ANNEX A

STATEMENT OF WORK

Software Defined Wide Area Network (SD-WAN)

Client Solution

FINAL Version 5.0
December 20, 2021

Table of Contents

Index of Figures

1 INTRODUCTION

1.1 Purpose

(1) Shared Services Canada (SSC) intends to procure a Software Defined Wide Area Network (SD-WAN) "Solution" as rapidly as possible to meet immediate operational requirements.

(2) The Government of Canada networks connect more than 3500 sites located in more than 1300 cities and towns. SSC provides network services to 42 federal departments and agencies. Client sites vary from critical locations which require very high availability such as Departmental regional headquarters and high visibility offices, to remote locations that are not easily or rapidly accessible.

(3) SSC has refreshed its Network and Security Strategy to align with current best practices, and to be adaptable to future requirements for its network and security services. Software-Defined Networking, and in particular SD-WAN, is a cornerstone to executing SSC's Network and Security Strategy.

(4) The need for the revised strategy is further reinforced by looking at the data that traverses the government networks—everything from Government of Canada corporate data to real-time video traffic to the personal information of Canadians interacting with Government Departments and Agencies.

(5) Consistent with this strategy, SSC plans to procure an SD-WAN Solution for international locations and to meet immediate operational requirements. Since SSC intends to centrally manage overlay networks for its Clients, the SD-WAN Solution to be procured will be from a single Original Equipment Manufacturer (OEM) solution provider.

1.2 Business Outcomes

(6) SSC expects that the SD-WAN Solution will provide the following key benefits:

a) Better user experience through end-to-end visibility and ability to automatically monitor and enhance QoS and performance by application and location;

b) Improved reliability and better control over traffic leveraging the ability to use multiple transport paths based on defined Service Level Agreement (SLAs) and policies;

c) Enhanced security through centralized visibility and control over network assets and services including the ability to immediately detect incidents and respond to them by pushing security policies to all SD-WAN devices across the network;

d) Increased network resiliency through self-healing, auto-recovery and automation;

e) Simplified WAN management through centralized configuration across all networks;

f) Zero-Touch-Deployment to minimize manual intervention by on-site technicians;

g) The ability to manage traffic across all logical networks;

h) Lower average cost for bandwidth with the ability to reduce cost and/or provide much higher bandwidth via greater use of Broadband network services; and

i) Eliminate technological barriers to Information and Communications Technology (ICT) accessibility.

1.3 Approach

(7) The contract that may result from this solicitation will enable SSC to purchase an SD-WAN Solution to meet the near-term operational requirements for one or more of its Clients.

(8) The SD-WAN Solution will include SD-WAN edge devices, SD-WAN controller and orchestration software and / or hardware as may be required according to the Solution that is contracted for, and a Subscriber Web Portal that will enable SSC to administer all aspects of the SD-WAN overlay networks centrally. The SD-WAN Solution provided will not include the underlay network services (e.g. MPLS, broadband Internet, carrier Ethernet).

(9) SSC intends to purchase:

a) 416 SD-WAN edge devices of varying capabilities to accommodate different site characteristics;

b) two redundant sets of the Controller and Orchestration hardware and / or software that is necessary for the SD-WAN Solution;

c) the licensing required to activate and enable the features of all components of the SD- WAN Solution; and

d) an initial 5 years of maintenance and support services for all SD-WAN equipment, provided according to the defined maintenance service levels.

(10) SSC will install and deploy all components of the SD-WAN Solution.

(11) SSC will manage the SD-WAN Solution with the Controller and Orchestration components that it acquires through the Contract.

2 SOLUTION OVERVIEW

2.1 Solution Model

(12) The SD-WAN Solution service model is shown in Figure 1.

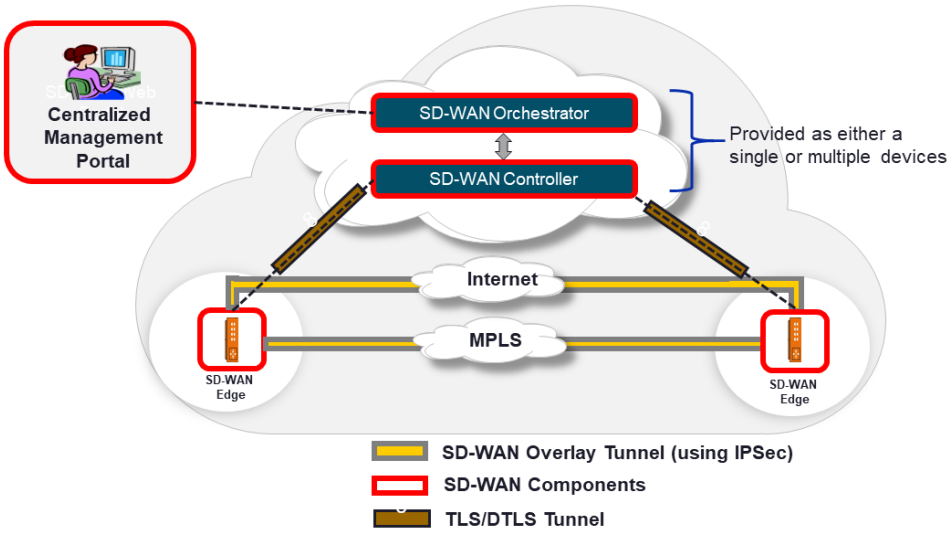

Figure 1: SD-WAN Service Model

2.2 Scope

(13) The Contractor must provide an SD-WAN Solution that at a minimum includes:

a) Hardware and virtual Edge Devices:

b) Controller and Orchestration hardware and / or software that includes a centralized management capability;

c) Licensing; and

d) Maintenance and Support.

(14) The SD-WAN Solution provided will not include the underlay network services (e.g. MPLS, broadband Internet, Carrier Ethernet).

2.2.1 SD-WAN Edge Device

(15) An SD-WAN Edge Device implements data plane routing functionality. It makes routing decisions based on policies sent by the associated SD-WAN Controller. The Edge Device is most often physically located at the Client premises.

2.2.2 SD-WAN Controller and Orchestration

(16) The SD-WAN Controller and Orchestration service provides the service management of the SD-WAN Solution including service fulfilment, performance control, usage, analytics, security and policy. It is responsible for configuring the end-to-end SD-WAN service between the SD-WAN Edge Devices. It provides a centralized management capability with a wide variety of features for the SD-WAN Solution that includes the authorized creation of policies and the immediate provisioning of resources and bandwidth for applications or specific traffic.

2.2.3 Licensing

(17) SD-WAN solutions typically require licensing to enable various different and / or tiered levels of features and capabilities that the SD-WAN Solution’s components provide.

2.2.4 Maintenance and Support

(18) Maintenance and Support services are defined to be all of the necessary hardware, software, firmware, license, subscription and resource support that are necessary for fault restoration, ongoing functional operation and preventative maintenance for all SD-WAN Solution components.

3 SOLUTION PROVISIONING

(19) The Contractor must provide all SD-WAN Solution hardware, software, licensing and maintenance that are necessary to fulfill the requirements identified in this SOW.

3.1 Hardware Configurations

(20) The Contractor must provide all SD-WAN hardware devices with the appropriate hardware configuration required to enable Canada to successfully deploy and operate the SD-WAN solution with all of the required features identified in this SOW .

(21) All of the SD-WAN devices that the Contractor provides must be mountable in a 19-inch rack.

(22) The Contractor's SD-WAN controller / orchestration Solution must be provided with the hardware configuration (e.g. model, CPU, memory, storage) required to be able to manage at least 500 SD-WAN Edge devices with each SD-WAN device connected to at least two SD-WAN controllers. In the event that an SD-WAN Solution requires more than one device to perform the controller and orchestration deployment functions, then all of the devices need to be provided as a comprehensive unit with the pricing for the entire unit included in Annex B). All components of the comprehensive group of devices must be clearly described in Annex C with a detailed description of the hardware configuration (e.g. model, CPU, memory, storage, etc).

(23) The Contractor must provide SD-WAN Edge Devices as summarized in Figure 2 Hardware Configurations. The SD-WAN Edge Devices must:

a) be provided with the appropriate hardware (CPU, memory and storage) to support SD-WAN requirements identified in Table 2 and Section 5.1 Scalability;

b) provide minimum data-plane encryption throughput with Internet Mix (IMIX) traffic profile and zone-based layer 4 firewall enabled;

c) support a minimum number of SDWAN Edges within specified overlay topology; and

d) support a minimum of two independent transport networks.

(24) The Contractor must provide SD-WAN Edge Devices and licenses, as summarized in Figure 2 below, that conform to the following categorizations:

a) Category 1: SD-WAN Edge device with the appropriate hardware configuration (CPU, memory, storage) to provide up to 200 Mbps of encrypted data plane throughput with Internet Mix (IMIX) traffic and zone-based layer 4 firewall enabled. There must be at least 2 x 1 Gigabit Ethernet LAN ports, 2 x 1 Gigabit Ethernet WAN port. The device must provide an out-of-band management port. The device must support a minimum of 50 devices with dual transport connections (e.g. MPLS and Internet) in a fully meshed overlay topology.

b) Category 2: SD-WAN Edge device with the appropriate hardware configuration (CPU, memory, storage) to provide up to 500 Mbps of encrypted data plane throughput with Internet Mix (IMIX) traffic and zone-based layer 4 firewall enabled. There must be at least 2 x 1 Gigabit Ethernet LAN ports, 2 x 1 Gigabit Ethernet WAN port. One of the WAN ports must support 100 Base-TX. The device must provide an out-of-band management port. A redundant power supply must be provided for each device. The device must support a minimum of 200 devices with dual transport connections (e.g. MPLS and Internet) in a fully meshed overlay topology.

c) Category 3: SD-WAN Edge device with the appropriate hardware configuration (CPU, memory, storage) to provide up to 2 Gbps of encrypted data plane throughput with IMIX traffic and zone-based layer 4 firewall enabled. There must be at least 4 x 1 Gigabit Ethernet LAN ports and 4 x 1 Gigabit Ethernet WAN ports per device. The device must provide an out-of-band management port. A redundant power supply must be provided for each device. The device must support a minimum of 500 IPSec endpoints with dual transport connections (e.g. MPLS and Internet) in an overlay topology.

d) Category 4: SD-WAN Edge device with the appropriate hardware configuration (CPU, memory, storage) to provide up to 10 Gbps of encrypted data plane throughput with IMIX traffic and zone-based layer 4 firewall enabled. There must be at least 4 x 10 Gigabit Ethernet LAN ports and 4 x 10 Gigabit Ethernet WAN ports per device. The device must provide an out-of-band management port. A redundant power supply must be provided for each device. The device must support a minimum of 1000 IPSec endpoints with dual transport connections (e.g. MPLS and Internet) in an overlay topology.

e) SD-WAN Virtual Edge with the software required for up to 2 Gbps throughput of encrypted IMIX traffic and zone-based layer 4 firewall enabled.

	Edge Device Category 1	**Edge Device Category 2**	**Edge Device Category 3**	**Edge Device Category 4**
IPSec Encryption Throughput (IMIX Traffic) and zone-based layer 4 firewall enabled	200 Mbps	500 Mbps	2 Gbps	10 Gbps
Minimum number of ports	2 x 1 Gigabit Ethernet LAN ports 2 x 1 Gigabit Ethernet WAN ports	2 x 1 Gigabit Ethernet LAN ports 2 x 1 Gigabit Ethernet WAN port (1 WAN port must support 100 Base-TX)	4 x 1 Gigabit Ethernet LAN ports 4 x 1 Gigabit Ethernet WAN ports	4 x 10 Gigabit Ethernet LAN ports 4 x 10 Gigabit Ethernet WAN ports
Minimum SD-WAN Edge devices supported	50	200	500	1000
Redundant Power Supply	No	Yes	Yes	Yes
Out-of-band management port	Yes	Yes	Yes	Yes
Form Factor	Maximum 1 rack unit	1 rack unit	1 or 2 rack units	1 or 2 rack units

Figure 2: Hardware Configurations

3.2 Edge Devices

(25) The Contractor must ensure that the SD-WAN products that it offers to provide conform, at a minimum, to the functionality and technical specifications that are identified in this SOW.

(26) The Contractor must ensure that all SD-WAN hardware devices and hardware components that it provides are new (i.e. never previously used or refurbished).

3.3 Controller and Orchestration

(27) The Contractor must provide a redundant set of the Controller and Orchestration hardware and / or software that is necessary for its proposed SD-WAN Solution. That is, if the Contractor's SD-WAN Solution requires one piece of equipment for Controller functionality and one piece of equipment for Orchestration functionality, then the Contractor must provide two Controller pieces of equipment and two Orchestration pieces of equipment and all of the software / licensing required for the equipment's functionality. The controller and orchestration solution must be configurable to be highly available in an active-active or active-standby mode.

(28) The Contractor must provide a centralized management capability for its SD-WAN Solution that can be used by Canada to create, monitor and manage all SD-WAN overlay networks; and perform all necessary licensing activities.

3.4 Licensing

(29) The Contractor must provide the licensing required to activate all of the features and capacity required to meet all of the requirements specified in this SOW (i.e. the highest level of licensing to meet all of the requirements that are specified in this SOW). The subscription model / licensing must be provided for five years after the date of component receipt.

3.5 Management and Security Features

(30) The Contractor's SD-WAN Solution must support the following management and security features:

a) WAN virtualization;
b) network abstraction;
c) elastic traffic management;
d) route optimization;
e) dynamic path selection;
f) application aware routing;
g) device configuration using templates;
h) certificate management;
i) element management;
j) software management and automated updates;
k) traffic and performance statistics; and
l) policy-driven centralized management.

(31) The Contractor must provide a detailed description of the management and security features that will be available through the licensing of its proposed SD-WAN Solution.

3.6 Maintenance and Support

3.6.1 Support

(32) The Contractor must provide all components of its SD-WAN Solution with five years of maintenance and support services that begins no sooner than the date of the delivery of a component of the SD-WAN Solution.

(33) The Contractor must act as the intermediary and facilitate Canada's direct access to the OEM's technical support service and online self-service tools when requested by Canada to facilitate the work efforts of Canada's resources.

(34) The Contractor's maintenance and support services must at a minimum include:

a) Technical resource support that is available by telephone, email and the OEM's online support platform,

b) Access to SD-WAN components firmware and security updates from the OEM's online platform, and

c) Access to the OEM's online learning and knowledge base resources.

3.6.2 Hardware Maintenance

(35) The Contractor must provide an advance replacement Return Merchandise Authorization (RMA) service whenever it is notified by Canada of any hardware failure during the 5-year maintenance and support service term.

(36) The Contractor must provide the advance replacement RMA service by shipping hardware that is identical to the hardware that Canada identifies to have failed within one business day of notification by Canada. Any request by the Contractor to replace identical hardware/functionality must be approved by Canada.

4 SECURITY

4.1 ITSG-33

(37) The Canadian Centre for Cyber Security (CCCS) has provided guidelines to Canada on IT Security Risk Management (https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33). These guidelines assist in the implementation of Canada's security standards, policies, and guidelines through the development lifecycle of a system.

(38) The Contractor must provide an SD-WAN solution that uses FIPS 140-2 Level 1 and / or FIPS 140-3 validated cryptographic modules as per CCCS ITSP.40.111. Modules which are in the process of being reviewed by NIST may be accepted, but must be on the published list of modules in process list at https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list or the https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/IUT-List.

4.2 General

(39) The Contractor's SD-WAN Solution must provide a centralized view of all security-related data.

(40) The Contractor must provide an SD-WAN Solution which provides a zone-based layer 4 firewall.

(41) The Contractor's SD-WAN Solution must provide the ability to segregate the network by zone, environment type (e.g. production, pre-production, test and by organization (e.g. department, agency).

(42) The Contractor's SD-WAN Solution must provide the ability for administrators to create and manage VRFs (or VPNs) to separate traffic.

(43) The Contractor's SD-WAN Solution must provide the ability for administrators to segregate and virtually isolate network traffic based on tenant profile and security policies.

(44) The Contractor's SD-WAN Solution must provide real-time security monitoring and reporting.

(45) The Contractor's SD-WAN Solution must forward the logging events of all SD-WAN devices to a centralized logging server hosted on Canada's premises.

(46) The Contractor's SD-WAN Solution must support access control lists (ACLs).

(47) The Contractor's SD-WAN Solution must support centralized patch management of the SD-WAN Edge Devices and Management Portal to stay current against any security vulnerabilities (including firmware updates) published by the OEM.

4.3 Authentication

(48) The Contractor's SD-WAN Solution must support the management of public keys for security services including Transport Layer Security (TLS) and Internet Protocol Security (IPSec).

(49) The Contractor's SD-WAN Solution must support Terminal Access Controller Access Control System (TACACS+) user authentication for administrative access to SD-WAN devices.

(50) The Contractor's SD-WAN Solution must support the enrollment and renewal of device certificate manually.

(51) The Contractor's SD-WAN Solution must support enrollment and renewal of device certificate via PKI integration protocols such as SCEP (Simple Certificate Enrollment Protocol), EST (Enrollment over Secure Transport) or ACME (Automatic Certificate Management Environment.

(52) The Contractor's SD-WAN Solution must support PKI Certificate Authority rollover.

(53) The Contractor's SD-WAN Solution must provide the capability to disassociate an SD-WAN edge (containing an invalid/revoked certificate) from the SD-WAN fabric.

(54) The Contractor's SD-WAN Solution must use certificates on all controllers.

4.4 User Management

(55) The Contractor's SD-WAN Solution must provide a management capability that enables an administrative user to configure access that, at a minimum, provides the following functions:

a) Add, delete, edit and configure user to perform operations on a device;
b) Manage password for each user with the option of using two-factor authentication;
c) Add, delete, edit and configure a User Group to perform operations on a device;
d) Add, delete users to a User Group; and
e) Logs and reports on changes.

(56) The Contractor's SD-WAN Solution must support role-based access control (RBAC) with authentication authorization accounting (AAA) using TACACS+ to provide the ability to limit user permissions to view / configure by logical network.

4.5 Control Plane

(57) The Contractor's SD-WAN Solution must protect the confidentiality, integrity and availability of control plane communication between SD-WAN Controllers and Edge Devices using Transport Layer Security (TLS/DTLS) or IP Security (IPSec) as recommended in document ITSP.40.062 Guidance on Securely Configuring Network Protocols (Version 2).

4.6 Data Plane

(58) The Contractor's SD-WAN solution must protect the confidentiality, integrity and availability of data transport between SD-WAN Edge Devices using IP Security (IPSec) as recommended in document ITSP.40.062 Guidance on Securely Configuring Network Protocols (Version 2 including:

a) An IPSec Security Association (SA) must be established by IKEv2;

b) Encapsulating Security Protocol (ESP) must be used in tunnel mode;

c) Encapsulating Security Protocol (ESP) Security Association (SA) key lifetime must not exceed 8 hours; and

d) IKEv2 SA authentication lifetime of must not exceed 24 hours..

5 TECHNICAL REQUIREMENTS

5.1 Scalability

(59) The Contractor's SD-WAN Solution must be scalable to support at least 2,000 SD-WAN Edge devices from the same OEM in the event that Canada acquires additional SD-WAN Devices in subsequent procurements.

(60) The Contractor's SD-WAN solution must be scalable to 16 VPNs.

(61) The Contractor's SD-WAN solution must support a minimum of 1000 devices within a single VPN.

(62) The Contractor's SD-WAN Solution must support a minimum of 200 devices with dual transport connections (e.g. MPLS and Internet) in a fully meshed overlay topology.

(63) The Contractor's SD-WAN Solution must support a minimum of 50,000 NAT sessions per edge device.

(64) The Contractor's SD-WAN Solution must provide interfaces with speeds up to 10 Gbps.

(65) The Contractor's SD-WAN Solution must support a minimum of 500 user accounts with role-role-based control capability.

5.2 Deployment

(66) The Contractor's SD-WAN Solution must support zero-touch provisioning to deploy and configure SD-WAN devices.

(67) The Contractor's SD-WAN Solution must support hub and spoke, full mesh, partial mesh and point-to-point topologies on overlay networks.

(68) The Contractor's SD-WAN Solution must support dual stack configuration (IPv4 and IPv6).

(69) The Contractor's SD-WAN Solution must allow administrators to push configuration templates to SD-WAN devices.

(70) The Contractor's SD-WAN Solution must provide the ability to do out-of-band management to remotely manage devices when in-band management via control plane cannot manage the SD-WAN device.

(71) The Contractor's SD-WAN Solution must provide the ability to deploy multiple SD-WAN edge devices for higher availability without losing any SD-WAN functionality such as application visibility, traffic steering and security features when enabled.

(72) The Contractor's SD-WAN Solution must provide capability to distribute overlay routes such that a path between two (2) SD-WAN Edge Devices can be accomplished via one or more SD-WAN Edge Devices (e.g. A VPN connected at Edge A and Edge C can traverse Edge B).

5.3 Availability

(73) The Contractor's SD-WAN Solution must provide the capability to cluster geographically separated SD-WAN controllers across cloud and/or on-premise configuration to maintain high-availability.

(74) The Contractor's SD-WAN Solution must provide SD-WAN Edge Devices that provide sub-second failover to an alternate path connected to the same device.

5.4 Performance

(75) The Contractor's SD-WAN Solution must have the capability to identify and classify application traffic flows. The application flow criteria can be defined using the following:

a) Pre-defined application signatures for popular cloud/SaaS applications. The pre-defined signatures must be capable of dynamically updating on a regular basis; and

b) Custom application signature criteria including one or more of the following:

i) IP source and/or destination address (IPv4/IPv6 host or prefix);

ii) IPv4 protocol or IPv6 next header (IANA Protocol Numbers Registry);

iii) Transport source and/or destination port (IANA Service Name and Port Number Registry); and/or

iv) Heuristic/algorithmic matching of Uniform Resource Locator (URL) with support for wildcard characters (Eg; *.application.gc.ca).

(76) The Contractor's SD-WAN Solution must detect and monitor latency, jitter and packet loss by WAN link.

(77) The Contractor's SD-WAN Solution must provide capability to enable forward error correction (FEC) between SD-WAN Edge devices.

(78) The Contractor's SD-WAN Solution must be able to support real time link measurement and QoS in the following ways:

a) Dynamically route traffic along the preferred path based on policy and/or application type;

b) Map QoS classes of overlay networks onto the QoS classes of underlay networks using DSCP; and

c) Support up to 5 QoS queues, including Low Latency Queue.

(79) The Contractor's SD-WAN Solution must route traffic based on the best performing link at a site as determined by latency, jitter and packet loss.

(80) The Contractor's SD-WAN Solution must support the asymmetric nature of DSL / cable-based internet service and route traffic accordingly to meet the specified traffic profile policies.

(81) The Contractor's SD-WAN Solution must enable an administrator to centrally push policies to specific devices or all devices on the network with a single request.

(82) The Contractor's SD-WAN Solution must automatically reroute lower priority application traffic to other links to protect the performance quality of higher priority applications traffic (e.g. VoIP) defined through policies.

5.5 Centralized Management - Graphical User Interface

(83) The Contractor's SD-WAN Solution must provide a centralized view of network health, network incidents and troubleshoot all logical networks from a single graphical user interface (GUI) provided through a browser-accessible portal with a holistic dashboard view and detailed drill-downs with the ability to monitor and configure the following:

a) VPN - Configure and view all VPN tunnels including the status (e.g. state, jitter, latency, packet loss percentage) of incoming and outgoing data;

b) Ports – Ability to configure and view all ports on SD-WAN edge and controller devices;

c) Applications – View all application and application groups running on the network including the VPN tunnels they are currently running on;

d) Policies – Configure and view all SD-WAN policies;

e) Links - Configure and change network topology on demand and report the status of all links; and

f) Security Profiles – Ability to configure and view all security profiles.

(84) The Contractor's SD-WAN Solution Management Portal must function with a variety of commercial browsers including Microsoft Edge and Google Chrome.

(85) The Contractor's SD-WAN Solution must provide a graphical view of the physical or logical topology, including subsets.

(86) The Contractor's SD-WAN Solution must enable the ability to monitor all control connections between SD-WAN devices and controllers.

(87) The Contractor's SD-WAN Solution must provide the ability to monitor the health of any device (e.g. state, traffic, temperature, CPU%, memory, power supply).

(88) The Contractor's SD-WAN Solution must enable administrators with the ability to:

a) create a custom application group which contains a subset of the applications which can be detected and monitored by the SD-WAN device.

b) define performance metrics which can be assigned to application and/or application group.

c) create customized application classification definitions.

(89) The Contractor's SD-WAN Solution must support role-base access controls.

5.6 Policy Management

(90) The Contractor's SD-WAN Solution must enable network administrators to centrally:

a) Create and apply enterprise policies to all SD-WAN devices on the network;

b) Create application-aware policies to dynamically route traffic based on application and / or application type (e.g. real-time, transactional, bulk);

c) Create path-based profiles which can define path preference when QoS thresholds are exceeded or when link failure / brownout situations occur; and

d) Create templates which can be used to configure multiple devices.

5.7 Protocol Support

(91) The Contractor's SD-WAN Solution must provide support for:

a) Internet Protocol version 4 (IPv4) (RFC 791, RFC 2474);

b) Internet Protocol version 6 (IPv6) (RFC 2460);

c) Port-channelling using Link Aggregation Control Protocol (LACP) (802.1AX-2008, formerly 802.3ad) or static configuration;

d) Simple Network Management Protocol (SNMP) v2 and V3;

e) NAT (Network Address Translation);

f) Border Gateway Protocol (BGP) (2-byte BGP ASN, 4-byte ASN and BGP-Multiprotocol (BGP-MP));

g) Open Short Path First version 2 (OSPFv2) for IPv4 and OSPFv3 for dual-stack IPv4/IPv6;

h) Dynamic Host Configuration Protocol (DHCP) and DHCP relay services including DHCPv6 (stateless and stateful), NAT64 and SLAAC for IPv6;

i) Protocol Independent Multicast (PIM);

j) IETF IP flow information Export (IPFIX) protocol and/or Netflow version 9 protocol;

k) Network Timing Protocol (NTP);

l) Virtual Router Redundancy Protocol (VRRP) or equivalent;

m) IPSec including Encapsulating Security Payload (ESP);

n) Link Layer Discovery Protocol (LLDP) (802.1AB); and

o) Internet Group Management Protocol (IGMP) v2/v3.

5.8 Interface Support

(92) The Contractor's SD-WAN Solution must support the following interfaces on provided SD-WAN devices as required:

a) Fast Ethernet as per IEEE 802.3u 100BASE-TX via either 10/100/1000BASE-T auto-negotiation or Small Form-factor Pluggable (SFP) at 100 Mbps as per SFF INF-8074;;

b) Gigabit Ethernet as per IEEE 802.3ab at 1,000 Mbps;

c) 10 Gigabit Ethernet as per IEEE 802.ae and IEEE 802.3-2008an at 10,000 Mbps;

d) Small form-factor pluggable (SFP) at 1,000 Mbps as per SFF INF-8074; and

e) Small form-factor pluggable (SFP) at 10,000 Mbps as per SFF 8431 4.1.

(93) The Contractor's SD-WAN Solution must support various traffic types including MPLS, Broadband Internet and Carrier Ethernet.

5.9 Cloud Support

(94) The Contractor's SD-WAN Solution must support connectivity to a variety of IaaS, PaaS and SaaS in a multi-cloud environment. As a minimum, the solution must be able to access a variety of cloud services including Amazon Web Services (AWS), Microsoft Azure Cloud Services and Microsoft 365.

(95) The Contractor's SD-WAN Solution must support path optimization for cloud applications and must recognize cloud traffic type (e.g. Office 365) and route cloud traffic over the optimal link defined by the policy.

(96) The Contractor's SD-WAN solution must recognize and distinguish between SaaS and IaaS application and traffic types within cloud applications (such as MS Teams media traffic).

5.10 API Support

(97) The Contractor's SD-WAN Solution must provide support for Representational State Transfer (REST) APIs (i.e. RESTful APIs) and Open APIs.

(98) The Contractor's SD-WAN Solution must provide the ability to integrate and automate with APIs with at least the following categories:

a) Management: ability to integrate with external monitoring, provisioning, inventory and change management systems; and

b) Cloud: ability to develop interfaces with cloud platforms (using programming languages).

5.11 Reporting

(99) The Contractor's SD-WAN Solution must provide traffic visibility and be able to measure and report on link level metrics that at a minimum include latency, packet loss, jitter, link capacity and utilization, round trip time and link error rate.

(100) The Contractor's SD-WAN Solution must measure end user application performance attributes (e.g. response time), error rate and transaction time.

(101) The Contractor's SD-WAN Solution must provide QoS reporting (i.e. classification, marking, metering, dropping, queuing and scheduling functionality).

(102) The Contractor's SD-WAN Solution must provide an overview of the bandwidth used across each WAN link including total bytes sent and received.

(103) The Contractor's SD-WAN Solution must provide a geographic view (i.e. a map) with real-time status of all SD-WAN devices and links.

(104) The Contractor's SD-WAN Solution must support the display of application traffic data in graphical format.

(105) The Contractor's SD-WAN Solution must provide a view of the status of each port on a specific SD-WAN device.

(106) The Contractor's SD-WAN Solution must provide a report on all policies, including security policies, applied to a specific device or group of SD-WAN devices.

(107) The Contractor's SD-WAN Solution must provide event logging and reporting such as system event reports, security alerts and alarms, zone based firewall events, etc.

(108) The Contractor's SD-WAN Solution must provide tenant and site performance reports with analytics capabilities such as top applications by bandwidth, top applications with highest latency, top applications with highest jitter, links with highest usage, sites / devices not meeting SLAs, etc, by tenant and site.

(109) The Contractor's SD-WAN Solution must provide the ability to create custom reports.

(110) The Contractor's SD-WAN Solution must provide historical reporting as required (e.g. daily, weekly, monthly).

ASSOCIATED DOCUMENTS

ANNEX B – LIST OF DELIVERABLES AND PRICING

ANNEX C – TECHNICAL EVALUATION CRITERIA