our future through science

Request for proposals (RFP)

For the Supply of Network and Security equipment, software and services to the CSIR

RFP No. 3395/09/10/2020

Proposal Specification

Annexure A

1. NETWORKING AND SECURITY TECHNICAL REQUIREMENTS

The goal of this RFP is for the Bidders to provide the Networking and Security solution for the CSIR as per the information below.

CSIR ideal network diagram is as follow

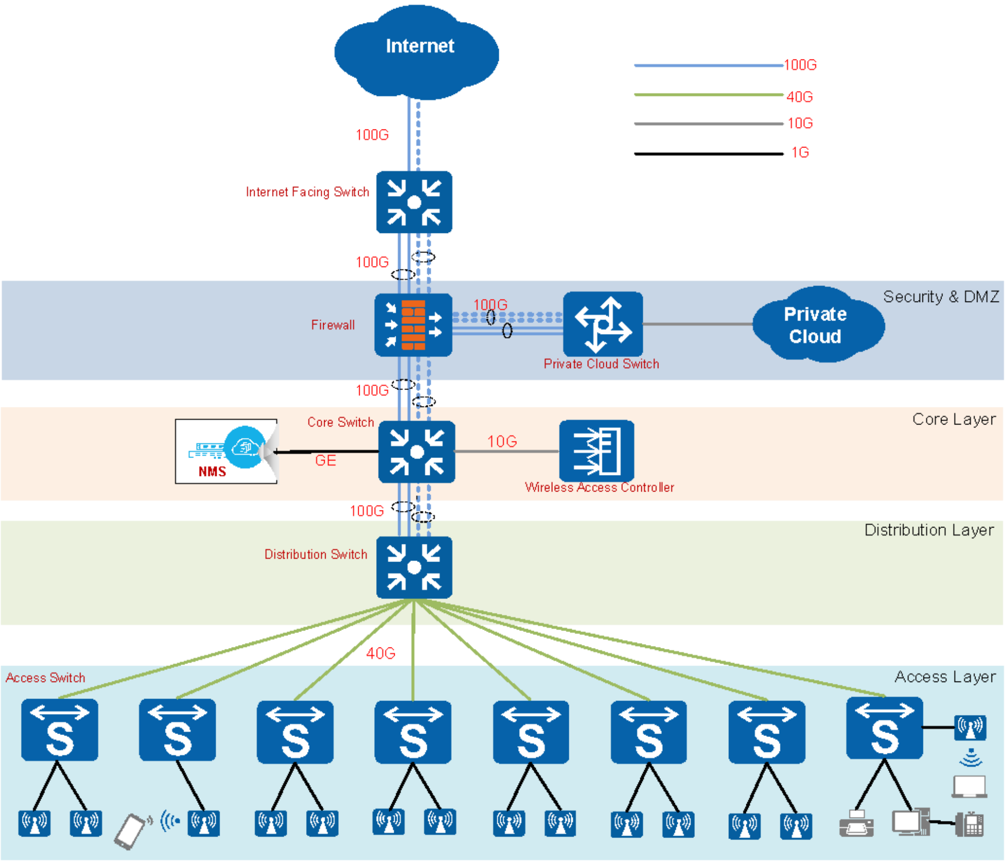

Figure 1: CSIR IDEAL NETWORK

The solution must provide the following features and functionality:

- All the Network and Security devices must have redundant power supply.
- The solution provided must at least be fully compatible with Network Access Control
- The proposal must include a 42U Rack with smart PDUs to host the hardware equipment

1.1 Access Layer

The supplier must provide a minimum of 10 Access switches with the following:

- a minimum of 48 x 1Gig UPOE 802.3af/at/bt compliant ports.
- a minimum of 1440W available PoE power, to power Access Points with higher power demands.
- a minimum of 2 X 40G uplink ports to connect to the distribution layer switch and should be scalable to 2 X 100G uplink ports
- support redundant power supply for device redundancy
- support a minimum of 12 x 100M/1G/2.5G/5G ports of nBase-T Ethernet (IEEE 802.3bz) for Access Point connectivity and should be scalable to a minimum of 24 X 100M/1G/2.5G/5G and 10G ports of nBase-T Ethernet (IEEE 802.3bz)
- support (OSPF, ISIS, RIP) Layer 3 routing protocols.
- support (IGMP v1, 2, and 3, PIM) to achieve dynamic multicasting.
- support a data stacking solution to achieve simplicity, scalability, and flexibility.
- be able to support a packet sampling technology like Netflow, IPFIX, Netstream, sFlow or other similar technologies for network security and monitoring.
- be able to be managed by a centralised controller, WebUI, CLI and API for network management and control.
- at least support programmability via an API like (RESTconf, NetConf) with industry standard models (YANG etc) for network administration and expansion of future capabilities
- support AAA / Network Access Control to enable simplified Network Segmentation based on policies defined in Network Access Control
- include all relevant SFP's and or Active Optical Cables.

1.2 Distribution Layer

The Distribution Switching Layer must consist of the following:

- support 10 x 40G ports and must be scalable up to 20 x 40G ports to ensure connectivity to the access layer switches and potential future growth
- support a minimum of 4 x 100G ports and must be scalable to 6 x 100G ports to comply with current requirements and future expansion.
- 25G port capability to ensure compatibility for potential future requirements
- 10G port capability to ensure compatibility for potential future requirements.
- 4Tbps or more of switching capacity to ensure sufficient capacity and throughput.
- support redundant power supply for device redundancy
- support (OSPF, ISIS, RIP and BGP) Layer 3 routing protocols.
- support (IGMP v1, 2, 3, PIM) to achieve dynamic multicasting.
- be able to be managed by a centralised controller, WebUI, CLI and API for network management and control.
- be able to support a packet sampling technology like Netflow, IPFIX, Netstream, sFlow or other similar technologies for network security and monitoring.
- at least support programmability via an API like (RESTconf, NetConf) with industry standard models (YANG etc) for network administration and expansion of future capabilities

- support AAA / Network Access Control to enable simplified Network Segmentation based on policies defined in Network Access Control
- include all relevant SFP's and or Active Optical cable

1.3 Private Cloud Switch

The Private Cloud Switch must consist of the following:

- support at least 6 x 100G ports to comply with uplink requirements and future potential expansion.
- support a minimum of 20 x 25Gps ports to comply with current requirements and potential future expansion.
- 10GE port capability to ensure compatibility for potential future requirements.
- 3Tbps or more of switching capacity to ensure sufficient capacity and throughput.
- be able to be managed by a centralised controller, WebUI, CLI and API for network management and control
- at least support programmability via an API like (RESTconf, NetConf) with industry standard models (YANG etc) for network administration and expansion of future capabilities
- support AAA / Network Access Control to enable simplified Network Segmentation based on policies defined in Network Access Control
- include all relevant SFP's and or Active Optical cable.

1.4 Core Switch

The Core Switch must consist of the following:

- support a minimum of 100G, 40G, 25G, 10G and 1 G Ethernet speeds to comply with current and future expansion.
- support a minimum of 12 x 1GE/10GE RJ45 copper interfaces to comply with current and future expansion.
- at least support telemetry and SNMP capabilities and should provide real-time visibility into switch and fabric states.
- 6Tbps or more of switching capacity to ensure sufficient capacity and throughput.
- support at least 6 x 100G ports and must be scalable up to 12 x 100G ports to comply with uplink requirements and future potential expansion.
- support redundant power supply for device redundancy
- be able to be managed by a centralised controller, WebUI, CLI and API for network management and control
- at least support programmability via an API like (RESTconf, NetConf) with industry standard models (YANG etc) for network administration and expansion of future capabilities
- support AAA / Network Access Control to enable simplified Network Segmentation based on policies defined in Network Access Control
- be able to support a packet sampling technology like Netflow, IPFIX, Netstream, sFlow or other similar technologies for network security and monitoring.
- include all relevant SFP's and or Active Optical cables

1.5 Internet Facing Switch

The Internet-facing switch must consist of the following:

- support at least 8 x 100Gbps ports and must be scalable up to 12 x 100Gbps ports to comply with uplink requirements and future potential expansion.
- support at least a minimum of 12 x 10G SFP+ interfaces to comply with current requirements and future expansion.
- 25G port capability to ensure compatibility for potential future requirements
- 40G port capability to ensure compatibility for potential future requirements
- 6Tbps or more of switching capacity to ensure sufficient capacity and throughput.
- support redundant power supply for device redundancy
- be able to be managed by a centralised controller, WebUI, CLI and API for network management and control
- at least support programmability via an API like (RESTconf, NetConf) with industry standard models (YANG etc) for network administration and expansion of future capabilities
- support AAA / Network Access Control to enable simplified Network Segmentation based on policies defined in Network Access Control
- be able to support a packet sampling technology like Netflow, IPFIX, Netstream, sFlow or other similar technologies for network security and monitoring.
- include all relevant SFP's and or Active Optical cable

1.6 Wireless Access Controller

The Wireless Access Controller (WAC) must consist of the following:

- be an appliance-based controller and must be able to support a minimum of 100 AP's and must be expandable to support 250 AP's
- a minimum of 5G forwarding performance to ensure sufficient throughput.
- a minimum of 2 x 10G interfaces to ensure redundancy and throughput.
- support 802.11ax capable access points to ensure compatibility with WIFI6
- uplink port must support load balancing and trunk link aggregation to ensure sufficient throughput and redundancy.
- include network management for the product
- support rolling AP upgrades to simplify network operations and update access points without widespread disruption.
- support for web content filtering
- allow for software patching and seamless AP additions
- be able to support network segmentation
- at least support programmability via an API like (RESTconf, NetConf) with industry standard models (YANG etc) for network administration and expansion of future capabilities
- support integration into Location-based services
- be able to support the Simple Network Management Protocol (SNMP) v1, v2c, v3
- support AP RF group creation and automatic assignment.
- support zero-touch provisioning through Plug and Play
- be compatible with the existing CHPC Cisco Identity Services Engine.
- configuration must include all relevant SFP's and or Active Optical cable

1.7 Indoor Access Points

The Indoor Access Points must consist of the following:

- a minimum of 14 Indoor Access Points.
- be compliant with IEEE 802.11a/b/g/n/ac/ac Wave 2/ax standards to ensure compliance with WIFI6.
- support a minimum of 2.4G 4x4 + 5G 6x6 dual bands with internal antennas to ensure compatibility with current requirements and compliance with WIFI6.
- support for BLE(Bluetooth Low Energy).
- be controlled and managed by a centralised controller to ensure management of the solution.
- be compatible with the existing CHPC Cisco Identity Services Engine.
- support MU-MIMO and OFDMA.
- support internal antennas to comply with building aesthetics .
- uplink interface must support a minimum of 1, 2,5 & 10 Gig Ethernet (RJ-45) (IEEE 802.3bz / nBaseT) to ensure sufficient throughput of the uplink port.
- support both the 802.3at and 802.3bt standards to comply with switch POE standards.
- a built in IoT module or expansion ports that can support IoT standards like RFID,Zigbee,etc.

1.8 Outdoor Access Points

The Outdoor Access Points must consist of the following

- a minimum of 2 Outdoor Access Points.
- at least be compliant with the IEEE 802.11a/b/g/n/ac wave2 standards to ensure compliance with the AC Wave 2 standard.
- support 4x4 MU-MIMO with a minimum of 3 spatial streams on both the 2.4G and 5G radios to ensure compatibility with current requirements.
- support Multiuser and Single-user MIMO
- support operating temperature ratings of -40 to +65 degrees Celsius to ensure outdoor environment compatibility.
- be compatible with the existing CHPC Cisco Identity Services Engine
- be compliant with IP67 environmental rating to ensure outdoor environment compatibility.
- be controlled and managed by a centralised controller to ensure management of the solution.

1.9 Next Generation Firewall (NGFW)

The NGFW must consist of the following:

- be scalable up to a minimum of 12 x 100G interfaces to comply with current design requirements.
- at least have IPS, Antivirus, URL filtering, and malware protection with a minimum throughput of 30Gig or above to comply with current requirements and future expansion.
- be able to support VPN.
- a maximum of 2 x 100G interfaces on a single line expansion slot to ensure that the network will not be interrupted if the line expansion slot module fails.
- at least support visibility and advanced security capabilities.
- support supervisors in an active/standby or active/active switchover configuration for supervisor redundancy.
- be scalable to support a minimum of 960G throughput to comply with current and future requirements.
- data flows must be equally distributed to the service processing units to prevent performance bottlenecks.
- support service processing unit redundancy without interrupting service transmission to ensure service continuity.
- line processing unit/module must be compatible with different interface cards (10GE, 40GE, 100G) to avoid additional cost if different network speeds are required in the future.
- support cross-board port bundling to improve throughput and port density.
- support redundant power supply for device redundancy.
- include management for the product
- include all relevant SFP’s and or Active Optical cable

1.10 Monitoring

- The supplier must provide a Network Monitoring tool, the tool should be able to generate reports, e-mail real-time alerts, Bandwidth monitoring/usage, dashboards, visibility in Network traffic, Alarms, able to view top talkers, troubleshooting applications, servers, including private cloud, End-user monitoring, customisable to allow integration of scripts, real-time event log, and troubleshooting network performance.
- The suppliers must to explain the solution upgrade process and also provide a detailed plan on how the existing configurations and Firewall Access Control Lists will be migrated to the new equipment

2. IMPLEMENTATION

The installation and setup of the system must be performed at the CHPC facility in

Rosebank, Cape Town.

- The supplier must provide a support engineer on-site, available 8 am–4:30 pm Monday through Friday, with the exception of Public holidays, beginning on the project initiation date until project completion. The support engineer will be expected to work closely with CHPC staff to develop, configure, test the system until the acceptance stage and it is ready to run the production workloads.
- It is also expected that the knowledge of the system configuration, installation, and maintenance package will be transferred to CHPC staff during this period.
- The supplier must provide a project plan for the configuration and Installation of new equipment and clearly explain the solution upgrade process and provide a detailed plan on how the existing configurations and Firewall Access Control List will be migrated to the new equipments

3. WARRANTY AND LICENCES

- The cost of the proposed system shall include all warranties and licensing (if applicable) for all hardware and any software, delivered with the system. This must include hardware that is not manufactured by the primary Vendor. Warranties and licenses (if applicable) shall be for a period of 3 years of operation.
- The start date of the year of full production operation is defined as the day of machine acceptance.

4. MAINTENANCE, SUPPORT AND TECHNICAL SERVICES

- Hardware support will require replacement of failed or faulty critical components by the next business day or sooner. A critical component is defined as one that is required to enable 90% of the system to be able to run projects successfully. Software support will require telephone and email response to problem calls and questions. Response to software support calls to be next business day or sooner.
- Bidders should describe both the hardware and software support provided for the proposed system during the support period.
- Bidders should specify the location of the nearest parts depot and explain the conditions under which support will be contracted out to a third party.
- Bidders must provide information on how they anticipate delivering and supporting their proposed solution, paying particular attention to the personnel and skills available within their organisation.

5. SKILLS TRANSFER AND TRAINING

- Each proposal must include the implementation process that the Vendor will follow to work together with the CHPC staff.
- Bidders must commit to on-site skills transfer for system administration of the equipment and software as part of their proposal.
- Skills transfer shall commence before the implementation and prior to the beginning of the Acceptance Testing Period.
- Training must be onsite for two (2) CSIR personnel.

The Skills transfer and training for the technical team should include the following topics:

- System Operation and Advanced Administration

➢ Software installation and updating;
➢ System monitoring;
➢ System reconfiguration;
➢ Network configuration and modification;
➢ System security

The bidder must describe all proposed training (if not specified) and documentation relevant to the proposed solutions utilising the following methods:

- Classroom training
- Onsite training
- Online documentation
- Online training

6. ACCEPTANCE TEST SUITE

- The Acceptance test suite will form part of the contractual agreement with the successful bidder and will be evaluated after the successful implementation of the proposed solution.
- Acceptance of the Network solution will be assessed using Iperf. This consists of a tool for active measurements of the maximum achievable bandwidth on IP Networks, it supports tuning of various parameters related to timing, buffers and protocols (TCP, UDP, SCTP) with IPv4 and IPv6, for each test it reports the bandwidth, loss, and other parameters.