
| | Immediate replacement of the equipment and/or its parts. | |
| | The Supplier shall replace a factory defective unit with a new unit within 30 days upon delivery of the item. | |
| | The Supplier must provide a certificate for the above services as part of the technical requirements. | |
| Certification | Must be certified with ICSA labs Advance Threat Defense certified with 100% unknown threat detection for 7 consecutive quarters from Q1-Q4, 2021 & Q1-Q3, 2022. | |
| | The Supplier must be an authorized reseller of the brand being offered. Must provide Authorization certificate from the Manufacturer or Vendor. | |

| **SERVER ENCLOSURE, ESSENTIAL, 42U, 800W X 1170D, 1200KG, BLACK, FLAT PACK** | | |
|---|---|---|
| **ITEM** | **SPECIFICATIONS** | **COMPLIANCE** |
| **Technical Specifications** | Must be 42RU Data Center Rack Cabinet | |
| | Must be Lightweight but sturdy bolted design provides a generous static and dynamic weight capacity | |
| | Must be Depth adjustable 19" vertical mounting rails in 6.35mm increments | |
| | Must be Vendor neutral, and compatible with all 19" standard IT equipment. | |
| | Must Quick release and field reversible doors | |

| | | |
|---|---|---|
| | Must be 42U cabinet with castors fits through a standard doorway | |
| | Must have Two-piece lockable side panels that provide easy access to the interior | |
| | Must include Leveling feet | |
| | Must be 71% airflow perforated doors | |
| | Must have a Static load rating of 1,200 kg | |
| **Standards & Materials:** | | |
| **Standard:** | EIA-310D, IEC-60297-2 | |
| **Material:** | high-grade cold and hot rolled steel/all materials RoHS compliant | |
| **Finishing:** | 5 stage iron phosphate pre-treatments followed by tough scratch resistant powder coat paint | |
| **Color:** | Black, low gloss textured | |
| **PDU** | Must include flexible (hot-swap) modular type 16-Outlets PDU | |
| | Plug/Connector Type: IEC 60320 C14. Receptacle: IEC 60320 C13 | |
| **Warranty** | Must be 2 Years warranty on parts and labor. | |
| **Installation** | Must include Installation, configuration, and setup. | |
| **Support Service Requirement** | The Supplier must provide the following: | |
| | * Unlimited corrective maintenance/ repair services within the warranty period | |
| | * Twenty-four (24) hours by seven (7) days (Monday to Sunday) technical support and must meet the following response and resolution time: | |
| | > Within one (1) hour for phone or email support | |
| | > Within four (4) hours for on-site support | |
| | > For onsite support, the Supplier must attend to and repair the defective unit within two (2) business days | |
| | > In case of outside repair within the 1-year warranty period, the Supplier shall provide a service unit to the OSG within three (3) days upon pull out of the unit. The repaired hardware or replacement for the pulled-out hardware/unit must be delivered within fifteen (15) calendar days from the issuance of service unit. | |
| | * The Supplier should replace a factory defective unit with a new unit within 30 days upon delivery of the item. | |
| **Certification** | The Supplier must be an authorized reseller of the brand being | |

| | | |
|---|---|---|
| | offered. | |
| **SUPPLY OF 2KVA UPS** | | |
| **Technical Specifications** | Must be online double-conversion with 0.9 Power Factor Correction (PFC) system | |
| | Must be Rackmount UPS and includes a Rail kit. | |
| | Must be installed with the data cabinet and will use the attached 16-outlet PDU. | |
| | Must constantly monitor power conditions and regulates voltage and frequency | |
| | Must have Intelligent Power Software | |
| | Must have 1 IEC C14 (10A) Input connections | |
| | Must have 8 IEC C13 (10A) sockets | |
| | Must have the following communications ports: | |
| | * 1 USB port | |
| | 1 serial RS232 port | |
| | 1 mini-terminal block for Remote Power Off | |
| | 1 mini-terminal block for Output relay communications port | |
| | Must have 1 slot for Network-M2, Network-MS, ModBus-MS or Relay-MS cards | |
| **Warranty** | Must be 3 Year warranty on parts and labor for UPS and 2 Years warranty on parts and labor for the battery. | |
| **Installation** | Must include Installation, configuration, and setup for the UPS | |
| **Support Service Requirement** | The Supplier must provide the following: | |
| | * Unlimited corrective maintenance/ repair services within the warranty period | |
| | * Twenty-four (24) hours by seven (7) days (Monday to Sunday) technical support and must meet the following response and resolution time: | |
| | > Within one (1) hour for phone or email support | |
| | > Within four (4) hours for on-site support | |
| | > For onsite support, the Supplier must attend to and repair the defective unit within two (2) business days | |
| | > In case of outside repair within the 1 year warranty period, the Supplier shall provide a service unit to the OSG within three (3) days upon pull out of the unit. The repaired hardware or replacement for the pulled-out hardware/unit must be delivered within fifteen (15) calendar days from the issuance of service unit. | |
| | * The Supplier should replace a factory defective unit with a new unit within 30 days upon delivery of the item. | |

| | | |
|---|---|---|
| **Certification** | The Supplier must be an authorized reseller of the brand being offered. Must provide Authorization certificate from the Manufacturer or Vendor. | |
| **WIRELESS LAN INFRASTRUCTURE UPGRADE** | | |
| **INDOOR ACCESS POINTS (20 units)** | | |
| **Features** | Must belong to the latest Top 4 of the Leaders Group of Gartner's Magic Quadrant for Enterprise Wired and WLAN Infrastructure Report for 2021 (must provide certificate) | |
| | Must be compatible and interface with existing OSG WLAN Infrastructure. | |
| | Must be 1.49 Gbps maximum real-world speed (HE80/HE20) | |
| | Must be WPA3 and Enhanced Open security | |
| | Must have built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices | |
| | Must have OFDMA for enhanced multi-user efficiency | |
| | Must be IoT-ready Bluetooth 5 and Zigbee support | |
| | Must be designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients. | |
| | Must support Orthogonal frequency-division multiple access (OFDMA) | |
| | Must support cellular optimization | |
| | Must support up to 2 spatial streams (2SS) and 80MHz channel bandwidth (HE80) | |
| | Must support handling multiple Wi-Fi 6 capable clients on each channel simultaneously, regardless of device or traffic type. | |
| | Must support Channel utilization optimization by handling each transaction via smaller sub-carriers or resource units (RUs) | |
| | Must support controller-less mode and can provide SLA-grade performance by allocating radio resources, such as time, frequency, and spatial streams, to specific traffic types | |
| | Must support Layer 7 deep packet inspection (DPI) to identify user roles and applications. The APs will dynamically allocate the bandwidth needed | |
| | Must support the elimination of sticky client issues by placing Wi-Fi 6 capable devices on the best available AP | |
| | Must support Wi-Fi 6 aware client optimization by steering mobile devices to the best AP based on available bandwidth, types of applications being used, and traffic type –even as users roam. | |
| | Must support Advanced Cellular Coexistence (ACC) uses built-in filtering to minimize the impact of interference from cellular | |

| | | |
|---|---|---|
| | networks automatically, distributed antenna systems (DAS), and commercial small cell or femtocell equipment. | |
| | Must support continuous monitoring and reporting hardware energy consumption. can also be configured to enable or disable capabilities based on available PoE power | |
| | Must support integrated Bluetooth 5 and 802.15.4 radio (for Zigbee support) to simplify deploying and managing IoT-based location services | |
| | Must support Target Wake Time (TWT) by establishing a schedule for when clients need to communicate with an AP | |
| | Must support for stronger encryption and authentication is provided via the latest version of WPA for enterprise-protected networks. | |
| | Must support WPA2-MPSK MPSK enables simpler passkey management for WPA2 devices | |
| | Must support VPN Tunnels can be used to establish a secure SSL/IPsec VPN tunnel to a VPN concentrator | |
| | Must support Trusted Platform Module (TPM) for secure storage of credentials and keys, and boot code | |
| | Must support flexible management platform either standalone, controller-less, controller-based, cloud-based, and on-premises NMS using unified OS | |
| | Must support zero-touch provisioning | |
| | Must support Transmit beamforming (TxBF) Increased signal reliability and range | |
| | Must support Passpoint Wi-Fi (Release 2) (Hotspot 2.0) | |
| | Must support Seamless cellular-to-Wi-Fi carryover for guests | |
| | Must support Dynamic Frequency Selection (DFS) Optimized use of available RF spectrum | |
| | Must support Maximum Ratio Combining (MRC) Improved receiver performance | |
| | Must support Cyclic Delay/Shift Diversity (CDD/CSD) Greater downlink RF performance | |
| | Must support Space-Time Block Coding Increased range and improved reception | |
| **Technical Specifications** | Must be Indoor, dual radio, 5GHz, and 2.4GHz 802.11ax 2x2 MIMO | |
| | Must have Two spatial streams Single User (SU) MIMO for up to 1.2Gbps wireless data rate with 2SS HE80 802.11ax client devices | |
| | Must be Up to 256 associated client devices per radio | |
| | Must be 16 BSSIDs per radio | |
| | Must support the following frequency bands: (Country-specific restrictions apply) 2.400 to 2.4835GHz / 5.150 to 5.250GHz /5.250 to 5.350GHz /5.470 to 5.725GHz /5.725 to 5.850GHz | |

| | | |
|---|---|---|
| | Available channels are dependent on the configured regulatory domain | |
| | Must support the following radio technologies:<br>• 802.11b: Direct-sequence spread-spectrum (DSSS)<br>• 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)<br>• 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to 8 resource units | |
| | Must support the following modulation types:<br>• 802.11b: BPSK, QPSK, CCK<br>• 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM (proprietary extension)<br>• 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM (proprietary extension)<br>• 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM | |
| | Must be 802.11n high throughput (HT) support: HT20/40 | |
| | Must be 802.11ac very high throughput (VHT) support: VHT20/40/80 | |
| | Must be 802.11ax high efficiency (HE) supports: HE20/40/80 | |
| | Must support the following data rates (Mbps):<br>• 802.11b: 1, 2, 5.5, 11<br>• 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54<br>• 802.11n: 6.5 to 300 (MCS0 to MCS15, HT20 to HT40), 400 with 256-QAM<br>• 802.11ac: 6.5 to 867 (MCS0 to MCS9, NSS = 1 to 2, VHT20 to VHT80), 1,083 with 1024-QAM<br>• 802.11ax (2.4GHz): 3.6 to 574 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)<br>• 802.11ax (5GHz): 3.6 to 1,201 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE80) | |
| | 802.11n/ac/ax packet aggregation: A-MPDU, A-MSDU | |
| | Transmit power: Configurable in increments of 0.5 dBm | |
| | Maximum (aggregate, conducted total) transmit power (limited by local regulatory requirements):<br>• 2.4 GHz band: +21 dBm (18dBm per chain)<br>• 5 GHz band: +21 dBm (18 dBm per chain)<br>Note: conducted transmit power levels exclude antenna gain. For total (EIRP) transmit power, add antenna gain. | |
| **Accessories** | Must include mount bracket (same brand) | |
| **Warranty** | With at least a Lifetime Warranty on parts and include one (1) Year next business day support. | |
| **WLAN CONTROLLER ORCHESTRATOR FOR HIGH AVAILABILITY (1 unit)** | | |
| | Support for new 802.11ax (Wi-Fi 6), WPA3 and Enhanced Open | |

| | | |
|---|---|---|
| | - and existing standards | |
| | Dynamic Segmentation enforces wired and wireless access policies to simplify and secure the network | |
| | Application awareness for 3,000+ applications without additional hardware | |
| | Built-in AI-powered wireless/RF optimization | |
| | Automate deployment with Zero Touch Provisioning and hierarchical configuration | |
| | Supports Controller Clustering that improves reliability using enhanced high availability (HA), adopts configurations seamlessly based on hierarchy, and reduces or eliminates maintenance windows by enabling Live Upgrades. | |
| | Supports RFProtect that provides advanced spectrum analysis and wireless intrusion protection (WIPS/WIDS) to help identify and mitigate Wi-Fi and non-Wi-Fi sources of interference to contain potential security risks. | |
| | As an enhancement of Adaptive Radio Management, AirMatch automates network-wide RF channels, channel width, and transmits power to optimize the highest density environments | |
| | Supports hierarchical configuration and improved visibility as it uses a centralized, multi-tiered architecture that consolidates all deployment models (e.g., all-conductor, single-conductor/multiple-local, and multiple-conductor/local) with a single approach. | |
| | Enables licensing pools to manage licenses based on site requirements dynamically. | |
| | Supports live upgrade that eliminates the need for planned maintenance windows or downtime. Each Controller Cluster or individual service modules (AppRF, AirGroup, ARM, etc.) can also be selectively upgraded without impacting the rest of the network. | |
| | Supports hitless failover as user sessions and AP traffic within a Controller Cluster are load balanced to optimize network utilization during peak periods and maximize availability during unplanned outages. | |
| | Users can roam between floors, buildings or across the entire network without any re-authentication, change to their IP address, or loss of firewall state. | |
| | Support for WPA3 brings stronger encryption and authentication methods, while Enhanced Open brings | |

| | | |
|---|---|---|
| | automatic encryption security to open networks. New WPA2-MPSK feature enables simpler passkey management for WPA2 devices - should the Wi-Fi password on one device need to be changed; no additional key changes are needed for other devices on the network. | |
| | Supports Multizone feature in which the same AP infrastructure can terminate two different SSIDs on two different controllers while maintaining complete separation and security for all networks, policies, management and visibility. | |
| | Must provide a single-pane-glass deployment and management of OSG existing WLAN infrastructure | |
| | Virtual appliance that operates on x86 platforms in a hypervisor environment and can reside with other virtualized appliances delivering key features such as authentication, encryption support, security policy, rogue detection and suppression, and security firewall. | |
| | Supports up to a maximum of 500 devices (APs and WLAN controllers) with host system requirement of at least 6 vCPU (hyper-threaded), 8 GB memory, and 8 GB flash/disk. | |
| **Warranty** | Must include software support services for (1) Year next business day support. | |
| **NETWORK ACCESS SWITCH (1 unit)** | | |
| **Key Features** | Enterprise-class Layer 2 connectivity with support for ACLs, robust QoS, and static routing | |
| | Convenient built-in 1/10GbE uplinks | |
| | Management flexibility with support for Cloud-management, easy-to-use Web GUI, and CLI | |
| | Software-defined ready with REST APIs | |
| | Simple deployment with Zero Touch Provisioning | |
| **Quality of Service (QoS)** | Traffic prioritization (IEEE 802.1p) for real-time classification | |
| | Class of Service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ | |
| | Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums | |
| | Large buffers for graceful congestion management | |

| | | |
|---|---|---|
| **Resiliency and High Availability** | Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops in STPbased networks | |
| | IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm | |
| | IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are required, and legacy support for IEEE 802.1d and IEEE 802.1w | |
| **Performance** | Up to 176 Gbps in non-blocking bandwidth and up to 98.6 Mpps for forwarding | |
| | Selectable queue configurations that allow for increased performance by defining several queues and associated memory buffering to best meet the requirements of network applications | |
| **Connectivity** | 48x ports 10/100/1000BASE-T Ports 4x 1G/10G SFP ports | |
| | Supports PoE Standards IEEE 802.3af, 802.3at | |
| | 1x USB-C Console Port<br>1x USB Type A Host port | |
| | Supports fixed power supply with up to 370W of Class 4 PoE power, and fixed fans | |
| | Jumbo frames allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9198 bytes | |
| | Packet storm protection against broadcast and multicast storms with user-defined thresholds | |
| **Management** | Built-in programmable and easy-to-use REST API interface | |
| | sFlow (RFC 3176) is ASIC-based wire speed network monitoring and accounting with no impact on network performance; network operators can gather a variety of network statistics and information for capacity planning and real-time network monitoring purposes | |
| | Industry-standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments | |
| | Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection and local and remote syslog capabilities allow | |

| | | |
|---|---|---|
| | logging of all access | |
| | SNMP v2c/v3 provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions | |
| | Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms and events | |
| | TFTP and SFTP support offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security | |
| | Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time | |
| | IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications | |
| | Dual flash images provide independent primary and secondary operating system files for backup while upgrading | |
| | Multiple configuration files can be stored in a flash image | |
| | Ingress and egress port monitoring enable more efficient network problem solving | |
| **Layer 2 Switching** | VLAN support and tagging for IEEE 802.1Q (4094 VLAN IDs) and 512 VLANs simultaneously | |
| | Bridge Protocol Data Unit (BPDU) tunneling transmits STP BPDUs transparently, allowing the correct tree | |
| | MVRP allows automatic learning and dynamic assignment of VLANs | |
| | STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) | |
| | Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network | |
| | Port mirroring duplicates port traffic (ingress and egress) to a | |

| | | |
|---|---|---|
| | monitoring port; supports 4 mirroring groups | |
| **Layer 3 Services** | Address Resolution Protocol (ARP) determines the MAC address of another IP host in the same subnet; supports static ARPs | |
| | Domain Name System (DNS) provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server | |
| | Supports internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility | |
| **Security** | Access control list (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header | |
| | Enrollment over Secure Transport (EST) enables secure certificate enrollment, allowing for easier enterprise management of PKI | |
| | Management access security for both on- and offbox authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services | |
| | Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks | |
| | Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications | |
| | Switch CPU protection provides automatic protection against malicious network traffic trying to shut down the switch | |
| | ICMP throttling defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic | |
| | Dynamic ARP protection blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data | |
| | Port security allows access only to specified MAC addresses, which can be learned or specified by the administrator | |
| | MAC address lockout prevents particular configured MAC | |

| | | |
|---|---|---|
| | addresses from connecting to the network | |
| | MAC Pinning allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected | |
| | Private VLAN (PVLAN) provides traffic isolation between users on the same VLAN; typically a switch port can only communicate with other ports in the same community and/or an uplink port, regardless of VLAN ID or destination MAC address. This extends network security by restricting peer-peer communication to prevent variety of malicious attacks. | |
| **Accessories** | Must include compatible 2x 10G multimode transceiver for the uplink to the proposed core switches | |
| **Warranty** | With at least a Lifetime Warranty on parts and include one (1) Year next business day support. | |
| **NETWORK CORE SWITCH (1 unit)** | | |
| **Key Features** | Stackable Layer 3 switches with BGP, EVPN, VXLAN, VRF, and OSPF with robust security and QoS | |
| | For enhanced visibility and troubleshooting, Network Analytics Engine (NAE) automatically monitors and analyzes events that can impact network health. Advanced telemetry and automation provide the ability to easily identify and troubleshoot network, system, application, and security related issues easily, through the use of python agents, CLI-based agents, CLI-based agents and REST APIs | |
| | Empowers IT teams to orchestrate multiple switch configuration changes for smooth end-to-end service rollouts through NetEdit that introduces automation that allows for rapid network-wide changes, and ensures policy conformance post-network updates. Intelligent capabilities include search, edit, validation (including conformance checking), deployment and audit features. | |
| | Flexible cloud-based or on-premises management for unified network operations of wired, WLAN, SD-WAN, and public cloud infrastructure. Designed to simplify day zero through day two operations with streamlined workflows. | |
| | Supports Dynamic Segmentation that enables seamless mobility, consistent policy enforcement, and automated configurations for wired and wireless clients across networks of all sizes. | |
| | Supports an easy-to-use mobile app simplifies connecting, stacking and managing switches for unparalleled deployment | |

| | | |
|---|---|---|
| | convenience. | |
| **Quality of Service (QoS)** | Strict priority (SP) queuing and Deficit Weighted Round Robin (DWRR) | |
| | Traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues | |
| | Transmission rates of egressing frames can be limited on a per-queue basis using Egress Queue Shaping (EQS) | |
| | Large buffers for graceful congestion management | |
| **Resiliency and High Availability** | High performance front plane stacking for up to 10 switches in a stack via chain or ring topology | |
| | Flexibility to mix both modular and fixed switch series models within a single stack | |
| | Hot-swappable power supplies and fans | |
| | Provides N+1 and N+N redundancy for high reliability in the event of power line or supply failures | |
| | Supports Virtual Router Redundancy Protocol (VRRP) that allows groups of two routers to dynamically back each other up to create highly available routed environments. | |
| | Supports Unidirectional Link Detection (UDLD) that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks. | |
| | Support for IEEE 802.3ad LACP to up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm. | |
| | Ethernet Ring Protection Switching (ERPS) supports rapid protection and recovery in a ring topology | |
| | IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w | |
| **Performance** | Up to 496 Gbps in non-blocking bandwidth and up to 369 Mpps for forwarding | |
| | Supports 10GbE/25GbE uplinks and large TCAM sizes ideal for mobility and IoT deployments in large campuses with several thousand clients | |
| | Switch Virtual Interfaces (dual stack) capacity up to 1,024 | |

| | | |
|---|---|---|
| | MAC table capacity up to 32,768 entries. | |
| | VRF capacity up to 256. | |
| **Connectivity** | 48x ports 10/100/1000BaseT and 4x 1G/10G/25G/50G SFP56 ports | |
| | 1x USB-C Console Port<br>1x OOBM port<br>1x USB Type A Host port<br>1x Bluetooth dongle to be used with Mobile App | |
| | Jumbo frames allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9198 bytes | |
| | Packet storm protection against broadcast and multicast storms with user-defined thresholds | |
| | Smart link enables simple, fast converging link redundancy and load balancing with dual uplinks avoiding Spanning Tree complexities | |
| **Management** | Scalable ASIC-based wire-speed network monitoring and accounting with no impact on network performance; network operators can gather various network statistics and information for capacity planning and real time network monitoring purposes. | |
| | Management interface control enables or disables each of the following depending on security preferences, console port, or reset button | |
| | Industry-standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments | |
| | Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access | |
| | SNMP v2c/v3 provides SNMP read and trap support of industry-standard Management Information Base (MIB), and private extensions | |
| | Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms and events | |
| | TFTP and SFTP support offers different mechanisms for | |

| | | |
|---|---|---|
| | configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security | |
| | Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time | |
| | IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications | |
| | Dual flash images provides independent primary and secondary operating system files for backup while upgrading | |
| | Multiple configuration files can be stored to a flash image | |
| | Ingress and egress port monitoring enable more efficient network problem solving | |
| | Precision Time Protocol allows precise clock synchronization across distributed network switches as defined in IEEE 1588. Needed for time critical applications like AVB, smart grid power automation, etc. Supports transparent clock E-E | |
| **Layer 2 Switching** | VLAN support and tagging for IEEE 802.1Q (4094 VLAN IDs) | |
| | IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs | |
| | MVRP allows automatic learning and dynamic assignment of VLANs | |
| | VXLAN encapsulation (tunnelling) protocol for overlay network that enables a more scalable virtual network deployment | |
| | Bridge Protocol Data Unit (BPDU) tunnelling Transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs | |
| | Port mirroring duplicates port traffic (ingress and egress) to a monitoring port; supports 4 mirroring groups | |
| | STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) | |
| | Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network | |

| | | |
|---|---|---|
| | IPv4 Multicast in VXLAN/EVPN Overlay support allows PIMSM/IGMP snooping in the VXLAN Overlay | |
| | IPv6 VXLAN/EVPN Overlay support, allows IPv6 traffic over the VXLAN overlay | |
| | VXLAN ARP/ND suppression allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network | |
| **Layer 3 Services** | Address Resolution Protocol (ARP) determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network | |
| | Dynamic Host Configuration Protocol (DHCP) simplifies the management of large IP networks and supports client; DHCP Relay enables DHCP operation across subnets, and DHCP server centralizes and reduces the cost of IPv4 address management | |
| | Domain Name System (DNS) provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server | |
| | Supports internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility | |
| | Route maps provide more control during route redistribution; allow filtering and altering of route metrics | |
| **Layer 3 Routing** | Supports Border Gateway Protocol (BGP) that provides scalable, robust, and flexible IPv4 and IPv6 routing, and also supports BGP-4 that delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks with graceful restart capability | |
| | Supports Open shortest path first (OSPF) delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery. | |
| | Supports Policy-based routing uses a classifier to select traffic that can be forwarded based on policy set by the network | |

| | | |
|---|---|---|
| | administrator | |
| | Dual IP stack maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design | |
| **Security** | Access control list (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header | |
| | ACLs also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis | |
| | Management access security for both on- and offbox authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services | |
| | Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks | |
| | Supports multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards | |
| | Supports MAC-based client authentication | |
| | Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3 | |
| | Switch CPU protection provides automatic protection against malicious network traffic trying to shut down the switch | |
| | ICMP throttling defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic | |
| | Port security allows access only to specified MAC addresses, which can be learned or specified by the administrator | |
| | MAC address lockout prevents particular configured MAC addresses from connecting to the network | |
| | Secure Sockets Layer (SSL) encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch | |
| | MAC Pinning allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port | |

| | | | |
|---|---|---|---|
| | | until the clients logoff or get disconnected | |
| **Accessories** | | Must include compatible 2x 10G multimode transceiver for the downlink to the proposed access switch | |
| | | Must include compatible 4x 1G multimode transceiver for the uplink and downlink to OSG existing WLAN Controller | |
| | | Must include compatible 2x 10G DAC cable for core switch 1 and 2 links providing high availability and resiliency | |
| **Warranty** | | With at least a Lifetime Warranty on parts and include one (1) Year next business day support | |
| **SUPPORT SERVICES RENEWAL** | | | |
| | | The proposal must include 1-year support services renewal for OSG's existing WLAN Controller. | |
| | | Delivers service-level agreements but not limited to:<br>• Hardware Replacement Support<br>• Remote HW Diagnosis & Support<br>• Software Technical Unlimited Support<br>• SW Technical Support<br>• SW Electronic Support<br>• Standard Response | |
| **SERVICES** | | | |
| | | Configuration, Integration of existing Network Policy Manager and Deployment Services with Knowledge Transfer | |
| | | Must provide a detailed scope of services. | |
| **1x (ONE) SERVER RACK TYPE** | | | |
| **Form Factor** | | 1U Rack Server | |
| **Processor** | | Can support up to two (2) Intel Xeon Processors<br>Must have 2x Intel Xeon Silver 4208 8C 85W 2.1GHz Processor | |
| **Memory** | | Can support up to 768GB of system memory<br>Must have a total of 128GB using 32GB TruDDR4 2933MHz 2Rx4 | |
| **Storage** | | 6x 2.4TB 10K SAS 2.5" HDD or 10TB usable on RAID5 | |
| **Power Supply** | | Dual, Hot-plug, Redundant Power Supply (1+1) 750W | |
| **Network Interface** | | 2x Integrated 1 GbE RJ-45 ports and 2-ports 1Gbe RJ45 via LOM | |
| **Optical Disk Drive** | | Must have external DVD-RW | |
| **Ports** | **Front** | 2x 1x USB 2.0 port with management access and 1x USB 3.0 port | |
| | **Rear** | 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port. | |

| | | |
|---|---|---|
| **Management** | *Mounting of remote ISO/IMG files via remote console<br>*Mounting files from Network: - Mount an ISO or IMG image file from a file server ( HTTPS, CIFS, NFS ) to the host as a DVD or USB drive<br>*Remotely controlling server power (Power on, Power off, Restart)<br>*Monitoring system status and health<br>*Remotely deploying an operating system<br>*Must support remote management through industry-standard interfaces such as IPMI Version 2.0, SNMP Version 3.0, CIM. | |
| **Features** | *Intelligent and adaptive system performance with energy efficient Intel Turbo Boost 2.0 Technology<br>*Intel Hyper-Threading Technology boosts performance<br>*Continuous monitoring of system parameters, triggers alerts and performs recovery actions in case of failure to minimize downtime<br>*Proactive Platform Alerts for components such as voltage regulators, fans, memory, power supplies, subcomponent temperatures, and server ambient | |
| **Manpower** | *Must have 3 Professional Certified Engineers<br>*Must have a certification granted by the supplier/manufacturer of the brand being offered. | |
| **Warranty** | 3YRs 24x7, 4HR Response | |
| | | |
| **SUPPLY OF NETWORK-ATTACHED STORAGE SOLUTIONS** | | |
| **Technical Specifications** | Must be 2U 8-Bay Rackmount and must include Rail Kit | |
| | Must be 2.5" and 3.5" SATA HDD/SSD drives compatible | |
| | Must be expanded to 12 bays | |
| | Must have Unified Data Management Operating System with support for the Btrfs file system | |
| | Mut provides schedulable and near-instantaneous data protection for shared folders and LUNs | |
| | Must be capable of File and folder-level data restoration | |
| | Must be capable to detects and recovers corrupted files using mirrored metadata and RAID configurations | |
| | Must be capable of Inline compression | |
| **Backup Solutions** | Must have the following features: | |
| | Must be capable of protecting Windows PCs and servers, VMs, other file servers, and even Google Workspace and Microsoft 365 cloud applications. | |
| | Must be capable to consolidates backup tasks for physical and | |

| | | |
|---|---|---|
| | virtual environments and enabling rapid restoration of files, entire<br>physical machines, and VMs. | |
| | Must be capable of Active Backup for Google Workspace and Microsoft 365 | |
| | Must have a private cloud solution for file sharing, concurrent document editing, emails, instant messaging, and others. | |
| | Must be capable of Virtualization | |
| | Must support local backup, network backup, and data backup to public clouds | |
| **Back up Tools** | • DSM configuration backup, macOS Time Machine support, Synology Drive Client desktop application<br>• Shared folder sync supports a maximum of 16 tasks | |
| **Snapshot Replication** | • Maximum number of snapshots for shared folders: 1,024<br>• Maximum number of replications: 32 | |
| **Hardware Specifications** | Must be Quad-core, 2.2 GHz Processor | |
| | Must be 4 GB DDR4 ECC SODIMM and expandable up to 32 GB Memory | |
| | Must be Hot swappable drives Compatible | |
| | Must have • 2 x USB 3.2 Gen 1 ports • 1 x Expansion port (eSATA) external ports | |
| | Must have 4 x 1GbE RJ-45 LAN Port | |
| | Must be Wake on LAN/WAN compatible | |
| | Must have PCI 3.0 slots: • 1 x 4-lane x8 slot • Supports 10GbE/25GbE network interface cards2 and M.2 NVMe SSD adapter cards for SSD cache | |
| | Must have Scheduled power on/of | |
| | Must have 2x System Fans | |
| | Must include 6 x 12TB Enterprise SATA 6 Gb/s 7,200 rpm HDD (must be the same brand) | |
| **HDD Specifications** | Must be 6.0 Gb/s, 3.0 Gb/s, 1.5 Gb/s interface speed | |
| | Must be 256 MiB Buffer size | |
| | Must be 242 MiB/s Maximum sustained data transfer speed | |
| | Must be 2,500,000 hours MTTF | |
| | Must be 550 total TB transferred per year workload rating | |
| **DSM Specifications** | | |
| **Networking protocols** | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) | |
| **File systems** | • Internal: Btrfs, ext4<br>• External: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT | |
| **Supported RAID** | Hybrid RAID (SHR), Basic, JBOD, RAID 0, RAID 1, RAID 5, | |

| | | |
|---|---|---|
| types | RAID 6, RAID 10 | |
| Storage management | • Maximum single volume size: 108 TB<br>• Maximum system snapshots: 65,53610<br>• Maximum internal volumes: 64 | |
| SSD cache | • Read/write cache support<br>• 2.5" SATA SSD support<br>• M.2 NVMe SSD support | |
| File sharing capabilities | • Maximum local user accounts: 2,048<br>• Maximum local groups: 256<br>• Maximum shared folders: 512<br>• Maximum concurrent SMB/NFS/AFP/FTP connections: 1,000 | |
| Privileges | Windows Access Control List (ACL), application privileges | |
| Directory services | Connects with Windows AD/LDAP servers enabling domain users to login via SMB/NFS/AFP/FTP/File Station using their existing credentials | |
| Security | Firewall, shared folder encryption, SMB encryption, FTP over SSL/TLS, SFTP, rsync over SSH, login auto block, Let's Encrypt support, HTTPS (customizable cipher suite) | |
| Supported clients | Windows 7 onwards, macOS 10.12 onwards | |
| Supported browsers | Chrome, Firefox, Edge, Internet Explorer 10 onwards, Safari 10 onwards, Safari (iOS 10 onwards), Chrome (Android 6.0 onwards) on tablets | |
| File Server & Synchronization | | |
| Drive | Synchronizes files across Windows, macOS, Linux, Android and iOS. The built-in cross-platform portal allows access to data anytime and anywhere.<br>• Maximum number of hosted files: 1,000,000<br>• Maximum number of concurrent connections for PC clients: 550 | |
| File Station | Provides virtual drives, remote folders, Windows ACL editor, compression/extraction of archived files, bandwidth control for specific users/groups, creation of sharing links, and transfer logs. | |
| FTP Server | Supports bandwidth control for TCP connections, custom FTP passive port ranges, anonymous FTP, FTP over TLS/SSL and SFTP protocols, network booting with TFTP and PXE support, and transfer logs. | |
| Presto File Server | Enables high-speed data transfer over WAN through the exclusive SITA technology between Synology NAS and desktop. | |
| Cloud Sync | Offers one or two-way synchronization with public cloud storage providers including Alibaba Cloud OSS, Amazon S3-compatible storage, Backblaze B2, Baidu Cloud, Box, Dropbox, | |

| | | |
|---|---|---|
| | Google Cloud Storage, Google Drive, hubiC, MegaDisk, Microsoft OneDrive, OpenStack Swift-compatible storage, Tencent COS, WebDAV servers and Yandex Disk. | |
| **Universal Search** | Enables global search of applications and files. | |
| **Warranty** | Must be 3 Year warranty on parts and labor. | |
| **Installation** | Must include Installation, configuration, and setup. | |
| **Support Service Requirement** | The Supplier must provide the following: | |
| | * Unlimited corrective maintenance/ repair services within the warranty period | |
| | * Twenty-four (24) hours by seven (7) days (Monday to Sunday) technical support and must meet the following response and resolution time: | |
| | > Within one (1) hour for phone or email support | |
| | > Within four (4) hours for on-site support | |
| | > For onsite support, the Supplier must attend to and repair the defective unit within two (2) business days | |
| | > In case of outside repair within the 1-year warranty period, the Supplier shall provide a service unit to the OSG within three (3) days upon pull out of the unit. The repaired hardware or replacement for the pulled-out hardware/unit must be delivered within fifteen (15) calendar days from the issuance of service unit. | |
| | * The Supplier should replace a factory defective unit with a new unit within 30 days upon delivery of the item. | |
| **Certification** | The Supplier must be an authorized reseller of the brand being offered. | |
| **SUPPLY OF NEXT GENERATION FIREWALL** | | |
| **General Specifications** | Performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port. | |
| | Must be capable of proxy-less and non-buffering inspection technology that provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing the file and stream size limitations and can be applied on common protocols as well as raw TCP streams. | |
| | Must have a single-pass DPI architecture that simultaneously scans for malware, intrusions, and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture. | |
| | Must have a multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation, and hypervisor level analysis technology to execute suspicious code and analyzes behavior, providing comprehensive visibility to | |

| | | |
|---|---|---|
| | malicious activity. | |
| | identify and mitigate even the most insidious modern threats, including future Meltdown exploits. It even detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. | |
| | scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, key loggers, and other malware in files of unlimited length and size across all ports and TCP streams. | |
| **Hardware** | | |
| Form Factor | The system must be of one (1) unit rack mountable. | |
| Interfaces | The system's interface must include:<br>1 Gbe Interfaces – 16x 1 Gbe<br>10G SFP+ - 3x 10G SFP+<br>USB 3.0 – 2x USB 3.0<br>Management interfaces - 1 GbE, 1 Console | |
| Management | CLI, Web GUI, NSM | |
| Built-in storage | 64 GB M.2 | |
| **Performance** | | |
| Throughput | The system must have the minimum throughput requirements (or higher):<br>Firewall Inspection Throughput – 5.2 Gbps;<br>Threat Prevention throughput – 3.0 Gbps;<br>Application inspection throughput – 3.6 Gbps;<br>IPS throughput – 3.4 Gbps;<br>Anti-malware inspection throughput – 2.9 Gbps;<br>TLS/SSL decryption and inspection throughput (DPI SSL) – 800 Mbps;<br>VPN throughput – 2.1 Gbps; | |
| Connections | The system must be capable of handling:<br>Connections per second - 21,000/sec;<br>Maximum connections (SPI) – 1,500,000;<br>Max DPI-SSL Connections – 125,000;<br>Maximum connections (DPI) – 500,000; | |
| IPsec VPN | The system must be capable of handling 50 (up to 1000 Concurrent IPSec VPN Clients) | |
| SSL-VPN | The system must be capable of handling 2 (up to 500 Concurrent SSL-VPN Clients) | |
| **Authentication** | The system must support LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, and Common Access Card (CAC). | |
| **Software** | | |
| Superior threat prevention and performance | The system must be qualified as a next-generation firewall (NGFW) and Multi-core hardware architecture. | |

| | | |
|---|---|---|
| Protection against unknown attacks | The system must have a Cloud-based multi-engine analysis that catches unknown and highly evasive advanced malware | |
| Threat intelligence and automation for memory-based signatures | The system must be capable of Memory inspection. This allows the system to see the instructions and sequences before they can be executed without the code. | |
| Network control and flexibility | The system must have a powerful operating system, Application Control Intelligence, Network segmentation and VLAN and Wireless Security. | |
| Robust Networking Capabilities | The system must have extensive switching and routing capabilities and supports high availability. | |
| Anti-malware | The system must be capable of<br>• Stream-based malware scanning<br>• Gateway anti-virus<br>• Gateway anti-spyware<br>• Bi-directional inspection<br>• No file size limitation | |
| **Secure SD-WAN** | The system must have:<br>• Future-proof against an ever-changing threat landscape by investing in a NGFW with multi-gigabit threat analysis performance.<br>• Provide direct and secure internet access to distributed branch offices instead of back-hauling through corporate headquarters.<br>• Allow distributed branch offices to securely access internal resources in corporate headquarters or in a public cloud, significantly improving application latency.<br>• Automatically block threats that use encrypted protocols such as TLS 1.3, securing networks from the most advanced attacks.<br>• Reduce complexity and maximize efficiency using a central management system delivered through an intuitive single pane of glass user interface. | |
| TLS/SSL/SSH decryption and inspection | The system must have:<br>• TLS 1.3 with enhanced security<br>• Deep packet inspection for TLS/SSL/SSH | |

| | | |
|---|---|---|
| | • Inclusion/exclusion of objects, groups, or hostnames<br>• SSL control<br>• Enhancements for DPI-SSL with CFS<br>• Granular DPI SSL controls per zone or rule<br>• Advanced threat protection<br>• Memory Inspection<br>• Cloud-based multi-engine analysis<br>• Virtualized sandboxing<br>• Hypervisor-level analysis<br>• Full system emulation<br>• Broad file type examination<br>• Automated and manual submission<br>• Real-time threat intelligence updates<br>• Block until verdict | |
| Intrusion Prevention | The system must have<br><br>• Signature-based scanning<br>• Automatic signature updates<br>• Bi-directional inspection<br>• Granular IPS rule capability<br>• GeoIP enforcement<br>• Botnet filtering with a dynamic list<br>• Regular expression matching | |
| Firewall | The system must be capable of:<br><br>• Stateful packet inspection<br>• reassembly-free deep packet inspection<br>• DDoS attack protection (UDP/ ICMP/SYN flood)<br>• IPv4/IPv6 support<br>• Biometric authentication for remote access<br>• DNS proxy<br>• Full API support<br>• Switch integration<br>• SD-WAN scalability<br>• SD-WAN Usability Wizard1<br>• Connections scalability (SPI, DPI, DPI SSL)<br>• Enhanced dashboard<br>• Enhanced device view<br>• Top traffic and user summary<br>• Insights into threats | |

| | | |
|---|---|---|
| | • Notification center | |
| Application Identification | The system must have:<br>• Application control<br>• Application bandwidth management<br>• Custom application signature creation<br>• Data leakage prevention<br>• Application reporting over NetFlow/IPFIX<br>• Comprehensive application signature database | |
| Virtual Private Network | The system must be capable of:<br>• Secure SD-WAN<br>• Auto-provision VPN<br>• IPSec VPN for site-to-site connectivity<br>• SSL VPN and IPSec client remote access<br>• Redundant VPN gateway<br>• Mobile Client for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire<br>• Route-based VPN (OSPF, RIP, BGP) | |
| High Availability | The system must be capable of<br>• A/P high availability with state sync<br>• High Availability - Active/Standby with state sync | |
| IPv6 | The system must support IPv6 | |
| **Environment** | | |
| Input power | • The system must be capable of running at 100-240 VAC, 50-60 Hz. | |
| Power Consumption | The system must not consume more the 36.3W of power. | |
| Humidity | The system must be 5-95% non-condensing. | |
| **Security Services** | | |
| Real-Time Updates | The system must be supported by<br>• Real-time threat intelligence updates<br>• Automatic signature updates | |

| | | |
|---|---|---|
| Advanced Protection | The system has complete suite of security services for firewalls that features Gateway Security, Content Filtering Service, Anti-Spam, 24x7 Support, ATP, Memory Inspection, DNS Security, Cloud Management and Cloud based Reporting – 7 Days. | |
| **Implementation Services** | | |
| Scope of Services | Must include Configuration, Testing, Documentation and Knowledge Transfer | |
| | The engineer must be available **24x7 Monday to Sunday** | |
| | The engineer must have a certification granted by the supplier/manufacturer of the brand being offered. | |
| **Support Services** | | |
| Enhanced Support | The system must include email and phone support for customers during local business hours; for two years. | |
| Firmware Upgrades | The system must include firmware upgrades during its warranty period. | |
| Comprehensive Support | The system must have Global Support available 8x5 or 24x7. | |
| **Accreditation** | | |
| Standards | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMPs, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | |
| Certifications (in progress) | The system must have certifications under Common Criteria NDPP Firewall with VPN and IPS | |
| Brand/Standard | The technology or brand must either be American or European for a more Global Standard compliance. | |
| Local Support | The brand must have local second level of support via its distributor that is compliant with global standard like ISO or Duns and Bradstreet to maintain a quality-of-service delivery. | |
| The local support must include the following: | | |
| | **2 Year Support Services**<br>**24x7 Monday to Sunday**. | |
| | Phone/Remote Technical Support | |
| | Onsite Technical Support with 2 to 4 hours Response Time | |
| | Corrective Maintenance for 5 Cases Per Year | |
| | The Supplier must provide full documentation for the Activity Plan on the installation of patches and upgrades and Root Cause Analysis of incidents encountered. | |
| | The Supplier must provide onsite support for the installation and deployment of software patches and version upgrades. | |
| | The Supplier must provide a procedure for support and problem escalation. | |
| | * Submission of Activity/Service Report within 5 calendar days | |

| | | |
|---|---|---|
| | after rendering service | |
| | Semi-Annual Preventive Maintenance visits during Regular Business Hours | |
| | Immediate replacement of the equipment and/or its parts. | |
| | * The Supplier shall replace a factory defective unit with a new unit within 30 days upon delivery of the item. | |
| | The Supplier must provide a certificate for the above services as part of the technical requirements. | |
| Certification | Must be certified with ICSA labs Advance Threat Defense certified with 100% unknown threat detection for 7 consecutive quarters from Q1-Q4, 2021 & Q1-Q3, 2022. | |
| | The Supplier must be an authorized reseller of the brand being offered. Must provide Authorization certificate from the Manufacturer or Vendor. | |

Prepared by the Technical Working Group – ICT Equipment:

SSS MARICAR T. MENDOZA

SSS JOEL N. VILLASERAN

SS II OMAR T. GABRIELES

SS II JOSEPH RYAN C. ABALOS

SS II PANTAS M. DE LEON

AS III MARIVI A. TUMAMBING

AS I MARY CLYDEEN L. VALENCIA

CAO JESSICA L. CASTRO

SAO JOY Y. CHUA

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO III AMELITO V. DUCUT

COMPRO III AUGUSTUS MARK B. DICHOSO

RECOMMENDING APPROVAL:

**ASG SHARON E. MILLAN-DECANO**
Bids and Awards Committee (BAC) Chairperson

**SSS AILEEN E. DALWATAN**
BAC - Vice Chairperson

**SSS CHERYL ANGELINE M. ROQUE-JAVIER**
BAC- Member

**SS LEANNE MAUREEN S. APOLINAR**
BAC – Member

**ASIII ALANNA GAYLE ASHLEY B. KHIO**
BAC – Member

**ASIII EMILE JUSTIN D. CEBRIAN**
BAC – Member

**DIRECTOR BERNADETTE M. LIM**
BAC – Member

Approved/Disapproved:

**MENARDO I. GUEVARRA**
Solicitor General

Certified Funds Available:

**BERNADETTE M. LIM**
Dir IV – FMS