Service Definition

Fujitsu Software Defined Networking (SD-WAN) High Assurance Draft v 2.5

G-Cloud 14

Contents

1: Introduction to Software Defined Wide Area Networking (SD-WAN) Technology

Software Defined WAN (SD-WAN) is licensed based technology that uses software-defined networking concepts to distribute network traffic across a wide area network (WAN). SD-WAN is deployed offering a cost-effective way to connect offices to Buyers own datacentres and to SaaS or cloud-based applications. An SD-WAN provides automation, centralisation and flexibility, which creates a more agile WAN environment for Public Sector organisations. The SD-WAN architecture will create a virtual overlay that abstracts underlying private or public WAN connections, such as Multiprotocol Label Switching (MPLS), internet broadband, fibre, wireless satellite or 4g or equivalent Mobile network connectivity (LTE). This overlay capability means Buyers may keep their existing WAN links, or to supplement the WAN with cost effective connectivity while the SD-WAN centralises network control and enables real-time application traffic management over the links. Typically, a centralised controller is used to manage the SD-WAN. The controller is a software client that directs data flows between two points and distributes network and security policies to all connected devices. The controller enables staff to program network edge devices with a range of provisioning options. SD-WAN minimizes the need for network engineers to manually configure routers in branch locations.

For G Cloud, Fujitsu's SD-WAN service is positioned as an overlay capability where Fujitsu provides the Buyer with hosting infrastructure, software and edge device options to operate SD-WAN technology. For deployment, the Buyers plug their WAN links into the edge device, see Figure 1.

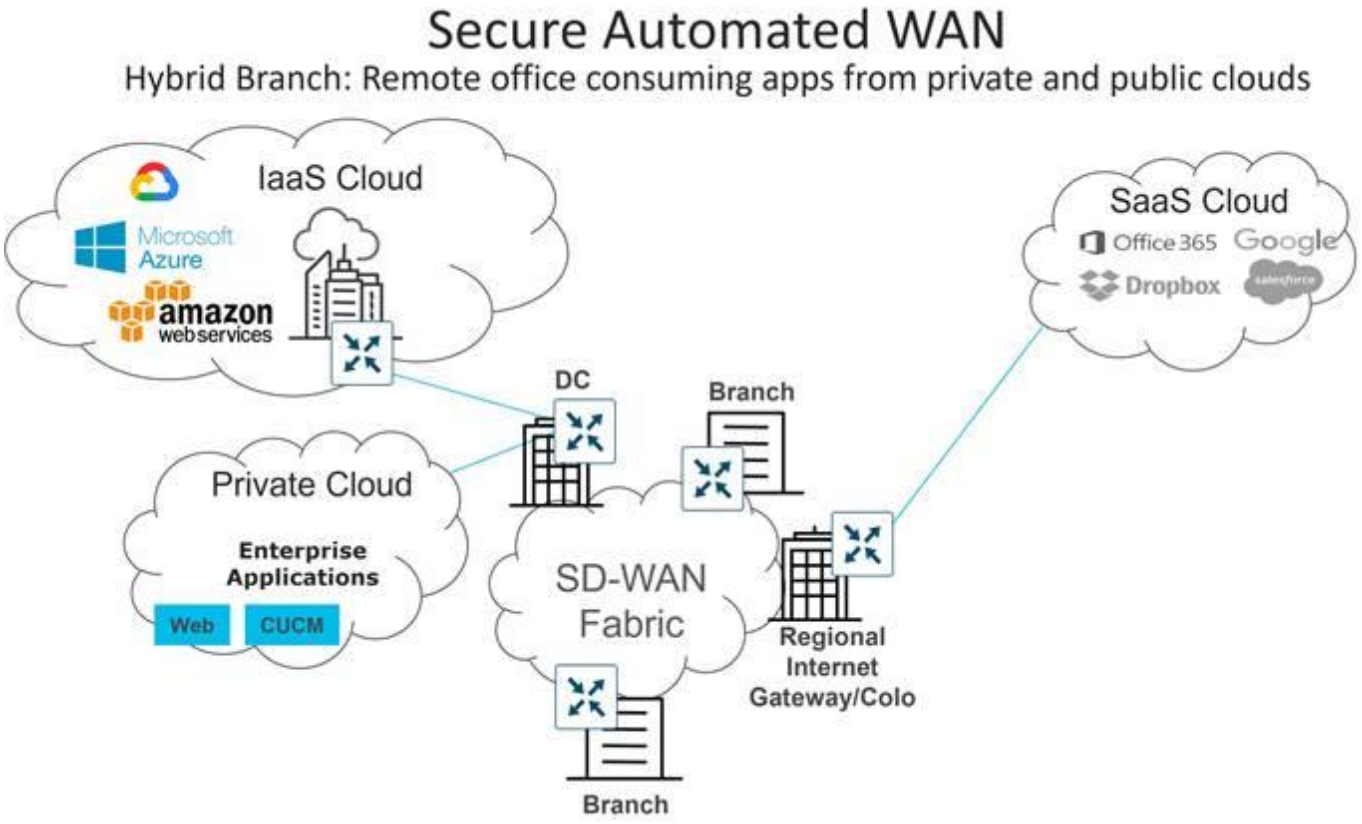

Figure 1: SD-WAN Schematic

The following sections provide a technical overview of the features functionality and service options using Fujitsu's SD-WAN offerings. This document assumes the Buyer has a technical appreciation of SD-WAN technology. Buyers new to SD-WAN technology are advised to click on following link SD-WAN Overview for more information on the capabilities of SD-WAN. Or to seek guidance from your Fujitsu representative.

1.1: Fujitsu's SD-WAN Offerings

Fujitsu's SD-WAN is a fully deployed and certified subset of Fujitsu's wider Software Defined Networking services portfolio. Fujitsu's SD-WAN G Cloud service comprises of three service offerings on shared platforms all supporting OFFICIAL, with service and solution uplifts to support handling caveats (such as SENSITIVE), and or to align with Critical National Infrastructure "CNI" and NCSC guidance as standard. – please see Critical National Infrastructure Guidance for details.

For Buyers seeking an SD-WAN solution to support SECRET, exclusive assets additional hardware and devices would be required, some of which may need to be deployed within the Buyer environment. This will be advised by Fujitsu and any impact on request.

Fujitsu's SD-WAN offering uses best of breed vendors technology providing Buyers a full rich catalogue of services and functionality defined in the Service Packs using;

- AWS or Azure infrastructure using nominated locations (for Service Pack 1).
- Fujitsu's certified UK datacentres hosting SD-WAN infrastructure combined with Fujitsu's UK Facility Security Clearance (FSC) (formerly known as List X) facilities (for Service Pack 2).
- Fujitsu's certified UK PASF Assured datacentres hosting SD-WAN infrastructure and UK Facility Security Clearance (FSC) (formerly known as List X) facilities (for Service Pack 3).

All three Service Pack offerings regardless of hosting environment provide an assured and secure network overlay solution, complying with NCSC guidance.

Fujitsu's SD-WAN solution allows the Buyers to disaggregate traditional WAN connectivity and services to adopt a bearer of opportunity strategy. Fujitsu's SD-WAN solution has proven deployments for UK Public Sector at scale using MPLS, DIA or Internet connectivity, Satellite, 5g, private bearers and or as required a blend of connectivity solutions.

With all Service Pack offerings, the Buyer shall perform end user management of the platform using the portals provided. Alternatively, the Buyer can subscribe to itemised managed services from Fujitsu using the SFIA rate card (or day rate fractions thereof). Details of the services available are provided in each Service Pack charges catalogue.

Fujitsu's SD-WAN service extends into providing secure connectivity to Public Cloud Service providers, with proven configurations detailed (in association with the vendors) for all Service Pack offerings. The Service Packs provide a choice of infrastructure and management solutions, as follows:

- Service Pack 1, is a commodity offering based on a Cisco Catalyst SD-WAN solution (using vendor recommended software SD WAN in a Azure or AWS cloud environment hosting the SD-WAN Orchestrators. This infrastructure will be monitored by Fujitsu for availability with the Buyer performing end user management or additional services can be supported by Fujitsu UK network operations centres (OFFICIAL only).
- Service Pack 2, based on a Cisco Catalyst SD-WAN solution (using vendor recommended software SD WAN with integration into other platforms using Fujitsu's own dedicated infrastructure with all Orchestrators and tooling deployed in the UK using certified datacentres and FSC Accredited facilities. Note the features and functionality align to Fujitsu's multitenant offering and certain functionality may not be available (in comparison to Service Pack 1) due to current NSCS guidance. The service is supported by Fujitsu UK (Defence and National Security) network operation centres (OFFICIAL SENSITIVE & Above). All Fujitsu staff managing the service are at a minimum Security Cleared (SC). Service complies with relevant HM Government Information Assurance and Security guidance.
- Service Pack 3, based on a Cisco Catalyst SD-WAN solution (using vendor recommended software SD WAN with integration into other platforms using Fujitsu's own dedicated infrastructure with all Orchestrators and tooling deployed in the UK using certified datacentres PASF and FSC Accredited facilities. Service Pack 3 is designed for the Law Enforcement Community (LEC). Supported by Fujitsu UK (Defence and National Security) network operation centres. All Fujitsu staff managing the service are at a minimum Security Cleared (SC) and Non-Police Personnel Vetting (NPPV). Service complies with relevant NCSC Information Assurance and Security guidelines (Note the service description for Service Pack 3 has been "redacted". Upon identification of end user and in accordance with the LEC Authority Security Aspect Letter, Fujitsu will provide copies of the unredacted or removed contents.)

The services provided under Service Pack 1 include use of Cisco Catalyst SD-WAN pilot licences, testing facilities and services to support Buyer model office environments for the testing of new software functionality.

The services provided for Service Pack 2 and 3 include pre-production environments aligned to the Buyer environment to support Fujitsu testing, patching and software updates supporting changes to recommended release software) and model office requirements.

The Service Pack offering will be dependent on the security and Information Assurance requirements of the Buyer. In the case of Service Pack 3 the SD-WAN platform meets the published certification requirements of Police Digital Service (PDS) and complies with Police Assured Secure Facilities (PASF) requirements.

Prior to award of any contract (or Service Pack selected) specialist SD-WAN solution architects will be assigned to define the functionality and to agree with the Buyer the Information Assurance requirements (suitability of Service Pack selected). This is not chargeable and reflects Fujitsu's commitment to establish suitability of the G Cloud SD-WAN service for the Buyer prior to contract award. This process will ensure the full scope of the service is understood and will be summarised in a Statement of Work which can be used in any award of contract.

All Service Pack charges applicable for professional services are calculated from the SFIA rate card or fractions thereof. The Professional Services include (test, assurance, project management, transition design, deployment and service management).

1.2: Cisco SD-WAN Gold Star Software

Fujitsu SD-WAN service is deployed on compatible Cisco Gold Star "certified" software, with vendor updates deployed by Fujitsu to maintain relevant compliance with published G-Cloud 14 information assurance standards, as expressly detailed in the Service Packs, and the feature compatibility defined in each Service Pack. Use of Cisco Gold Star versions to support new functionality shall be introduced in accordance with the Variation process and will be subject to testing and validation using the Fujitsu G-Cloud Rate Card – UK Onshore charges as detailed in the Supplier's Platform pricing document.

1.3: Hosting Charges

For Service Pack 1 using Azure or AWS infrastructure hosting charges are included in the Cisco Catalyst SD-WAN Licence charges detailed in the Supplier's Platform pricing document.

For Service Pack 2 using Fujitsu's certified UK datacentres hosting and UK Facility Security Clearance (FSC) (formerly known as List X) facilities hosting charges are detailed in the Supplier's Platform pricing document.

For Service Pack 3 using Fujitsu's Police Assured Secure Facilities (PASF) certified UK datacentres hosting and UK Facility Security Clearance (FSC) (formerly known as List X) facilities hosting charges (Shared Orchestration Platform Hosted List X Fujitsu Datacentres) are detailed in the Supplier's Platform pricing document.

1.4: Licences and Capacity

The Buyer is responsible for the capacity selection of the Cisco Catalyst SD-WAN licenses using the catalogue options (SD-WAN Software subscription charge per site, DNA Advantage) as detailed in the Supplier's Platform pricing document. During the Term of the Call- Off Contract the Buyer may request, via the Variation process, Fujitsu to manage licenses sourced by the Buyer from Cisco. The Variation request will be impacted by Fujitsu for any additional charges to deploy and operate the service using the Buyers licenses and any applicable Fujitsu Catalyst SD-WAN License termination charges.

Access by Fujitsu will be required to the Buyers Cisco Smart Account. The Buyer will be responsible for all license charges from the vendor (Cisco). Details are provided in the relevant Service Pack that contain this option.

1.5: Edge Device Hardware

The Buyer may request edge device hardware to be deployed at sites which can be:

1.5.1 Rented from Fujitsu as optional catalogue items (Appliances) in the Supplier's Platform pricing document.

The recommended G Cloud 14 edge device for new installations is the Advantech device.

For Buyers with DELL 4600 devices deployed at sites, Fujitsu's break fix service will include if required the replacement of the faulty device with a matching DELL 4600 model. In the event DELL 4600 maintenance replacement devices are no longer available, Fujitsu will provide notice to the Buyer of its intention to replace the faulty devices with an Advantech device. The replacement activity performed on site will also include exchanging other DELL edge devices in Active-Active or Active-Standby configuration for design consistency.

Charges for Break Fix services for the DELL 4600 devices are detailed in the Supplier's Platform pricing document, Edge Device Break Fix Dell Devices.

1.5.2 Management of edge devices provided by the Buyer for the Call-Off Term.

The Buyer via the Variation process may request the replacement of Fujitsu rented edge devices (DELL or Advantech), using the Buyers supplied Cisco second generation (G2) edge devices. Fujitsu will manage the Buyers supplied G2 edge devices on its behalf in accordance with the Service Pack Service Level Agreement. In accordance with the Variation process, Fujitsu shall impact the charges for product testing, changes to the edge policies, templates and software, deployment changes on site for installation, ITHC, and charges to amend service documentation. Charges calculated in the Variation process will be in accordance with the G-Cloud Rate Card – UK Onshore charges, detailed in the Supplier's Platform pricing document.

Charges for Break Fix services for the Buyers Cisco G2 edge devices are detailed in the Supplier's Platform pricing document, Edge Device Break Fix Cisco Devices aligned to service pack 3 SLA (project deployments).

The Replacement of Fujitsu rented devices will incur a Charge per device for wiping in accordance with Appliance Data Wipe Charge in the Supplier's Platform pricing document.

1.6: Statement of Work Purpose

To aid the Buyer, all applicable charges associated with the SD-WAN (for services selected) will be summarised in the Statement of Work. The Statement of Work shall confirm the defined services and outline deployment timescales to be performed by Fujitsu for the Buyer. Upon agreement of the Statement of Work, and award of the G Cloud 14 call off contract a detailed implementation plan and agreed milestone dates will be provided confirming timescales and dependencies.

1.7: Fujitsu and Cisco SD-WAN Rebranding Update

To achieve simplification and consistency, Fujitsu's SD-WAN solution (ex Viptela) has been rebranded as Fujitsu SD-WAN. From IOS XE SD-WAN Release 17.12.1a and Catalyst SD-WAN Release 20.12.1, this is also aligned with Cisco new naming conventions. The following component changes are applicable.:

- **Cisco vManage** henceforth **Cisco Catalyst SD-WAN Manager**
- **Cisco vAnalytics** henceforth **Cisco Catalyst SD-WAN Analytics**
- **Cisco vBond** henceforth **Cisco Catalyst SD-WAN Validator**
- **Cisco vSmart** henceforth **Cisco Catalyst SD-WAN Controller**
- **Cisco Controllers** henceforth **Cisco Catalyst SD-WAN Control Components.**

Whilst Fujitsu transition current SD-WAN contracts (including G Cloud arrangements) and update user guides to the new branding names, some inconsistencies will be present in this documentation due to a phased approach to the user interface updates of the software product, or Information Assurance / Certification status of documentation. If in any doubt, please refer to your Fujitsu representative.

2: Service Pack 1 SD-WAN Overview (Azure Cisco Cloud SD-WAN solution)

Fujitsu's SD-WAN Service Pack 1 is based on the Cisco Catalyst SD WAN deployed an Azure or AWS cloud environment. This service and where relevant Fujitsu certifications or procedures aligns to G Cloud 14 Framework guidance and to NCSC's 14 Cloud Security Principles. The platform availability and Buyer portals are managed by Fujitsu from its UK based Service Management Centres and ITSM tool sets (ServiceNow) and where provided service management procedures will align to ITIL v4.

With Service Pack 1 the Buyer is responsible for the end user management of the platform using the portals provided, or the Buyer can subscribe to a range of itemised ITIL based managed services from Fujitsu using the SFIA rate card.

2.1: SD-WAN infrastructure Technical Description

Fujitsu's Service Pack 1 comprises of Cisco SD-WAN Controllers such as Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controllers. The solution offers a ready to consume offering. Service Pack 1 can be enhanced using the optional catalogue and SFIA rate card managed services.

Fujitsu's Service Pack 1 is offered as a multitenancy solution: The hosting of Cisco SD-WAN controllers such as Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller will be shared across multiple buyers, and the design of the platform and components shared cannot be enhanced or amended by the Buyer (it is an out of the box service).

The salient features of this service are:

- The data plane, the control plane, and the management plane traffic for each Buyer are isolated
- Fujitsu's SD-WAN always run on the latest long-lived star-marked release
- Buyer agrees to external management of their Virtual Account (VA)
- Software-Defined AVC (SD-AVC) and web certificates are available and managed by Fujitsu and or Cisco
- The Fujitsu SD-WAN will be hosted in Azure Cloud.
- The features and functionality of Fujitsu SD-WAN Service Pack 1 can be found using the following link Feature Matrix.

Please see Figure 2 for a high level schematic of a deployed users instance:

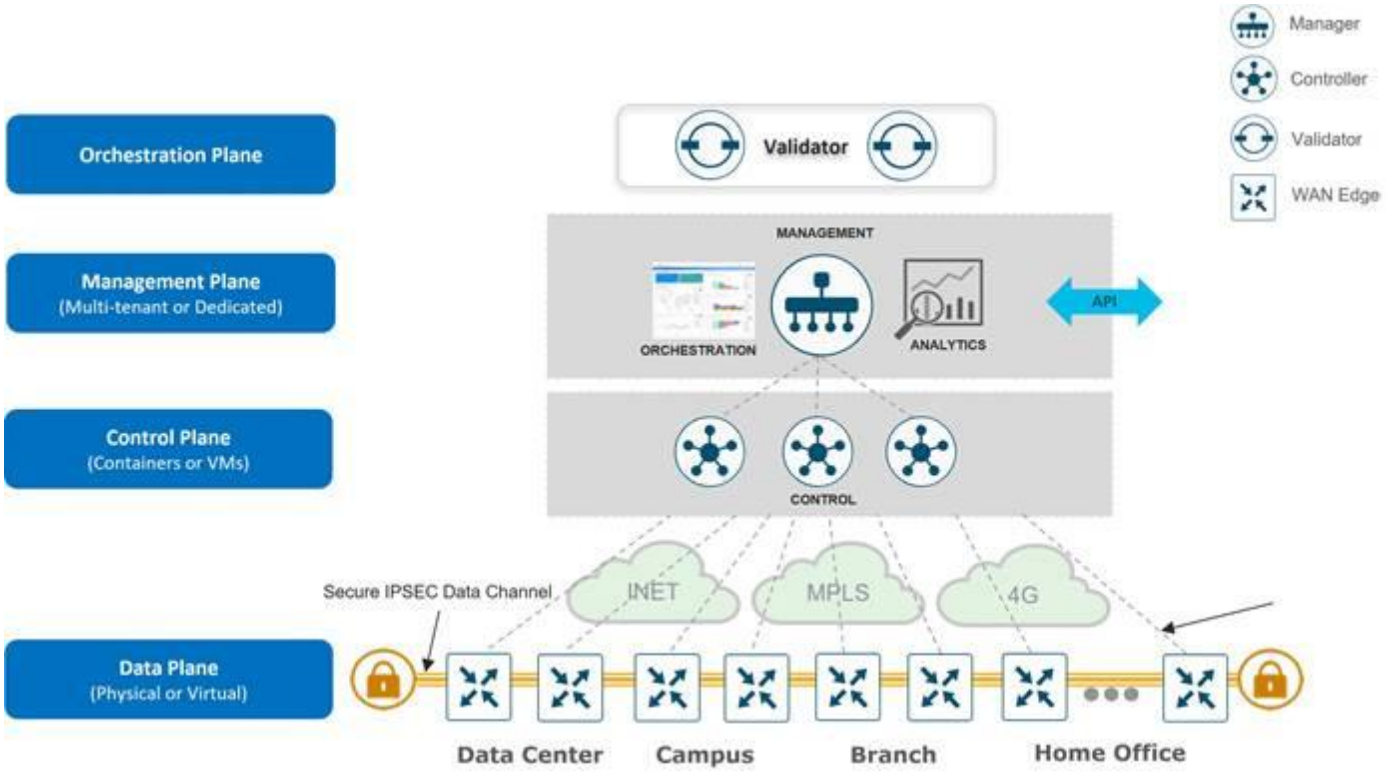

Figure 2: High level schematic of a deployed users instance

With Service Pack 1 by default, a single Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller is deployed in the primary European cloud region and an additional Cisco SD-WAN Validator and Cisco SD-WAN Controller are deployed in the secondary or backup region.

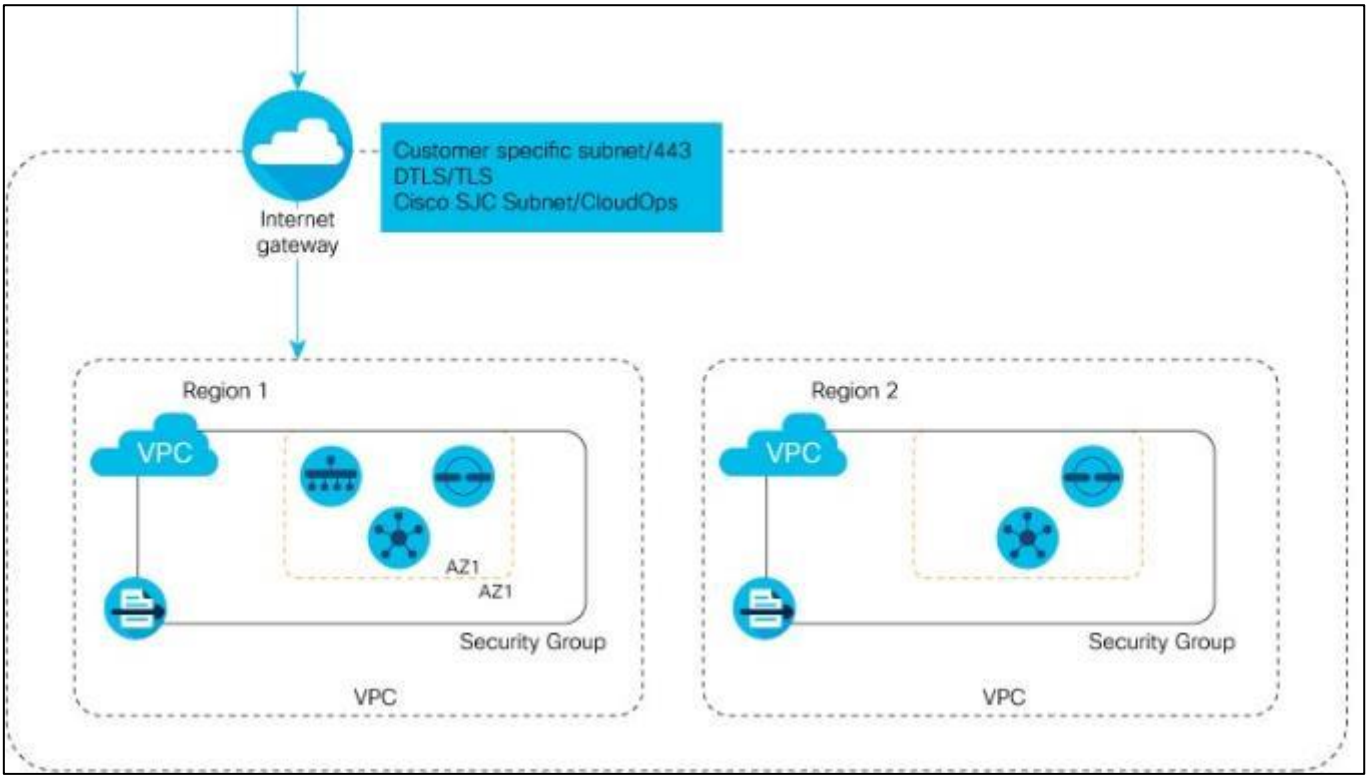

Figure 3: Fujitsu's SD-WAN deployed infrastructure

Solution Overview

Fujitsu's SD-WAN connects any user to any application with integrated capabilities for multi-cloud, security, predictive operations, and enhanced network visibility —all on a Secure Access Service Edge (SASE)-enabled architecture. Fujitsu's SD-WAN enables a Buyer to transform its IT infrastructure by delivering network connectivity that's cloud-agnostic, efficient and simpler to manage operational costs and increases control and visibility across the entire digital service delivery chain. Fujitsu's SD-WAN Manager provides a highly visualized dashboard that simplifies network operations. It provides centralised configuration, management, operation, and monitoring across the entire SD-WAN fabric.

Fujitsu's SD-WAN offers integrated security, including full-stack multilayer security capabilities as optional services deployed from the cloud see figure 4. This integrated security can provide real-time threat protection where and when it is needed — for branches connecting to multiple Software-as-a-Service (SaaS) or Infrastructure as a Service (IaaS) clouds, datacentres, or the internet, further accelerating the transition to a SASE-enabled architecture. Service Pack 1 can also be fully integrated with Cisco Umbrella, which offers protection against security blind spots and cyberthreats.

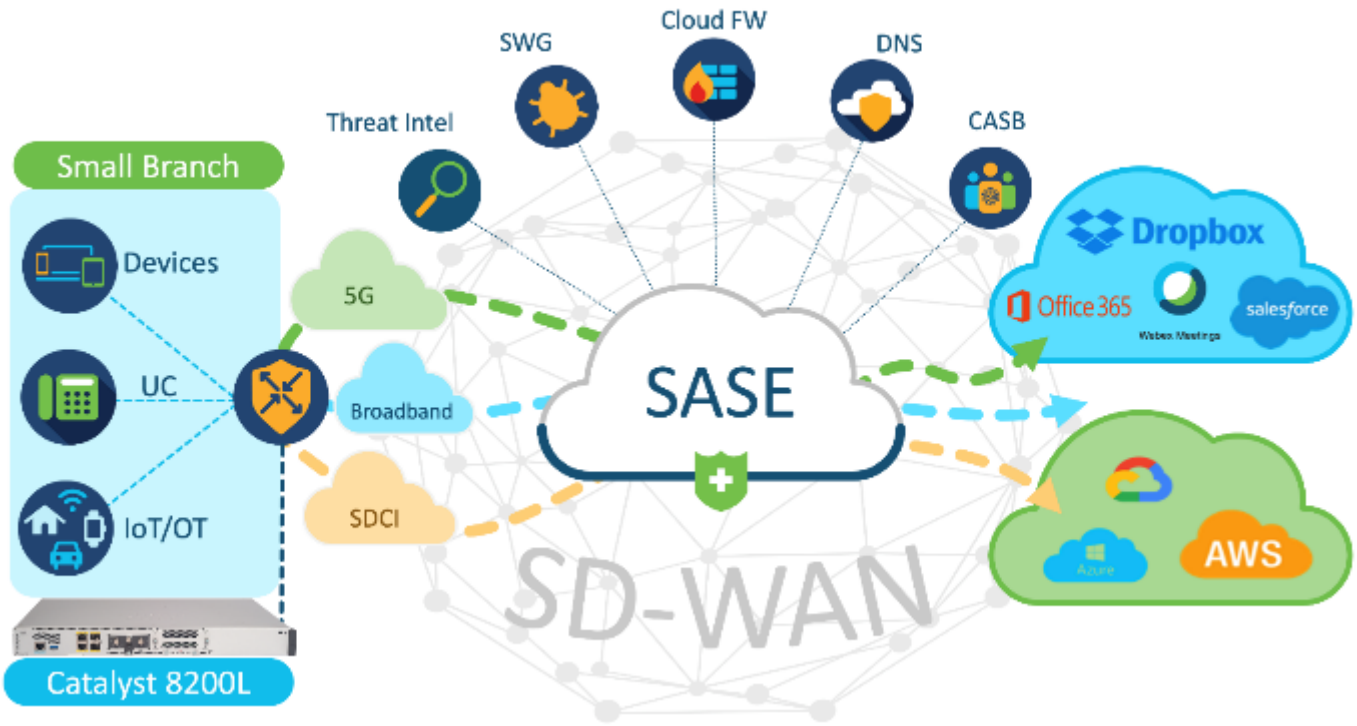

Figure 4: Fujitsu's SD-WAN SASE Applications (on demand)

Using the SD-WAN Manager (**Figure 5**), a Buyer can connect to all data centres, core and campus locations, branches, colocation facilities and cloud infrastructure. To enable this interconnection, Fujitsu's SD-WAN applies the Overlay Management Protocol (OMP) to the entire network. Fujitsu's SD-WAN simplifies IT operations with automated provisioning, unified policies, and streamlined management.

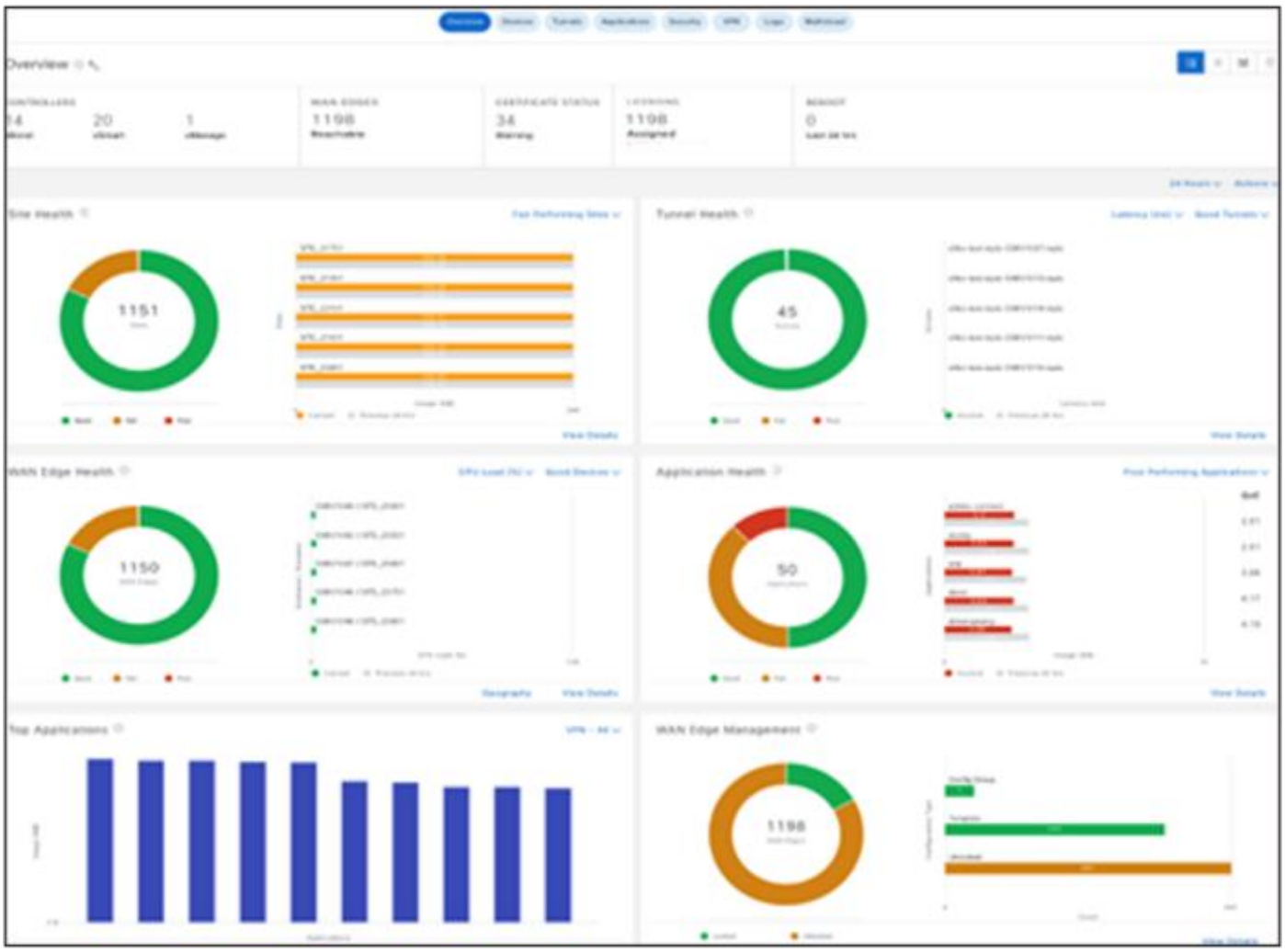

Figure 5: Fujitsu SD-WAN Manager dashboard showing network and application health

Fujitsu's service provides a flexible architecture to extend SD-WAN to any environment (Figure 6) Fujitsu's SD-WAN automatically discovers, authenticates, and provisions both new and existing devices.

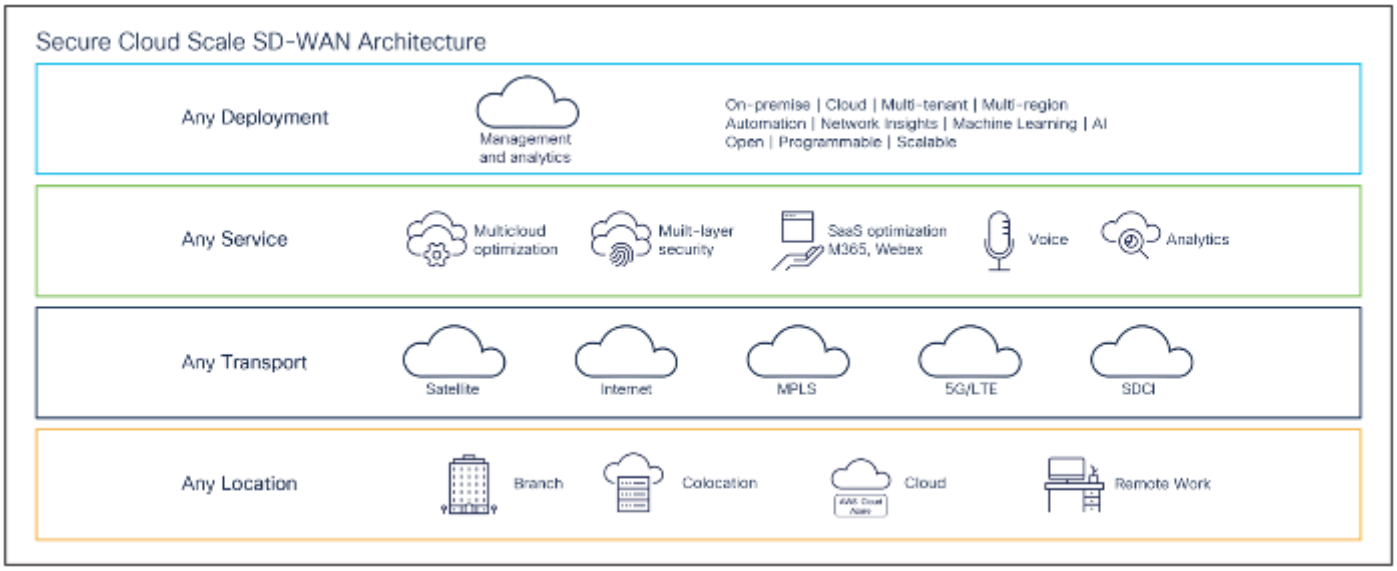

Figure 6: Flexible and scalable architecture for network transformation

2.2: Multicloud Choice and Control

Fujitsu's SD-WAN provides the ability to connect any WAN location to multiple cloud platforms or any other enterprise, enabling increased connection speeds and connection reliability. Fujitsu's SD-WAN Cloud OnRamp creates a WAN extension for Buyer IaaS workloads, provides dynamic path selection for optimal SaaS application performance, consolidates branch office egress points into regional colocation facilities, and automates cloud-agnostic branch connectivity with cloud interconnect. Monitoring underlay performance via Fujitsu SD-WAN Manager, Cloud OnRamp automatically selects the fastest, most reliable path to the cloud infrastructure. In the event of network service interruptions, Cloud OnRamp will adjust paths as necessary, helping ensure improving continuous uptime and predictable performance.

2.3: SD-WAN Cloud OnRamp for Multicloud

Fujitsu's SD-WAN enables the WAN to IaaS environments such as Amazon Web Services, Google Cloud, and Microsoft Azure to be simple, automated, and secure. In the Fujitsu SD-WAN console, network and operations teams will automate virtual private cloud connections to IaaS environments, extending the Fujitsu SD-WAN OMP to the cloud. Fujitsu's SD-WAN applies automated connectivity requirements (loss, latency, and jitter) to find the optimal path to cloud IaaS applications, adjusting the IPsec route as needed to help ensure service delivery and performance while monitoring the hosting infrastructure for anomalies.

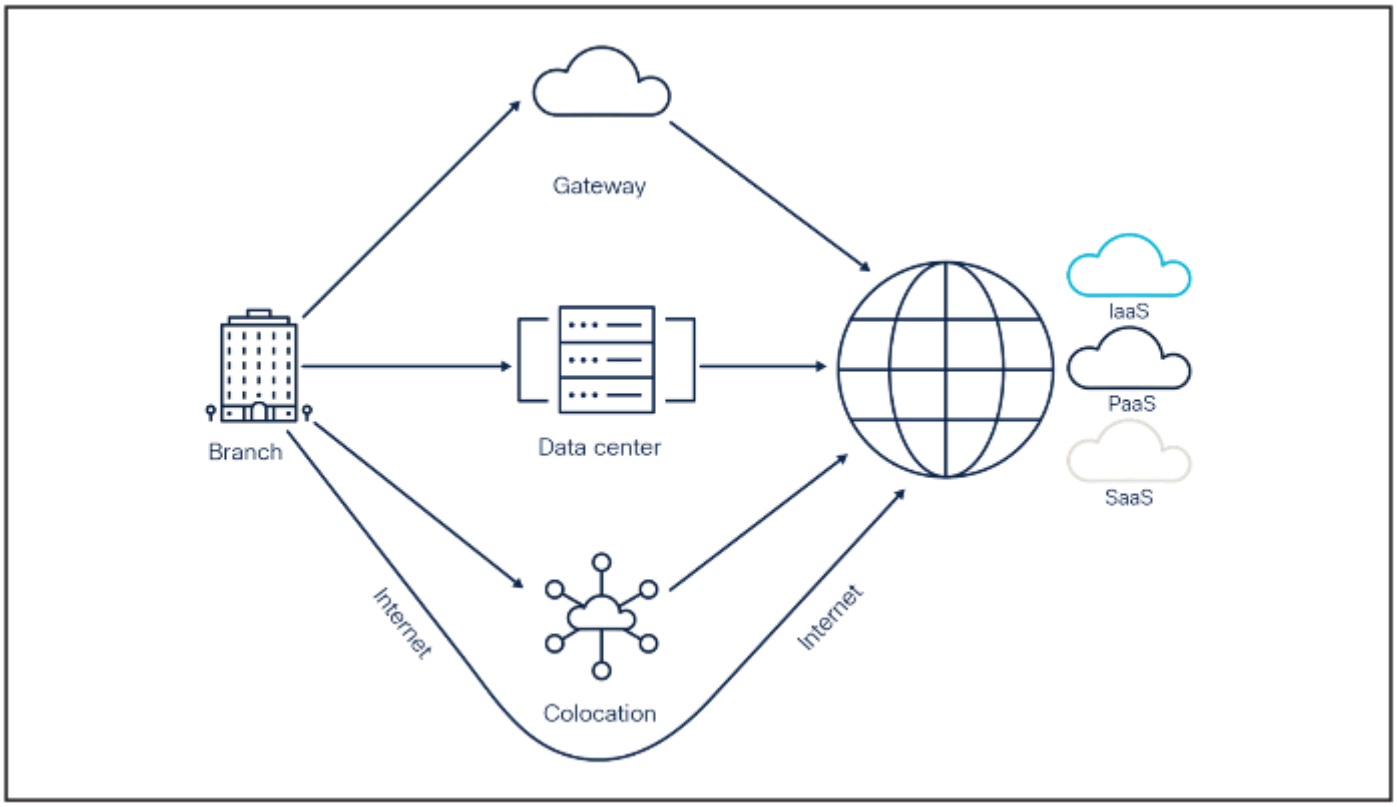

Figure 7: Fujitsu's SD-WAN Cloud OnRamp for IaaS, PaaS, and SaaS applications

2.4: SD-WAN Cloud Hub

Fujitsu's SD-WAN Cloud Hub leverages SD-WAN to interconnect branch sites, on-premises datacentres, and the cloud using a public cloud service provider's backbone (AWS, Google Cloud, or Microsoft Azure) as an underlay. Cloud Hub reduces provisioning time with site-to-cloud network automation as well as offering high availability and multiple points of presence across the world using a cloud service provider's global infrastructure for site-to-site connectivity (**Figure 7**:). It should be noted Buyers will still be required to provide connectivity for the sites, and that connectivity will be used to access the cloud hub.

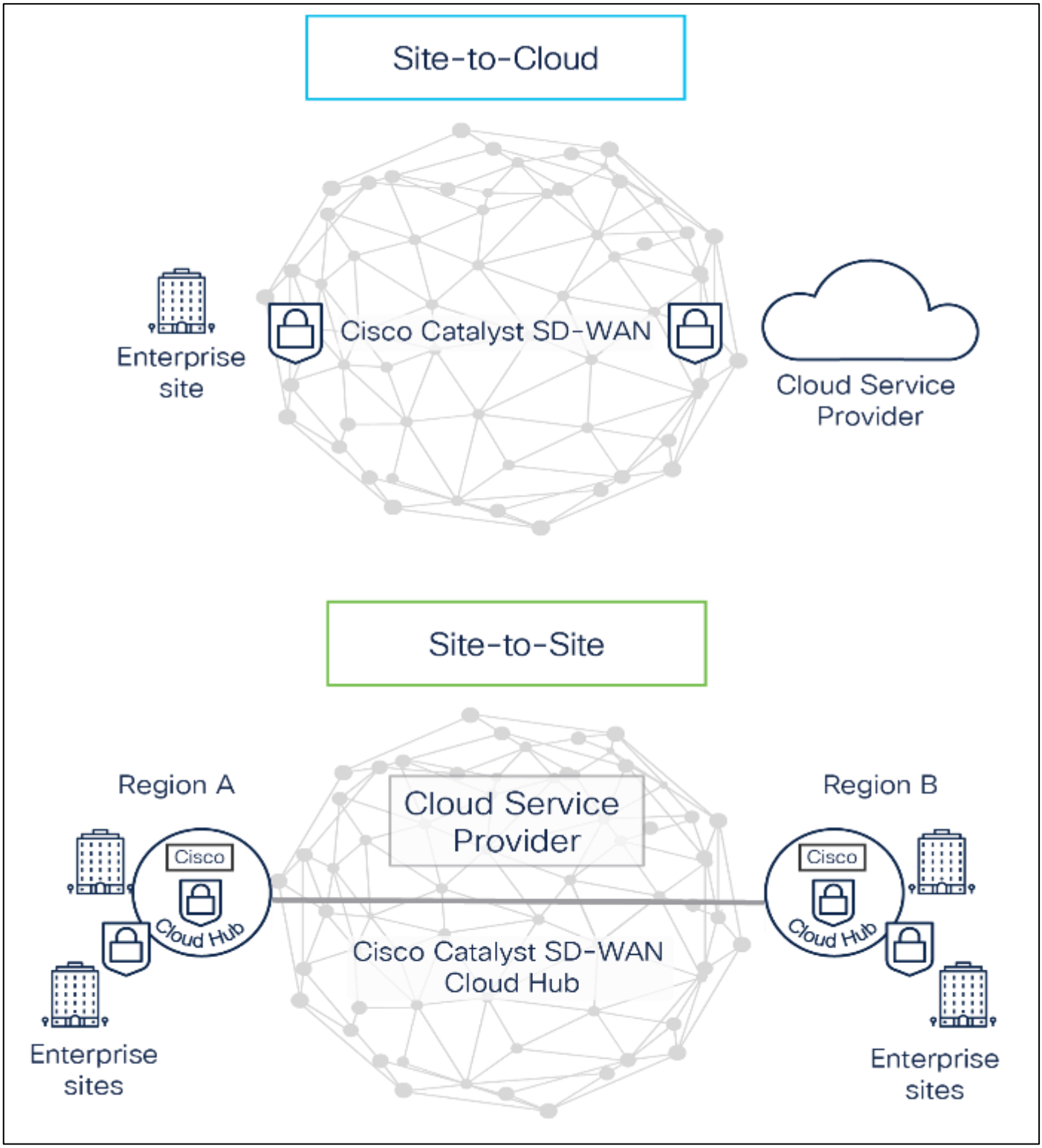

Figure 8: Fujitsu's SD-WAN Cloud Hub

2.5: SD-WAN Cloud OnRamp for SaaS

In addition to building application workloads in IaaS cloud environments, Buyers may also be using SaaS applications for streamlined operations. Connectivity to these applications may require sharing resources with other users on distant hardware. Fujitsu's SD-WAN Cloud OnRamp for SaaS makes connecting to and securing these SaaS environments easier to manage.

Fujitsu's SD-WAN Cloud OnRamp selects the fastest, most reliable path to SaaS applications (**Figure 9**), engaging in real-time traffic steering to deliver the best user experience no matter where they are located. Should an

internet service issue cause connectivity that falls below Buyer agreed thresholds, Cloud OnRamp finds the next best path to help ensure continued application performance. In addition, the solution automates best path selection for custom and standard NBAR (Network Based Application Recognition) applications, allowing Buyers to enable Cloud OnRamp for SaaS capabilities with the application of their choice.

Fujitsu's SD-WAN Cloud OnRamp for SaaS has been designed to support other services (for example) Fujitsu's large scale cloud communication, collaboration, and video capabilities. Fujitsu's SD-WAN segregates Unified Communications or Collaboration (UC) traffic from generic internet traffic and routes it via the best path from a specific branch router to deliver a seamless, consistent, and high-quality user experience (see figure 9). The solution enables improved performance for Microsoft 365. Features such as informed network routing and URL categorization, giving users deeper abilities to manage and route traffic within Microsoft 365 to improve efficiency, and performance across the entire suite of applications.

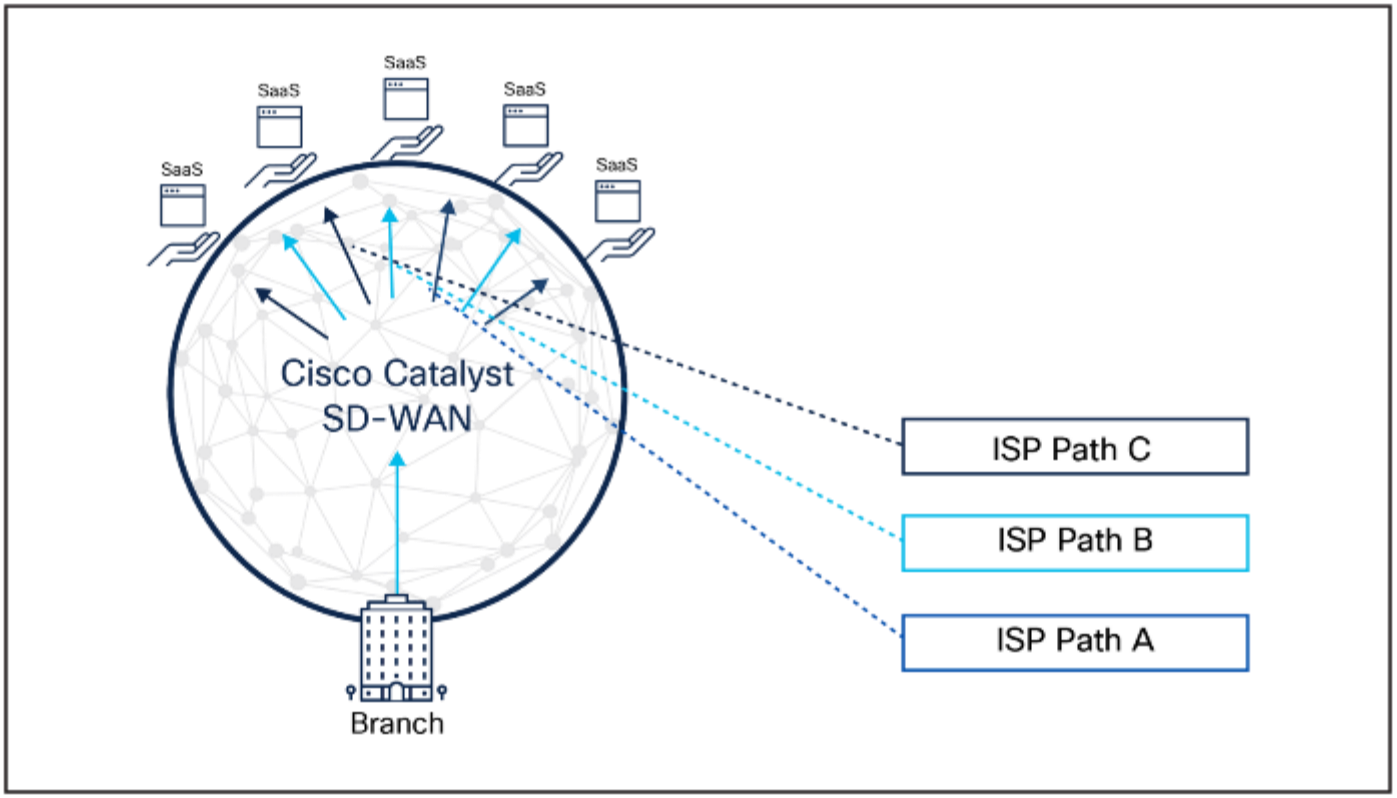

Figure 9: Dynamic path selection in Fujitsu's SD-WAN Cloud OnRamp for SaaS

2.6: Fujitsu SD-WAN Cloud Interconnect

Fujitsu's SD-WAN Cloud Interconnect (10) extends the use of cloud agnostic backbone to connect from site to site and site to multiple clouds. Fujitsu's Cisco Catalyst SD-WAN's offers an optional integration capability for Buyers with Equinix to provision on-demand branch connectivity to multiple sites and to cloud provider networks like Amazon Web Services (AWS), Google Cloud, and Microsoft Azure, directly from your SD-WAN controller. Part of Cisco SD-WAN Cloud OnRamp, Cisco SD-WAN Cloud Interconnect is integrated with Equinix Network edge, a network service that deploys the Cisco Catalyst 8000V Edge Software virtually at Equinix Datacentres and interconnects to the cloud in minutes using Equinix Fabric.

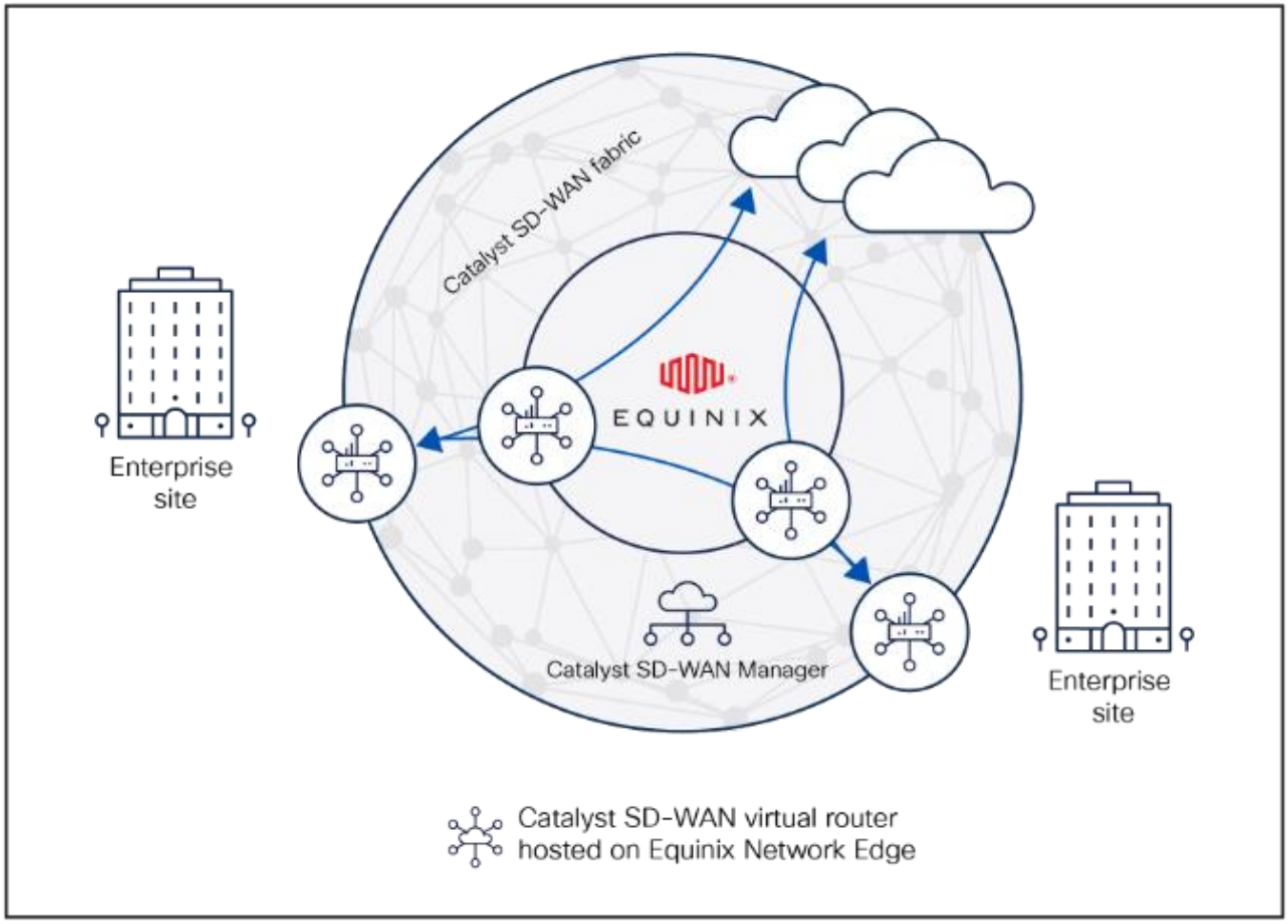

Figure 10: Fujitsu SD-WAN Cloud Interconnect

2.7: Analytics and Insights

Applications are more distributed, and across Public Sector the Internet is becoming the new enterprise WAN. As SD-WAN has transformed to connect users across multicloud, branch, datacentres, and a hybrid workforce, IT and network operation teams are challenged to deliver reliable connectivity, application experience, and security over networks and services they don't own or directly control. In parallel, networks and devices generate a multitude of data points across potentially thousands of sites, network paths, applications, and distributed users. It has become challenging to digest and make sense of this data. Time spent on the identification of issues and troubleshooting requires significant resources and impacts productivity.

Fujitsu SD-WAN Analytics the data remains hosted in the cloud simplifies network operations by providing granular network insights, predictivity, and automation that not only heighten network integrity but also deliver optimal application experience. SD-WAN Analytics aggregates a large volume of telemetry data and correlates application performance with underlying networks for operational insights, in a highly visualised and simplified manner. SD-WAN Analytics enhances network visibility, establishes historical benchmarks, and expedites root-cause isolation, ultimately enabling Buyers to take the necessary corrective actions and control of the user experience. Fujitsu SD-WAN provides via a secure portal Analytics as standard which is a SaaS component of the solution that provides enhanced visibility into the network and application performance, along with historical trend information to establish benchmarks and expedite root cause analysis.

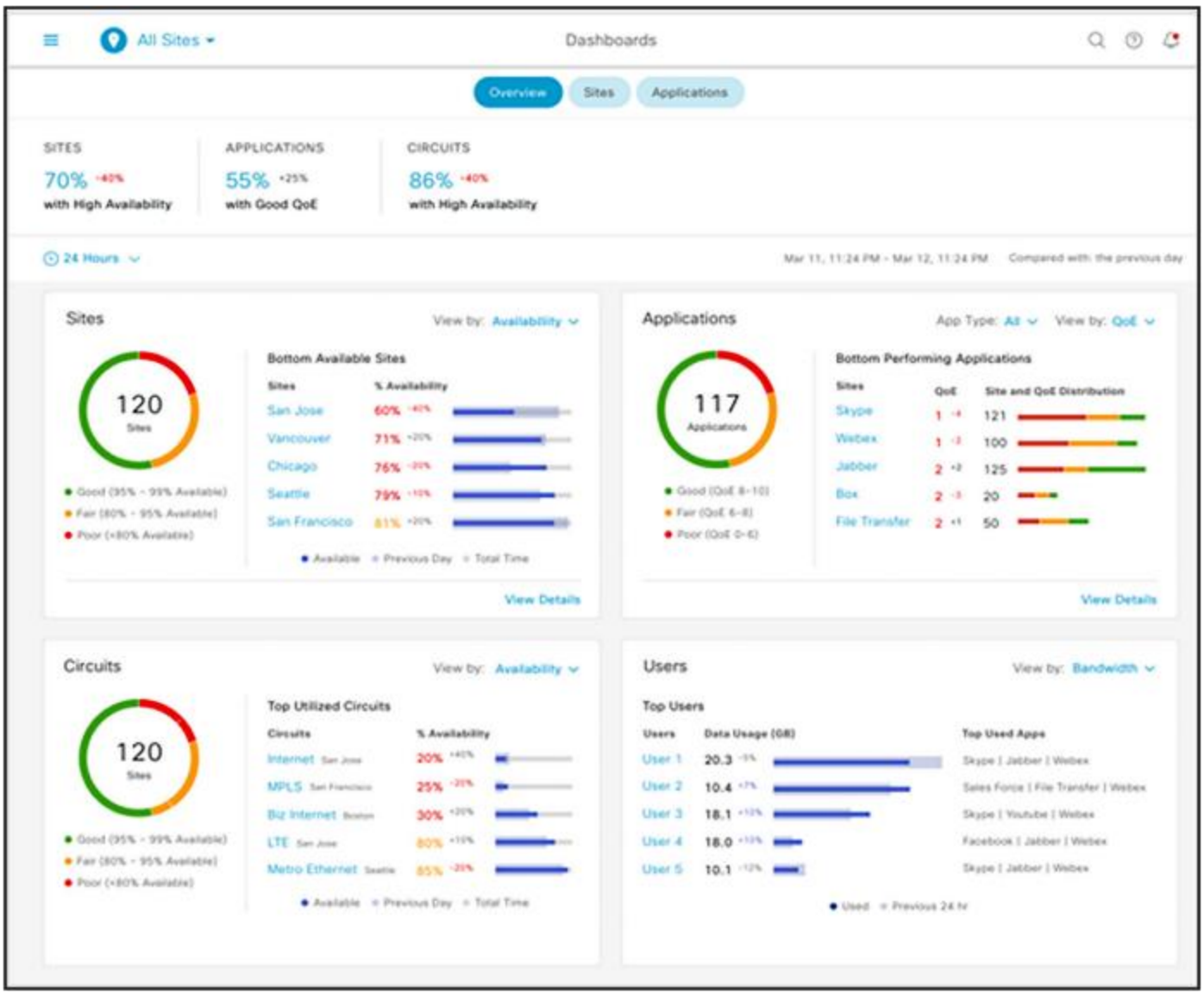

Figure 11: Fujitsu SD-WAN Analytics

2.8: SD-WAN platforms (edge devices)

For Service Pack 1 Fujitsu offers a selection of platforms and appliances to enable Buyers to deploy SD-WAN anywhere (Figure 12). These edge platforms combine cloud networking capabilities with multilayer security support, hardware-accelerated encryption, and robust port flexibility to offer flexible, secure cloud connectivity in SD-WAN that scales.

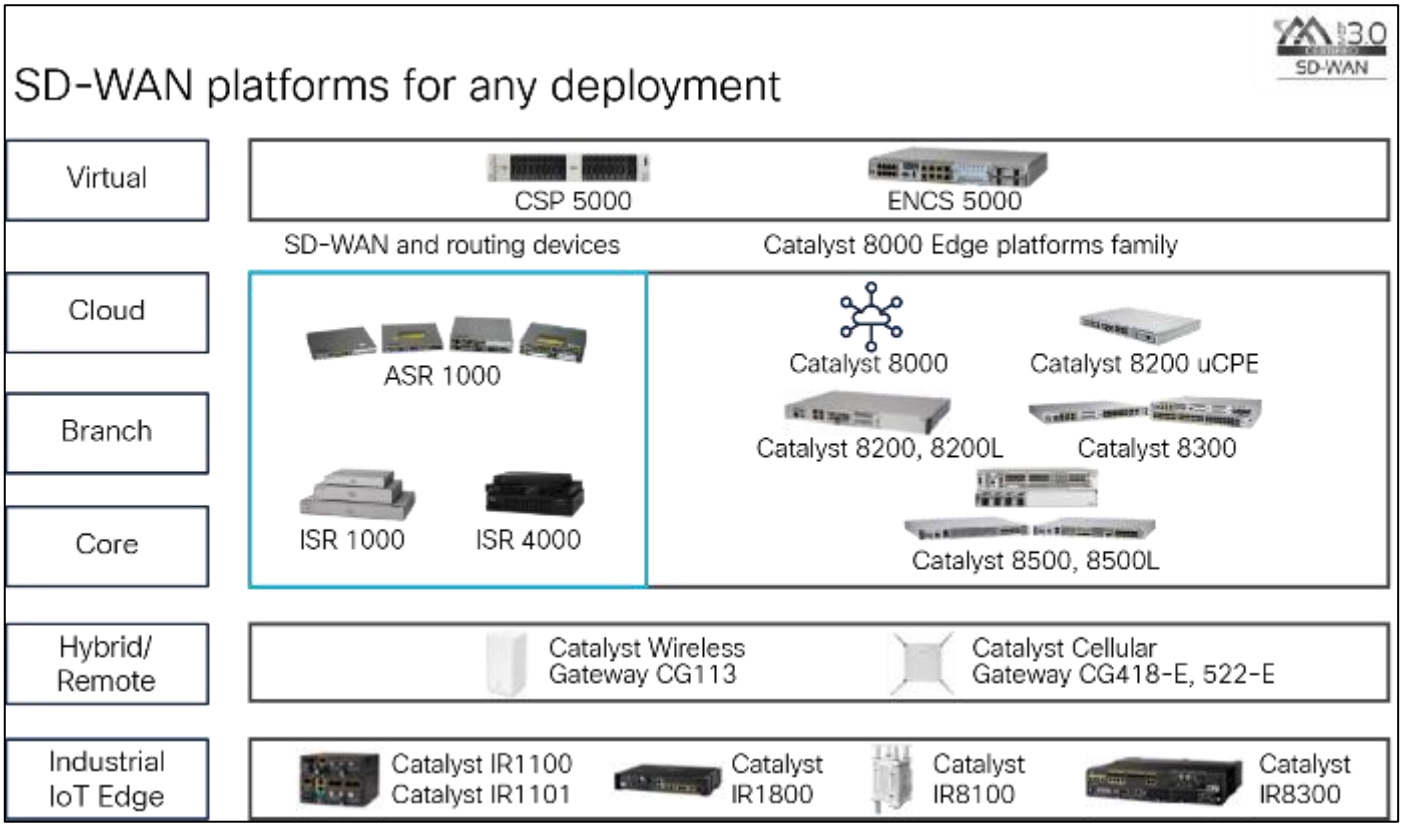

Figure 12: Fujitsu SD-WAN platform capabilities

Fujitsu's edge devices offer reliable security, connectivity, and application storage for IoT. Buyers can deploy Catalyst SD-WAN on Catalyst 8500, 8300, and 8200 Series edge Platforms or on Cisco 1100 Series Integrated Services Routers (ISRs) with a single image for Cisco IOS® XE. Catalyst SD-WAN can also be deployed on SD-Branch solutions such as the Catalyst 8200 Series edge uCPE and Cisco Unified Computing System (**UCS**) E-Series.

Fujitsu SD-WAN can now be extended into, industrial facilities, vehicles, and factories with the Catalyst 1101, 1800, 8100, and 8300 industrial routers for mission-critical use cases.

For colocation, Buyers can simplify WAN management with Fujitsu SD-WAN Cloud OnRamp. Buyers can deploy regional hub solutions on the Cloud Services Platform 5000, or connect SD-WAN with the Catalyst 8500 Series.

Fujitsu Cloud Catalyst SD-WAN extends control and connectivity to cloud environments such as Amazon Web Services, Google Cloud, and Microsoft Azure. Deploy Catalyst SD-WAN in cloud environments through the Cisco Catalyst 8000V edge Software or the Cloud Services Router C8000V Series.

Further information on Cisco edge device compatibility can be found here edge Devices

Note additional functionality deployed on Cisco edge devices such as Umbrella will be subject to validation and capacity of the edge device deployed.

2.9: SD-WAN Software Subscription Licensing

Fujitsu's SD-WAN Software subscription licensing is simple and easy to understand, we align to the Cisco Catalyst SD WAN licence model and support three feature tiers: they are Cisco Essentials, Cisco DNA Advantage, and Cisco DNA Premier, see Figure 13. For Public Sector and CNI users Cisco DNA Advantage is recommended as the minimum software level. All licences provided are subject to automatic refresh to the latest vendor software included within the catalogue tariffs provided.

Benefits:

- The latest innovations through simple subscription tiers
- Available across the portfolio
- Easy licence portability across on-premises and cloud

- Easy upgrade across tiers
- Software Support Service (SWSS) included.

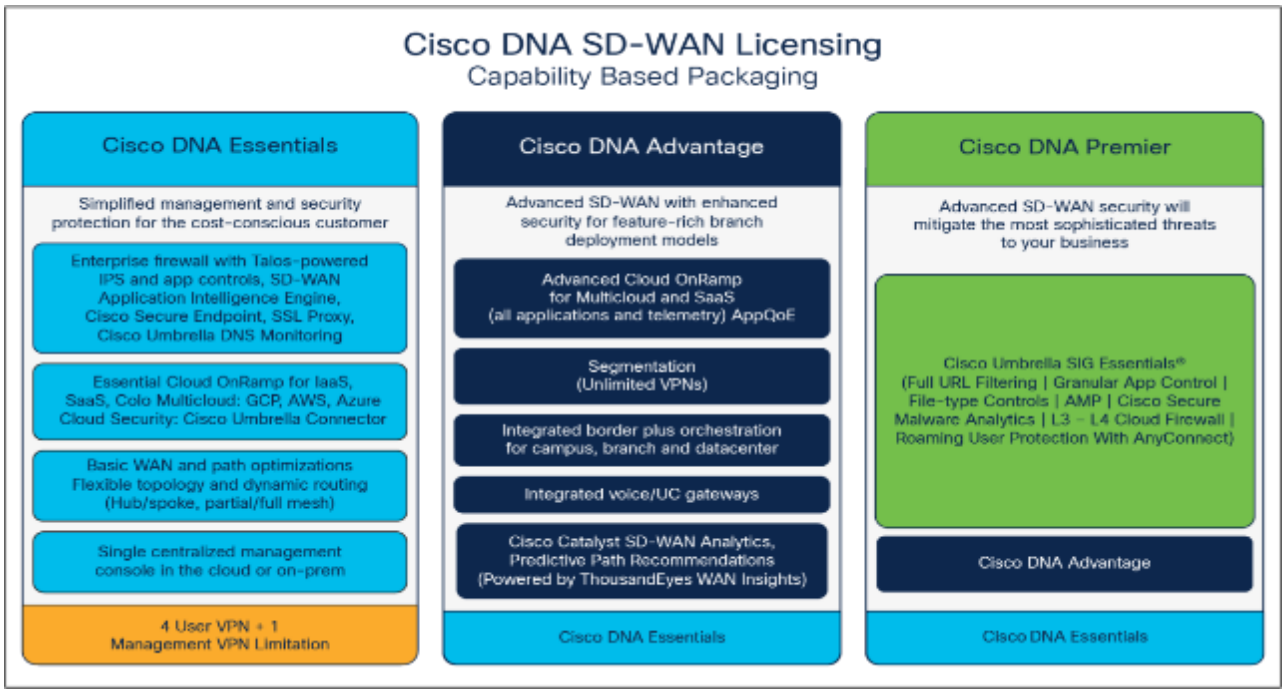

Figure 13: Cisco DNA Software subscription licensing for SD-WAN and routing

2.10: Prominent Features

- latest long-lived star-marked release provided through an automated upgrade program managed by Fujitsu or the Buyer
- Fully integrated security configured via Fujitsu Catalyst Manager.
- Access to Distributed Security Enforcement (DSE) framework using Cisco DNA Premier, which includes - Embedded security (Next Generation Firewall), fabric security, SD-WAN integration with cloud security, monitoring and visibility and certifications and compliance.
- On-premises Security Advanced IPS, AMP with Sandboxing, URL-Filtering, TLS proxy, Unified logging, Identity Firewall support.
- Cloud Security Integration via Cisco DNA Premier with Cisco Umbrella for an integrated single vendor SASE Solution.
- Modular SASE solution through integration with third-party Security Service edge (SSE) cloud security provides, including Zscaler, Netskope, Palo Alto, Cloudflare, and Skyhigh.
- Integration with third-party SIEM, including Splunk, Microsoft Sentinel and Live Action, enhances monitoring and visibility, offering actionable insights into network and security events.
- A centralized view of network security events with actionable threat data for security operations centre teams through the Catalyst SD-WAN Manager Security dashboard.
- Routing intelligence and threat intelligence on a trustworthy infrastructure, certified under Cisco SD-WAN NCSC Cloud Security Principles Assertions
- Separate and dedicated components for the control plane, data plane, and management and orchestration of the WAN.
- Flexibility to implement overlay, underlay, physical, and virtual networks.
- Voice and unified communications support.
- IPv6 support (BGP, OSPF).

- Robust IP multicast support
- Enables network traffic control, enhances efficiency by eliminating traffic redundancy, and reduces server and CPU loads.
- Efficiently handles one-to-many or many-to-many communications.
- Provides multicast capability across platforms (Protocol Independent Multicast Source-Specific Multicast [PIM-SSM], Internet Group Management Protocol [IGMP] v2, and IGMP v3).

2.11: Fujitsu Catalyst G Cloud Aligned Certifications

- Aligned to G Cloud Guidance
- Aligned to ITIL v4 for service management
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

In addition, the third-party platform selected by Fujitsu is aligned to:

- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- Infosec Registered Assessors Program (IRAP December 2021)
- Information System Security Management and Assessment Program (ISMAP)
- Cloud Computing Compliance Controls Catalogue (C5)
- EU Cloud Code of Conduct (CoC)
- Third Party Cybersecurity Compliance Certificate (CCC)
- National Institute of Standards and Technology (NIST) 800-171
- European Union Cybersecurity Certification Scheme on Cloud Services (EUCS)

3: Service Pack 1 Fujitsu SD-WAN Service Delivery

3.1: Service Management

Fujitsu's ISO/IEC 27001, operations are certified by Bureau Veritas (Reference IND17.0595/UUK002399)

Fujitsu is an ITIL® aligned and ISO/IEC20000-1 conformant supplier, deploys, manages and continually improves Service Management processes that are underpinned by standard technologies.

The Service Management process that Fujitsu will deploy for managing the Service under the agreed scope (as defined in the Statement of Works) will include the following key processes and functions:

- Incident Management
- Problem Management
- Event Management
- Change Management
- Availability Management
- Capacity Management.

Fujitsu's Service Pack 1, SD-WAN solution, is a Buyer managed platform with an optional managed service catalogue from Fujitsu to provide supplementary services. The service aligns to NCSC Cloud Security Principles and meets the requirements of infrastructure to comply with OFFICIAL. The Buyer's attention is drawn to the Responsibilities Matrix. This table details the extent of the operational management responsibilities of the Buyer or Fujitsu (unless enhanced via the optional service catalogue).

3.2: Service Demarcation Responsibilities

The table below provides the service demarcation points between the Buyer and Fujitsu or its technology partner (Cisco), further clarity will be provided in the Statement of Work if required:

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
Overlay Provision from Fujitsu SD-WAN Portal	Buyer	Buyer responsible for all connectivity and bearer performance
Fujitsu will provision cloud-hosted controllers for Cisco Catalyst SD-WAN overlay, configure a unique admin password with an expiry time of a week, and hand over Cisco SD-WAN Manager to the Buyer.	Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report infrastructure incidents and to raise service requests
Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure / CPU and Data Disk Utilisation	Buyer and Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report infrastructure incidents and to raise service requests
Protective Monitoring by Fujitsu will comprise of the Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure only. Note service excludes edge device monitoring, firewall configuration connection of new devices or the monitoring of data traversing the Buyer network	Managed by Fujitsu	
A Fujitsu Service Desk will be provided to enable the Buyer to report incidents requiring assistance related to any Buyer provided Protective Monitoring service	Managed by Fujitsu	
Buyer is responsible via the Cisco Catalyst SD-WAN Manager controller SecOps dashboard to view and manage network security events	Managed by Buyer	

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
and actionable threat data to effectively maintain its cyber resilience.		
Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure / Loss of connectivity to network interfaces	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure / Failure to reach instances	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services / Expiry notification of controller SSL certificates	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services / Availability of the Cisco SD-WAN Manager web server	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services/Loss of control connection to the controllers	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services / Capacity management of Cisco Catalyst SD-WAN Controllers	Managed by Fujitsu	Fujitsu monitors and upgrades the instance capacity and expansion to clusters based on the number of devices on the overlay.
Onboard to Cisco SD-WAN Analytics	Buyer	Cisco SD-WAN Analytics is by default onboarded for cloud-delivered Cisco Catalyst SD-WAN Buyers
Renew controller certificates (before expiration)	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Upgrade software / Controller software upgrade	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the er to report incidents and to raise service requests
Upgrade software / edge device/node software upgrade	Buyer	Buyer responsible for the upgrade of software as advised by Fujitsu upon release
Upload and manage edge images in Cisco SD-WAN Manager Software Repository	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Respond to Fujitsu notifications to authorise the service window, instance reboot, review, or verify changes carried out by Fujitsu	Buyer	
Create Smart Accounts (SA) or Virtual Accounts (VA) on software.cisco.com and attach Cisco Catalyst SD-WAN subscribed devices to the SA/VA	Buyer	
Allow external management of SA/VA on PNP Connect	Managed by Fujitsu	Do Not allow external management of SA/VA on PNP Connect before provisioning fabric in Cisco Catalyst SD-WAN Portal. The provisioning workflow automatically enables the external management.
Accept external management of SA/VA and map tenant VA to Buyer's SA/VA	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
Define configure and deploy device configuration templates and policies through Cisco SD-WAN Manager	Buyer	Note Buyer responsible for defining policies and resulting performance
Perform user activities that require logging in to Cisco SD-WAN Manager. For example, template and policy configuration, and edge device management	Buyer	Note Buyer responsible for defining policies and resulting performance
Web server certificates	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
edge serial sync with credentials	Buyer	Cloud-delivered Cisco Catalyst SD-WAN buyers can sync edge serials without credentials (using Single-Sign-On)
Manage allowed access-list with Buyer's source public IP ranges for management access of controllers.	Buyer	
To renew controller certificates on time or upon notification from Fujitsu	Buyer	
Before making any changes in the Cisco Catalyst SD-WAN Portal, take the on-demand snapshot using the procedure, and configuration backup using procedure	Buyer	
In case of dedicated overlay, configure the third interface on Cisco SD-WAN Manager with static IP or DHCP based IP to use it for SD-AVC feature.	Buyer	

Table 1: Service Demarcation Responsibilities

The Cisco SD-WAN Validator and Cisco SD-WAN Controllers are stateless services. Cisco SD-WAN Manager automatically pushes the configurations once they are attached to templates.

3.3: Fujitsu Service Monitoring

Fujitsu monitors the health of cloud-hosted overlays and troubleshoots if there are any issues.

- Fujitsu's service is backed by a monitoring system that checks the health of Cisco Catalyst SD-WAN controllers and generates alerts. The check includes the health of Cisco SD-WAN Manager, application or web server, other micro services, and configuration or statistics databases.
- Fujitsu will take proactive action for cloud infrastructure issues, which are beyond the control of the Buyers. Fujitsu will notify the Buyer about the potential issues and request the Buyer to open a service request for further investigation.
- Fujitsu will manage alerts based on notifications from the cloud provider environments on instance up or down states and CPU, network inactivity status.
- Fujitsu will resolve the alerts proactively if it doesn't require a down time of the services. Notify the Buyer when services flap.
- Fujitsu will send 30-, 15-, and 5-day notices to the Buyers to renew expiring certificates on Cisco SD-WAN Manager. Cisco Catalyst SD-WAN controller certificates have a validity of one year.

3.4: Fujitsu Cloud Infrastructure Support

- Fujitsu will carry out disaster recovery workflows, including snapshot volumes or configurations. Restore Cisco SD-WAN Manager clusters based on volumes or configurations.
- Fujitsu will provision custom subnetting to extend Buyer premises network into cloud-hosted overlay network.

3.5: Fujitsu Capacity Management

Fujitsu will monitor the number of devices per overlay along with the controller instance capacity parameters such as CPU, disk, and memory utilizations to ensure sufficient capacity is provided for the Buyer.

4: Service Pack 1 Service Level Agreement

4.1: Service Level

As standard Fujitsu SD-WAN Core Service (excluding edge hardware) shall meet or exceed the performance standards described below ("Service Level"). A Buyer is eligible for Service Credits if Catalyst SD-WAN Core Service fails to meet the Service Levels, Table 2.

Service Level		Management Period
Control Plane	During each Measurement Period, the Availability of the Control Plane will be 99.99% or greater.	Calendar month starting from the date the Service is provisioned
Management Plane	During each Measurement Period, the Availability of the Management Plane will be 99.99% or greater	

Table 2: Service Levels

4.2: Service Credits

If Fujitsu's fails to meet the Service Level for a given Measurement Period, Fujitsu will issue a Service Credit consistent with the table below, table 3.

Availability Percentage	Days credited
<99.99% and ≥ 99.9%	3 days
<99.9% and ≥ 99.0%	7 days
<99%	15 days

Table 3: Service Credits

4.2.1: Service Credit Limitations

a) Service Credits below are in addition to the Buyer rights detailed in the G Cloud Call Off Contract.
b) The aggregate maximum Service Credit across all Service Levels for any Measurement Period will be 15 days of additional service days for that Measurement Period regardless of whether the Service Credit relates (a) to falling below the Availability Percentage for the Control Plane.
c) The Buyer must claim within 30 days from the date of the Qualifying Outage. Failure to comply will forfeit any right to receive a Service Credit, excluding any remedies provisioned or available under the G Cloud 14 Call Off Contract.

4.3: Service Credit Calculation

If during a 31-day month, two (2) Qualifying Outages occur—one Qualifying Outage lasting 60 minutes and another Qualifying Outage lasting 11 minutes—then the Service Level for Management Plane will be calculated as described below:

Total Service Time = * 31 (days in Measurement Period) * 24 hours * 60 minutes = 44,640 minutes Total Qualifying Outage Time = 60 + 11 = 71 minutes

Availability Percentage = (44,640 – 71) / 44,640 * 100 = 99.8%

In this example, the Service Credit provided, would be an amount equal to 7 days.

4.3.1: Non-Qualifying Outages

Buyers will not be eligible for Service Credits if Fujitsu fails to meet the Service Level for any of the following reasons:

- Scheduled maintenance or emergency maintenance ('emergency maintenance' is unscheduled maintenance where Fujitsu or our technology partner Cisco performs work to prevent or mitigate an outage or degradation of the Cloud Service or to prevent or mitigate a security incident),
- Due to Buyer integrations or any applicable third-party software, hardware, or services not provided by Fujitsu,

- Failure to use the Cloud Service or perform responsibilities in accordance with Your applicable agreement (e.g., EULA or General Terms), Offer Description, Enterprise Agreement, or the Documentation,
- Failure by the Buyer to apply updates or upgrades when made available,
- Events described as Force Majeure, Internet outages, pandemics, acts of government, industry-wide shortages, failures, or delays of common carriers; or
- If Cisco monitoring of the Cloud Service is disabled by the Buyer.

4.3.2: Definitions

"Availability" is calculated as follows and converted into a percentage.

$$\frac{\text{Total Service Time – Total Outage Time Total}}{\text{Service Time}}$$

Fujitsu SD-WAN Core Service means the Control Plane and the Management Plane and excludes all other features, like the Catalyst SD-WAN Analytics feature and the Catalyst SD-WAN Portal:

"Qualifying Outage" means the time that the Core Services are not functioning as described in the Offer Description or Documentation.

"Service Credits" means additional days Fujitsu will add to Your Cloud Service Use Term (or as a service credit against current billing).

"Total Outage Time" means the aggregate total time for all Qualifying Outages during a Measurement Period (rounded upward to the nearest minute).

To calculate Total Outage Time, each Qualifying Outage will:

- Begin when Fujitsu logs an incident ticket based on identification of a Qualifying Outage or upon confirming a Qualifying Outage; and
- End when the Fujitsu SD-WAN Core Service are restored.

"Total Service Time" means the total number of minutes in a Measurement Period (calculated by multiplying:

60 (minutes) by 24 (hours) by the number of calendar days in the Measurement Period).

4.4: Optional Enhanced Service Level Agreement

Enhanced service levels can be offered by Fujitsu which can be defined in the Statement of Work. Enhanced services will be subject to the SFIA rate card for costing purposes. It should be noted platform availability and service desk support enhancements will be constrained by the service capacity of Fujitsu's technology partners.

5: Service Pack 2 SD-WAN UK Deployed solution

Fujitsu's SD-WAN Service Pack 2 is based on the Cisco Catalyst SD-WAN software, as a shared platform with Fujitsu enhancements to support Higher Information Assurance requirements and hosting in its certified UK infrastructure. All service management facilities are provided in the UK from Fujitsu Defence and National Security facilities offering a Sovereign based solution.

Fujitsu's SD-WAN Service aligns with NCSC's 14 Cloud Security Principles providing a highly available and secure SD-WAN platform. The service includes NCSC aligned Protective Monitoring capabilities (defined use cases as detailed in the Statement of Work) with service uplifts to provide or support Buyer SOC capabilities as an optional service. The service provision enables the Buyer to manage the end user services using portals and tooling provided by Fujitsu.

Service Pack 2 also comprises of service management options from Fujitsu providing a full range of ITIL based managed services calculated using the SFIA rate card as detailed in the service catalogue. Service Pack 2 today supports Buyers who require OFFICIAL Caveat SENSITIVE) and or Critical National Infrastructure "CNI" compliant services (aligned to NCSC guidance). All Fujitsu staff associated with managing the SD-WAN service hold as a minimum SC security clearance.

For Buyers seeking an SD-WAN solution to meet a higher-level SECRET classification, then exclusive assets and additional security devices would be required, which may need to be deployed within the Buyer environment.

As a shared platform the features and functionality of Service Pack 2 will be in accordance with the services deployed across all (HM Government Crown Departments) on the shared platform. Buyers are advised to seek guidance (using the Statement of Work) from Fujitsu to validate the service meets its functional requirements.

Fujitsu's SD-WAN connects a user to any application with integrated capabilities for multicloud, security, predictive operations, and enhanced network visibility. Fujitsu's SD-WAN enables Buyers to transform IT infrastructure by delivering network connectivity that's cloud-agnostic, efficient and simpler to manage, reduces operational costs and increases control and visibility across the entire digital service delivery chain. It should be noted additional gateways or security devices as detailed in the optional catalogue may be required for multicloud and hybrid deployments to reflect choice of network bearers or information assurance, this will be advised in the Statement of Work.

5.1: Solution overview

Fujitsu's SD-WAN comprises of separate orchestration, management, control, and data planes all deployed within Fujitsu's UK certified datacentre environments, they key functional aspects comprise of

- The orchestration plane assists in the automatic onboarding of the SD-WAN routers into the SD-WAN overlay.
- The management plane is responsible for central configuration and monitoring.
- The control plane builds and maintains the network topology and makes decisions on where traffic flows.
- The data plane is responsible for forwarding packets based on decisions from the control plane.
- WAN connectivity is the responsibility of the Buyer to provide.

Please refer to Figure 14 for generic schematic of the Fujitsu SD-WAN solution.

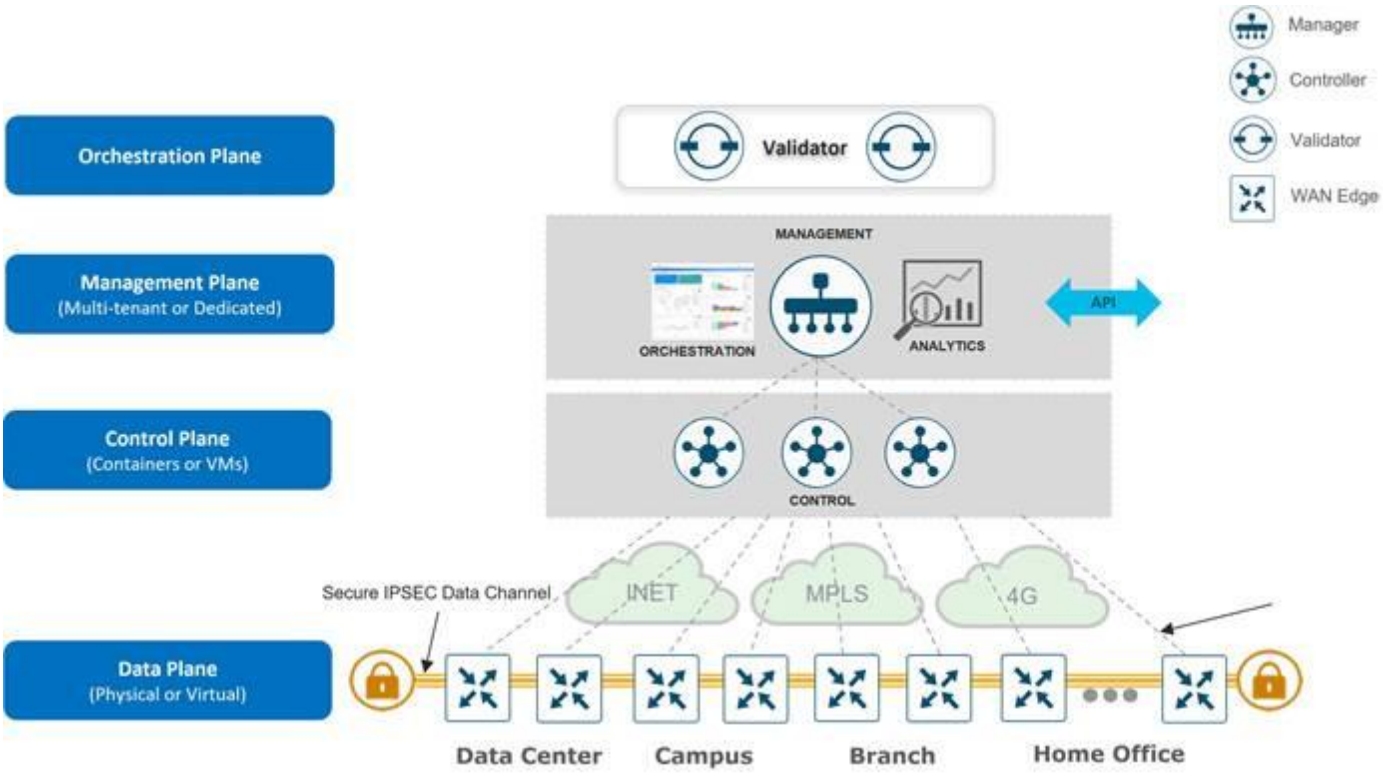

Figure 14: **Overview of Fujitsu SD-WAN solution planes**

The primary components for Fujitsu's SD-WAN solution consist of the SD-WAN Manager network management system (management plane), the SD-WAN Controller (control plane), the SD-WAN Validator (orchestration plane), and the WAN edge router (data plane).

- SD-WAN Manager - This centralized network management system is software-based and provides a GUI interface to easily monitor, configure, and maintain all Fujitsu's SD-WAN devices and their connected links in the underlay and overlay network. It provides a single pane of glass for Day 0, Day 1, and Day 2 operations.
- SD-WAN Controller - This software-based component is responsible for the centralized control plane of the SD-WAN network. It maintains a secure connection to each WAN edge router and distributes routes and policy information via the (OMP), acting as a route reflector. It also orchestrates the secure data plane connectivity between the WAN edge routers by reflecting crypto key information originating from WAN edge routers, allowing for a very scalable, IKE-less architecture.
- SD-WAN Validator - This software-based component performs the initial authentication of WAN edge devices and orchestrates SD-WAN Controller, Manager, and WAN edge connectivity. It also has an important role in enabling the communication between devices that sit behind Network Address Translation (NAT).
- WAN edge router - This device, available as either a hardware appliance or software-based router, sits at a physical site or in the cloud and provides secure data plane connectivity among the sites over one or more WAN transports. It is responsible for traffic forwarding, security, encryption, quality of service (QoS), routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and more.

Figure 15 demonstrates several aspects of Fujitsu's SD-WAN solution. This sample topology depicts two WAN edge sites, each directly connected to a private MPLS transport and a public Internet transport.

The SD-WAN control complex (the two SD-WAN Controllers, the SD-WAN Validator, along with the SD-WAN Manager, is hosted in Fujitsu's UK certified datacentres) and is reachable directly in this instance using Internet transport (this could also be MPLS etc). In addition, the topology also includes cloud access to SaaS and IaaS applications.

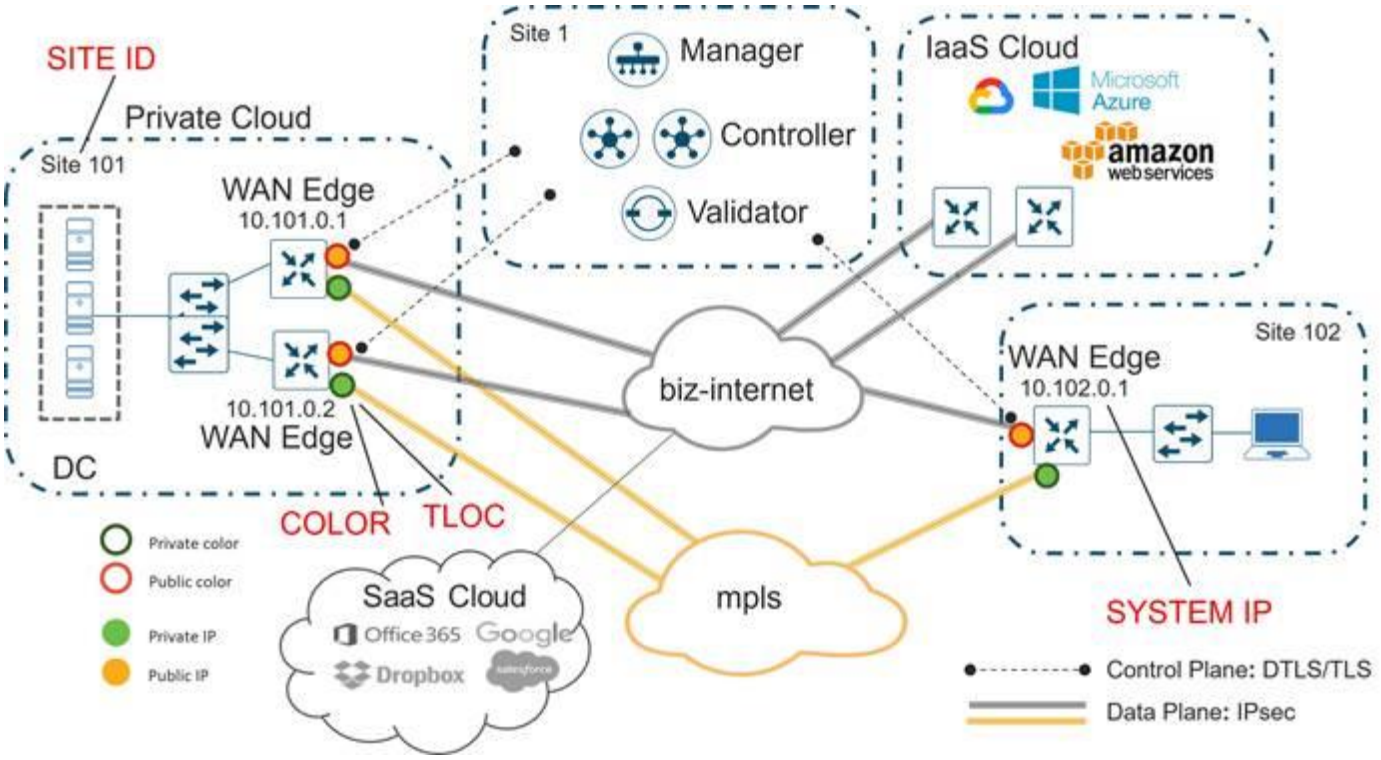

Figure 15: **Example SD-WAN topology**

The WAN edge routers form a permanent Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) control connection to the SD-WAN Controllers and connect to both of the SD-WAN Controllers over each transport. The routers also form a permanent DTLS or TLS control connection to the SD-WAN Manager, but over just one of the transports. The WAN edge routers securely communicate to other WAN edge routers using IPsec tunnels over each transport. The Bidirectional Forwarding Detection (BFD) protocol is enabled by default and runs over each of these tunnels, detecting loss, latency, jitter, and path failures.

For Service Pack 2 Fujitsu has deployed certified configuration design ITSM tool sets and protective monitoring capabilities details of which can be provided upon request the toolsets deployed include; ServiceNow, Zabbix, Elastic, Veeam, Broadcom Malware and Tenable.

For a technical overview and Buyer design considerations for Catalyst SD-WAN please refer to the following link Solution Overview.

Fujitsu's SD-WAN connects a user to approved applications with integrated capabilities for multicloud, security, predictive operations, and enhanced network visibility. Fujitsu SD-WAN Manager provides a secure visualised dashboard that simplifies network operations providing centralised configuration, management, operation, and monitoring across the entire SD-WAN fabric.

Fujitsu SD-WAN offers integrated security, including full-stack multilayer security capabilities as optional services, additional gateways or security devices which are detailed in the optional catalogue. Additional devices may be required to reflect information assurance requirements which shall be advised in the Statement of Work. This integrated security can provide threat protection where and when it is needed — for branches connecting to multiple Software-as-a-Service (SaaS) or IaaS clouds, datacentres, or the internet. Fujitsu SD-WAN can be fully integrated with the optional Cisco Umbrella, which offers protection against security blind spots and cyberthreats. Note deployment subject to Buyer Information Assurance requirements.

Using the SD-WAN Manager (see **Figure 16**) Fujitsu's SD-WAN simplifies IT operations with automated provisioning, unified policies, and streamlined management.

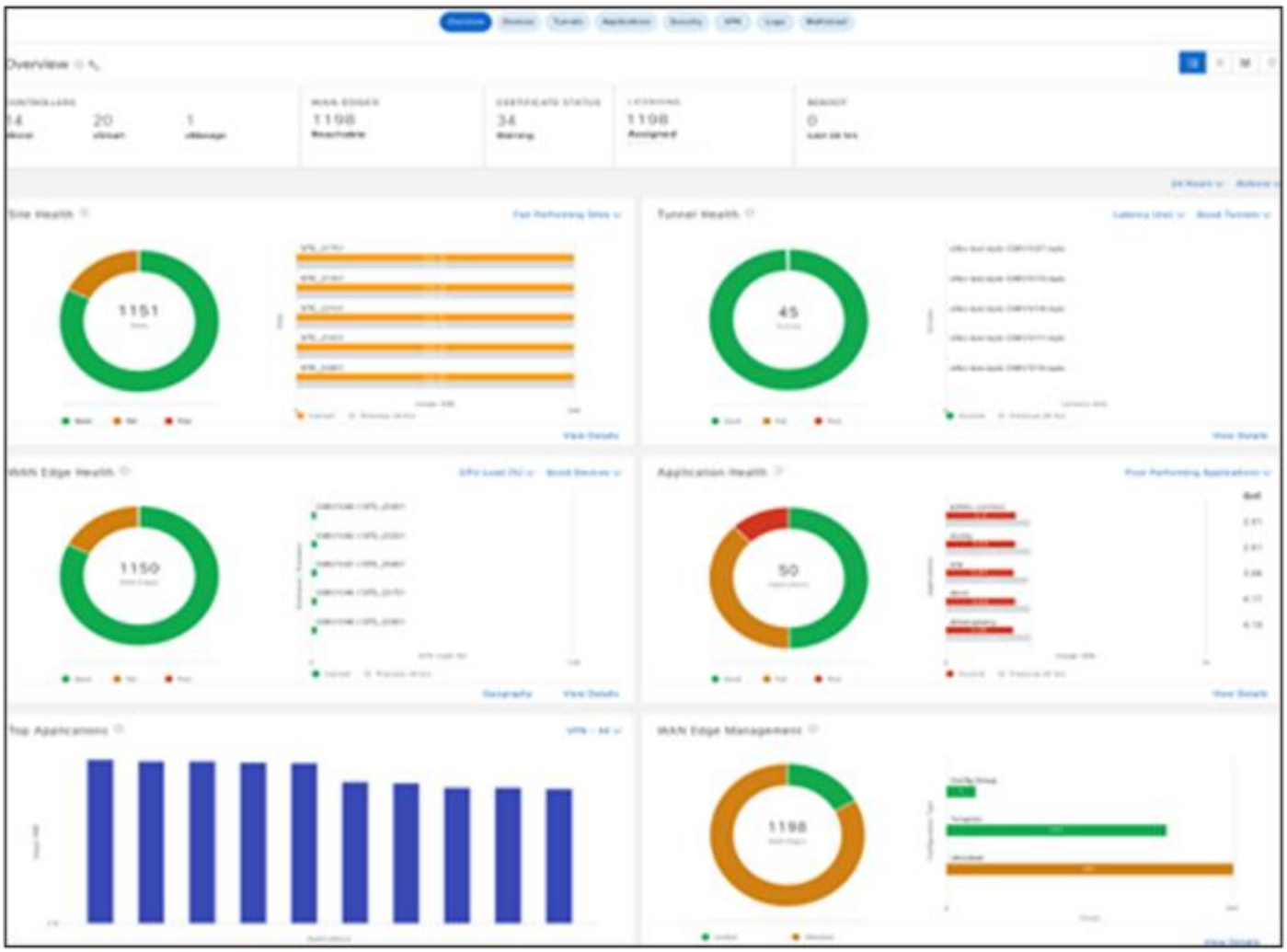

Figure 16: Fujitsu SD-WAN Manager dashboard showing network and application health

Fujitsu's service provides a flexible architecture to extend SD-WAN to any environment (Figure 17).

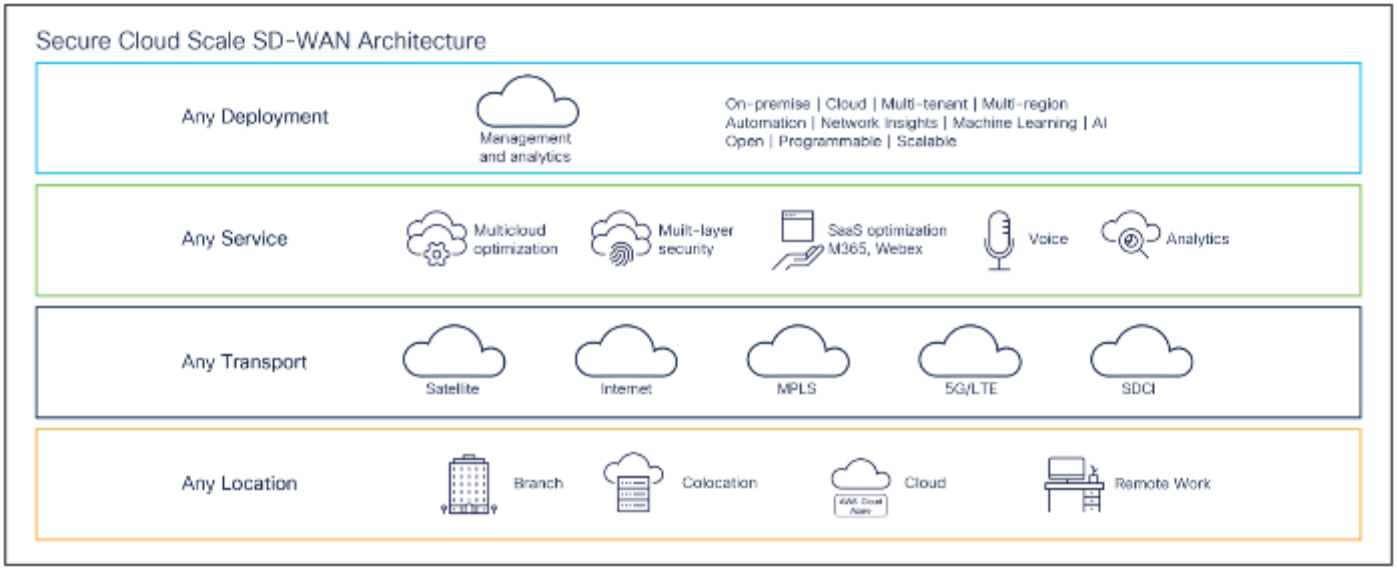

Figure 17: Flexible and scalable architecture for network transformation

5.2: Multicloud Choice & Control

Fujitsu's SD-WAN provides the ability to connect to multiple cloud platforms or other enterprise, supporting enhanced connectivity and reliability. Fujitsu's SD-WAN Cloud OnRamp creates a WAN extension for Buyer IaaS workloads, provides dynamic path selection for optimal SaaS application performance, consolidates branch office egress points into regional colocation facilities, and automates cloud-agnostic branch connectivity with cloud interconnect. This functionality will be subject to design review to reflect Buyer Information Assurance Policies. Monitoring underlay performance via Fujitsu's SD-WAN Manager, Cloud OnRamp automatically selects the fastest, most reliable path to the cloud infrastructure. In the event of network service interruptions, Cloud OnRamp will adjust paths as necessary, helping ensure improving continuous uptime and predictable performance.

5.3: SD-WAN Cloud OnRamp for Multicloud

Fujitsu's SD-WAN makes connecting the WAN to IaaS environments such as Amazon Web Services, Google Cloud, and Microsoft Azure simple and secure (Figure 18). This functionality will be subject to design review to reflect Buyer Information Assurance Policies. In the Fujitsu SD-WAN console, network and operations teams can create virtual private cloud connections to IaaS environments, extending the Fujitsu SD-WAN OMP to the cloud. Fujitsu's SD-WAN applies automated connectivity requirements (loss, latency, and jitter) to find the optimal path to cloud IaaS applications, adjusting the IPsec route as needed to help ensure service delivery and performance while monitoring the hosting infrastructure for anomalies.

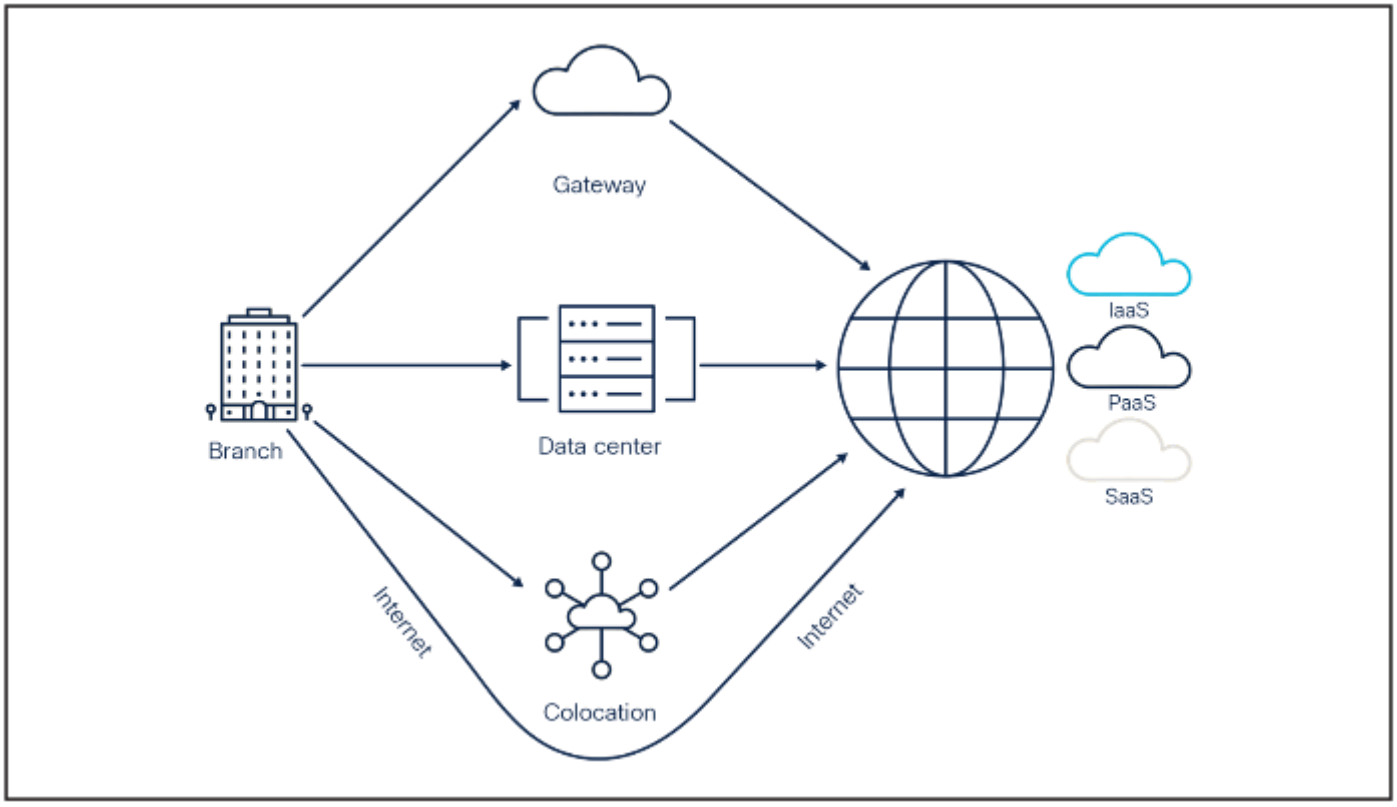

Figure 18: Fujitsu's SD-WAN Cloud OnRamp for IaaS, PaaS, and SaaS applications

5.4: SD-WAN Cloud Hub

Fujitsu's SD-WAN Cloud Hub leverages SD-WAN to interconnect branch sites, on-premises datacentres, and subject to the Buyer Information Assurance policies can also use a public cloud service provider's backbone (such as AWS, Google Cloud, or Microsoft Azure) as an underlay. Cloud Hub reduces provisioning time with site-to-cloud network automation as well as offering high availability and multiple points of presence across the world using a cloud service provider's global infrastructure for site-to-site connectivity (Figure 19). Note, Buyers are responsible for site connectivity which shall be used to connect to the SD-WAN Cloud Hub service.

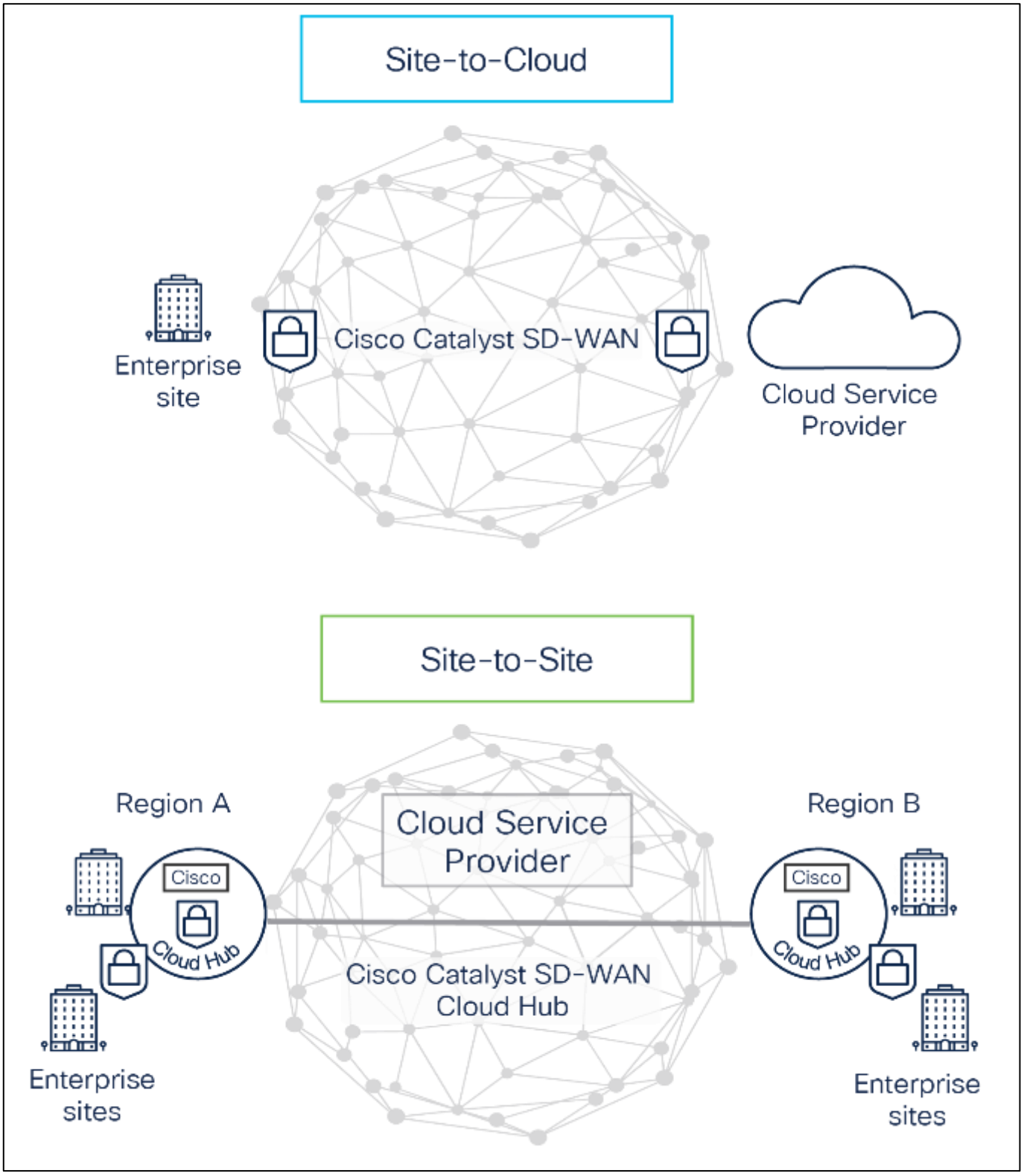

Figure 19: Fujitsu's SD-WAN Cloud Hub

5.5: SD-WAN Cloud OnRamp for SaaS

Buyers may also be using SaaS applications. Connectivity to these applications may require sharing resources with other users on distant hardware. This functionality will be subject to design review to reflect Buyer Information Assurance Policies. Fujitsu's SD-WAN Cloud OnRamp for SaaS makes connecting to and securing these SaaS environments simple. Fujitsu's SD-WAN Cloud OnRamp selects the fastest, most reliable path to SaaS applications (Figure 20), engaging in real-time traffic steering to deliver the best user experience no matter where they are located. Should a network service issue cause connectivity that falls below Buyer agreed thresholds, Cloud OnRamp finds the next best path to help ensure continued application performance. In addition, the solution

automates best path selection for custom and standard NBAR (Network Based Application Recognition) applications, allowing Buyers to enable Cloud OnRamp for SaaS capabilities with the application of their choice.

Fujitsu's SD-WAN Cloud OnRamp for SaaS has been designed to support applications (for example) Fujitsu's cloud communication, collaboration, and video capabilities. Fujitsu SD-WAN segregates UC traffic from generic internet traffic and routes it via the best path from a specific branch router to deliver a seamless, consistent, and high-quality user experience. The solution enables improved performance for Microsoft 365. Features such as informed network routing and URL categorization, giving users deeper abilities to manage and route traffic within Microsoft 365 to improve speed, efficiency, and performance across the entire suite of applications.

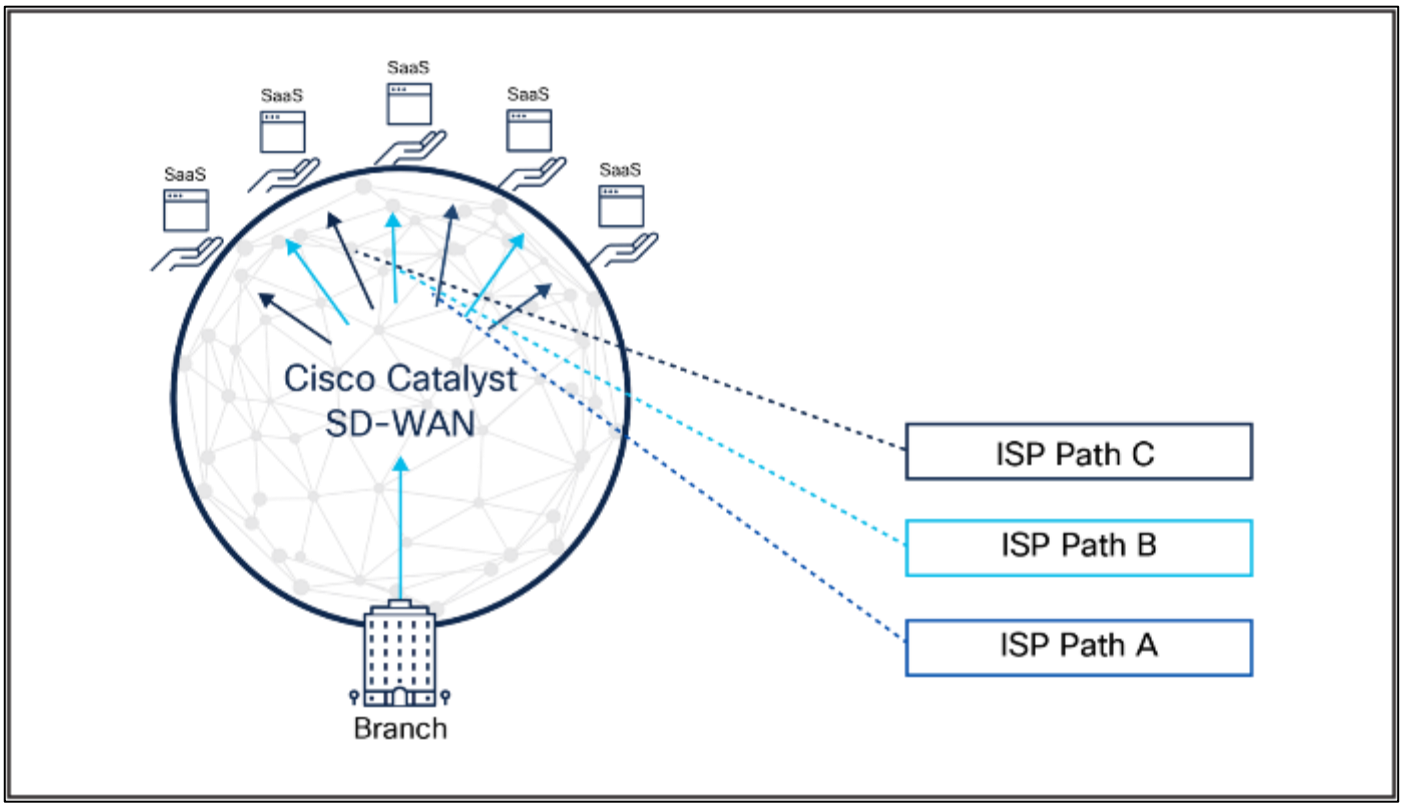

Figure 20: Dynamic path selection in Fujitsu's SD-WAN Cloud OnRamp for SaaS

5.6: Fujitsu SD-WAN Cloud Interconnect

Fujitsu's SD-WAN Cloud Interconnect (Figure 21) extends the use of cloud agnostic backbone to connect from site to site and site to multiple clouds. This functionality will be subject to design review to reflect Buyer Information Assurance Policies. The Cloud OnRamp solution automates on-demand connectivity between multiple sites and cloud provider networks and secure Fujitsu's secure infrastructure directly from the SD-WAN controller. This solution delivers reliable network performance while decreasing operational costs and complexity. Cloud Interconnect provides a single, easy-to-use console to automate deployment of connections.

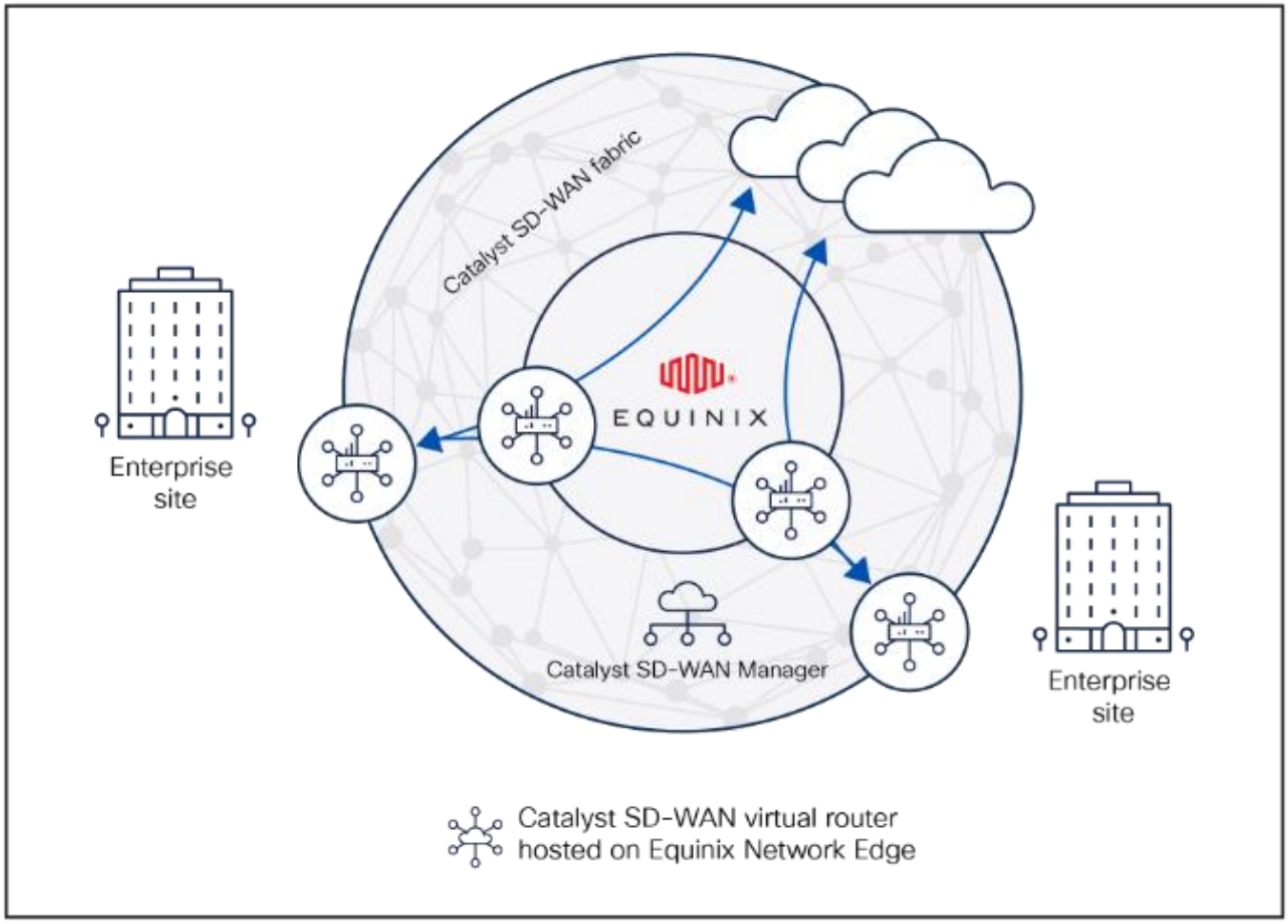

Figure 21: Fujitsu SD-WAN Cloud Interconnect

5.7: Analytics and Insights

Applications are more distributed than ever, and across Public Sector the internet is becoming the new enterprise WAN. As SD-WAN has transformed to connect users across multicloud, branch, datacentres, and a hybrid workforce, IT and network operation teams are challenged to deliver reliable connectivity, application experience, and security over networks and services they don't own or directly control. In parallel, networks and devices generate a multitude of data points across thousands of sites, network paths, applications, and distributed users. It has become difficult to digest and make sense of this data. Time spent on the identification of issues and troubleshooting requires significant resources and further prolongs negative impacts on productivity.

Fujitsu's Live NX Analytics Figure 22 capabilities simplify network operations by providing granular network insights, predictivity, and automation that not only heighten network integrity but also deliver optimal application experience. Fujitsu's Analytics aggregates a large volume of telemetry data and correlates application performance with underlying networks for operational insights, in a highly visualised and simplified manner. Fujitsu's Analytics enhances network visibility, establishes historical benchmarks, and expedites root-cause isolation, enabling Buyers to take the necessary corrective actions and control of the user experience. Fujitsu's SD-WAN provides via a portal Analytics as standard which provides enhanced visibility into the network and application performance, along with historical trend information to establish benchmarks and expedite root cause analysis.

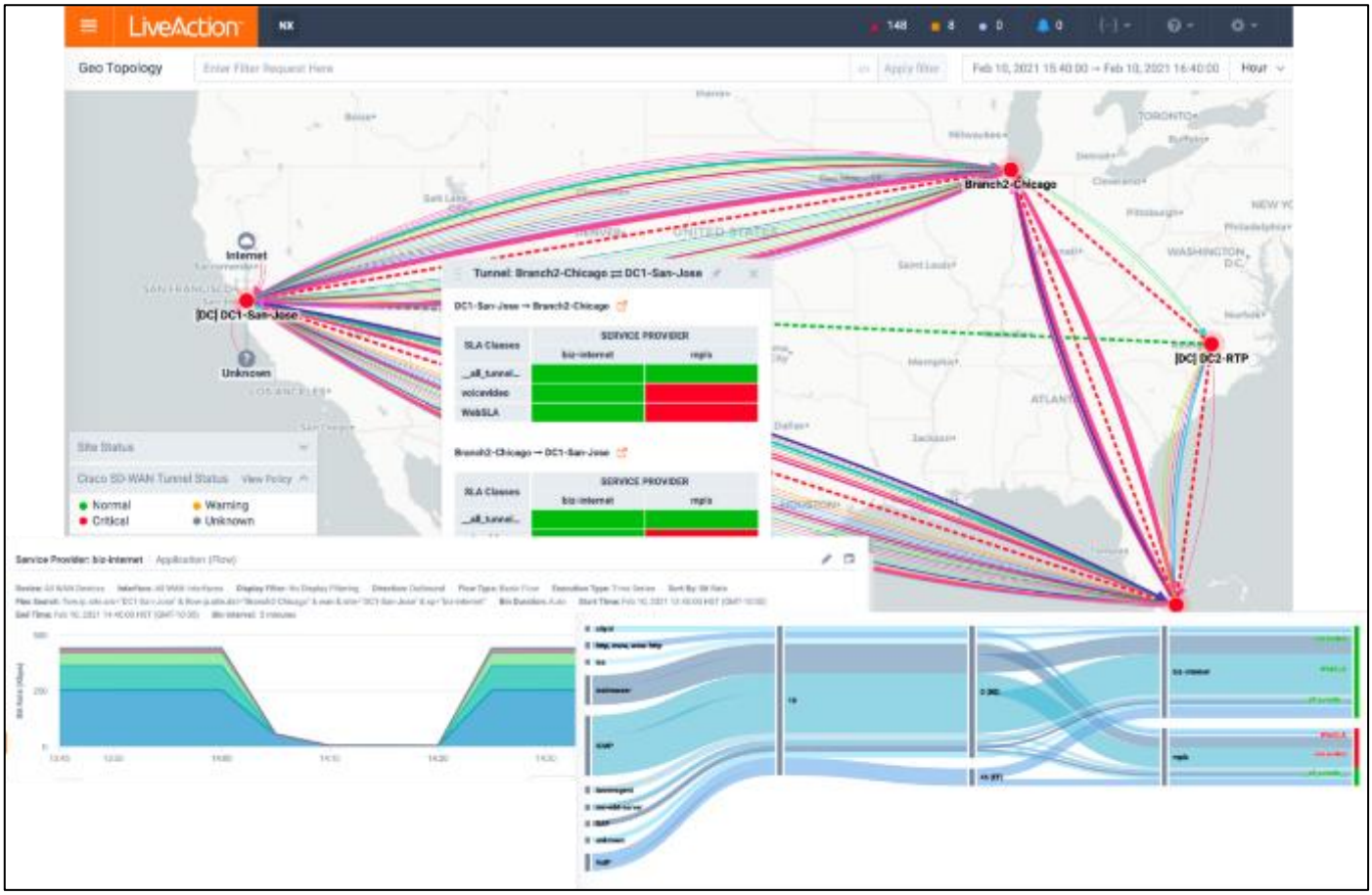

Figure 22: Fujitsu Live NX SD-WAN Analytics

5.8: SD-WAN platforms (edge devices introduction)

Fujitsu offers a selection of edge platforms and appliances to enable a Buyer to deploy the SD-WAN anywhere. For Service Pack 2 Fujitsu has developed secure edge devices using commercial off the shelf (COTS) products based on universal Customer Premises Equipment (uCPE). Fujitsu's uCPE enables Buyers through service chains to deploy additional applications such as Secure Access Service edge supporting Next Generation Firewall (NGFW), Industrial / Internet of Things (IOT) devices, and or other SDN based applications. The only limitation is the capacity of the edge device to support additional applications which will be advised by Fujitsu.

In addition to Fujitsu's uCPE, we also provide the full range of Cisco edge devices and new IoT devices. Cisco edge devices today use out of the box security credentials. Fujitsu's uCPE devices support a zero-touch process (developed by Fujitsu for secure deployments). All edge platforms provided by Fujitsu combine innovative cloud networking capabilities with multilayer security support, encryption, and robust port flexibility to offer flexible, secure cloud connectivity in SD-WAN that scales. Fujitsu will work with the Buyer to optimise edge deployment design.

5.9: SD-WAN platforms (uCPE devices)

The uCPE devices offered by Fujitsu are based on the DELL VEP range and Advantech devices, the devices support:

- COTS X.86 hardware computing platform (currently Dell VEP- 1485 / VEP-4600, Advantech)
- Deployed with NFVI (ADVA Ensemble Connector)
- Deployed with cEdge VNF hosting the Cisco Catalyst 8000v
- Optional SAT VNF hosting a vTA (Paragon service assurance)

DELL VEP 1485

The Dell VEP-1485, is shown below:

Figure 23: uCPE (Dell VEP-1485)

Parameter	Specification	Notes
Model	Dell VEP-1485	
Network ports	6x RJ45 (10/100/1000baseT)	Used for WAN/LAN connectivity
	2x SFP/SFP+ (1Gbps/10Gbps)	Used for connecting UCPE secondary and warm standby devices using TLOC extensions
Management Ports	Micro-USB	Console port, covered by removable plate
USB	2x USB 3.0 Type A	Mounting from USB is disabled at the end of OBC build
Wi-Fi	Not fitted	
Processor	Intel Atom C-3000 X-86	
CPU	16x CPU (1485)	
Memory	16GB	
Storage	240GB	Internal SDD
Operating System	Rocky OS	Built during OBC build
NFVI	Adva EC	Built during OBC build
Switch	Adva EC – vSwitch	Configured by ESO/LOSS
Hypervisor	Adva EC – KVM	VNF build by ESO/LOSS

Table 4: Technical specifications of the Dell VEP-1485 uCPE deployments

DELL VEP-4600

Usually deployed for sites requiring in excess of 1Gbps throughput. The Dell VEP-4600 employs the same NFVI, cEdge and SAT solution, but provides additional computing resource for improved throughput performance.

Figure 24: uCPE (Dell VEP-4600)

The following table summarises the technical specifications of the Dell VEP-4600 used uCPE deployments.

Parameter	Specification	Notes
Model	Dell VEP-4600	
Chassis network ports	4x RJ45 (10/100/1000baseT)	Used for WAN/LAN connectivity
	2x SFP/SFP+ (1Gbps/10Gbps)	Used for connecting UCPE secondary and warm standby devices using TLOC extensions
Interface Module network ports	2x RJ45 (10.100/1000baseT)	Used for WAN/LAN connectivity
	2x SFP/SFP+ (1Gbps/10Gbps)	Used for WAN/LAN connectivity
Management Ports	1x RJ45 (10/100/1000baseT)	CPU
	1x RJ45 (10/100/1000baseT)	BMC
USB	2x USB 3.0 Type A	USB 3.0 - Mounting from USB is disabled at the end of OBC build
	1x micro USB Type B	Available for console port
Console ports	1x serial RJ45	CPU
	1x serial RJ45	BMC
Wi-Fi___33	None	
Processor	Intel Xeon-D 2100 X-86	
CPU	16x CPU	
Memory	32GB	
Storage	240GB	Internal SDD
Operating System	Rocky OS	Built during OBC build
NFVI	Adva EC	Built during OBC build
Switch	Adva EC – vSwitch	Configured by ESO/LOSS

Hypervisor	Adva EC – KVM	VNF build by ESO/LOSS

Table 5: Technical specifications of the Dell VEP-4600 used uCPE deployments

Advantech FWA-3050 / 3051

The Advantech range, uCPE device, from Fujitsu replaces the Dell VEP-4600 devices.

The Advantech range supports:

- Throughput of 1Gbps to 2.5Gbps.
- Dual power supplies (e.g. datacentres or high availability sites).

The Advantech range employs the same NFVI, cEdge and SAT solution, but provides additional computing resource for improved throughput performance.

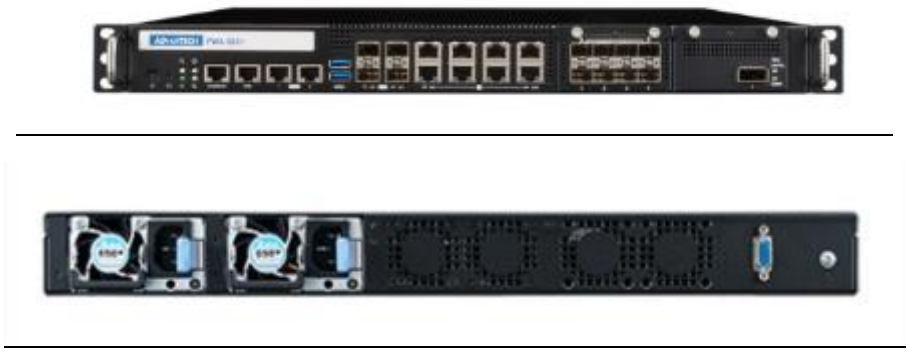

Figure 25 uCPE Advantech Range

The following table summarises the technical specifications of the Advantech devices.

Parameter	Specification	Notes
Model	Advantech FWA-/ 3050 or 3051	Selection by Fujitsu depending on through put requirements or SD-WAN functionality deployed.
Chassis network ports	8x RJ45 (10/100/1000baseT)	Used for WAN/LAN connectivity
	4x SFP/SFP+ (1Gbps/10Gbps)	Used for 10Gbps WAN/LAN and fibre WAN connectivity. Used for connecting UCPE secondary and warm standby devices using TLOC extensions
Network Module Cards	8x SFP+ (10Gbps)	Optional NMC-1012
Management Ports	1x RJ45 (Console)	Serial console port
	2x RJ45 (10/100/1000baseT)	Management LAN
	1x IPMI 2.0	Baseboard Management Controller (BMC)
USB	2x USB 3.0 Type A	USB 3.0

		Mounting from USB is disabled at the end of OBC build
	1x VGA Display Port	Rear mounted VGA
Wi-Fi module	None	
Processor	Intel Xeon D-2876NT	
CPU	8 or 16x CPU	
Memory	24 or 32GB	
Storage	2TB	Internal SSD
Operating System	Rocky OS	Built during OBC build
NFVI	Adtran EC	Built during OBC build
Switch	Adtran EC - vSwitch	Configured by LOSS
Hypervisor	Adtran EC - KVM	VNF build by LOSS

Table 6 uCPE (Advantech Technical Specification)

5.10: Ensemble Connector for uCPE devices

On the Fujitsu's SD-WAN uCPE Fujitsu deploys Adva Ensemble Connector. Ensemble Connector is a highly scalable, high-performance virtualisation platform for hosting multi-vendor VNFs. It enables pure-play virtualisation: open software running on open commercial off-the-shelf servers. This eliminates vendor lock-in so that Fujitsu is free to mix and match best-of-breed software and hardware. This includes the following functionality:

- KVM hypervisor and Virtual Switch connector to support flexible VNF service chains.
- Supports multiple service chains with Cisco cEdge virtual routers, vTA and a range of WAN/LAN connectivity options.
- Fujitsu's SD-WAN Cedge virtual router service chain provides Ethernet connectivity with the platform network ports.
- Docker Openstack, encryption and router
- Lightweight OSS

The ESO/LOSS orchestration service allows VNF service chains to be modified in the field without the need for a site visit or on-site configuration.

5.11: Cisco edge devices

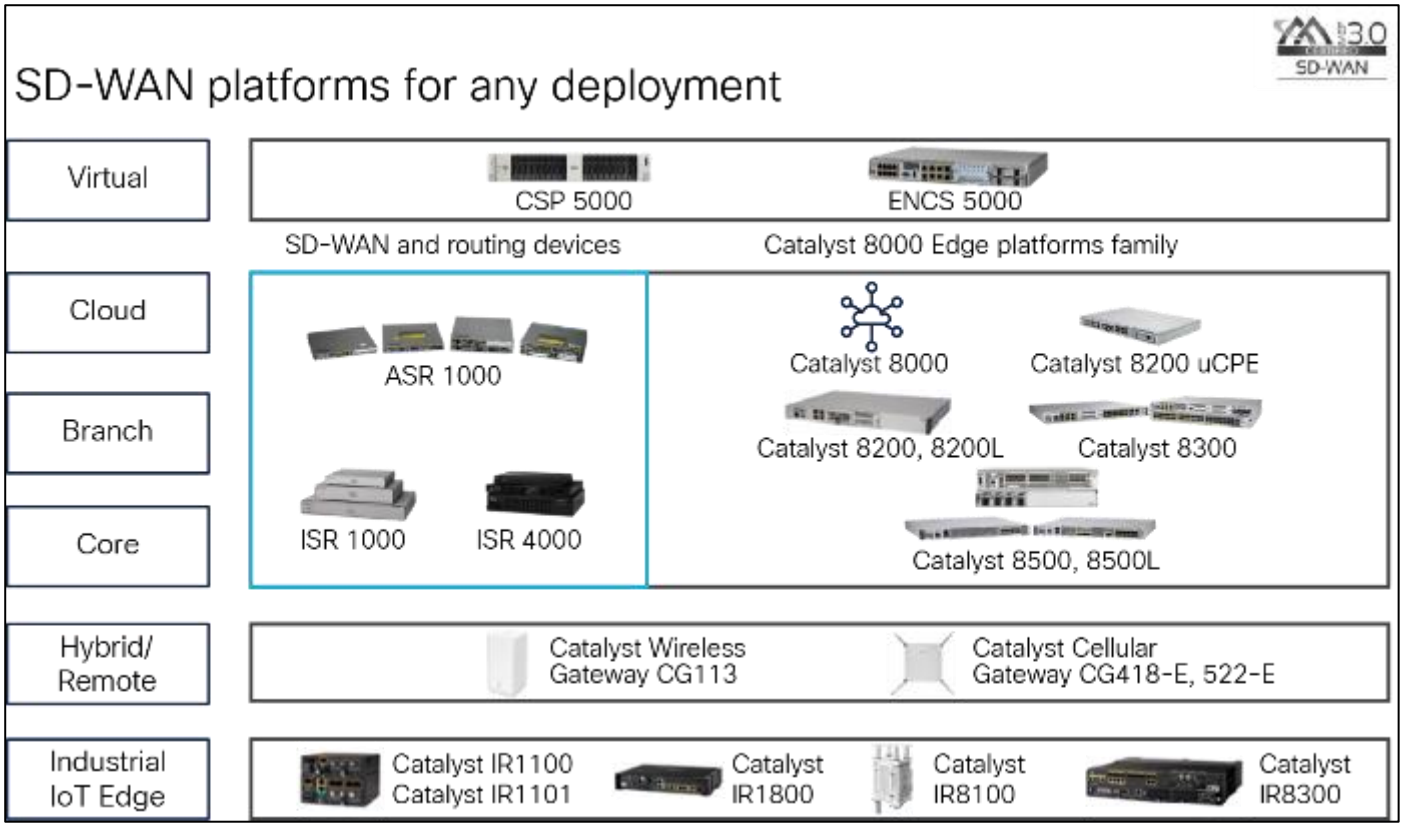

Figure 26: Fujitsu SD-WAN platform capabilities

Fujitsu's edge devices offer reliable security, connectivity, and application storage for IoT. Buyers can deploy Catalyst SD-WAN on Catalyst 8500, 8300, and 8200 Series edge Platforms or on Cisco 1100 Series Integrated Services Routers (ISRs) with a single image for Cisco IOS® XE. Catalyst SD-WAN can also be deployed on SD-Branch solutions such as the Catalyst 8200 Series edge uCPE and Cisco Unified Computing System (**UCS**) E-Series.

Fujitsu SD-WAN can now be extended into, industrial facilities, vehicles, and factories with the Catalyst 1101, 1800, 8100, and 8300 industrial routers for mission-critical use cases.

For colocation, Buyers can simplify WAN management with Fujitsu SD-WAN Cloud OnRamp. Buyers can deploy regional hub solutions on the Cloud Services Platform 5000 or connect SD-WAN with the Catalyst 8500 Series.

Fujitsu Cloud Catalyst SD-WAN extends control and connectivity to cloud environments such as Amazon Web Services, Google Cloud, and Microsoft Azure. Deploy Catalyst SD-WAN in cloud environments through the Cisco Catalyst 8000V edge Software or the Cloud Services Router C8000V Series.

Further information on Cisco edge device compatibility can be found here edge Devices

Note additional functionality deployed on Cisco edge devices such as Umbrella will be subject to validation and capacity of the edge device deployed.

5.12: Fujitsu SD-WAN Software Subscription Licensing

Fujitsu's SD-WAN Software subscription licensing aligns to the Cisco licence model, and we support the three feature tiers: Cisco DNA Essentials, Cisco DNA Advantage, and Cisco DNA Premier. Service Pack 2 is deployed with DNA Advantage as standard.

Benefits:

- The latest innovations through simple subscription tiers
- Easy licence portability across on-premises and cloud
- Easy upgrade across tiers

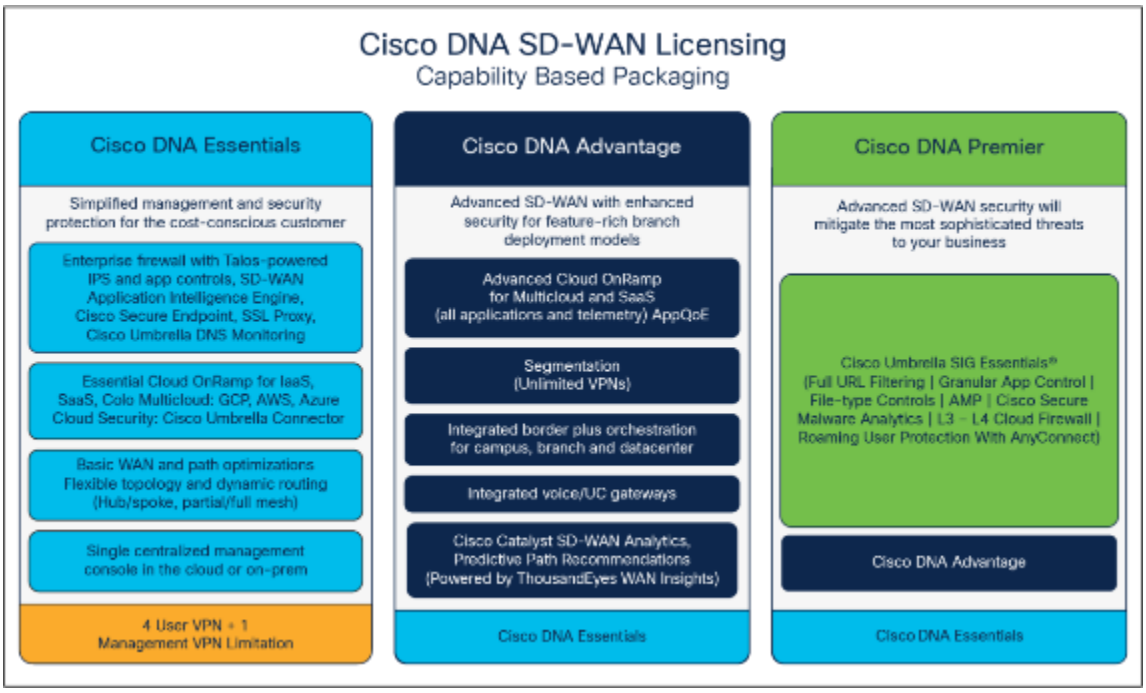

Figure 27: Cisco DNA Software subscription licensing for SD-WAN and routing

5.13: Prominent Features

- Vendor approved Software deployed after functional testing completed.
- Integrated security uplifts.
- Uplifts to Distributed Security Enforcement (DSE) framework, which includes - Embedded security (Next Generation Firewall), fabric security, SD-WAN integration with cloud security, monitoring and visibility and certifications and compliance. Subject to Information Assurance and device capacity
- On-premises Security with ability to support NGFW, Advanced IPS, AMP with Sandboxing, URL-Filtering, TLS proxy, Unified logging, Identity Firewall support.
- Optional Cloud Security Integration with Cisco Umbrella for an integrated single vendor SASE Solution.
- Modular SASE solution through integration with third-party SSE cloud security provides, including Zscaler, Netskope, Palo Alto, Cloudflare, and Skyhigh.
- Integration with third-party SIEM, including Splunk, Microsoft Sentinel and Live Action, enhances monitoring and visibility, offering actionable insights into network and security events.
- A centralised view of network security events with actionable threat data for security operations centre teams through the Catalyst SD-WAN Manager Security dashboard.
- Routing intelligence and threat intelligence on a certified trustworthy infrastructure.
- Separate and dedicated components for the control plane, data plane, and management and orchestration of the WAN.
- Flexibility to implement overlay, underlay, physical, and virtual networks.
- Voice and unified communications support.
- IPv6 support (BGP, OSPF).
- Robust IP multicast support
- Enables network traffic control, enhances efficiency by eliminating traffic redundancy, and reduces server and CPU loads.
- Efficiently handles one-to-many or many-to-many communications.
- Provides multicast capability across platforms (Protocol Independent Multicast Source-Specific Multicast [PIM-SSM], Internet Group Management Protocol [IGMP] v2, and IGMP v3).

5.14: Support for Security and Information Assurance

Fujitsu will support the Buyer certification process and consultancy for the SD-WAN service. This will be subject to confirmation upon agreement over Buyer requirements (as detailed in the Statement of Work). Access to the Orchestration high-level design documentation will be provided to the Buyer to support accreditation activity. Please note associated ITHC tests requested by the Buyer to support the accreditation process will be charged using the rates from the agreed published SFIA Rate Card.

6: Service Pack 2 Fujitsu SD-WAN Service Delivery

Fujitsu's ISO/IEC 27001, operations are certified by Bureau Veritas (Reference IND17.0595/UUK002399). Fujitsu implements the following best service and security practice:

- Established Data Protection Act program across Fujitsu's UK business
- Certified for Cyber Essentials for Fujitsu EMEA
- Certified for Cyber Essentials Plus DNS UK operations
- Fully compliant with ISO/IEC20000 IT service management
- Business continuity planning certified to ISO/IEC22301:2012
- Fully complies with ISO27002-2013 Information Technology – Security Techniques
- Operates ISO27036 – for supply chain security
- A relationship model aligned to ISO440001.

An active participant in:

- The Information Security Forum, Standard of Good Practice
- Information Security Forum Securing the supply chain – implementation guide
- Information Security Forum Securing the supply chain – preventing your suppliers' vulnerabilities becoming your own.
- HMG's joint best practice security working groups.

To enable certification continuity across all procedures and operations, Fujitsu carries out the Deming "Plan-Do-Check-Act" (PDCA) cycle.

Fujitsu is an ITIL® aligned and ISO/IEC20000-1 conformant supplier, and deploys, manages, and continually improves Service Management processes that are underpinned by standard technologies.

6.1: Service Management

Fujitsu is an ITIL® aligned and ISO / IEC20000-1 conformant supplier, and deploys, manages and continually improves Service Management processes that are underpinned by standard technologies.

The Service Management process that Fujitsu will deploy for managing the Service will include the following key processes and functions:

- Incident Management
- Problem Management
- Event Management
- Change Management
- Availability Management
- Capacity Management.

Fujitsu's Service Pack 2 is a Buyer managed service based on the Cisco Catalyst SD-WAN software, with Fujitsu enhancements to support Higher Information Assurance requirements. All service management facilities are provided in the UK from Fujitsu Defence and National Security offering a Sovereign based solution. The SD-WAN orchestrators and management tooling are deployed in Fujitsu's certified UK datacentres supported with UK Facility Security Clearance (FSC) (formerly known as List X) UK facilities for service operations. The service and Buyer portals are managed by UK Fujitsu staff all holding at a minimum SC security clearance.

The Buyer's attention is drawn to the Responsibilities Matrix in Table 5 below. This table details the extent of the operational management responsibilities of the Buyer or Fujitsu (unless enhanced via the optional service catalogue). In all cases service requests and support will be delivered via the nominated Fujitsu SD-WAN Service Desk as advised.

6.2: Service Demarcation Responsibilities

The table below provides the service demarcation points between the Buyer and Fujitsu further clarity will be provided in the Statement of Work if required:

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
Underlay Provision	Buyer	Buyer responsible for all connectivity and bearer performance
Fujitsu will provision hosted controllers for SD-WAN overlay and Cisco SD-WAN Manager with access for the Buyer.	Fujitsu	
Monitoring and troubleshooting of Fujitsu's SD-WAN Cloud controller infrastructure / CPU and Data Disk Utilisation	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Protective Monitoring by Fujitsu will comprise of the Monitoring and troubleshooting of Fujitsu's SD-WAN Cloud controller infrastructure, based on MITRE ATT&CK framework Service using Elasticsearch, Kibana and Logstatsh stack.	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Buyer responsible for edge device monitoring, firewall configuration connection of new devices or the monitoring of data traversing the network	Buyer	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
Buyer is responsible via the Fujitsu portal/ SD-WAN Manager controller SecOps dashboard to view and manage network security events and actionable threat data to effectively maintain its cyber resilience. An optional SIEM feed can be provided to the Buyer.	Buyer	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring and troubleshooting of Fujitsu's SD-WAN Cloud controller infrastructure/Loss of connectivity to network interfaces	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring and troubleshooting of Fujitsu's SD-WAN Cloud controller infrastructure/Failure to reach instances	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu's SD-WAN services /Availability of the Fujitsu Portal	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu's SD-WAN services/Loss of control connection to the controllers	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Disaster recovery/Take periodic volume-based snapshots	Managed by Fujitsu	The volume-based and config-based snapshot is for the entire platform Cisco SD-WAN Manager cluster, not for a particular tenant.
Disaster recovery/Take periodic configuration-based backups	Managed by Fujitsu in accordance with its processes and procedures available upon request	The volume-based and config-based snapshot is for the entire platform Cisco SD-WAN Manager cluster, not for a particular tenant
Disaster recovery/On-demand snapshots	Managed by Fujitsu	The volume-based and config-based snapshot is for the entire platform Cisco SD-WAN Manager cluster, not for a particular tenant
Disaster recovery/Restore overlay based on volume or configurations	Managed by Fujitsu	The volume-based and config-based snapshot is for the entire platform Cisco SD-WAN Manager cluster, not for a particular tenant
SD-WAN Analytics	Buyer to manage Fujitsu to support	LiveAction (LiveNX) Analytics is by default onboarded for cloud-delivered Cisco Catalyst SD-WAN Buyers.
Renew controller certificates (before expiration)	Managed by Fujitsu	
Upgrade software/Controller software upgrade	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Upgrade software/edge device/node software upgrade	Managed by Fujitsu	
Respond to Fujitsu notifications to authorise the service window, instance reboot, review, or verify changes carried out by Fujitsu	Buyer	
Accept external management of SA/VA and map tenant VA to Buyer's SA/VA	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
Define configure and deploy device configuration templates and policies through Cisco SD-WAN Manager	Buyer	Note Buyer responsible for defining policies and resulting performance
Perform user activities that require logging in to Cisco SD-WAN Manager. For example, template and policy configuration, and edge device management	Buyer	Note Buyer responsible for defining policies and resulting performance
Web server certificates	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
edge serial sync with credentials	Buyer	Cloud-delivered Cisco Catalyst SD-WAN Buyers can sync edge serials without credentials (using Single-Sign-On)
Before making any changes in the Portal, take the on-demand snapshot using the procedure, and configuration backup using procedure	Buyer	

Table 7: Service Demarcation Responsibilities

6.3: Fujitsu Cloud Infrastructure Support

- Fujitsu will carry out disaster recovery workflows, including snapshot volumes or configurations. Restore Cisco SD-WAN Manager clusters based on volumes or configurations.
- Fujitsu will provision custom subnetting to extend Buyer premises network into cloud-hosted overlay network.

6.4: Fujitsu Capacity Management

Fujitsu will monitor the growth of devices per overlay along with the controller instance capacity parameters such as CPU, disk, and memory utilisation. Follow a pre-set guideline to increase the capacity of the service instances as needed.

7: Service Pack 2 Fujitsu SD-WAN Service Levels

Fujitsu SD-WAN Core Service shall meet or exceed the performance standards described below ("Service Level").

7.1: Service Availability.

Service	Availability Target	Availability Measurement
Catalyst SD-WAN Core Service	99.99%	24x7x365 over a quarterly period. Availability will be defined as the ability of the core platform to provide SD-WAN "Data Path Functionality between edge nodes
High Availability (HA) Sites	99.99%	24x7x365 over a quarterly period. edge device availability will be defined as the ability for the edge HA solution to route traffic in accordance with the routing and policies programmed from the Catalyst SD-WAN Manager to provide defined SD-WAN functionality (assumed Fujitsu managing)
Standard Sites (Single edge)	99.99%	24x7x365 over a quarterly period. edge device availability will be defined as the ability for the edge device to route traffic in accordance with the routing and policies programmed from the Catalyst SD-WAN Manager to provide defined SD-WAN functionality (assumed Fujitsu managing)

Table 8: Service Availability SLAs

7.2: Service Level Response Time

Service Measure	Description	Support Hours	Target Response Time
Priority 1 (Major) Standard	Major business disruption: critical user or user group unable to operate, or an entire service experiencing significant reduction in system performance	Incident resolution 09:00-17:00 Mon-Fri GMT/BST excluding any public holidays with uplifts to 24x7 365 support cover see catalogue Note platform monitored 24x7 365 days. Faults may be reported 24x7 365 days	1 hour
Priority 1 (Major) Premium	Major business disruption: critical user or user group unable to operate, or an entire service experiencing significant reduction in system performance	24x7x365 days	1 hour
Priority 2 (Medium)	Partial service disruption to a live/production service.		2 hours
Priority 3 (Low)	Minor disruption: single user or user group experiencing problems, but with circumvention available.		8 hours
Priority 4 (Very Low)	Enquiry: single user or user group requiring assistance but with no direct impact on business. For example, a request for information.		24 hours

Table 9: Service Measure

7.3: Edge Device SLAs

7.3.1: High Availability edge sites

	Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1)	Performance Indicator only
HARDWARE	**P1**	Hardware failure of All edge devices preventing site connectivity.	24x7x365	30 minutes	8 hours	98% of all hardware faults fixed within 8 hours	100% of hardware faults fixed in 24 hours.
	P2	Hardware failure of a single edge device not preventing site connectivity.	24x7x365	30 minutes	72 hours	98% of all hardware faults fixed within 72 hours	100% of hardware faults fixed in 96 hours.
SOFTWARE	**P1**	Failure of All edge devices preventing site connectivity.	24x7x365	30 minutes	4 hours	98% of all faults (where remote support capable) fixed within 4 hours	100% of faults where remote support capable) fixed within in 8 hours.
	P2	Failure of a single edge device not preventing site connectivity.	24x7x365	30 minutes	8 hours	98% of all faults (where remote support capable) fixed within 8 hours	100% of faults where remote support capable) fixed within 24 hours.

Table 10: edge Device SLAs – High Availability edge Sites

7.3.2: Standard edge sites

	Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1)	Performance Indicator only
HARDWARE	**P1**	Hardware failure of a single edge device preventing site connectivity.	24x7x365	30 minutes	12 hours	98% of all hardware faults fixed within 12 hours	100% of hardware faults fixed in 24 hours.
SOFTWARE	**P1**	Failure of a single edge device preventing site connectivity.	24x7x365	30 minutes	4 hours	98% of all faults (where remote support capable) fixed within 4 hours	100% of faults (where remote support capable) fixed within in 8 hours.

Table 11: edge Device SLAs – Standard edge Sites

7.3.3: Edge Device Replacement SLAs

Service	Support Hours	Resolution Time	Resolution Target (1)
High Availability Sites	24x7x365	72 hours	100% of all hardware replacements delivered to site within 72 hours
Standard Sites	24x7x365	72 hours	100% of all hardware replacements delivered to site within 72 hours

Table 412: edge Device SLAs – Replacement SLA

All service levels have a target that 95% will be fixed within the SLA, subject to a minimum volume as advised.

The incident period is measured based on the timings from ITSM; from incident raised to the time at which the incident is set to 'resolved'.

7.4: Service Desk

Fujitsu's Service Desk will provide a Single Point of Contact for incident recording, updates and resolution or fault diagnostics to your IT Staff. Fujitsu will diagnose and analyse faults and manage the fault through to resolution. Access to the Fujitsu UK Service Desk to log Incidents and Service Requests is available 24x7 via telephone or email.

Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1) (SLA)	Resolution Target (2)
P1	Severe business disruption: Any existing core servers are unavailable or unable to be managed. Loss of all network connections or firewalls at core datacentres	24x7x365	30 minutes	4 hours	98% of all hardware faults fixed within 4 hours	100% of hardware faults rectified in 8 hours
P2	Major business disruption: Application services are unavailable or unable to be managed. Loss of a network or firewall connection at core datacentres Loss of core resilience but service to site operating	24x7x365	1 hour	8 hours	90% in 8 hours	100% in 16 hours
P3	Minor business disruption: Authority unable to manage resources within the user portal	Monday to Friday 0800-1700hrs (Excluding Bank Holidays)	5 hours	3 working days	90% in 3 working days	100% in 6 working days

Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1) (SLA)	Resolution Target (2)
P4	Minor disruption. Single user or user group experiencing problems with the user portal or API, but with circumvention available.	Monday to Friday 0800-1700hrs (Excluding Bank Holidays)	1 working day	5 working days	90% in 5 working days	100% in 10 working days
P5	Enquiry: Single user or user group requiring assistance but with no direct impacts on business. Example: a request for information or change request.	Monday to Friday 0800-1700hrs (Excluding Bank Holidays)	2 working days	10 working days	80% in 10 working days	100% in 20 working days

Table 513: Core Platform SLAs

7.4.1: Problem Management Priority Levels and Definitions

Ref	Definition	Resolution Target (1)	Performance Indicator
PM1	**Level 1 (P1):** The Problem poses significant risk to the Buyers business or operations in that the Incident or series of Incidents may result in significant adverse impact to the Buyers operations. No Workarounds have been identified to Resolve the Problem.	10 Working Days	20 Working Days
PM2	**Level 2 (P2):** The Problem poses no immediate risk to the Buyers business or operations but may, if not Resolved, result in degradation in the performance of a Service. Workarounds are available to Resolve the Problem.	1 Month	40 Working Days
PM3	**Level 3 (P3):** The Problem poses no risk to the Buyer business or operations but may in the long term impact on the overall performance of a Service	6 Months	N/A
PM4	The percentage of all Problems occurring during the Service Measurement Period that Fujitsu has Resolved within the relevant Resolution Time for each Problem. Problems shall only be considered as validly Resolved	95%	100%

Ref	Definition	Resolution Target (1)	Performance Indicator
	if the service desk has Resolved the Problem and notified the Buyer that it has Resolved such Problem by completing the relevant sections of the relevant Problem Record.		

Table 614: Problem Management SLAs

7.5: Service Reporting

Service Reporting encompasses the production and delivery of defined reports to accurately report against agreed Service Level Agreements. Excluding the Daily Service Update Report, which only provides volumetric data.

Fujitsu will provide the following reports on a Daily, Monthly and Quarterly basis:

Daily Reporting

Daily Service Update Report

Generate the Daily Service Update Report each Working Day with respect to the immediately preceding Working Day (Monday – Friday)

Information pertaining to Saturdays and Sundays to be included within Monday's report

Email the Daily Service Update Report to the SDM by 09:00 each day

7.5.1: Monthly Reporting

ITSM Monthly Service Reports (from SCSM)

- ITSM Service Reports are provided as part of the monthly service reviews and will generate the following pre-built reports on a monthly basis generated from the ITSM toolset:

Report Area	Report Name	Description
Change Management	List of Change Requests	Provides a list of change requests within a certain time frame. The data in this report includes the current status, category, and user to whom the request is assigned.
Incident Management	Incident Resolution	Provides the number of incidents, including the number of incidents past their targeted resolution time and the average time to resolution. You can filter the data by day, week, month, quarter or year.
Incident Management	List of Incidents	Provides a list of all incidents within a certain time frame. The data in this report includes the users to whom incidents are assigned, when the incidents were created, and the current status of the incidents.
Problem Management	List of Problems	Provides a list of all problems within a certain time frame.
Security Incident Management	List of Incidents	Provides a list of all security incidents within a certain time frame. The data in this report includes the users to whom incidents are assigned, when the incidents were created, and the current status of the incidents.
Configuration Items (CIs)	List of CIs	Provide a list of all CIs within the estate

Table 715: ITSM Monthly Service Reports

7.5.2: Additional Monthly Reports

- Forward Schedule of Change (derived via SCSM)
- Forward Schedule of Release (derived via SCSM)
- Patch Compliance Report/Statement of Conformance.

7.5.3: Quarterly Reporting

- Availability Reports

8: Service Pack 3 SD-WAN solution for the Law Enforcement Community

Service Pack 3 is a G Cloud SD-WAN service for the Law Enforcement Community (LEC) operating under the Police Digital Service (PDS) Police Assured Secure Facilities (PASF) scheme.

The description below provides a summary of the functionality of the service and optional services available, together with additional Buyer responsibilities if invoking the use of Buyer provided edge devices or licences.

Service Pack 3 is based on the Cisco Catalyst SD-WAN solution and complementing applications. The service provision is based on the Buyer managing the SD-WAN end user service using web application portals provided by Fujitsu. Service Pack 3 also comprises of service management options from Fujitsu calculated using the SFIA rate card as detailed in the catalogue.

Fujitsu SD-WAN enables Buyers to transform IT infrastructure by delivering network connectivity that's cloud-agnostic, efficient and simpler to manage, lowers operational costs and increases control and visibility across the entire digital service delivery chain. Additional gateways or security devices as detailed in the optional catalogue may be required to reflect choice of network bearers by the Buyer which shall be advised in the Statement of Work

8.1: Solution Overview and Description

Fujitsu's SD-WAN connects a user to Buyer approved applications with integrated capabilities for multicloud handoffs, security, predictive operations, and enhanced network visibility. Fujitsu's SD-WAN enables a Buyer to transform its IT infrastructure by delivering network connectivity that's cloud-agnostic, efficient and simpler to manage, lowers operational costs and increases control and visibility across the entire digital service delivery chain. Fujitsu's SD-WAN Manager provides a secure visualised dashboard that simplifies network operations. It provides centralised configuration, management, operation, and monitoring across the entire SD-WAN fabric. As agreed between the Buyer and Fujitsu

Fujitsu's SD-WAN can offer integrated security, including full-stack multilayer security capabilities as optional services. Fujitsu SD-WAN can be fully integrated with Cisco Umbrella, which offers protection against security blind spots and cyberthreats (hosting of Cisco Umbrella will be in nominated Cisco datacentres).

Using the SD-WAN Manager (Figure), a Buyer can connect to all their datacentres, core and campus locations, branches, colocation facilities, cloud infrastructure, and remote workers. To enable this interconnection, Fujitsu SD-WAN applies the Overlay Management Protocol (OMP) to the entire network. Fujitsu's SD-WAN simplifies IT operations with automated provisioning, unified policies, and streamlined management.

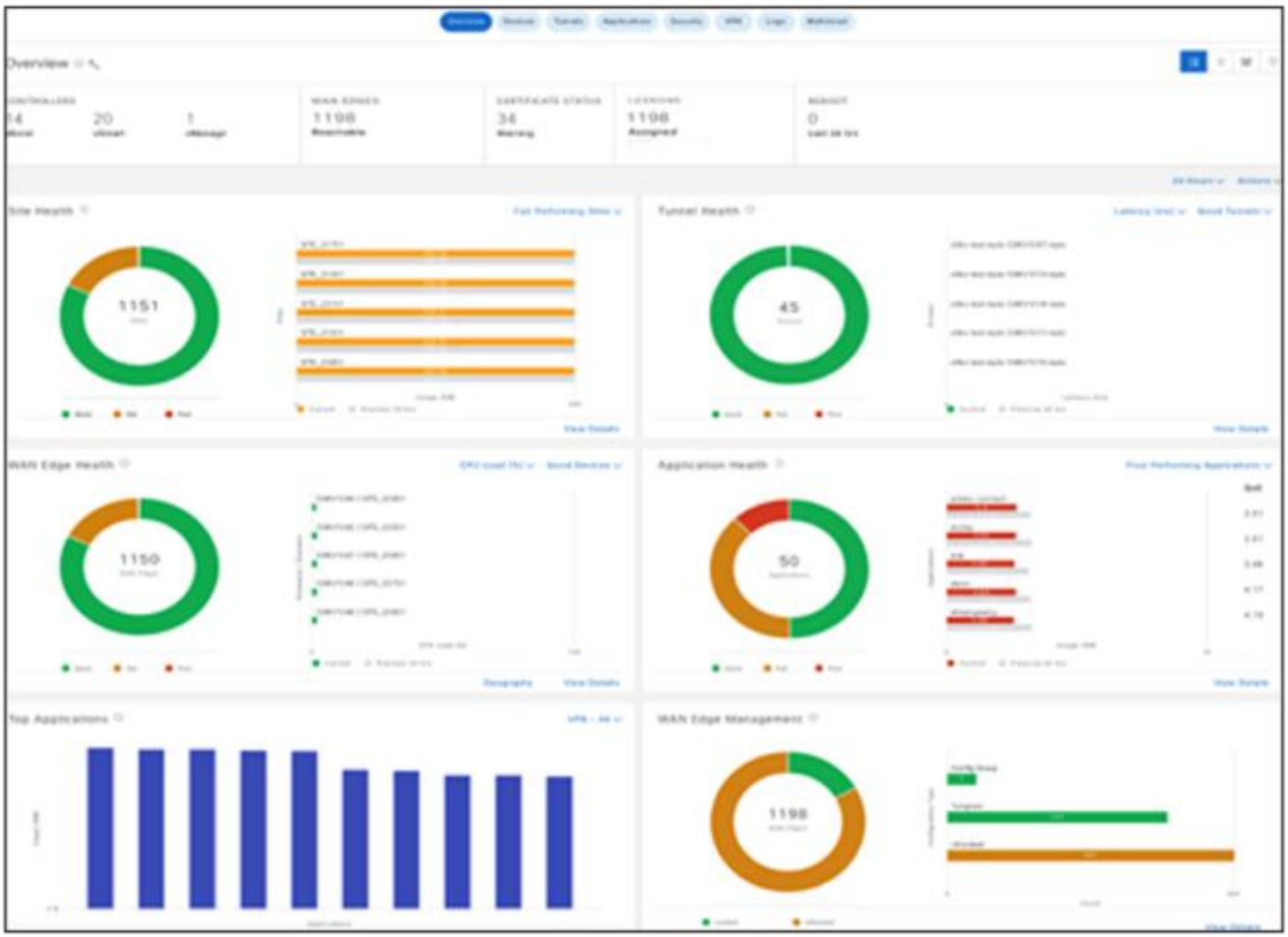

Figure 28: Fujitsu SD-WAN Manager dashboard showing network and application health

Fujitsu's service provides a flexible architecture to extend SD-WAN to any environment (Figure 29) Fujitsu's SD-WAN automatically discovers, authenticates, and provisions both new and existing devices.

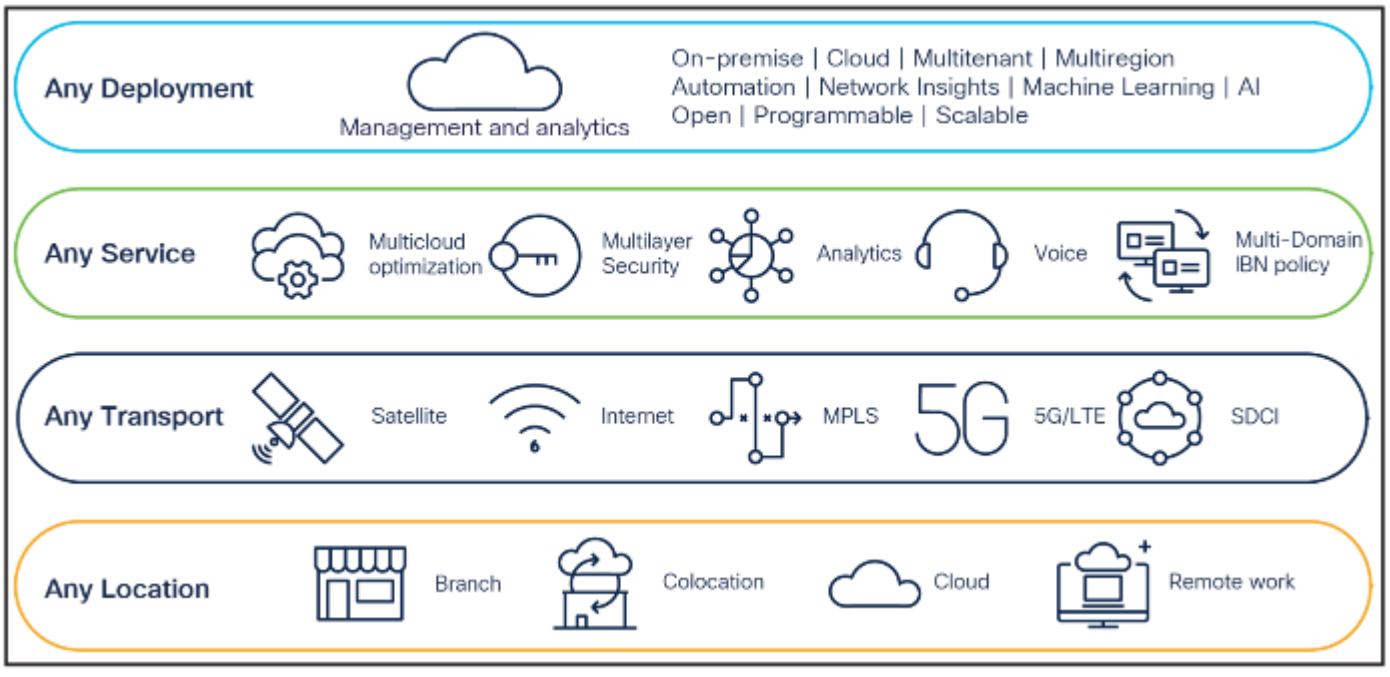

Figure 29: Flexible and scalable architecture for network transformation

8.2: LEC Service Pack 3 Constraints (Standards, Policies and Guidelines)

The solution described will be delivered in accordance with NCSC guidelines.

8.2.1: Aligns to PDS PASF assurance.

The known guidance documents are listed below:

a. Network Security

b. Using IPSec to Protect Data

c. Using TLS to Protect Data

d. Cloud Security Guidance

8.2.2: Service Pack 3 for LEC is delivered in accordance with the Buyers Security Aspects Letter (SAL).

Service Pack 3 comprising of a Fujitsu's SD-WAN service enables Buyers to manage and or out-task the management operating over Buyer provided network connectivity and is called an overlay network. For the LEC, network connectivity comprises of the PSNfP / PSN Assured (sun setting), a private MPLS network replacement for PSNfP, Internet connectivity, 5g (ISP) or satellite and is called the underlay network).

The Fujitsu's SD-WAN service includes SD-WAN network design, delivery, project management, SD-WAN network maintenance and SD-WAN network security services using the SFIA rate card.

Fujitsu's SD-WAN service comprises of the following main components:

a) **Core Platform –** Orchestration, management and control using Fujitsu's SD-WAN vManage, vBond and vSmart appliances. The core platform is operated with high availability in centralised compute infrastructure from Fujitsu's UK Facility Security Clearance (FSC) (formerly known as List X) locations.

b) **Edge devices –** The SD-WAN edge devices are deployed on Buyer sites, private clouds, and public clouds.

c) **SD-WAN Overlay –** The SD-WAN overlay provides encrypted data path connectivity between SD-WAN edge routers. The SD-WAN Overlay is transported over the Buyer provided underlay network infrastructure.

d) **Analytics portal –** Non-Cloud-based analytics provide an overview of SD-WAN network performance over time. This functionality is supported using Live NX hosted in UK Facility Security Clearance (FSC) (formerly known as List X) locations.

8.2.3: The Fujitsu's SD-WAN baseline service:

a) Manages SD-WAN components of the solution and their connectivity to a number of transport networks (the underlay networks).
b) Maintains secure management and control plane connectivity between the SD-WAN edge devices and the core platform.
c) Maintains the set of standard encryption tunnels built between the SD-WAN edge routers as required by the agreed SD-WAN overlay network topology.
d) Maintains the set of encrypted Security Associations between the edge devices as required by the overlay network topology.

8.2.4: The Fujitsu's SD-WAN monitors and reports via portals availability but does not maintain or operate the various underlay networks that the SD-WAN overlay is using for connectivity.

8.2.5: The Buyer shall provide routing policies. Application performance requirements shall be the responsibility of the Buyer to test.

8.2.6: The standard SD WAN service demarcation is shown below.

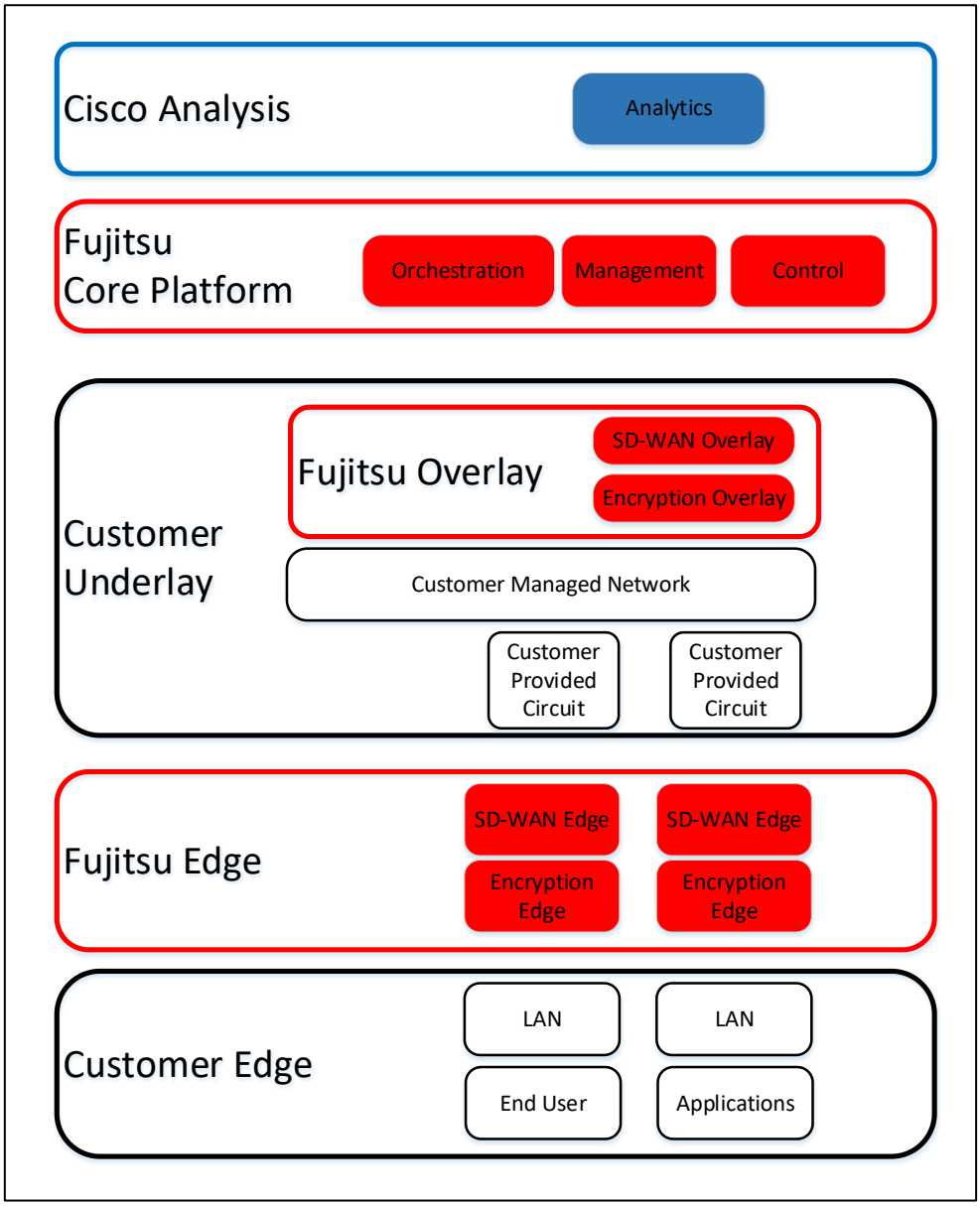

Figure 30: Standard SD-WAN Service Boundaries

8.2.7: Where the Fujitsu's SD-WAN management and control plane is running in Fujitsu infrastructure then Fujitsu shall also be responsible for incident and problem management for that infrastructure to ensure the control plane is available within the committed Service Level Agreement.

8.2.8: The G-Cloud SD WAN service demarcation is shown below.

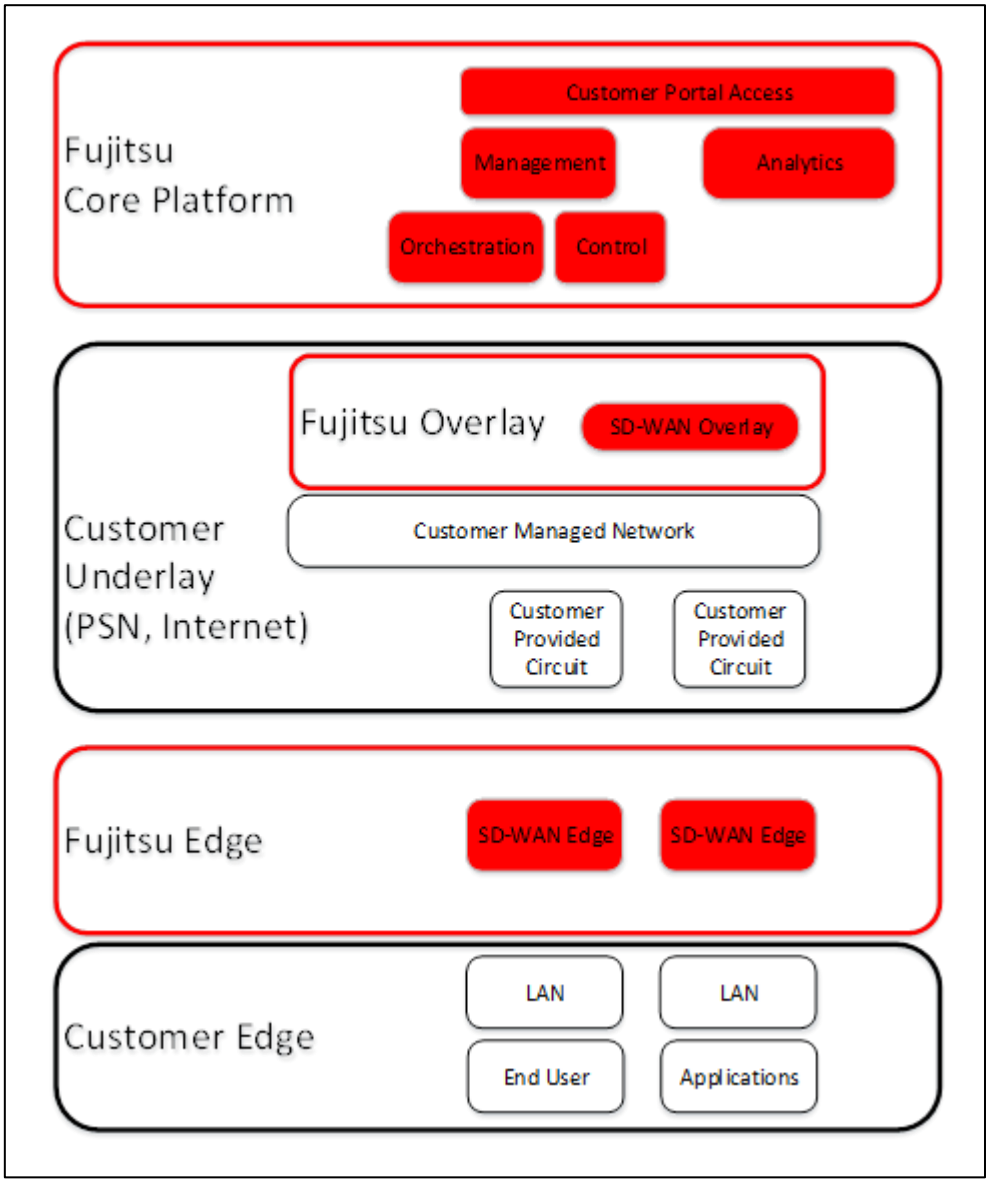

Figure 31: SD-WAN Service Boundaries

8.2.9: Fujitsu's SD-WAN solution combines Cisco SD WAN capabilities, as published by Fujitsu (functionality guide) with Network Function Virtualization (NFV) in a single Universal Buyer Premises Equipment (uCPE), as illustrated in figure 32

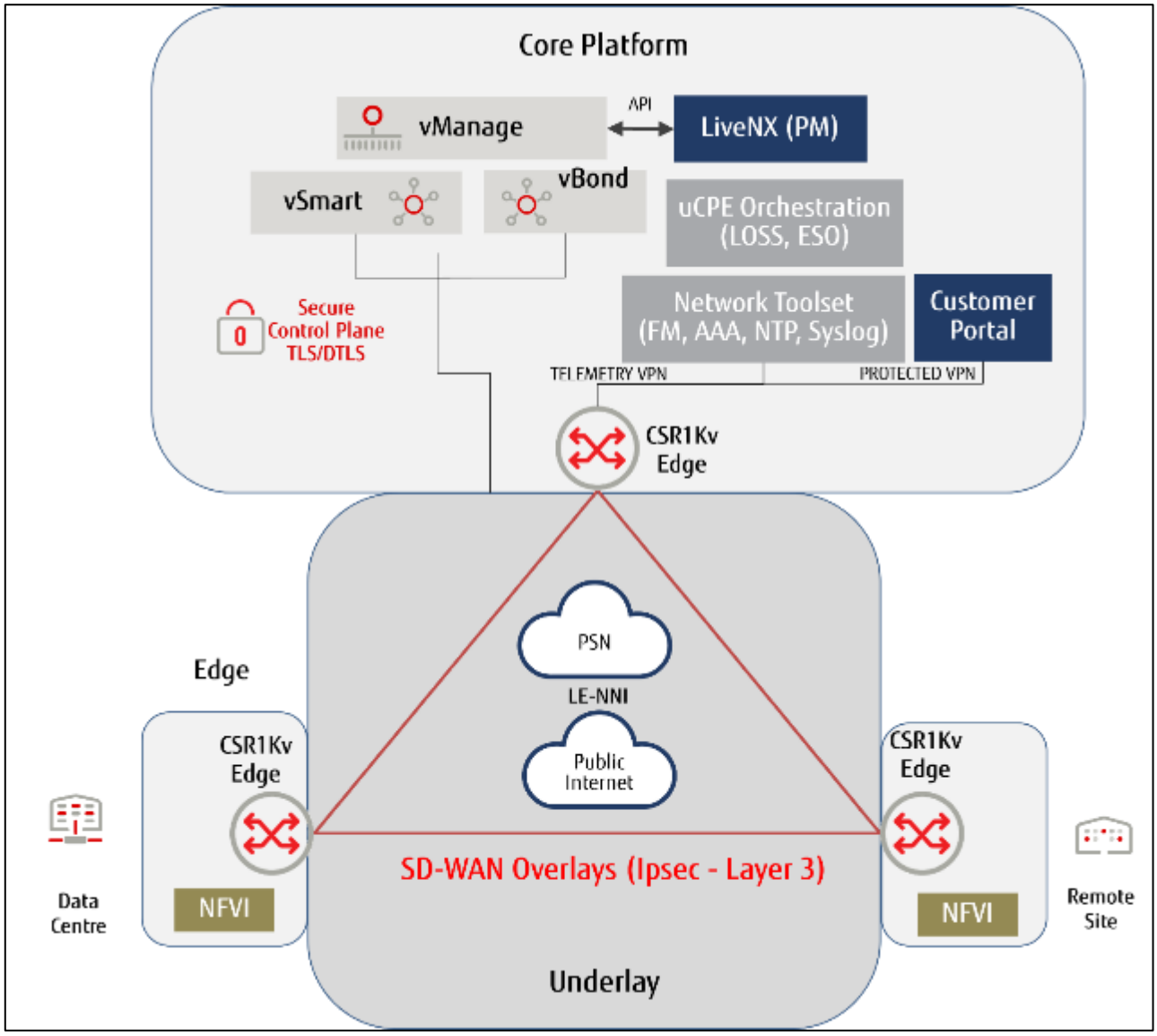

Figure 32: Fujitsu's SD-WAN Architecture

8.2.10: The Core Platform provides the SD WAN service orchestration, management and control functions and includes the following main solution components:

a) edge uCPE orchestration

i. Fujitsu Lightweight Operation Support System (LOSS) enables secure near zero-touch on-boarding of uCPE at Buyer sites. Adva Ensemble Service Orchestration (ESO) completes the on-boarding process with secure VNF service chain orchestration.

b) SD-WAN overlay management and control

i. Cisco vManage is a centralised dashboard that facilitates automatic configuration, management and monitoring of the SD WAN overlay network and SD WAN edge routers. Users login to vManage to centrally manage all aspects of the network life-cycle from initial deployment, ongoing monitoring and troubleshooting to change control and software upgrades.

ii. Cisco vSmart Controllers establish Secure Socket Layer (SSL) connections to all other components in the SD WAN network. They also run an Overlay Management Protocol (OMP) to exchange routing, security, and policy information. The centralised policy engine in vSmart Controllers provides policy constructs to manipulate routing information, access control, segmentation, extranets and service chaining.

iii. Cisco vBond Orchestrator facilitates the initial SD WAN router bring-up by performing authentication and authorisation of all elements into the network. Cisco vBond Orchestrator also provides the information on how each of the components connects to other components.

c) Network Performance

i. LiveNX performance management tool provides network and application analysis and reporting. The LiveNX appliance supports application monitoring and analysis.

d) Buyer portals

i. Buyer Portals are provided for the Cisco vManage and LiveNX management appliances. Remote access is provided to authorised users. Access to the portals is authorised by Role based Access Control (RBAC).

ii. The Buyer Portal provides web server access via a proxy service on the SD WAN overlay to Buyers.

iii. The Buyer Portal does not provide a Remote Access Service for access via the internet.

e) Infrastructure and enterprise management

i. Network Toolsets complete the management solution, with Zabbix event management, LiveNX performance management, real-time clock provision with Network Timing Protocol (NTP), Elasticsearch syslog collectors, private Domain Name System (DNS) servers, Public Key Infrastructure (PKI) services and Role Based Access Control (RBAC) authentication, Veeam backup and recovery services (BAR), file import/export facilities (IMPEX), download servers, firewalls, intrusion prevention/detection services (IPS/IDS) and anti-virus checking.

ii. Syslog messages generated by SD-WAN edge devices (C8000v, EC), managers (vManage) and controllers (vBond, vSmart) shall be forwarded to a nominated central Buyer syslog server from the Elasticsearch syslog collector via the SD-WAN overlay.

8.2.11: The edge devices provide Network Function Virtualisation Infrastructure (NFVI) to host SD-WAN and encryption virtual edge appliances:

a) The edge devices are universal Customer Premises Equipment (uCPE) providing compute, memory and network resources using commercial, off-the-shelf (COTS) servers.

b) The uCPE is available with both single and dual power supply options to allow for value for money at standard sites and higher availability at critical sites.

c) uCPE devices can be deployed in both non-resilient and high availability configurations, with warm standby units provided at non-resilient sites to minimise service interruption in the event of a device failure.

d) uCPE devices are pre-staged with the (NFVI) and a basic factory default SD–WAN edge router with WAN/LAN port connectivity in Fujitsu's secure pre-staging facility.

e) Once the uCPE has been installed on-site, using Fujitsu engineering or smart hands, it is on-boarded to the SD-WAN manager and controller using Fujitsu's Virtual edge on-boarding process.

f) After validation of the site installation, the SD-WAN edge is admitted to the SD-WAN overlay.

g) Once connected to the LEC toolset, the NFVI can be managed remotely from the ESO/LOSS toolset to modify the uCPE and SD-WAN service chain.

8.2.12: The SD-WAN overlay provides intent-based routing of the Buyers applications over segmented virtual private networks (VPNs) using IPsec encrypted tunnels:

a) The Fujitsu's SD-WAN overlay uses the underlay and internet transport networks.

b) The Fujitsu SD-WAN overlay provides network connectivity between SD-WAN edge routers.

c) The overlay protects data in transit using IPsec tunnels with PKI certificate-based authentication, AES-256 encryption and centralised key management.

d) The Fujitsu SD-WAN edge is deployed as a C8000v virtual router on the uCPE hosting platform.

e) C8000v edge routers are located at the Buyer site or in the cloud and provide data plane connectivity between sites via the SD-WAN overlay.

f) The edge routers provide packet forwarding decisions, policies and processes at each site in conjunction with the centralised vSmart controllers.

g) Fujitsu SD-WAN provides centralised dynamic routing using the vSmart controller and the Overlay Management Protocol (OMP).

h) The Fujitsu SD-WAN edge combines proactive overlay performance monitoring with application based routing policies to enable optimisation of network path selection.

i) Policies can be independently defined for applications, application groups, network segments (VRFs) and sites to meet different organisational and business needs.

j) Cflowd policies can be configured to gather and export detailed application flow information for analysis in the vManage and LiveNX management appliances.

k) The Fujitsu SD-WAN edge router includes a stateful enterprise firewall capability with application awareness.

8.3: Core Platform

8.3.1: Orchestration, Management and Control Architecture

a) The Core Platform provides orchestration, management and control of the integrated uCPE, SD WAN and analysis functions in a high availability (HA) architecture, as illustrated in Figure 33

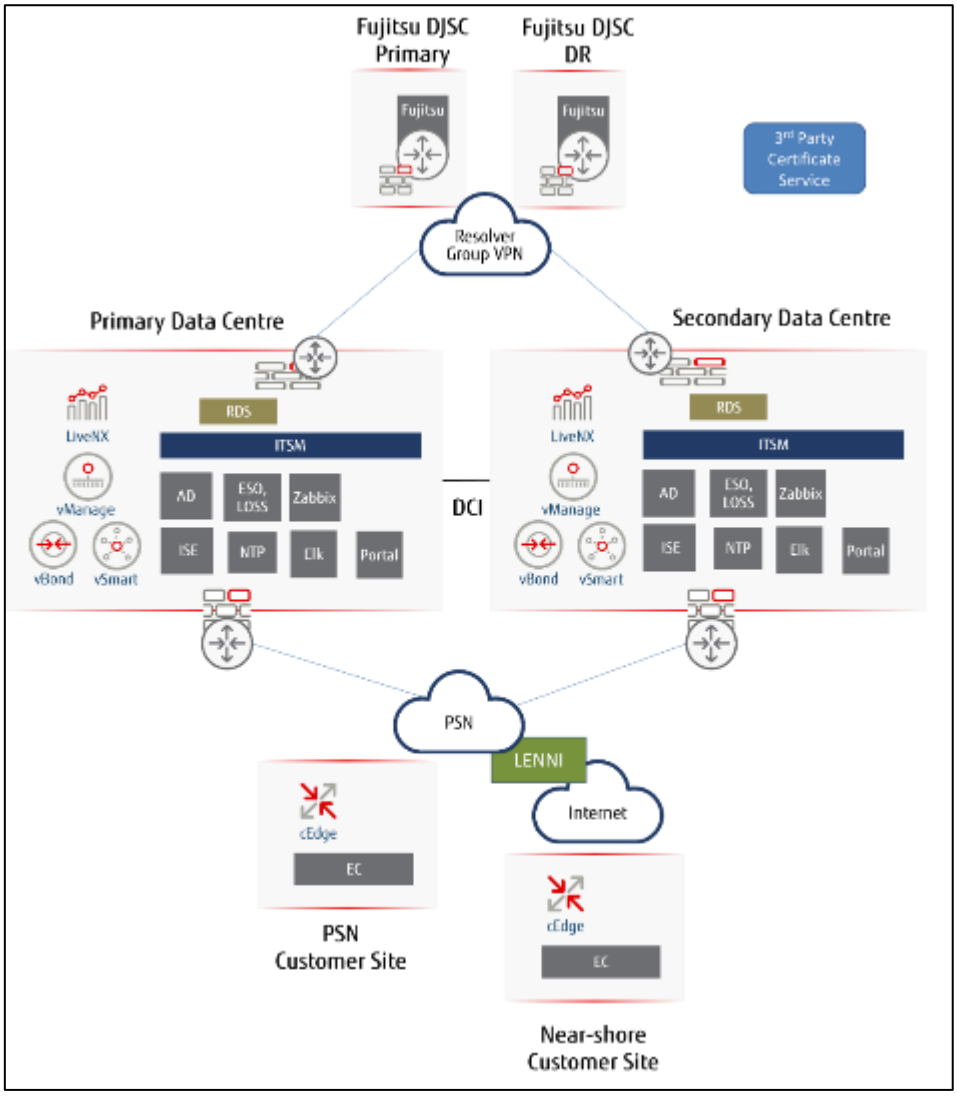

Figure 33: High Availability Toolset

b) The primary and secondary toolsets will be hosted on the Service platform operated at an OFFICIAL-SENSITIVE handling caveat.
c) The toolset will enforce secure protection of the Buyer data through use of secure management protocols, network and transport layer encryption, encryption of sensitive data at rest, security event logging and role-based access control.
d) The Fujitsu SD-WAN toolset will be deployed in a High Availability architecture, with each management, orchestration and controller appliance protected from failure by a backup appliance in the geo-separated secondary datacentre.
e) Individual appliances will be operated in active/active or active/standby mode, depending on the appliance and the service provided.

8.3.2: Toolsets

a) The LEC Catalyst SD-WAN toolset components of a single datacentre are illustrated in Figure 34

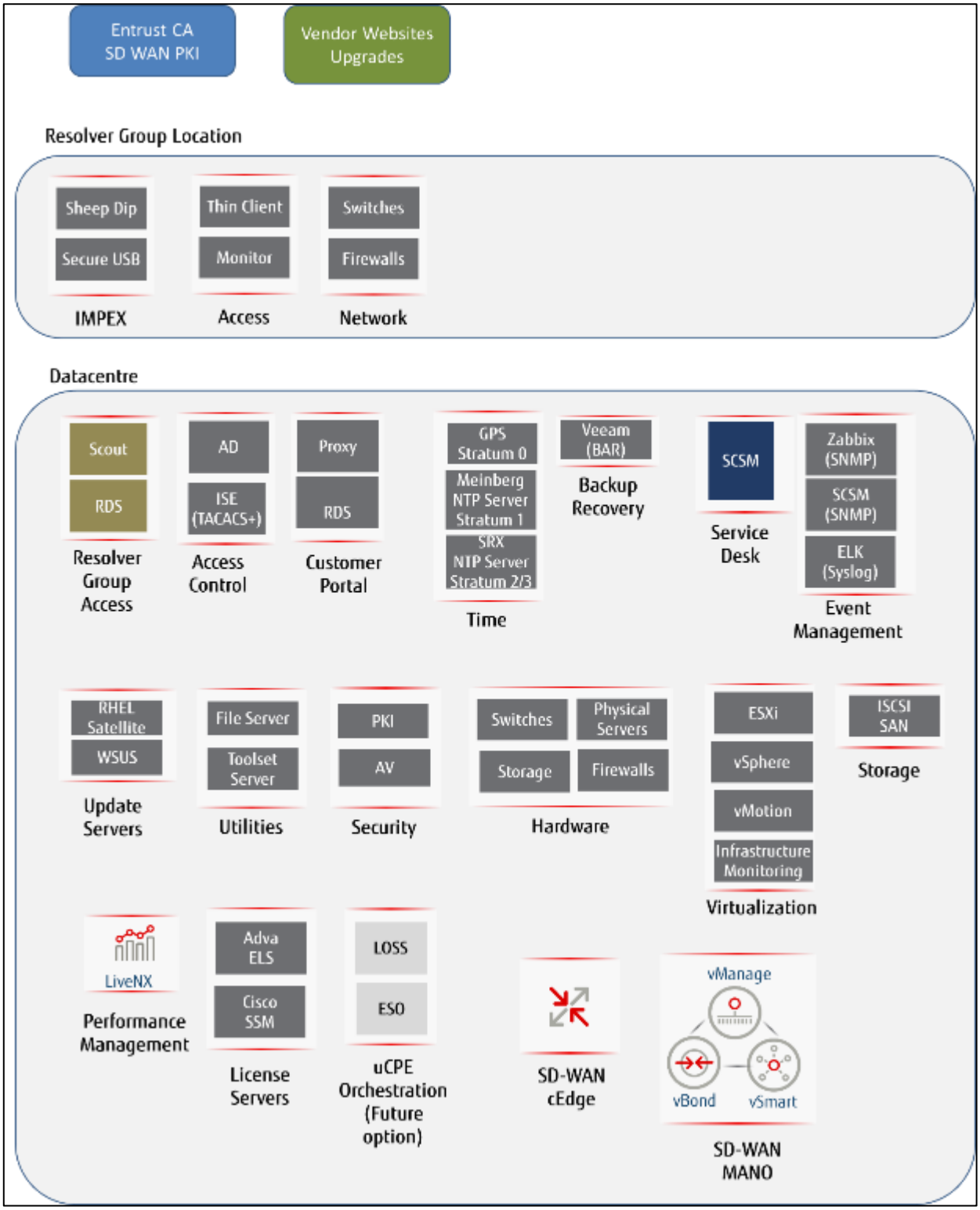

Figure 34: SD-WAN Toolset Components

b) The toolset is split into shared tools, providing management support for multiple Buyers operating at the same security classification, and dedicated tools supporting a single Buyer, as illustrated in figure 35.

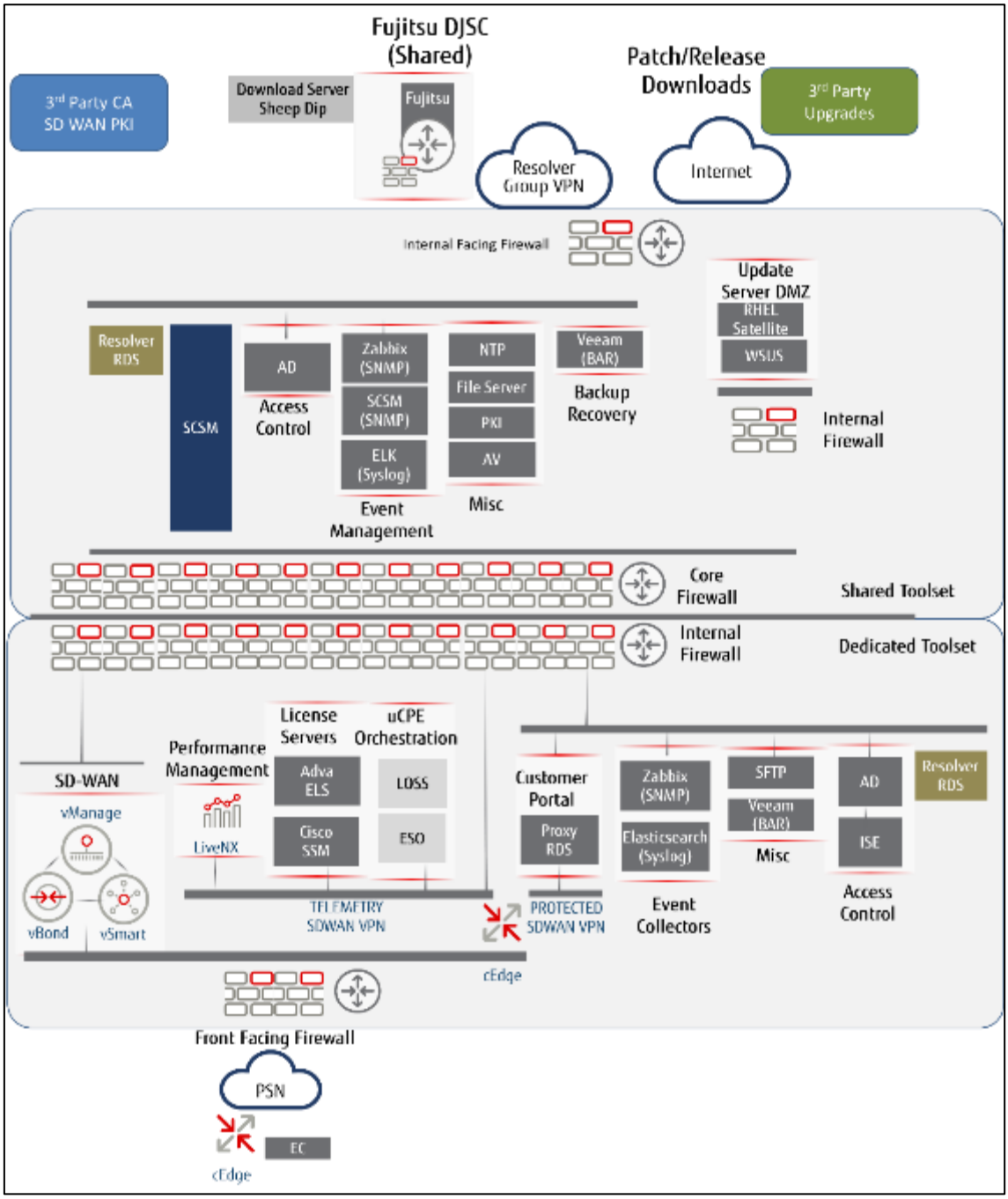

Figure 35: Dedicated and Shared Toolsets

c) The following toolset appliances and applications are shared with other Fujitsu SD-WAN Customers:

i. Windows System Centre Services Manager (SCSM)
ii. Windows file server
iii. Windows Server Update Services (WSUS)
iv. Redhat Linux (RHEL) satellite server
v. Mcafee anti-virus
vi. Windows Access Directory (AD)
vii. Meinberg NTP time servers with GPS time source.
viii. SCOUT terminal server and shared Remote Desktop Servers (RDS).
ix. Internal PKI CA
x. Keepass password manager

xi. Sheep dip with Symantec anti-virus

xii. Zabbix

xiii. Elasticsearch, Kibana and Logstash (ELK) stack

xiv. Veeam

xv. VMware vSphere (ESXi and vCentre)

d) The shared toolset supports the following functionality:

i. **Event Management:** Separate Zabbix proxies are provided to collect event notifications in each dedicated Buyer zone. The Zabbix servers in the shared zone provide management access to dedicated Buyer domains, event correlation capabilities and automated SCSM ticket generation.

ii. **Security event management:** Separate Elasticsearch collectors are provided in each dedicated Buyer zone. In the shared zone, an Elasticsearch, Kibana and Logstash (ELK) stack provides management access to dedicated Buyer domains and event correlation capabilities. ELK is integrated with Zabbix.

iii. **Internal Public Key Infrastructure:** The toolset provides PKI for web services and internal encryption services.

iv. **Access Control:** Microsoft Access Directory (AD) provides domain control in the shared zone with role-based access control (RBAC). The shared AD domain controller manages access to the dedicated zones.

v. **Fujitsu Toolset access:** The shared zone provides SCOUT terminal servers to enable remote access from resolver group thin clients. The shared Remote Desktop Server (RDS) provides access to the shared tools and access to the dedicated Buyer zones via a separate RDS in each zone.

vi. **Password management:** The shared Keepass generates and stores complex passwords for local accounts.

vii. **Real Time Clock:** All network devices and toolset appliances are locked to a common Universal Time Co-ordinated (UTC) source, provided by the toolset Network Timing Protocol (NTP) server. The NTP is locked to a Global Navigation Satellite System (GNSS) stratum 0 clock and provides a stratum 1 timing source.

viii. **Patching:** WSUS and RHEL satellite servers provide automated solution for identifying and downloading patches for Windows and Linux servers.

ix. **Import/Export:** Download server and sheep-dip antivirus servers are provided to facilitate secure import and export of files, including software images and reports. Files are downloaded, checked for viruses and malware and copied to a secure USB for transfer to the thin client and download to the shared toolset file server.

x. **Backup and recovery:** Veeam is used to provide automated file and VM server backup for replication and disaster recovery.

xi. **Virtualization Infrastructure:** VMware vSphere provides the datacentre virtualisation platform.

e) The following toolset appliances are dedicated to Service Pack 3 SD-WAN users:

i. Fujitsu SD-WAN vManage, vBond, vSmart

ii. Performance Management: LiveNX

iii. uCPE orchestration: ESO, LOSS

iv. Syslog collector: Elastic Stack

v. Event management collector: Zabbix

vi. Keepass password management

f) Note: The SD WAN vManage, vBond, vSmart and LiveNX applications are dedicated for LEC (per user group) to support sensitive configuration and application data relating to the network and user applications.

i. **uCPE Orchestration:** The Fujitsu Lightweight Operation Support System (LOSS) and Adva Ensemble System Orchestrator (ESO) provide orchestration of the uCPE, the Kernel-based Virtual Machine (KVM) hypervisor (edge Connect), Virtual Network Functions (VNFs) and service chaining. LOSS and ESO are only used during service chain orchestration.

ii. **SD WAN:** The SD-WAN toolset includes the Cisco SD-WAN orchestrator (vBond), controller (vSmart) and manager (vManage). vManage provides single pane of glass management of Fujitsu's SD-WAN solution and include REST API for integration with other toolsets.

iii. **Event Collector:** edge device events and notifications are forwarded to the Zabbix event management collector using SNMP traps.

iv. **Security Event Collector:** Syslog messages are reported to the dedicated Elasticsearch collector. The Elasticsearch syslog collector relays messages to the Buyer's Security Incident and Event Management (SIEM) platform via the SD-WAN overlay.

v. **Performance Management:** The LiveAction performance management solution (LiveNX) is fully integrated with vManage and provides network Service Level Agreement (SLA) reporting and application analysis.

vi. **Public Key Infrastructure:** The SD-WAN solution uses a 3rd party certificate signing service (Entrust Platinum) as the root certificate authority (root CA), with the SD-WAN vManage acting as the PKI root CA for the edge devices.

vii. **Password management:** The dedicated Keepass generates and stores complex passwords for local accounts in the dedicated toolset and remote network devices.

viii. **Buyer Portal Access:** A dedicated windows server proxy provides secure user access to the LEC dedicated SD-WAN and LiveNX toolsets.

8.3.3: Management Connectivity

a) The following table summarises the LEC SD-WAN toolset management and control connectivity.

Remote Function	Toolset Device	Secure Communication Channel	Datacentre Terminating Network Device	Transport Network
Fujitsu Resolver Groups	Thin client and Remote Desktop Service	[redacted]	[redacted]	[redacted]
Buyer Portal	Proxy and Remote Desktop Server	[redacted]	SD-WAN cEdge (C8000v) (Dedicated)	MPLS / PSN / LENNI SD-WAN overlay – PROTECTED
Buyer SIEM	Elasticsearch syslog collector	[redacted]	SD-WAN cEdge (C8000v) (Dedicated)	[redacted]
vManage, vBond, vSmart	vBond	[redacted]	vBond	MPLS / PSN/Internet underlay
vManage, vSmart	vManage, vSmart	[redacted]	vManage, vSmart	MPLS / PSN/Internet underlay
cedge (C8000v)	vManage, vSmart	[redacted]	vManage, vSmart (Dedicated)	MPLS / PSN/Internet underlay
cedge (C8000v)	vBond	[redacted]	vBond (Dedicated)	
	NTP server	[redacted]	cEdge (C8000v) (Dedicated)	MPLS/PSN/Internet SD-WAN overlay – Telemetry VPN
	Syslog		Syslog collector (Dedicated)	
	LiveNX (Flexible Netflow)		cEdge (C8000v) (Dedicated)	
	ISE (TACACS+)		cEdge (C8000v) (Frontend)	
	Zabbix (SNMP traps)		cEdge (C8000v) (Frontend)	
	LOSS/ESO		cEdge (C8000v) (Dedicated)	

Table 816: SD-WAN Management and Control Connectivity

8.4: Edge Devices

8.4.1: Universal CPE

a) The optional SD-WAN Virtual edge (shown in the figure 34 below) provided by Fujitsu is a universal Buyer Premises Equipment (uCPE) that supports virtual SD WAN edge routers and third-party Virtual Network Functions (VNFs) at aggregate WAN capacities of up to 4.5 Gbps. The Virtual edge supports both High Availability and Standard Availability modes of operation.

Figure 36: uCPE – Dell VEP 4600

b) The Virtual edge is provided in two variants, the VEP 4600 (8 port) and VEP 4600 (12 port).

c) Both the VEP-4600 variants fully support:

i. 4x WAN/LAN Ethernet ports

1. The VEP-4600 (8 port) has 4x 10/100/1000baseT RJ45 chassis ports and 4x 10/100/1000baseT RJ45 ports in one expansion slot. The 8-port variant supports 1x WAN port, 3x service VPN LAN ports and 3x service VPN WAN ports for pass-through connectivity, and 1x spare port.
2. The VEP-4600 (12 port) has 4x 10/100/1000baseT RJ45 chassis ports and 8x 10/100/1000baseT RJ45 ports in two expansion slots. The 12-port variant supports 1x WAN port, 3x service VPN LAN ports and 3x service VPN WAN ports for pass-through connectivity, and 5xspare ports for additional connectivity.

i. Kernel based Virtual Machine (KVM) with Ensemble Connect hypervisor supporting an open, standard interface for VNF service orchestration.

ii. SD WAN edge router (VNF)

d) Both uCPE are provided with the same compute and memory resource:

i. 8x vCPU

ii. 16GB RAM

iii. 240GB SSD storage

e) The DELL VEP-4600 edge device with dual power supply option.

i. Dual field replaceable power supply modules (1+1 redundancy)

ii. Field replaceable fan modules (3+1 redundancy)

iii. 4x RJ45 fixed chassis ports, with a factory fit option for an additional 4x or 8x RJ45 ports

f) The DELL edge devices and configuration build is deemed to satisfy the requirements of PDS / NPIRMT terminating hardware (end point devices) for encryption and the design deployed is subject to annual ITHC.

g) Implementation notes:

i. In order to support patching of the Intel Management Engine (e.g. to fix security vulnerabilities) an enhanced BIOS access level is required to allow remote upgrade.

ii. For the C8000v supports act/act HA using Virtual Router Redundancy Protocol (VRRP). In this mode traffic is switched between devices via an external WAN/LAN facing switch.

iii. The end user must provide resilient WAN/LAN interfaces and WAN/LAN facing switches to support HA operation using VRRP.

8.4.2: Edge device Topology

a) The LEC universal CPE service chain provides support for the following Virtual Network Functions (VNF) and external port connectivity:

i. C8000v VNF.

ii. C8000v VNF external WAN0 Ethernet port connectivity, which is associated with the pre-staged WAN IP configuration.

iii. Additional C8000v VNF external Ethernet ports, which are assigned to cedge service VPNs during on-boarding.

iv. C8000v VNF internal port for connection to the Ensemble Connect host.

b) Once on-boarded, the SD-WAN edge device ports are configured as defined in the following figure 37.

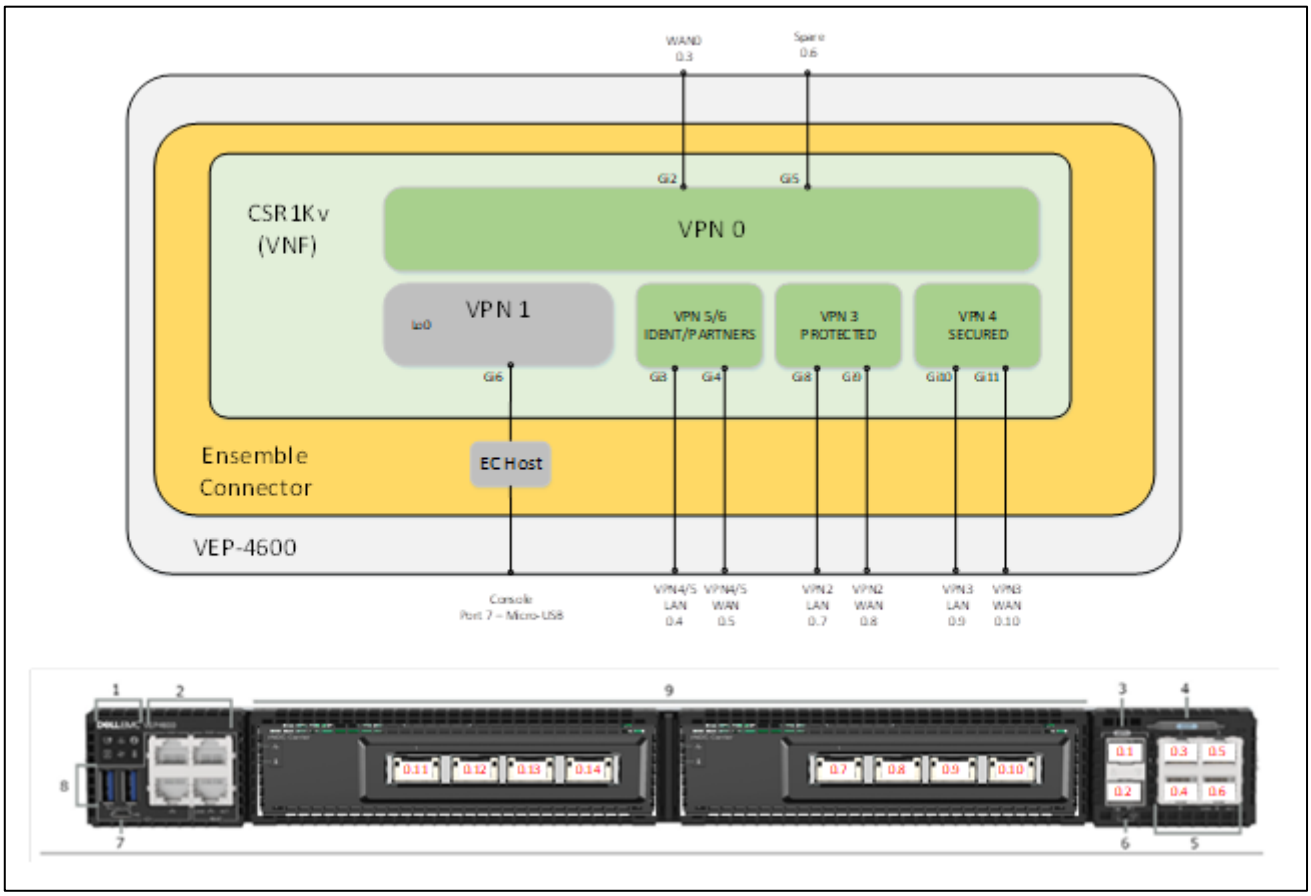

Figure 37: SD-WAN edge – Port Connectivity

c) The VEP-4600 console port provides access to the Adva EC host.

d) Local console access to the C8000v cedge is provided via the Adva EC host and requires separate user authentication.

8.4.3: Universal CPE (Dell 4600 Replacement Device)

Advantech FWA-3050 / 3051

The Advantech range, uCPE device, from Fujitsu replaces the Dell VEP-4600 devices.

The Advantech range supports:

- Throughput of 1Gbps to 2.5Gbps.
- Dual power supplies (e.g. datacentres or high availability sites).

The Advantech range employs the same NFVI, cEdge and SAT solution, but provides additional computing resource for improved throughput performance.

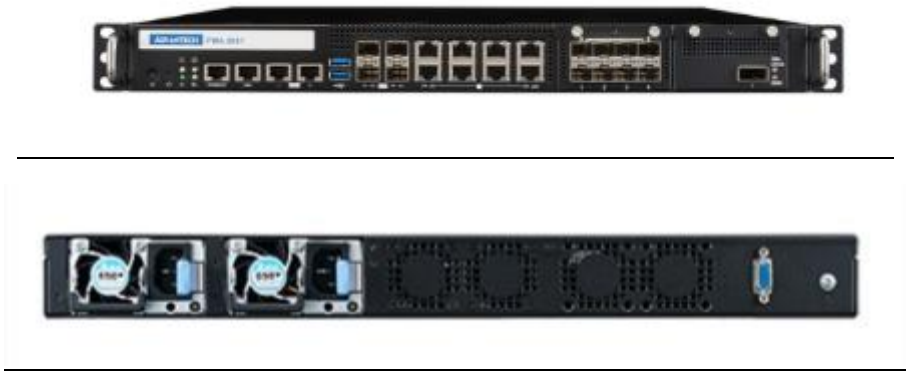

Figure 38 uCPE Advantech FWA-3050/ 3051

The following table summarises the technical specifications of the Advantech .

Parameter	Specification	Notes
Model	Advantech FWA-/ 3050 or 3051	Selection by Fujitsu depending on through put requirements or SD-WAN functionality deployed.
Chassis network ports	8x RJ45 (10/100/1000baseT)	Used for WAN/LAN connectivity
	4x SFP/SFP+ (1Gbps/10Gbps)	Used for 10Gbps WAN/LAN and fibre WAN connectivity. Used for connecting UCPE secondary and warm standby devices using TLOC extensions
Network Module Cards	8x SFP+ (10Gbps)	Optional NMC-1012
Management Ports	1x RJ45 (Console)	Serial console port
	2x RJ45 (10/100/1000baseT)	Management LAN
	1x IPMI 2.0	Baseboard Management Controller (BMC)

USB	2x USB 3.0 Type A	USB 3.0 Mounting from USB is disabled at the end of OBC build
	1x VGA Display Port	Rear mounted VGA
Wi-Fi module	None	
Processor	Intel Xeon D-2876NT	
CPU	8 or 16x CPU	
Memory	24 or 32GB	
Storage	2TB	Internal SSD
Operating System	Rocky OS	Built during OBC build
NFVI	Adtran EC	Built during OBC build
Switch	Adtran EC - vSwitch	Configured by LOSS
Hypervisor	Adtran EC - KVM	VNF build by LOSS

Table 17 uCPE (Advantech Technical Specification)

8.5: SD-WAN Overlay

8.5.1: Overlay Network

a) The SD-WAN overlay provides IPsec encrypted connectivity between SD-WAN edge devices, as illustrated in the following figure 39.

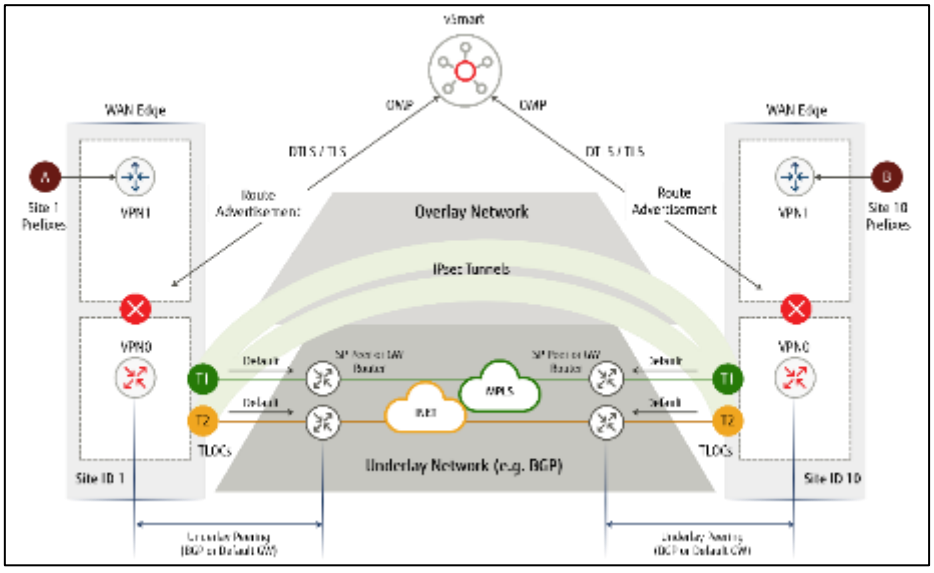

Figure 39: SD-WAN Overlay Site to Site Connectivity

a) The SD WAN overlay will provide:

i. Protection of confidentiality and integrity of Buyer traffic

ii. End-to-end segmentation of Buyer traffic using service VPNs.

b) The SD-WAN solution supports different VPN topologies in the SD-WAN overlay to satisfy different Buyer connectivity requirements.

c) VPN templates are used to control the network topologies that define how edge devices are connected via the overlay.

d) The following overlay topologies are supported:

i. Full mesh (default)

ii. Hub and spoke

iii. Dynamic mesh

e) The LEC Catalyst SD-WAN overlay topology will be configured in accordance with the information provided by the Buyer in the Cisco Site and Network Configuration & Application Policy Template.

f) Fujitsu SD-WAN overlay tunnels connected between MPLS / PSN connected sites shall be connected via the MPLS / PSN only.

g) Fujitsu SD-WAN overlay tunnels connected between internet connected sites shall be connected via the internet only.

h) The Buyer may, using Catalyst SD-WAN overlay tunnels, connect between MPLS / PSN and Internet connected sites, subject to dialogue with PDS/NPIRMT.

8.5.2: Overlay VPNs

a) The Fujitsu SD-WAN solution will be operated as a single organisation platform.

b) All Buyers (e.g. police forces and application providers) and Buyer networks (e.g. Closed User Groups or service VPNs) will use the SD-WAN transport VPN (VPN0) for connectivity of the SD-WAN overlay over the PSN/Internet underlay networks. VPN0 is the underlay network.

c) The Catalyst SD-WAN overlay will provide end-to-end segmentation of Buyer traffic, using Virtual Router Functions (VRF) in the service (Buyer LAN facing) side of the SD-WAN router and Virtual Private Networks (VPNs) across the SD-WAN overlay.

d) Fujitsu SD-WAN edge routers will maintain separate per-VPN routing tables for complete control plane separation.

e) Fujitsu SD-WAN overlay VPNs will be configured in accordance with the information provided by the Buyer in the Cisco Site and Network Configuration & Application Policy Template.

f) The SD-WAN overlay shall support the following VPNs:

i. VPN1: SD-WAN Telemetry (management).

ii. VPN2: Syslog

iii. VPN3: PROTECTED

iv. VPN4: SECURED

v. VPN5: IDENT1

vi. VPN6: PARTNERS

g) As a default Fujitsu SD-WAN will be operated with the following topologies:

i. PSN full mesh: All PSN connected sites, including LENNI edge devices, will be connected in a full mesh for the PROTECTED, SECURED, IDENT1 and PARTNERS VPNs.

ii. Internet full mesh: All internet connected sites, including the LENNI edge devices, will be connected in a full mesh for the PROTECTED, SECURED, IDENT1 and PARTNERS VPNs.

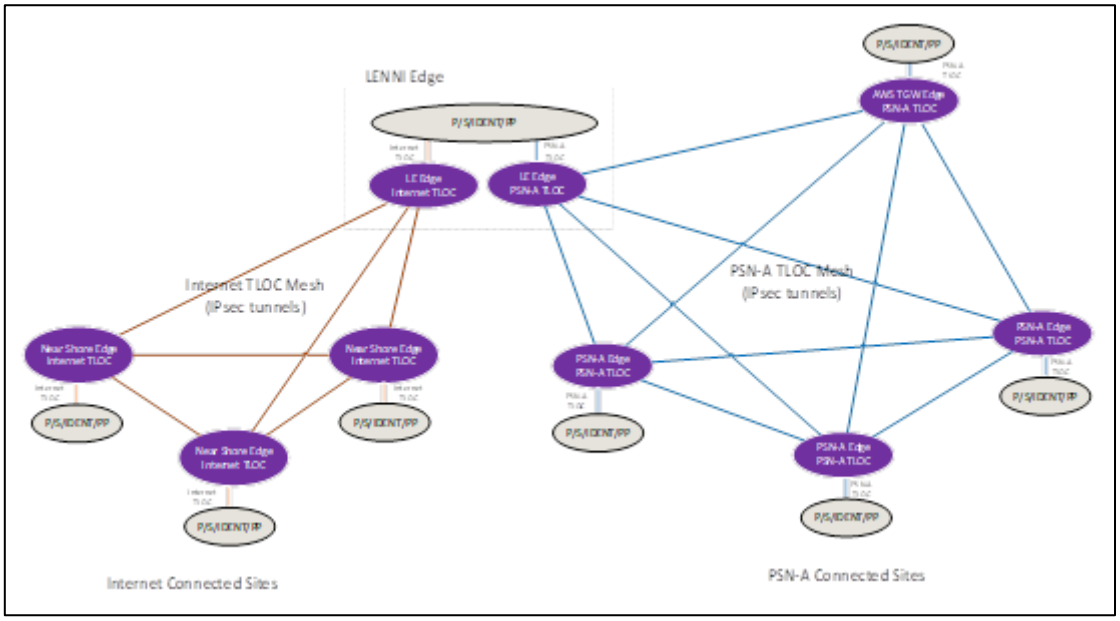

Figure 40: SD-WAN Service VPN Topologies

h) The SD-WAN Telemetry VPN (VPN1) is configured in a dual hub and spoke topology, providing resilient datacentre connectivity for each remote edge.

i. The LEC Syslog VPN (VPN2) is configured with connectivity limited to the SD-WAN datacentres and LENNI sites.

8.5.3: Dynamic Routing

a) The SD-WAN overlay supports dynamic routing between SD-WAN edge devices using the vSmart controller and Overlay Management Protocol (OMP).

b) Traditional dynamic routing protocols, including OSPF and BGP, can also be used in the service VPNs to learn routes in the Buyer LAN domain.

c) vSmart will advertise routes to each SD-WAN edge router in accordance with routing policies.

d) Routing policies shall be provided to route traffic that is being connected between PSN and internet connected sites via the LENNI SD-WAN edge.

e) Control policies will ensure symmetrical routing of traffic across the SD-WAN overlay.

8.5.4: Application Quality of Experience

a) The Fujitsu SD-WAN solution provides a multi-dimensional approach to Application Quality of Experience (AppQoE). An application bias is applied to traditional network functions like QoS and routing. Optimisation features are integrated into the router to supplement the networking functions.

i. **Application-Aware Routing:** This dynamically selects paths for specific application flows and groups based on SLA policies and real time network performance. It proactively manages application connectivity, replacing the old paradigm of selecting the most direct network path and hoping for the best. Note requires more than one network connection at the site.

ii. **Quality of Service (QoS):** QoS provides the basic traffic management functionality that allows application prioritisation. QoS includes traditional classification, policing, scheduling and shaping. AppQoE applies intelligence to the use of these facilities.

iii. **Forward Error Correction (FEC):** FEC and packet duplication features are used to remediate loss over poor quality circuits.

iv. **Application optimisation:** In addition to selecting the optimal path for an application, the SD-WAN solution also includes TCP optimisation. TCP optimisation fine-tunes the processing of TCP data traffic to decrease round-trip latency and improve throughput.

v. **Network connectivity:** Multiple high-speed transport network connections will be used to reduce latency and to provide path diversity.

vi. **Network analytics:** LiveNX virtual appliance supports individual network path and application flow monitoring. This will provide a rich data set that enables network diagnostics to proactively manage end user experience. Application analytics and reporting will identify poorly performing or congested network connectivity. Analysis will reveal how end users are using the network, which enhances focused network planning and capacity management.

b) The Fujitsu SD-WAN service includes capabilities to embrace migration to cloud based services.

i. **Cloud onRamp:** The Fujitsu SD-WAN solution optimises cloud connectivity by dynamically measuring SaaS application performance and selecting the best available path.

c) Details of the AppQoE features listed above are provided below.

8.5.5: Application Aware Routing

a) Application Aware Routing enables the ability to dynamically route traffic based on policies and real time connectivity performance (see figure 41 below).

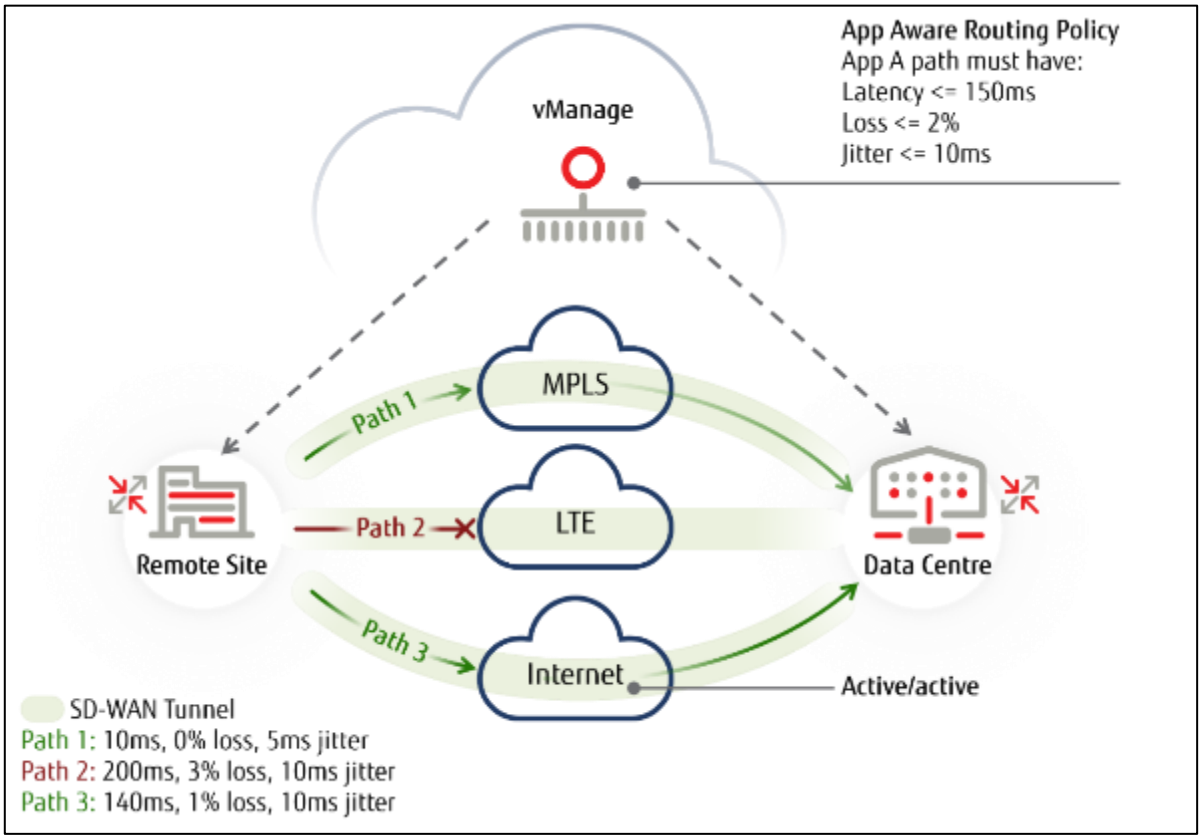

Figure 41: Application Aware Routing

b) Connectivity is monitored for latency, packet jitter and packet loss. Latency and jitter metrics enable policies to be defined for real time voice and video applications. Packet loss metrics identify network congestion, allowing applications to be diverted to a different path.

c) Localised and centralised policies can be defined to match applications and application groups, using one or more of the following criteria:

i. Source and destination IP address

ii. DSCP and Packet Loss Priority (PLP)

iii. Protocol

iv. Source and destination port

v. Custom source and destination prefix

vi. Next Generation Network-Based Application Recognition (NBAR2) application list

d) The Fujitsu SD-WAN edge router includes an integrated NBAR2 Deep Packet Inspection (DPI) engine to identify and classify applications including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. The NBAR2 DPI engine identifies a wide variety of applications from the network traffic flows using Layer 3 to Layer 7 data.

e) The Fujitsu SD-WAN edge Router supports the identification of TLS encrypted applications from Layer 3 (IP and DSCP) and Layer 4 (port and protocol) matching criteria.

f) Once an application or application group has been defined, a Service Level Agreement (SLA) is configured. The Service Level Agreement specifies the network path characteristics (loss, latency, and jitter) that the application can tolerate for optimised performance.

g) The Fujitsu SD-WAN solution monitors the performance of each network connection continuously, providing real time metrics to the local packet forwarding process and centralised controller. If a link is failing to meet the SLA targets defined for an application, the application will be diverted to the best available path (subject to any service definitions provided by the Buyer)

h) The Fujitsu SD-WAN edge routers use Bidirectional Forwarding Detection (BFD) to monitor all SD-WAN overlay tunnels. The BFD metrics are used to detect path liveliness and provide loss, latency and jitter quality measurements. The BFD metrics will indicate total loss of connectivity and service degradation.

i) The Fujitsu SD-WAN solution will use SLA-based policies to choose the optimal path for critical applications and will dynamically switch the path in the event those SLAs are not met.

j) The LiveNX analytics tool will provide reports based against the SLA policies in near real time. This information can be viewed by the Buyers via the portal provided.

k) These SLA policies define the rules for decisions made by Application-Aware Routing.

8.5.6: Fujitsu SD-WAN Overlay Quality of Service

a) The SD-WAN routers incorporate the QoS functions listed below, and illustrated in the following Figure 42:

i. Input classification

ii. Input policing

iii. Output policing

iv. Output rewriting

v. Output queuing and scheduling

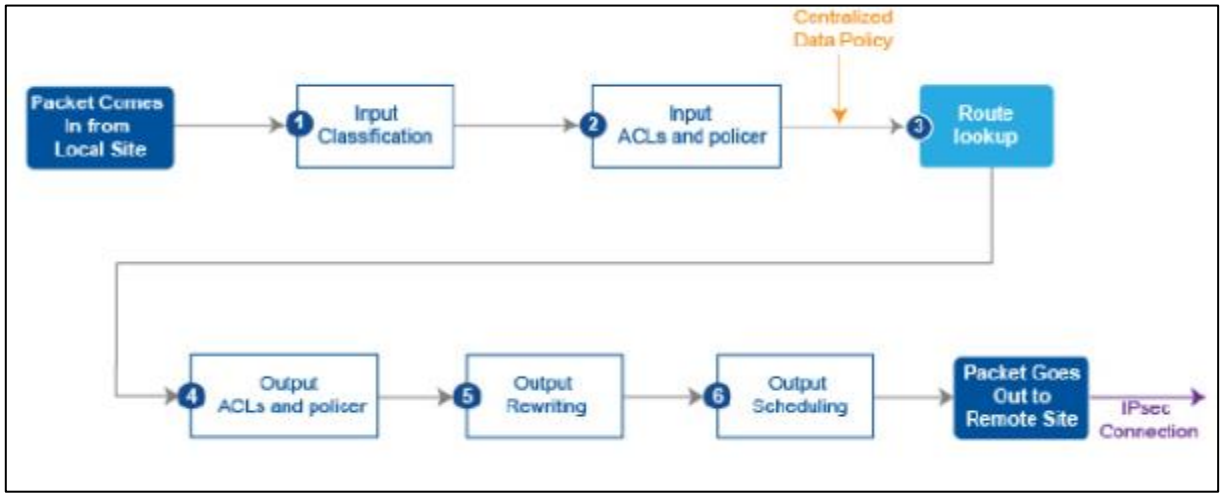

Figure 42: SD-WAN edge Router - QoS Components

b) Input classification maps packets to a defined traffic class, which is used later in the QoS pipeline to decide how a packet is treated.

c) The Fujitsu SD-WAN solution supports the classification of all packets based on:

i. Source and destination IP address,

ii. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers,

iii. Differentiated Services Code Point (DSCP) markings.

d) This allows the identification of IP conversations and applications by port utilisation, including applications that have been encrypted at Layer 4 using Transport Layer Security (TLS).

e) Deep Packet Inspection enables additional identification of unencrypted applications by including analysis of Layers 5-7.

f) The Fujitsu SD-WAN solution can be configured to treat Buyer LAN ports as trusted and map the end user DSCP markings to the outer header of the SD-WAN overlay IPsec tunnels, as shown in the Figure 43 below.

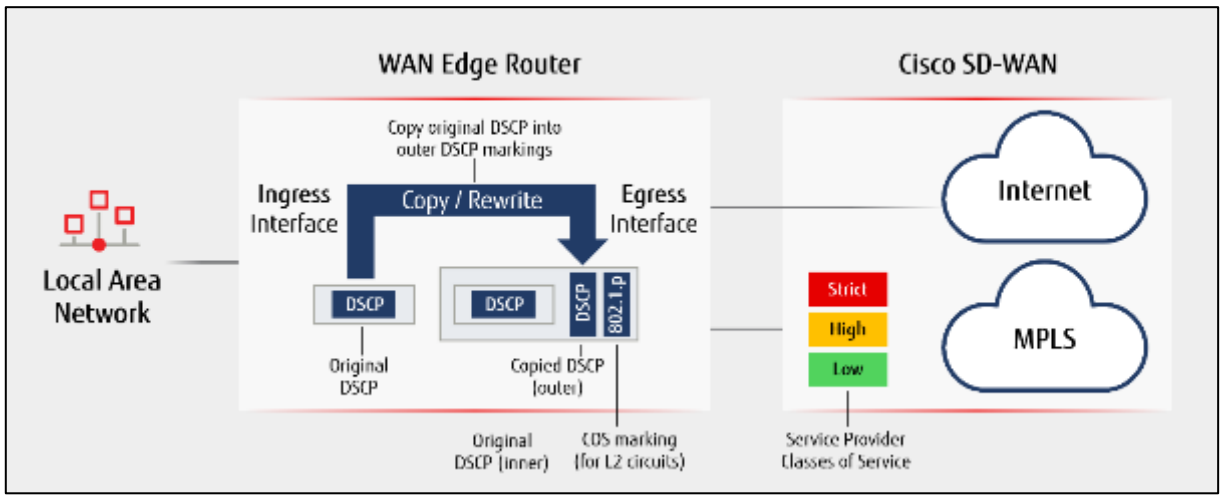

Figure 43: Overlay Tunnel DSCP Marking

g) If a port is untrusted, the SD-WAN router will mark the DSCP according to configurable policies. This ensures traffic classes will be honoured in QoS enabled transport networks such as the PSN.

h) If necessary, the Fujitsu SD-WAN edge router will re-mark the DSCP to ensure the flow is mapped to the correct traffic class in the transport network.

i) Queuing and scheduling allows traffic to be transmitted in order of priority at an interface. The SD-WAN router supports eight queues with a low latency queue for real time traffic.

j) Real-time applications are mapped to high priority traffic classes that ensure priority treatment in the SD-WAN router and QoS enabled transport networks.

k) The Figure below illustrates the mapping of traffic to strict, high and low priority queues according to application aware policies.

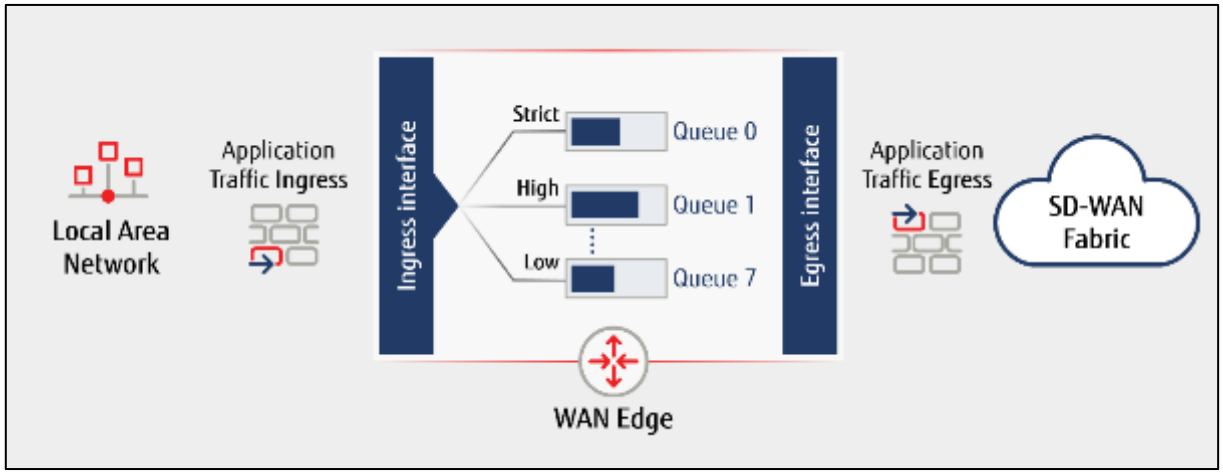

Figure 44: Application Aware Classification

l) Input and output policing controls the amount of traffic admitted or transmitted for a specified flow, application or application group. Non-compliant traffic is either re-marked for drop eligibility or dropped, depending on policy.

m) Shaping controls the maximum rate of traffic transmitted. Traffic will be queued until the shaper determines it can be transmitted in accordance with the defined rate. The SD-WAN router will use aggregate shaping at an interface to maintain compliance with the PSN/Internet WAN interface rate.

n) The Fujitsu SD-WAN solution supports the use of per-tunnel QoS at the hub sites of a hub and spoke topology to ensure smaller spoke sites are note starved of connectivity by larger sites sharing the same hub.

o) Per-tunnel QoS will shape the maximum rate of each SD-WAN tunnel, effectively partitioning the hub bandwidth between the spoke sites.

8.5.7: Fujitsu SD-WAN Underlay QoS

a) Underlay QoS is provided by the PSN or a private MPLS network

b) There is no QoS in the internet underlay

c) The DSCP marking of GRE and IPsec tunnels that are transported over the WAN transport network will be derived from the end user DSCP marking

d) Forward Error Correction (FEC)

e) FEC is a capability not supported by the baseline but available for deployment

f) FEC will recover lost packets on a link by sending extra "parity" packets for every pre-defined group of four packets. The receiving SD-WAN router will recover any lost packet from the group, using the received parity packet and performing an XOR calculation. This delivers user experience quality that is generally in line with MPLS. The Figure below demonstrates FEC and shows application packet number three lost on the WAN link:

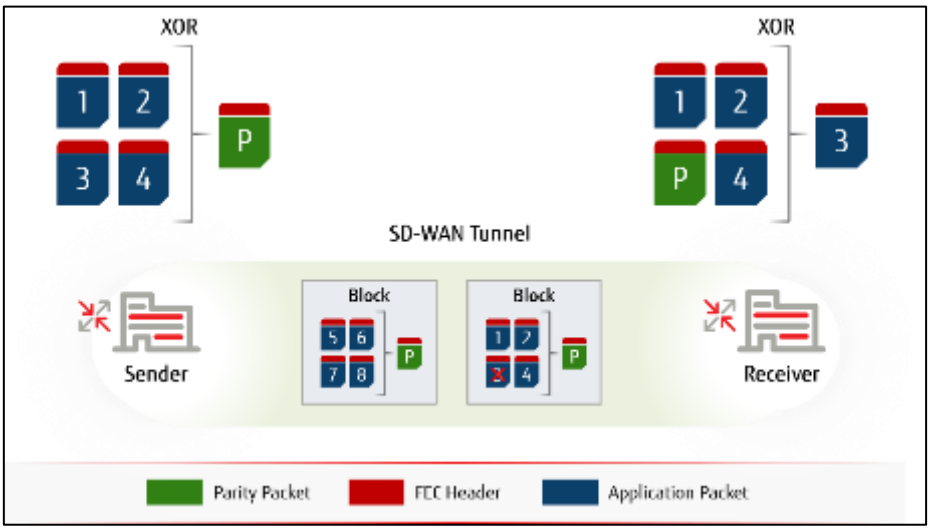

Figure 45: Forward Error Correction

g) FEC will incur bandwidth overhead (please seek clarity from Fujitsu as to impact) as it sends an extra packet for every four end user packets, but it does not duplicate every packet.

8.5.8: WAN Interface

a) Each SD-WAN edge device is capable of supporting up to four WAN network connections.

b) The Fujitsu SD-WAN edge solution supports 100Mbps, 1Gbps and 10Gbps Ethernet LAN and WAN interfaces (dependent on device selection). Sub-rate network connectivity is typically used to match the site bandwidth requirements of the site, ensuring value for money.

c) The Fujitsu SD-WAN router WAN interfaces can be shaped to the PSN/Internet CIR to ensure correct application of Quality of Service (QoS) and Application Quality of Experience (AppQoE) policies in the edge router.

d) The Fujitsu SD-WAN network interfaces will be shaped in accordance with the information provided by the Buyer

e) The Fujitsu SD-WAN edge device uses the following WAN interface configurations:

i. WAN interface is 10/100/1000baseT (RJ45)

ii. Auto-negotiation.

iii. Option to manually set speed (100Mbps or 1Gbps) and duplex (full, half or both)

iv. Single WAN interface per edge device.

v. No WAN interface shaping.

8.5.9: Overlay Resilience

a) The Fujitsu SD-WAN edge router optimises connectivity and autonomously resolves many network availability and performance issues as they occur, improving the end user Quality of Experience (QoE) and improving productivity.

b) Where a Buyer site has multiple WAN connections, the Fujitsu SD-WAN overlay network will be provided over all links, including the creation of multiple paths between two sites, in accordance with the network topology templates.

c) Multiple overlay paths are used to facilitate improvements in performance, resilience and capacity.

d) The following figure shows how a remote site connects to two datacentres, with resilient paths to both sites using different WAN networks.

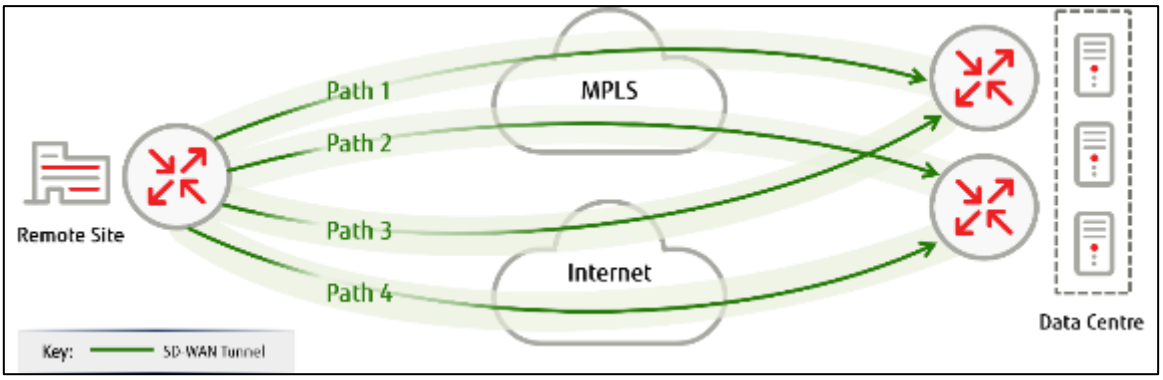

Figure 46: SD-WAN Overlay Path Resilience

e) Each overlay tunnel is monitored for liveliness and path quality using the Bi-directional Forwarding Detection (BFD) protocol.

f) If BFD detects loss of connectivity, traffic will be re-distributed across the available links.

g) By default, BFD is configured to monitor each link once every second and will declare loss of connectivity after the loss of seven BFD messages, enabling failover in less than eight seconds.

8.5.10: Internet Breakout and Cloud Connectivity

a) The Fujitsu SD-WAN solution supports the capabilities for cloud connect and internet breakout as illustrated in the following figure.

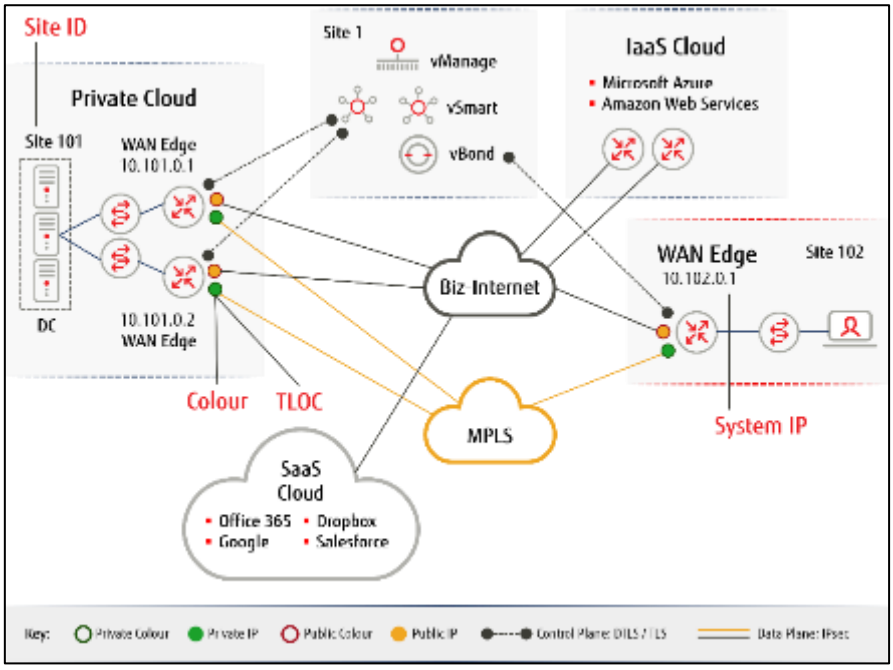

Figure 47: SD-WAN overlay Cloud Connectivity

b) Fujitsu SD-WAN solution supports the capability for native integration with third party cloud solutions including:

i. Integration with public cloud Secure Internet Gateways.

ii. Direction of application flows to regional colocation centres to consume Software as a Service (SaaS) and Infrastructure as a Service) applications to realise network level service chaining.

iii. Native integration with Azure Virtual WAN, Google Cloud and Amazon Web Services (AWS).

c) Fujitsu SD-WAN solution supports the capability for local, central, regional and SIG Internet breakout options, illustrated in **Figure 48**:, **Figure 49**:, and **Figure 50**:

i. Local breakout provides direct internet access at the site

ii. Remote breakout provides direct internet access at a regional hub site that is shared by spoke sites connected via the SD-WAN overlay.

iii. Central breakout provides direct internet access at a datacentre shared by remote sites connected via the SD-WAN overlay.

iv. SIG internet breakout forwards traffic to the nearest Zscaler Secure Internet Gateway Point of Presence.

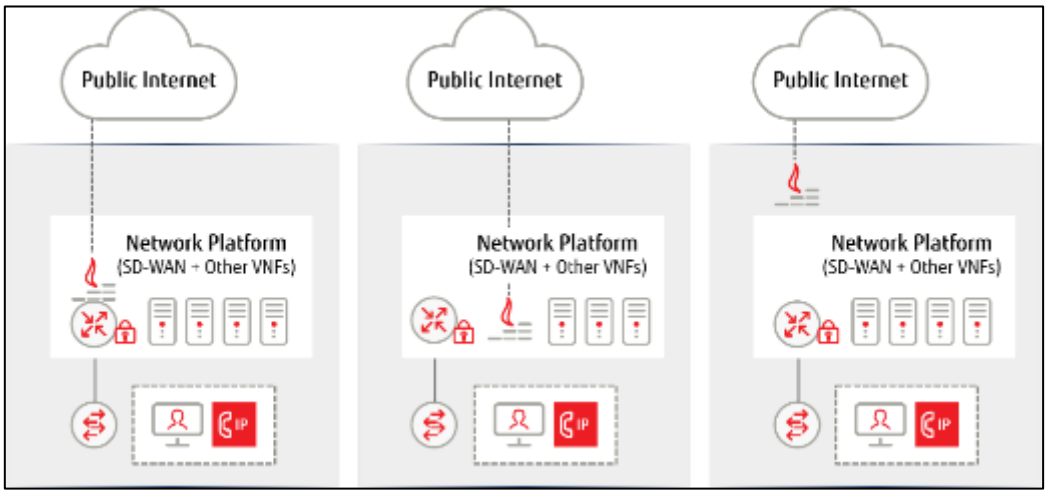

Figure 48: Local Internet Breakout

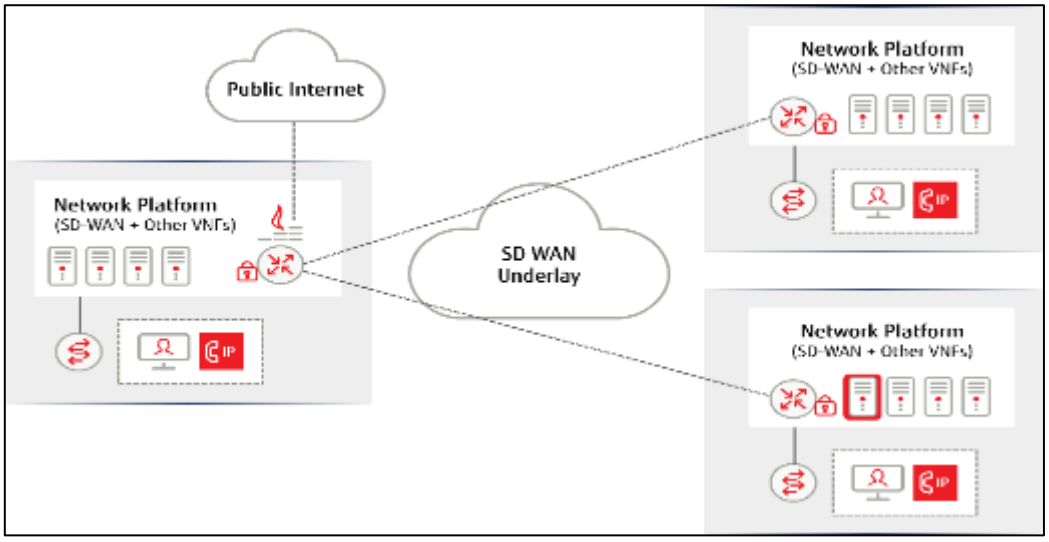

Figure 49: Regional/Central Internet Breakout

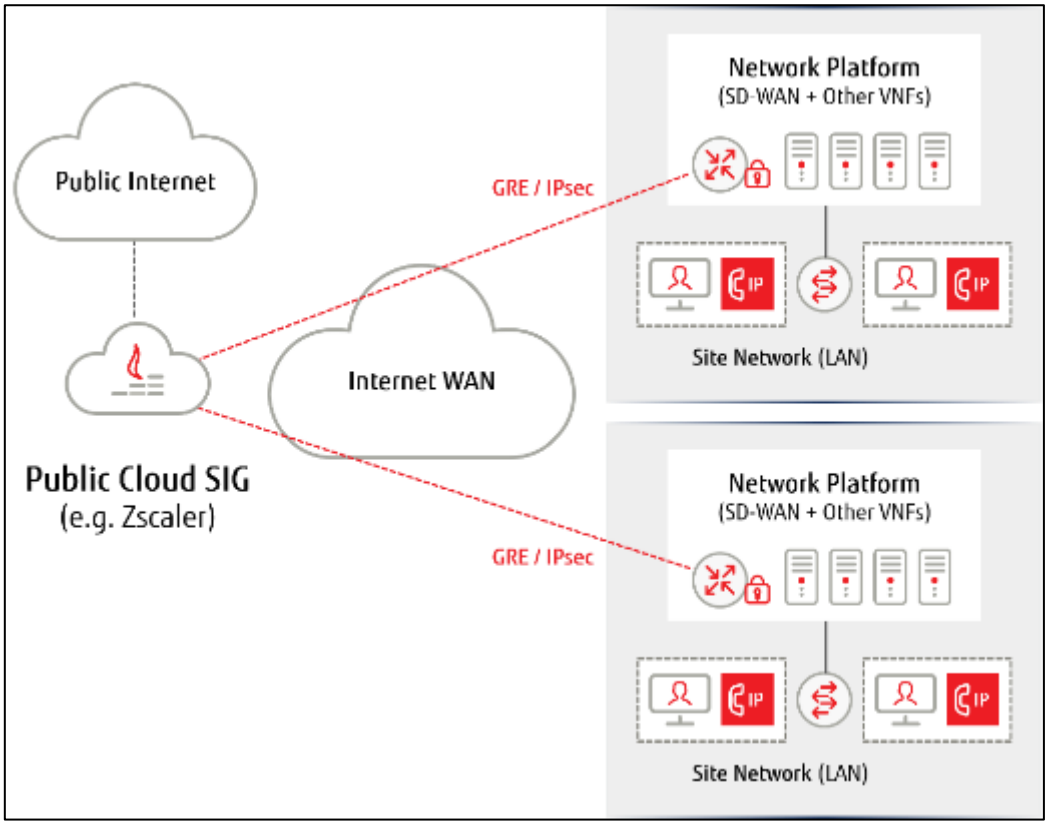

Figure 50: SIG Breakout

d) The Fujitsu SD-WAN solution supports site-wide and per-VPN policies to determine the traffic and application that are allowed to use the breakout. Both static and dynamic modes are supported.

i. With static breakout, fixed policies are defined to forward internet bound traffic to a defined breakout interface.

ii. With dynamic breakout, the internet policy defines multiple breakout interfaces. If the SD WAN overlay BFD mechanism detects loss of connectivity or path quality on a tunnel connecting to a regional, central or SIG breakout, an alternative breakout interface is selected.

a) For local, regional, and central breakout options, a firewall should be provided at the breakout interface to protect Buyer sites against internet threats.

b) Integration of Next Generation Firewall functionality with the SD-WAN and uCPE edge device is subject to change request.

c) Support for Fujitsu SD-WAN integration with 3rd party cloud providers using onRamp will be subject to a change request.

i. Note: Fujitsu SD-WAN edge devices are being provisioned in AWS in accordance using AWS infrastructure.

a) Support for Fujitsu SD-WAN internet and cloud breakout will be subject to a change request.

8.5.11: Fujitsu SD-WAN Templates and Policies

a) The SD-WAN management solution uses configuration and policy templates to simplify and improve management process accuracy.

b) Templates enable new sites and features to be added fast without requiring complex configurations through a command line interface (CLI).

c) The template approach reduces the risk of mis-configuring devices through CLI typo errors at deployment or in in service. Using a template also means that configurations are inherently compliant with the solution design and security assurance requirements.

d) Templates are applied from vManage. A vManage template can be attached to multiple WAN edge routers simultaneously. When changes are made to configuration templates, these changes are automatically propagated to all attached SD-WAN edge routers.

e) There are two types of configuration templates:

   i. Feature templates help build individual components of the router configuration, such as segmentation, interfaces, system, routing, logging, and device access.

   ii. Device templates provide the framework for the entire router configuration and are made up of feature templates. Templates are flexible and allow for highly customisable router configurations. Efficient device templates design allows minimal touch configuration of thousands of devices. When making an update to a template, the changes are propagated immediately to the SD-WAN edge routers. In case of configuration errors, the template configuration rolls back to its previous state, protecting the system against human errors.

f) Device templates reference a series of feature templates that make up the entire configuration of a device. The device templates include the following information:

   i. Basic information and IP address Management

   ii. Transport (WAN) and management VPN

   iii. Service (Buyer) VPN

   iv. System templates.

g) Feature templates allow simple and repeatable configuration of system level features, including:

   i. System identification

   ii. Logging

   iii. Authentication, Authorisation and Accounting (AAA)

   iv. Bi-directional Forwarding Detection (BFD) monitoring

   v. Overlay Management Protocol (OMP)

   vi. Security

   vii. Archive (optional)

   viii. Network Timing Protocol (NTP)

   ix. Virtual Private Network (VPN)

   x. Border Gateway Protocol (BGP) and Pen Shortest Pat First (OSPF) routing

   xi. VPN Interface configuration

   xii. Dynamic Host Configuration Protocol (DHCP server (optional)

   xiii. Login banner

   xiv. Local policy (optional)

   xv. Simple Network Management Protocol (SNMP)

   xvi. Bridge (optional).

h) VPN interface templates and routing protocol templates, such as BGP and OSPF, are configured under a VPN. DHCP server feature templates are configured under a VPN interface.

i) SD-WAN policies control data traffic flow among SD-WAN edge routers in the SD-WAN fabric. Policies relate to:

   i. Topology

   ii. Traffic flow

   iii. Local sites.

j) Topology policies: Centralised control policies operate on the routing and Transport Locator (TLOC) information within OMP and allow customisation of routing decisions. These policies can be used in configuring traffic engineering, path affinity, service insertion, and different types of VPN topologies (including full-mesh, hub-and-spoke or regional mesh).

k) Traffic flow policies: Data traffic policies influence the flow of traffic through the network, based on application signatures, fields in IP headers, or which VPN segment the traffic is using. Centralised data policies are used in configuring zone-based firewalls, service chaining, traffic engineering, and quality of

service (QoS). They include Application-Aware Routing to apply SLAs for applications and traffic steering, while activating AppQoE features, such as packet duplication.

l) Locally significant policies: Localised policies are used to handle traffic at a specific site. These include Access Control Lists (ACLs), Quality of Service (QoS), and route maps for OSPF, BGP or EIGRP.

m) Policies are defined by the administrator using the policy wizard under the configuration menu of vManage. Centralised policies are applied by vManage to the vSmart controllers and localised policies are applied from vManage directly to the WAN edge router.

8.5.12: Enterprise Firewall

a) The Enterprise Firewall is an optional service with Application Awareness and uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

b) A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows.

c) Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones.

d) A zone is a grouping of one or more VPNs.

e) Grouping VPNs into zones allows security boundaries to be established in the overlay network, enabling control of all data traffic that passes between zones.

f) Zone configuration consists of the following components:

i. **Source zone —** A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.

ii. **Destination zone —** A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.

iii. **Firewall policy —** A security policy, similar to a localised security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone.

1. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications.
2. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged.
3. Nonmatching flows are dropped by default.
4. Matching applications are denied.

iv. **Zone pair —** A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

g) Matching flows that are accepted can be processed in two different ways:

i. **Inspect —** The packet's header can be inspected to determine its source address and port. When a session is inspected, it is not necessary to create a service-policy that matches the return traffic.

ii. **Pass —** Allow the packet to pass to the destination zone without inspecting the packet's header at all. When a flow is passed, no sessions are created. For such a flow, a service-policy must be created that will match and pass the return traffic.

8.6: Application Monitoring

8.6.1: Overview

a) Fujitsu SD-WAN service includes an analytics service to support monitoring and analysis of Buyer application flows.

b) The analytics service provides the Buyer access to the LiveNX network and application performance monitoring platform.

c) Fujitsu uses the LiveNX platform to enable monitoring of the Fujitsu SD-WAN service:

i. uCPE availability monitoring and SLA reporting

ii. SD-WAN overlay monitoring and SLA reporting

iii. SD-WAN edge utilisation

d) The Buyer shall be provided access to the LiveNX platform to support the following capabilities:

i. Correlation of multiple data sets to provide views, graphs, and maps to illustrate the current state of applications and network performance.

ii. Application visibility and troubleshooting to gain a deep understanding of application traffic with full visibility of protocol and application type including video, voice, instant messaging, file transfer, etc.

iii. Application analysis to trouble shooting.

iv. Analysis of how the SD-WAN network is being used, how applications are performing, and which sanctioned or unsanctioned applications are being used.

8.6.2: Management Interface

a) LiveNX is managed via the LiveNX JAVA client or web User Interface (UI).

b) LiveNX shall be integrated with the SD-WAN vManage appliance through the REST API management interface.

8.6.3: Network Data

a) LiveNX shall collect the following SD-WAN performance data:

i. uCPE availability

ii. SD-WAN overlay BFD performance metrics (loss, latency, jitter and path failure)

iii. Fujitsu SD-WAN edge router WAN utilisation statistics

8.6.4: Application Flow Data

a) Application flow data shall be collected directly from SD-WAN edge devices using cflowd.

b) Cflowd is a flow analysis tool, used for analysing NetFlow traffic data. It monitors traffic flowing through the SD-WAN C8000v edge devices in the overlay network and exports flow information to a collector, where it can be processed by an IP Flow Information Export (IPFIX) analyser. For a traffic flow, cflowd periodically sends template reports to the flow collector. These reports contain information about the flows and the data is extracted from the payload of these reports.

c) Cflowd traffic flow monitoring is equivalent to Flexible Netflow (FNF). The cflowd software implements cflowd version 10, as specified in RFC 7011 and RFC 7012. Cflowd version 10 is also called the IP Flow Information Export (IPFIX) protocol.

d) The SD-WAN edge router cflowd-template defines the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the template is sent to the collectors (on Cisco vSmart Controllers and on Cisco vManage).

8.7: Buyer Portal Access

a) The SD-WAN service shall provide the following r Portal access to user authorised by the LEC Authority:

   i. vManage

   ii. LiveNX Client

b) Access shall be authenticated and authorised in accordance with the Role Based Access Control (RBAC) process, which includes:

   i. All accounts shall be assigned to an individual person.

   ii. Access shall be provided on a least privilege basis.

c) Access shall be provided to vManage and LiveNX Web server interfaces via a web server proxy, which will be accessed from End User Devices via the SD WAN overlay (PROTECTED VPN).

d) The Buyer Portal shall provide a Remote Desktop facility to support LiveNX access using the Java client.

e) End user devices shall be authenticated by policing certificates.

   i. Buyer to provide policing root CA certificates.

8.8: PSN and Internet Underlay

8.8.1: Underlay Network

a) The Fujitsu SD-WAN uses standards-based IP/Ethernet WAN interfaces with Network Address Translation to enable use of any IP-based networking technology, including PSN and MPLS Virtual Private Networks (VPNs) using private IP address space, and the Internet using public IP addressing.

b) The Fujitsu SD-WAN shall use the following underlay networks provided by the Buyer:

   i. Public Sector Network

   ii. Internet ISP

   iii. 5g ISP Connectivity

   iv. MPLS networks

c) The Buyer shall provide a WAN switch to facilitate connectivity of SD-WAN edge devices to the PSN CPE in both standard (active and warm standby) and HA (active / active) modes of operation.

d) Each site shall be operated in one of the following modes of operation:

   i. Standard, non-resilient active uCPE plus an active warm standby device with a single PSN/internet network connection.

   ii. High Availability, resilient active/active uCPE with resilient PSN/internet network connections and resilient PSN CPE operating in HSRP mode.

e) Support for other operating modes, including the following, is subject to change control:

i. High Availability, resilient uCPE with single PSN/internet network connections

ii. High availability sites using TLOC extensions.

f) The level of resilience provided by the network connectivity (e.g. diverse or fully diverse) shall be determined by the PSN service provided by the site and defined in the MSL.

g) The Buyer shall provide the following network connectivity information for each site:

i. IP subnet, mask and address allocations

ii. Circuit type (Ethernet)

iii. Link speed (10Mbps, 100Mbps, 1Gbps, 10Gbps)

iv. Committed rate (<= link speed)

v. Physical coding sublayer (10/100/1000baseT, 1000baseX, 1000baseT, 10GbaseX)

vi. Physical medium (copper, single mode fibre, multi-mode fibre)

vii. Physical layer (SR, LR)

h) The SD-WAN solution supports Network Address Translation at public internet interfaces.

8.8.2: Network Utilisation

a) The Fujitsu SD-WAN solution operates by default with ECMP for WAN connectivity, meaning it will load-balance two or more WAN circuits, thereby providing active-active load balancing by default. If a Buyer wishes to ensure traffic is routed via one particular transport network, there are preference mechanisms that force traffic to use one link rather than another.

b) The Fujitsu SD-WAN solution supports load balancing per flow within the overlay network. The SD-WAN fabric supports numerous methods of mapping any given application onto any of the available WAN transport links in any of the required service (LAN) side VPN:

i. Per-session active-active load sharing across multiple transports irrespective of the transport type (PSN or Internet).

ii. Per-session active-active weighted load sharing across multiple transports where certain configured ratios are applied for proportional traffic distribution.

iii. Active/standby for pinning application traffic to specific transport links with or without failover.

iv. SLA-based application aware routing, where the choice of transport is governed by meeting (or not meeting) desired loss, latency and jitter characteristics for the given application.

c) These forwarding methods are not mutually exclusive and can be leveraged all at once, while acting on different types of application traffic as defined by 6-tuple matching (including DSCP value) or DPI signatures.

8.9: LAN

8.9.1: LAN Integration

8.9.2: The Fujitsu SD-WAN supports features that simplify integration with Buyer Local Area Networks (LAN) and applications.

a) Use of standards-based IP/Ethernet interfaces, OSPF/BGP routing protocols and the Virtual Router Redundancy Protocol (VRRP) allow connectivity with standard LAN topologies.

b) The Buyer LAN shall provide any layer 2 connectivity required to support VRRP in resilient uCPE configurations.

c) Virtual Routing Functions maintain the logical separation of Buyer Closed User Group (CUG) traffic.

d) Layer 2-4 classification enables application-based policies for encrypted and unencrypted applications flows, while Deep Packet Inspection supports further analysis of unencrypted application flows.

e) The Buyer shall provide the LAN integration requirements to support discovery activities of each site Low Level Design, which shall include the following:

i. Buyer VLANs and subnets

ii. Buyer LAN gateway IP address allocation

iii. Static routes

iv. Dynamic routing details

v. VRRP requirements

8.9.3: Buyer VPNs

a) The Fujitsu SD-WAN solution allows Buyer traffic to be mapped to different VPN segments across the secure fabric using a single set of IPsec tunnels among the sites. VPN segments provide strict logical separation of traffic, have distinct VPN topologies, overlapping IP addresses and unique application and security policies. VPN segments will be connected with routing and security policies at individual sites.

b) The Fujitsu SD-WAN solution implements segmentation at the edge and allows for scalability into 100s of VPNs.

c) By default, the Fujitsu SD-WAN shall provide separate VRFs for the following Buyer LAN segmentation:

i. Protected LANs/VLANs

ii. Secure LANs/VLANs

iii. IDENT1 LANs/VLANs

iv. Policing Partners LANs/VLANs

8.9.4: Network Address Translation (NAT)

a) Fujitsu SD-WAN solution supports NAT on the Buyer LAN side. This will allow the support of overlapping IP subnets and re-use of existing IP subnets and schema on the Buyer LAN.

b) The LAN side addresses are redistributed to the overlay and advertised to all the remote branches using the Overlay Management Protocol (OMP). Thus, the remote host is aware of the path to reach inside hosts.

c) NAT will ensure that IP addresses in the overlay transport VPN are unique.

8.9.5: DHCP

a) The Fujitsu SD-WAN edge device supports the capability to provide DHCP services for the Buyer LAN.

b) No DHCP services are enabled by default for the SD-WAN service.

8.10: AWS edge

a) Fujitsu SD-WAN will provide support for edge devices deployed in the AWS cloud infrastructure as illustrated in the following Figure 51

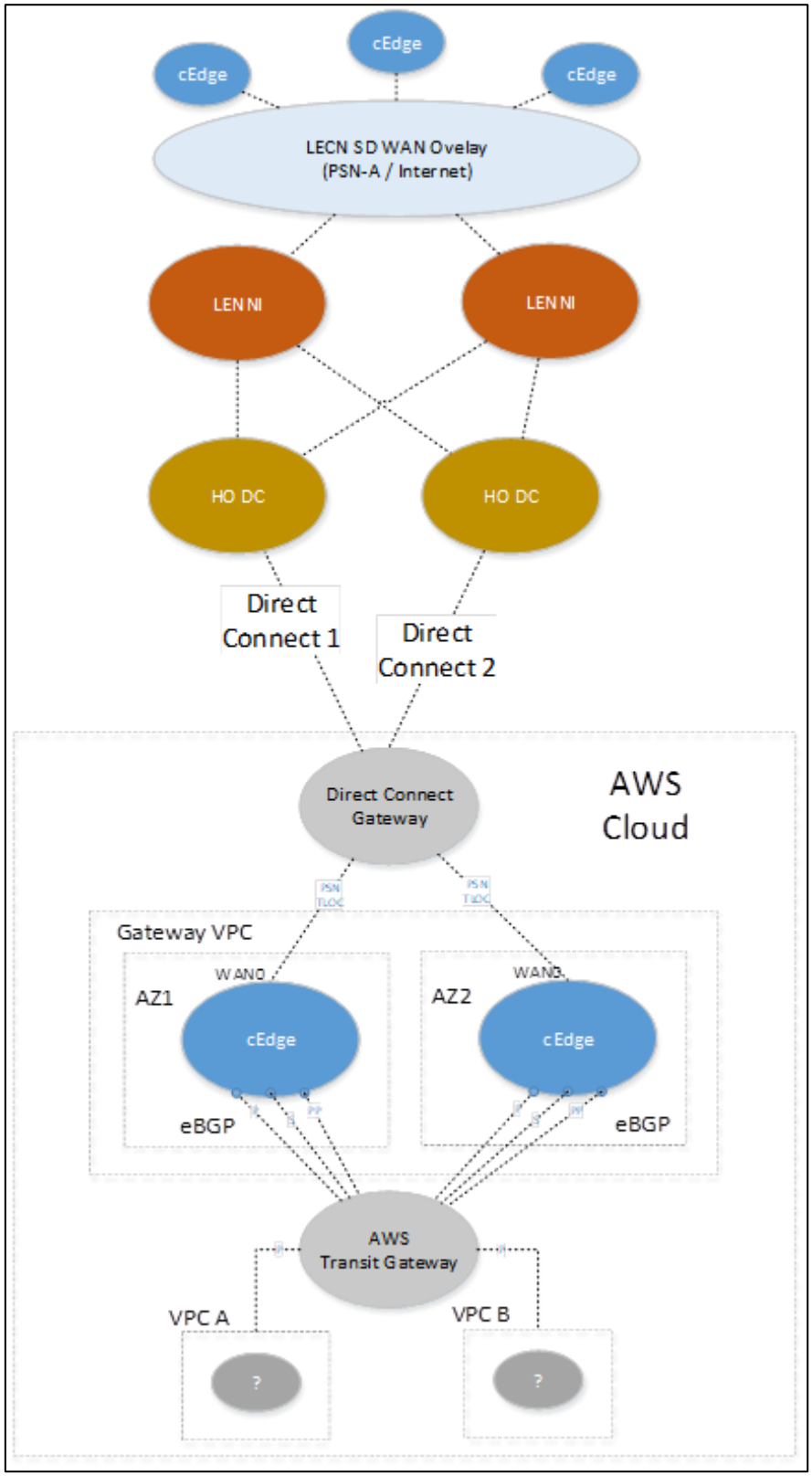

Figure 51: SD WAN – AWS TGW Integration

The Buyer is responsible for providing underlay connectivity between the Fujitsu SD-WAN and AWS infrastructure.

i. AWS is connected to the PSN via two AWS Direct Connect services providing 1:1 (active/active) resilience.

b) The Fujitsu SD-WAN service will provide the following information to enable initial build of the AWS edge instance:

i. Fujitsu SD-WAN DNA licensing

ii. edge device UUID

iii. edge device OTP

iv. Entrust root CA trust chain

c) The Fujitsu SD-WAN service will be responsible for on-boarding and managing the SD-WAN cedge instance.

d) The Fujitsu SD-WAN edge will establish eBGP peering with the Transit Gateway and advertise learned routes into OMP.

8.11: Availability & Resilience

8.11.1: Overview

a) The Fujitsu SD-WAN service provides a managed overlay service and provides availability service level agreements for the following aspects:

i. Fujitsu SD-WAN Core Platform availability, measured as the ability to maintain SD-WAN Overlay connectivity

ii. SD-WAN edge device availability

b) The following aspects of the service are provided by the Buyer and are outside the scope of the service:

i. Power and accommodation of edge devices at Buyer premises, including:

1. Building integrity
2. Heating, ventilation and air-conditioning
3. Power supply

ii. Underlay network connectivity

iii. WAN and LAN cabling and switching infrastructure

iv. LAN switching

v. Onsite assistance (excluding break fix)

c) The Fujitsu SD-WAN solution supports Core Platform, MANO, edge device, and overlay resilience as illustrated in [redacted]

Figure 50: SD-WAN Redundancy Mechanisms (Redacted)

a) Fujitsu SD-WAN will inherit transport layer resilience provided by the PSN/internet underlay, which is supplied by the Buyer.

b) Fujitsu SD-WAN provides fully meshed overlay connectivity between all sites in each service VPN. This enables application providers to provide dual homed connectivity to end user sites. The mechanism for switching end users from one application datacentre to another is outside the scope of the Fujitsu SD-WAN service.

c) At Buyer sites, Fujitsu SD-WAN edge devices shall be deployed in one of the following modes:

   i. High Availability (HA) mode, with two devices providing active/active operation

   ii. Standard Availability mode with one active device and one warm standby device.

8.11.2: Edge device High Availability

a) High Availability mode can be used at any site.

b) High Availability deployments protect against multiple layers of failure including:

   i. Loss of power

   ii. Device failure

   iii. WAN link failure

   iv. PSN/MPLS and Internet underlay network failure

   v. Fujitsu SD-WAN overlay tunnel failure.

c) The provision of separate power supplies is the responsibility of the Buyer site.

d) The remote edge (VEP-4600) provides dual power supply modules and supports full operation with one operational power supply.

e) In the event of a dual power or device failure Buyer LAN traffic will be routed via the remaining device and the WAN connections supported by that device.

f) Resilience against underlay failure is the responsibility of the PSN/MPLS/internet service provider. For HA sites with dual network circuits and CPE, resilience will be provided from Buyer edge to Buyer edge.

g) The High Availability solution is based on the following principles.

   i. **Device redundancy:** In High Availability mode, a primary and secondary device are provided, which operate in active/active mode. The active/active mode of operation permits usage of the resilient PSN connectivity using HSRP protected CPE and WAN Ethernet switching infrastructure.

Figure 51: HA Device Resilience (SD-WAN Overlay) Redacted

Figure 52 HA Device Resilience (Pass-through) Redacted@

   iii. Active/active mode of operation requires SD-WAN and EC hypervisor licences for each edge device.

   iv. The HA mode of operation has been defined by the HO LEC technical team.

   v. **edge - Service VPN VRRP:** The HA mode of operation requires the edge devices to use VRRP in each service VPN. VRRP provides a VIP as the SD-WAN default gateway for Buyer LAN devices (e.g. forces firewall), which can be reached from the Buyer LAN environment via an external LAN switch.

   vi. The HA pair uses VRRP WAN/LAN prefix tracking to monitor the status of the edge device WAN and LAN connectivity. If the WAN/LAN connectivity goes down, VRRP will move the VIP to direct Buyer LAN traffic to the other device and route traffic via the alternative WAN/LAN link.

   vii. **PSN CEP – HSRP SD-WAN** edge devices will forward traffic to the CPE Virtual IP (VIP) address in accordance with the ARP table. In the event of a CPE device failure, the SD-WAN ARP table will be updated in accordance with gratuitous ARPs sent by the active PSN CPE.

viii. **Forces Firewall – VRRP:** SD-WAN edge devices will forward traffic to the Forces Firewall Virtual IP (VIP) address in accordance with the ARP table. In the event of a firewall device failure, the SD-WAN ARP table will be updated in accordance with gratuitous ARPs sent by the active firewall.

ix. **SD-WAN OMP routing:** The SD-WAN OMP routing protocol ensures rapid recovery from both direct and indirect failure. To provide a resilient control plane, the solution regularly monitors the status of all WAN edge routers in the network and automatically adjusts to changes in the topology as routers join and leave the network.

8.11.3: Edge device Standard Availability

a) Standard Availability mode can be used at any site, and will be used as defined by the CA MSL. Standard deployments have less resilience against failures than HA deployments, but do maintain protection against multiple layers of network failure including:

i. Power supply failure.

ii. WAN link failure (if the site has multiple links)

iii. PSN / MPLS and Internet underlay network failure

iv. SD-WAN overlay tunnel failure.

b) The provision of separate power supplies is the responsibility of the Buyer site.

c) The remote edge (VEP-4600) provides dual power supply modules and supports full operation with one operational power supply.

d) The Fujitsu SD-WAN solution supports.

i. **Primary device:** In Standard mode, a single primary device provides full operational service.

ii. **Warm standby device:** In Standard mode, a secondary standby device is actively managed, but not connected to the Buyer LAN infrastructure. The warm standby provides an on-site break fix device that is ready to replace a failed primary device. The warm standby device is fully managed and maintained with the latest patches and software releases, monitored for defects and security incidents, and synchronised to the Buyer datacentre clock. In the event of a primary device failure, the Buyer LAN infrastructure needs to be moved to the secondary device. The DJSC will remotely copy the failed primary device configuration to the warm standby device. The Standard mode of operation permits usage of a single CPE interface using WAN Ethernet switching infrastructure (provided by the SD-WAN Buyer). The connectivity of traffic from both devices in a Standard configuration is illustrated in the following redacted figures

Figure 25: Standard Device Connectivity (SD-WAN overlay) Redacted

Figure 26: Standard Device Resilience (Pass-through) Redacted

iii. Standard mode of operation requires SD-WAN and EC hypervisor licences for each edge device.

iv. The Standard mode of operation has been defined by the HO LEC technical team.

e) In order to meet service restoration targets of less than 2 hours, local support or Buyer Smart Hands are required to move Buyer LAN connections from a failed primary edge device to the warm standby device.

8.11.4: Core Platform - Fujitsu SD-WAN MANO Availability

a) The Fujitsu SD-WAN provides a high availability management and orchestration (MANO) platform located in two separate datacentres (DC1 and DC2) using the following resilience capabilities:

i. Active/active orchestration (vBond), control plane (vSmart) and DNS.

ii. Active/standby management (vManage)

iii. Resilient PSN connectivity to each SD-WAN MANO

iv. Dynamic SD-WAN routing (OMP)

v. Autonomous edge and Datapath operation in the event of MANO failure (graceful restart).

b) Once the Fujitsu SD-WAN edge router has established the Catalyst SD-WAN overlay, in accordance with centralised templates and policies, each edge router uses local packet processing and forwarding to route

traffic between Buyer sites. In the event of control plane failures, the edge devices operate in Graceful Restart mode, which caches local routing and security parameters, allowing the device to continue to operate in the data plane.

c) **vBond:** The vBond orchestrator operates in active/active mode, with one vBond instance in each datacentre. When establishing management and control plane connectivity, edge devices requests primary and secondary vBond IP address details from the dedicated Fujitsu SD-WAN DNS server.

d) **SD-WAN DNS:** An active DNS server is provided in each datacentre. If an edge device does not receive vBond details from the primary DNS server, it will send a request to the secondary server.

e) **vSmart:** The vSmart controller operates in active/active mode, with one vSmart instance in each datacentre. When establishing management and control plane connectivity, edge devices establish an active connection with both vSmart controllers. If one of the vSmart controllers fails, the other one seamlessly takes over handling control of the network.

f) For correct operation, the control policies in each vSmart controller must be identical. To remain synchronised with each other, the vSmart controllers establish a full mesh of DTLS control connections, as well as a full mesh of OMP sessions, between themselves. Over the OMP sessions, the vSmart controllers advertise routes, TLOCs, services, policies, and encryption keys. It is this exchange of information that allows the vSmart controllers to remain synchronised.

g) **vManage:** vManage operates in active/standby mode, with one vManage instance in each datacentre. In normal operation only the active vManage is connected to the transport network and vBond established edge connectivity with this vManage instance. In the event of a vManage failure, a DJSC administrator manually copies the latest configuration database to the standby vManage and performs a Disaster Recovery failover to establish the standby vManage as the active controller. In order to support this process, the SD-WAN toolset server takes regular backups of the configuration database (at 8 hour intervals) and copies it to the opposite datacentre.

h) **SD-WAN OMP routing:** The SD-WAN OMP routing protocol ensures rapid recovery from both direct and indirect failure. To provide a resilient control plane, the solution regularly monitors the status of all WAN edge routers in the network and automatically adjusts to changes in the topology as routers join and leave the network.

i) **PSN connectivity:** The SD-WAN datacentres uses BGP dynamic routing via the DC interconnect to provide resilient PSN connectivity from each datacentre, as illustrated in the following figure.

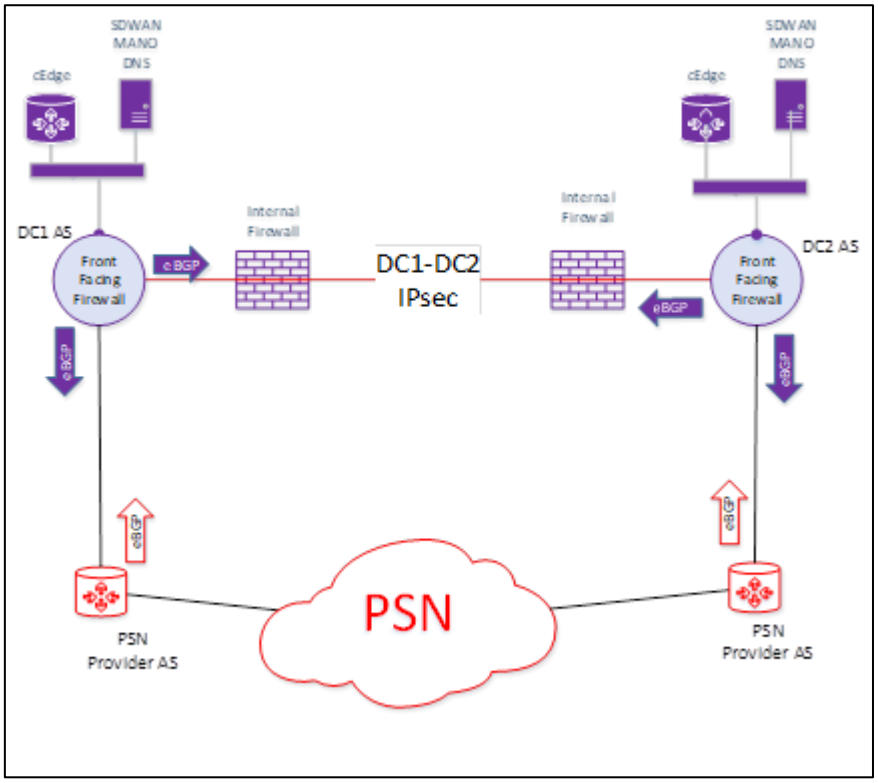

Figure 2752: Connectivity Resilience - BGP Dynamic Routing

8.11.5: Core Platform – Infrastructure and Enterprise Management Availability

a) The Fujitsu SD-WAN Core Platform provides high availability infrastructure and Enterprise Management across two separate datacentres (DC1 and DC2) using the following resilience capabilities:

i. Clustered server infrastructure

ii. Primary and backup storage

iii. Clustered and virtual chassis DC network equipment

iv. Backup and recovery with offsite backups stored as virtual tapes in opposite datacentre

v. High availability Enterprise Management applications

b) The Fujitsu SD-WAN Platform (GSA Buyer pod) is supported by a 2+1 vSphere High Availability cluster.

c) The Fujitsu SD-WAN Platform (GSA Buyer pod) provide primary and backup storage via iSCSI.

d) All DC firewalls are operated with dual power supplies and configured in a 1+1 active/standby cluster.

e) All DC switches are operated with dual power supplies and configured in a 1:1 active/active virtual chassis.

f) Remote access between BRA07/BSN01 resolver groups and the Core Platform is provided via resilient network connectivity, terminal servers and Remote Desktop Services.

g) The LiveNX performance management application is operated as a single server, with Veeam backup and replication providing server resilience and datacentre DR.

h) The Elasticsearch Enterprise Management toolsets is configured as a 3-node cluster in each datacentre with cross-cluster data replication.

i) The Zabbix Enterprise Management toolset is configured as an active/standby pair with automated failover.

8.12: Service Interruption

a) The following table defines the service impact due to a single network, device or controller component failure in the SD-WAN service.

LEC SD-WAN Component	LEC SD-WAN Service Impact (Single Component Failure)	Resilience Mechanism
SD-WAN edge (Standard)	<4 hours	Warm standby
SD-WAN edge (HA)	<5 minutes	VRRP
Single edge power supply	None	VEP-4600 dual power supplies
Buyer site PSN circuit (standard)	Refer to PSN provider SLA	Refer to PSN provider solution
PSN network	Refer to PSN provider SLA	Refer to PSN provider solution
SD-WAN MANO – vBond	None	Active / active vBond
SD-WAN MANO – vSmart	None	Active / active vSmart
SD-WAN MANO – vManage	Loss of SD-WAN management No loss of SD-WAN Overlay data path	vManage DR failover
SD-WAN DNS	None	Active / active DNS
LiveNX	Loss of application monitoring No loss of SD-WAN Overlay data path	LiveNX VM replication
ISE	None	Active / active ISE
NTP	None	SRX cluster NTP server active (DC1) / active (DC2)
Zabbix (SNMP)	None	Zabbix active /standby automated failover
Elasticsearch (Syslog)	None	3 node cluster

Table 918: SD-WAN Component Failure - Service Impact

b) Typical service interruption times due to common failure modes:

i. Failover due to device reboot or power failure on a HA platform will be in the order of < 5 minutes, which is defined by the time for VRRP to detect the failure and cause a routing change.

ii. Fujitsu SD-WAN router reboot (as an example, for software upgrade) will typically be 10 minutes.

iii. The uCPE platform will automatically reboot after restoration of power, resulting in a reboot of typically 10 minutes.

iv. Failover due to interface failures will be in the order of <5 minutes, which is defined by the time for VRRP to detect the failure and cause a routing change.

8.13: Backup and Recovery

8.13.1: VM Backup and Recovery

a) The core Platform provides a Veeam backup and replication solution for Virtual Machines and specified files.

b) The SD-WAN Core Platform VMs are automatically backed up daily by the Veeam backup solution.

c) Backups are stored locally and offsite in the opposite datacentre.

d) Backups are stored as encrypted virtual tapes in dedicated storage partitions.

8.13.2: MANO Configuration

a) In addition to VM backups, the LEC Fujitsu SD-WAN vManage configuration database is backed up at 8 hour intervals.

b) Fujitsu SD-WAN configuration database backups are performed automatically by the toolset server, stored locally and copied to the opposite datacentre.

c) In the event of a vManage DR failover, the latest vManage configuration database is restored on the standby vManage.

8.14: Disaster Recovery

a) The Fujitsu SD-WAN service offers a Business Continuity and Disaster Recovery (BCDR) with the following approaches:

i. DR datacentre

ii. Standby resolver group locations

iii. VM backup and replication

iv. High Availability Core Platform

b) The Platform is deployed in geographically separate primary and secondary datacentres in

c) The Platform primary resolver group is located in [redacted], with DR resolver group facilities provided in [redacted].

d) The Platform backup and replication solution allows recovery of individual VMs in both datacentres from backups stored in both datacentres.

e) The Fujitsu SD-WAN Platform also provides high availability resilience without invoking DR processes such as VM recovery:

i. Clustered server infrastructure

ii. Clustered and virtual chassis DC network equipment

iii. High availability MANO and Enterprise Management toolsets

f) Dependent on the nature of the functionality provided, individual toolsets are protected in one of the following active/active or active/standby modes of operation:

i. Active/active operation

ii. Active/standby with automated stateful database synchronisation or replication and administrator failover

iii. Active/standby with automated stateful database backup and administrator failover

iv. Active/- with automated virtual machine backup and manual recovery

v. Active/standby with automated failover

g) The following table summarises the High Availability and Disaster Recovery approaches for individual management functions in the SD-WAN toolset between datacentres.

Toolset	Application Level DR (DC1 to DC2)	Disaster Recovery (DC2)

Remote Desktop Service	Active / Active	VM recovery
LOSS/ESO (Not currently used in LEC SD-WAN)	Active/- with automated VM backup and manual recovery	VM recovery
vManage	Active / standby vManage (Automated database backup and admin failover)	VM recovery
vBond	Active / Active	VM recovery
vSmart	Active / Active	VM recovery
NTP server	Active / Active	VM recovery
Elasticsearch (Syslog)	Active / Standby (Data replication and automated failover)	VM recovery
LiveNX (Flexible Netflow)	Active/- with automated VM backup and manual recovery	VM recovery
ISE (RADIUS/ TACACS+)	Active / Active	VM recovery
Zabbix (SNMP traps)	Active / Standby (Automated database backup and admin failover)	VM recovery

Table 19: SD-WAN Core Platform Toolset Disaster Recovery Approach

8.15: Performance Management

8.15.1: Current Growth and Expected Growth

a) The Fujitsu SD-WAN edge routers are deployed using the Virtual edge uCPE approach.

8.15.2: Scalability

a) The Fujitsu SD-WAN deployment is based on multiple instances of SD-WAN management and controller appliances configured in high availability mode, with individual appliances being able to support up to 2000 edge devices.

b) All uCPE deployment support 8x vCPU, 16GB RAM and 240GB storage with a C8000v virtual router, which supports a throughput of up to 2Gbps.

8.16: Security

8.16.1: Control Plane Security

a) The LEC Catalyst SD-WAN control plane uses digital certificates with 2048-bit RSA keys to authenticate the SD-WAN edge routers in the network. The digital certificates are created, managed, and exchanged by standard components of the public key infrastructure (PKI):

i. Public keys — These keys are generally known.

ii. Private keys — These keys are private. They reside on each SD-WAN router and cannot be retrieved from the router.

b) Certificates are signed by a root certification authority (CA). The trust chain associated with the root CA needs to be present on all Cisco SD-WAN controllers and routers.

c) For the Fujitsu SD-WAN the root CA is provided by Fujitsu's CA service.

d) For vSmart controllers, vBond orchestrators, vManage systems, the certificates are managed manually. The Cisco SD-WAN software generates a unique private key–public key pair for each software image. The network administrator requests a Certificate Signing Request for each controller, which is sent to the issuing sub-CA of the root CA trust chain for signing and manually installed on the corresponding controller virtual appliance.

e) Control plane encryption is done by either DTLS, which is based on the TLS protocol, or TLS. These protocols encrypt the control plane traffic that is sent across the connections between SD-WAN devices to validate the integrity of the data. TLS uses asymmetric cryptography for authenticating key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

f) For the Fujitsu SD-WAN, TLS is used for vManage and vSmart communications and DTLS is used for vBond communications.

g) The Fujitsu SD-WAN design implements control plane integrity by combining two security elements: SHA-2 message digests, and public and private keys.

h) SHA-2 are cryptographic hash functions that generate message digests for each packet sent over a control plane connection. SHA-2 is a family that consists of six hash functions with digests that are 224, 256, 384, or 512 bits. The receiver then generates a digest for the packet, and if the two match, the packet is accepted as valid. SHA-2 allows verification that the packet's contents have not been tampered with.

i) The second component of control plane integrity is the use of public and private keys. When a control plane connection is being established, a local SD-WAN device sends a challenge to a remote device. The remote device encrypts the challenge by signing it with its private key, and returns the signed challenge to the local device. The local device then uses the remote device's public key to verify that the received challenge matches the sent challenge.

j) Then, once a control plane connection is up, keys are used to ensure that packets have been sent by a trusted host and were not inserted midstream by an untrusted source. The authenticity of each packet is verified through encryption and decryption with symmetric keys that were exchanged during the process of establishing the control connection.

8.16.2: Data Plane Security

a) The underlying foundation for security in the Fujitsu SD-WAN data plane is the security of the control plane.

b) Because the control plane is secure (all devices are validated, and control traffic is encrypted and cannot be tampered with) the Fujitsu SD-WAN devices can be confident in using routes and other information learned from the control plane to create and maintain secure data paths throughout a network of routers.

c) The data plane provides the infrastructure for sending data traffic among the routers in the Fujitsu SD-WAN overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The SD-WAN data plane implements the key security components of authentication, encryption, and integrity in the following ways:

d) Authentication, the SD-WAN control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:

i. As standard the 'traditional' Fujitsu SD-WAN key exchange model, the vSmarts sends IPsec encryption keys to each edge device.

ii. In the optional pairwise keys model, the vSmart sends Diffie-Hellman public values to the edge devices and they generate pairwise IPsec encryption keys using ECDH and a P-384 curve

iii. The LEC Fujitsu SD-WAN uses the optional pairwise keying model.

iv. By default IPsec tunnel connections use a modified version of the Encapsulating Security Payload (ESP) protocol for authentication on IPsec tunnels. This version of the protocol also checks the outer IP and UDP headers. Hence, this option supports an integrity check of the packet similar to the Authentication Header (AH) protocol.

v. **Encryption —** Data encryption is done using [redacted].

vi. **Integrity —** To guarantee that data traffic is transmitted across the network without being tampered with, the data plane implements several mechanisms from the IPsec security protocol suite:

1. The modified version of ESP uses an AH-like mechanism to check the integrity of the outer IP and UDP headers. You can configure the integrity methods supported on each router, and this information is exchanged in the router's TLOC properties. If two peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.

2. The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

8.16.3: Cipher Suites

a) vManage, vBond, vSmart and C8000v use the cipher suites listed in the following Table.

Cryptographic Operations	Control Plane (vBond/vSmart to C8000v)	Management Plane (vManage to C8000v)	Data Plane SD-WAN (C8000v to C8000v)	Data Plane Pairwise (C8000v to C8000v / 3rd Party)
Secure Protocols	[redacted]		IPsec Proprietary ESP	IPsec
Digital Signature Generation and Verification	2048-bit RSA		Control Plane	Control Plane
Key Agreement	[redacted]		vSmart control	ECDH-P-384
Symmetric Encryption and Decryption	[redacted]		[redacted]	[redacted]
Message Authentication	[redacted]		AES-GCM	AES-GCM

Table 20: Cryptographic Operations of Cisco SD-WAN

8.16.4: Internet Connectivity

a) For internet connections used as the underlay the SD-WAN will use [redacted] level 1 compliant SD WAN encryption algorithms.

8.16.5: TLS

a) From Service Commencement the Authority is responsible for certification and provision of TLS software meeting NPIRMT standards for the applications. The Fujitsu Managed Cisco SD-WAN will provide a connection (and routing) to support the TLS protected applications in accordance with the features and functionality of the Cisco SD-WAN version software guide.

8.16.6: Edge Device Security Boundary

a) The following figure defines the security boundary of the SD-WAN edge device.

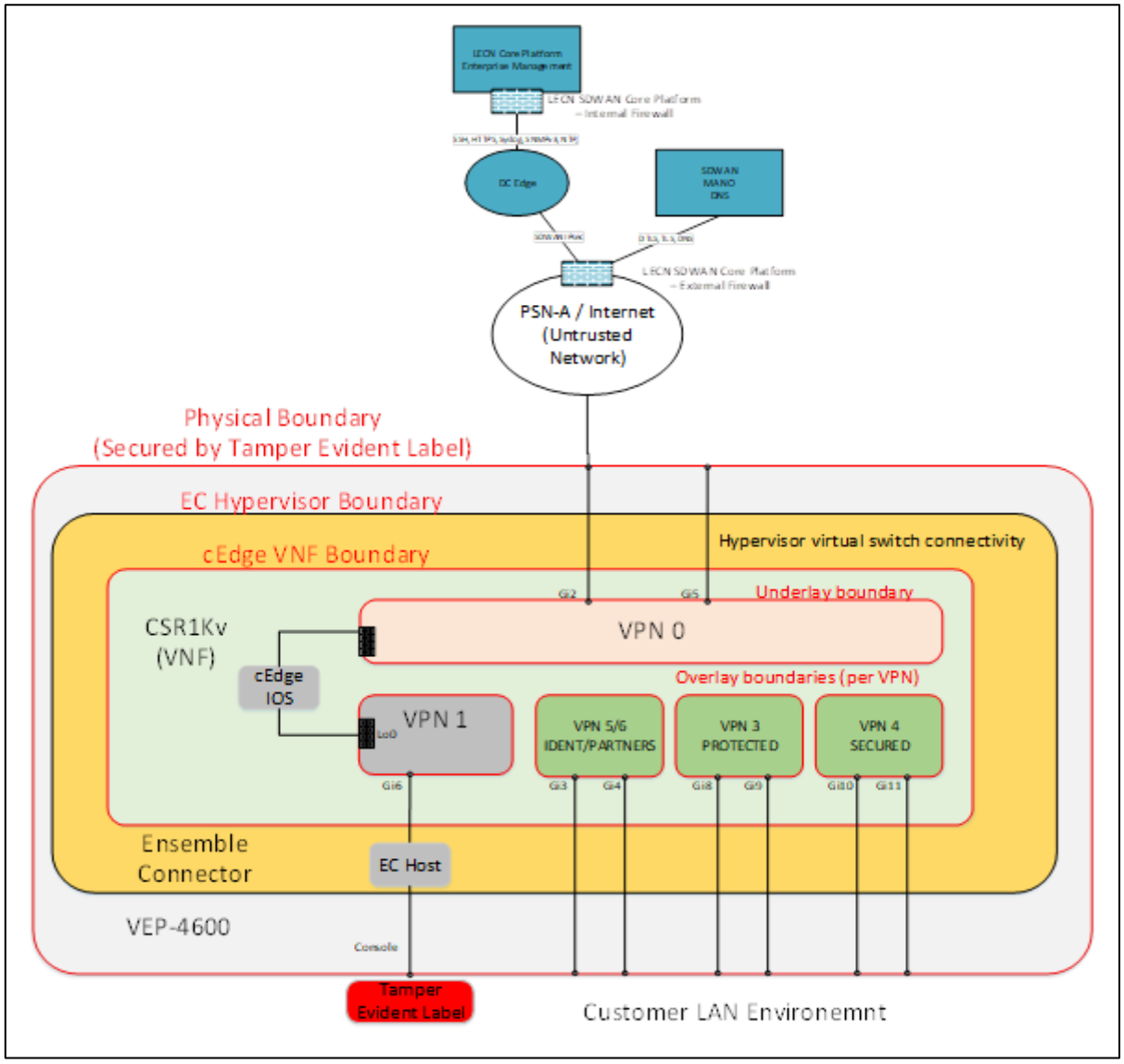

Figure 53: LEC SD-WAN edge – Port Connectivity

b) Unused ports are not allocated to a VPN and are disabled.

c) The only management and control plane access from the PSN/internet is the C8000v edge through DTLS, TLS, DNS.

d) The only data plane access from the PSN/internet is the SD-WAN overlay (IPsec).

e) The SD-WAN service VPNs cannot be accessed from the PSN/internet.

f) The Adva EC host cannot be accessed from the PSN/internet.

g) The Core Platform Enterprise Management infrastructure and toolsets can only be reached via the SD-WAN overlay Telemetry VPN (VPN1).

h) Fujitsu SD-WAN VPN1 has no external interfaces at the SD-WAN edge.

i) The Fujitsu SD-WAN edge includes the following firewalls on external facing interfaces:

   i. cEdge VPN0 host based firewall (PSN/internet underlay) - allow TLS, DTLS, DNS services only

   ii. cEdge VPN0 self-zone firewalls (PSN/internet underlay) - allow TLS/DTLS and DNS connectivity to/from LEC Core Platform only

   iii. cEdge vPN1 self-zone firewall (Core Platform) - allow management connectivity to/from LEC Core Platform only

j) The Core Platform includes the following firewalls on remote edge facing interfaces:

   i. PSN external firewall - allow TLS/DTLS and DNS connectivity to/from SD-WAN edge only

ii. Core Platform internal firewall (VPN1) - allow management connectivity to/from LEC SD-WAN edge only

8.16.7: Core Platform Security Boundary

a) The following figure (redacted) defines the security boundary of the Fujitsu SD-WAN edge device.

Figure 57: Core Platform Security Boundaries Redacted

b) Fujitsu SD-WAN MANO and DNS is located in a demilitarized zone:
   i. Physically separate external firewall provides access to the PSN
   ii. Front facing firewall permits access to VPN0 interfaces of MANO (vManage, vBond, vSmart) and cEdge in the datacentre.
   iii. Internal firewall permits access to management VPN (VPN512) of the SD-WAN MANO and DNS components; and service VPNs of the cEdge.

c) Front facing firewall provided PRIME IPsec connectivity to front facing firewall in opposite datacentre via DC interconnect for PSN connectivity resilience.

d) Front facing firewall only permits IPsec and IKE to be routed via internal firewall.

e) cEdge provides controlled access to the LEC Core Platform via SD-WAN overlay service VPNs:
   i. **VPN: 1** Enterprise Management toolset
   ii. **VPN2:** Elasticsearch syslog forwarding
   iii. **VPN3 – PROTECTED:** Buyer portal

f) Internal firewall permits access from SD-WAN overlay (VPN1) to Enterprise Management infrastructure and toolsets:
   i. NTP
   ii. LiveNX (cflowd, SNMPv3)
   iii. Elasticsearch (syslog)
   iv. Zabbix (SNMP)
   v. RDS (SSH)
   vi. ELS (HTTPS)
   vii. ISE (TACACS+)

g) The Core Platform internal firewall cannot be accessed from the PSN/internet.

9: LEC Service Pack 3 Buyer Supplied Components

9.1: Edge hardware replacement

9.1.1: The Buyer, in accordance with the Variation process may request Fujitsu replace the legacy DELL edge or Advantech edge devices, with the Buyers supplied Cisco Generation 2 range (G2) devices. The Charges for the deployed legacy DELL 4600 or Advantech edge devices and Adtran (ADVA) License application software (under DELL 4600 and ADVA Management for 8 core Appliance) are detailed in the Supplier's Platform pricing document and shall continue to apply until the Fujitsu rented edge devices are replaced with the Buyers Cisco G2 edge devices.

9.1.1.2 Upon removal of Fujitsu, legacy DELL 4600 or Advantech edge devices, the Buyer shall be responsible for the Charges to perform a data wipe of the devices (under Appliance Data Wipe) detailed in the Supplier's Platform pricing document.

9.1.2: The Buyer is responsible for the selection of Cisco G2 edge devices and warrants the devices selected are suitable for the service considering bandwidth throughput, functionality, CPU storage and compatibility with the Cisco Gold Star SD-WAN version deployed by Fujitsu.

9.1.2.1 The Buyer warrants the Cisco G2 edge devices support the Mean Time Between Failure (MTBF) requirements Fujitsu use to underpin the Service Level Agreement provided by Fujitsu detailed in paragraph 11

9.1.2.2 The Buyer warrants the Cisco G2 edge devices selected comply with Police Digital Service and NCSC standards for nominated CNI infrastructure.

9.1.2.3 To support the Buyers selection of Cisco G2 edge devices, the Buyer shall be responsible for all Charges from Fujitsu for periodic Cisco G2 edge device IT Health Checks and functional testing to comply with the certification and Service Level Agreement, in paragraph 11 of this Service Definition document. The Charges will be agreed in accordance with the Variation process. The Charges to perform the services required shall be in accordance the G-Cloud Rate Card – UK Onshore detailed in the Supplier's Platform pricing document.

9.1.3 The Buyer shall provide a detailed deployment plan, for the Cisco G2 edge devices sufficient for Fujitsu to schedule its resources. The plan shall include Fujitsu standard lead times, pre-staging activity, completion of all testing and system configuration changes as identified by Fujitsu. A minimum of four weeks' notice will apply to amend Fujitsu scheduled deployment and or test dates.

9.1.3.1 Compatibility testing with the Fujitsu deployed Cisco Gold Star SD-WAN version and IT Heath Check, shall be completed by Fujitsu before deployment of Cisco G2 edge devices may commence.

9.1.3.2 The Buyer shall be responsible for the delivery of the Cisco G2 edge hardware to the Fujitsu nominated secure storage facility.

9.1.3.3 The Buyer shall be responsible for the costs of the Cisco G2 edge device prestaging activity, creation of work instructions, security labels and shipment to the Buyers sites (by way of the deployment Charge per device) detailed in the Supplier's Platform pricing document.

9.1.3.1 The Buyer shall be responsible for edge device deployment Charges, incurred at a site, software changes, configuration changes to the service and creation of site-specific designs, these Charges shall be agreed in accordance with the Variation process. The Charges from Fujitsu to perform the Services required shall be in accordance G-Cloud Rate Card – UK Onshore detailed in the Supplier's Platform pricing document.

9.1.3.2 Fujitsu will deploy the current LEC Service pack 3 templates on to the Cisco G2 edge devices, in accordance with the SFIA rate card detailed in the Supplier's Platform pricing document.

9.1.3.3 Use of Configuration Groups for the Cisco G2 edge devices is not supported with the current LEC Service Pack 3 design.

9.1.3.4 The Buyer shall allow, without change or limitation, Fujitsu to deploy the LEC Service Pack 3 configuration (or changes as agreed and documented in accordance with the Variation process) and Fujitsu certificates on to the Buyers supplied Cisco G2 edge devices.

9.1.3.5 The Buyer shall provide assistance per site, "smart hands" to deploy the Cisco G2 edge devices as directed by Fujitsu, using all guidance, recommendations and the Fujitsu installation workbooks provided.

9.1.4 The Buyer shall be responsible for the provision of maintenance spares as required by Fujitsu (and the prompt replacement of returned faulty devices) to Fujitsu's nominated secure facility. In the event the Buyer fails to provide Fujitsu with maintenance spares the Service Level Agreement detailed in paragraph

11 of this Service Definition document, for edge devices shall be suspended until sufficient maintenance spares are provided.

9.1.5 The Cisco G2 edge devices shall be maintained by Fujitsu in accordance with the Service Level Agreement detailed in paragraph 11 of this Service Definition document.

9.1.5.1 The Buyer shall be responsible for the break fix services (project) for the Cisco G2 edge devices as detailed in the Supplier's Platform pricing document.

9.1.6 The Buyer shall upon ceasing the Fujitsu Service at a site, allow Fujitsu without change or limitation to perform a factory reset of Buyer supplied Cisco G2 edge devices. Upon resetting the Cisco G2 edge device to factory settings, Fujitsu responsibilities for device and Service at the site shall cease.

9.1.7 The configuration data of the edge device can be requested by the Buyer in accordance with the Variation process which will be impacted by Fujitsu for availability using the G-Cloud Rate Card – UK Onshore detailed in the Supplier's Platform pricing document. The data available and format provided will be in accordance with Fujitsu SD-WAN service stated policies and procedures.

9.1.8 Within 30 days of expiry of the Call-Off Term, Fujitsu will arrange for the return of all Buyer provided edge devices (spares or returned devices held in store) to the Buyer.

9.1.9 ACCSEC tracking of the edge devices will be transferred by Fujitsu to the Buyer upon ceasing responsibilities for the edge device deployed at the site.

9.2 Smart Account Access for Buyer SD-WAN Licences

9.2.1 The Buyer, using the Variation process may request Fujitsu deploy Buyers supplied Cisco SD-WAN licences. The Charges for Fujitsu's SD-WAN Software subscription charge per site detailed in the Supplier's Platform pricing document deployed for sites shall continue to apply until the Fujitsu licences are removed from Service.

9.2.1.1 The Buyer shall appoint Fujitsu to operate and manage the Buyers SD-WAN Licences purchased from Cisco by way of a Variation request in accordance with the Variation process, for use with the Buyers Cisco G2 edge device hardware only.

9.2.1.2 The Buyer shall be responsible for the cost of the Cisco of Catalyst SD-WAN Licences, suitable for the LEC Service Pack 3, as advised by Fujitsu.

9.2.1.3 The Buyer shall be responsible for the creation costs of a Home Office Smart Account together with a licensing arrangement that enables Fujitsu to deploy and manage the licences on its behalf.

9.2.1.4 The Buyer acknowledges all edge devices or cloud deployments allocated for Service Pack 3 will require a Cisco Catalyst SD-WAN license to operate, including licences deployed in Fujitsu's "infrastructure".

9.2.2 The Buyer shall be responsible for the termination charge of Fujitsu's SD-WAN Software subscription charge per site DNA Advantage detailed in the Supplier's Platform pricing document.

9.2.3 The Buyer acknowledges access, or integration with shall not be provided to the Buyer or to any appointed agent on its behalf access to Fujitsu's SD-WAN Smart Accounts or its Cisco License Server.

9.3 LEC Service Pack 3 NNI Development

LEC Service Pack 3 supports a Network-to-Network Interface (NNI) design service and managed service capability. The NNI will comprise of a physical or logical demarcation point, to be deployed in the Buyers facilities. The NNI connects Fujitsu's SD-WAN Service to the Buyers replacement SD-WAN Service.

The NNI will be used by the Buyer and Fujitsu as an assured method to allow traffic to traverse between both SD-WAN platforms with limited signalling protocol capability. The NNI shall serve as the SD-WAN boundary for responsibilities between Fujitsu and the Buyer and will be required before transition of services from Fujitsu to the Buyer can commence.

Upon receipt of a Variation request in accordance with the Variation process, from the Buyer, Fujitsu shall agree the timescales to create a statement of work and the proposed functionality to be deployed. The development of the NNI solution, any resulting testing, and deployment costs together with service management responsibilities will be subject to the charges from Fujitsu in accordance with the G-Cloud Rate Card – UK Onshore detailed in the Supplier's Platform pricing document.

10 Service Pack 3 LEC Service Delivery

Fujitsu's ISO/IEC 27001, operations are certified by Bureau Veritas. As an example, Fujitsu implements the following best service and security practice:

- Established Data Protection Act program across Fujitsu's UK business
- Certified for Cyber Essentials for Fujitsu EMEA
- Certified for Cyber Essentials Plus DNS UK operations
- Fully compliant with ISO/IEC20000 IT service management
- Business continuity planning certified to ISO/IEC22301:2012
- Membership and active participant in:
    - The Information Security Forum, Standard of Good Practice
    - Information Security Forum Securing the supply chain – implementation guide
    - Information Security Forum Securing the supply chain – preventing your suppliers' vulnerabilities becoming your own.
    - Active participant in UK HMG's joint best practice security working groups.

In addition, the Fujitsu proposed third-party platform has the following:

- Fully complies with ISO27002-2013 Information Technology – Security Techniques
- Operates ISO27036 – for supply chain security
- A relationship model aligned to ISO440001
- Operates under the PDS / NPIRMT / PASF Assurance scheme.

To enable certification continuity across all procedures and operations, Fujitsu carries out the Deming "Plan-Do-Check-Act" (PDCA) cycle.

Fujitsu is an ITIL® aligned and ISO/IEC20000-1 conformant supplier, and deploys, manages and continually improves Service Management processes that are underpinned by standard technologies.

The Service Management process that Fujitsu will deploy for managing the Service will include the following key processes and functions:

- Incident Management
- Problem Management
- Event Management
- Change Management
- Availability Management
- Capacity Management
- Protective Monitoring
- Access to design and deployment consultants to support project.

10.2 Service Demarcation Responsibilities

The table below provides the service demarcation points between the Buyer and Fujitsu further clarity will be provided in the Statement of Work if required:

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
Overlay Provision from Fujitsu SD-WAN	Buyer	Buyer responsible for all connectivity and bearer performance
Fujitsu will provision hosted controllers for Cisco Catalyst SD-WAN overlay and hand	Fujitsu	

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
over Cisco SD-WAN Manager access to the Buyer.		
Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure/CPU and Data Disk Utilisation	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Protective Monitoring by Fujitsu will comprise of the Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure only, based on MITRE ATT&CK framework Service using Elasticsearch, Kibana and Logstatsh stack.	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Note standard service excludes edge device monitoring, firewall configuration connection of new devices or the monitoring of data traversing the Buyer network	Managed by Fujitsu	
Buyer is responsible via the Fujitsu portal/Catalyst SD-WAN Manager controller SecOps dashboard to view and manage network security events and actionable threat data to effectively maintain its cyber resilience. An optional SIEM feed can be provided to the Buyer.		
Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure/Loss of connectivity to network interfaces	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring and troubleshooting of Fujitsu SD-WAN Cloud controller infrastructure/Failure to reach instances	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services /Availability of the Fujitsu Portal	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services / Loss of control connection to the controllers	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Monitoring of Fujitsu SD-WAN services / Capacity management of Cisco Catalyst SD-WAN Controllers	Managed by Fujitsu	Fujitsu monitors and upgrades the instance capacity and expansion to clusters based on the number of devices on the overlay.
Disaster recovery / Take periodic volume-based snapshots	Managed by Fujitsu	The volume-based and config-based snapshot is for the entire platform Cisco SD-WAN Manager cluster, not for a particular tenant.
Disaster recovery / Take periodic configuration-based backups	Managed by Fujitsu	The volume-based and config-based snapshot is for the entire

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
		platform Cisco SD-WAN Manager cluster, not for a particular tenant
Disaster recovery / On-demand snapshots	Managed by Fujitsu	The volume-based and config-based snapshot is for the entire platform Cisco SD-WAN Manager cluster, not for a particular tenant
Disaster recovery / Restore overlay based on volume or configurations	Managed by Fujitsu	The volume-based and config-based snapshot is for the entire platform Cisco SD-WAN Manager cluster, not for a particular tenant
Onboard to Cisco SD-WAN Analytics	Buyer	LiveAction (LiveNX) Analytics is by default onboarded for cloud-delivered Cisco Catalyst SD-WAN customers
Renew controller certificates (before expiration)	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Upgrade software / Controller software upgrade	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Upgrade software / edge device/node software upgrade	Managed by Fujitsu	
Upload and manage edge images in Cisco SD-WAN Manager Software Repository	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Respond to Fujitsu notifications to authorise the service window, instance reboot, review, or verify changes carried out by Fujitsu	Buyer	
Accept external management of SA/VA and map tenant VA to Buyer SA/VA	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Define configure and deploy device configuration templates and policies through Cisco SD-WAN Manager	Buyer	Note Buyer responsible for defining policies and resulting performance
Perform user activities that require logging in to Cisco SD-WAN Manager. For example, template and policy configuration, and edge device management	Buyer	Note Buyer responsible for defining policies and resulting performance
Web server certificates	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the Buyer to report incidents and to raise service requests
Edge serial sync with credentials	Buyer	Cloud-delivered Cisco Catalyst SD-WAN Buyers can sync edge serials without credentials (using Single-Sign-On)
Manage allowed access-list with Buyers source public IP ranges for management access of controllers.	Buyer	

Task	Shared Hosted Cloud Catalyst SD-WAN Responsibility	Comments
Before making any changes in the Portal, take the on-demand snapshot using the procedure, and configuration backup using procedure	Buyer	

Table 21: Service Demarcation Responsibilities

10.3 Fujitsu Cloud Infrastructure Support

- Fujitsu will carry out disaster recovery workflows, including snapshot volumes or configurations. Restore Cisco SD-WAN Manager clusters based on volumes or configurations.
- Fujitsu will provision custom subnetting to extend Buyers premises network into cloud-hosted overlay network.

10.4 Fujitsu Capacity Management

Fujitsu will monitor the growth of devices per overlay along with the controller instance capacity parameters such as CPU, disk, and memory utilisations. Follow a pre-set guideline to increase the capacity of the service instances as needed.

10.5 Protective Monitoring & SOC SIEM Support

Enhanced Protective Monitoring provided (optional service) shall be based on the defined use cases agreed with the Buyer(contained in [redacted]). Changes to use cases or resources will be subject to change control. Fujitsu will provide feeds from the Elasticsearch, Kibana and Logstatsh stack, to the Buyer's SIEM using the format agreed in [redacted]

10.6 Data wipe of edge equipment

Fujitsu will provide a data wipe of the DELL 4600 or Advantech edge equipment withdrawn from service by the Buyer or Fujitsu. This shall be chargeable in accordance with the Supplier's Platform pricing document.

11 Service Pack 3 Service Levels, LEC

Fujitsu SD-WAN Core Service shall meet or exceed the performance standards described below ("Service Level").

11.2 Service Availability

Service	Availability Target	Availability Measurement
Catalyst SD-WAN Core Service	99.99%	24x7x365 over a quarterly period. Availability will be defined as the ability of the core platform to provide SD-WAN "Data Path Functionality between edge nodes
High Availability (HA) Sites	99.99%	24x7x365 over a quarterly period. edge device availability will be defined as the ability for the edge HA solution to route traffic in accordance with the routing and policies programmed from the Catalyst SD-WAN Manager to provide defined SD-WAN functionality
Standard Sites (Single edge)	99.99%	24x7x365 over a quarterly period. edge device availability will be defined as the ability for the edge device to route traffic in accordance with the routing and policies programmed from the Catalyst SD-WAN Manager to provide defined SD-WAN functionality

Table 22: Service Availability SLAs

11.3 Service Level Response Time

Service Measure	Description	Support Hours	Target Response Time
Priority 1 (Major) Standard	Major business disruption: critical user or user group unable to operate, or an entire service experiencing significant reduction in system performance	Incident resolution 09:00-17:00 Mon-Fri GMT/BST excluding any public holidays with uplifts to 24x7 365 support cover see catalogue Note platform monitored 24x7 365 days. Faults may be reported 24x7 365 days	1 hour
Priority 1 (Major) Premium	Major business disruption: critical user or user group unable to operate, or an entire service experiencing significant reduction in system performance	24x7x365 days	1 hour
Priority 2 (Medium)	Partial service disruption to a live/production service.		2 hours
Priority 3 (Low)	Minor disruption: single user or user group experiencing problems, but with circumvention available.		8 hours
Priority 4 (Very Low)	Enquiry: single user or user group requiring assistance but with no direct impact on business. For example, a request for information.		24 hours

Table 23: Service Measure

11.4 Edge device SLAs

11.4.1 High Availability edge sites

	Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1)	Performance Indicator only
HARDWARE	**P1**	Hardware failure of All edge devices preventing site connectivity.	24x7x365	30 minutes	8 hours	98% of all hardware faults fixed within 8 hours	100% of hardware faults fixed in 24 hours.
	P2	Hardware failure of a single edge device not preventing site connectivity.	24x7x365	30 minutes	72 hours	98% of all hardware faults fixed within 72 hours	100% of hardware faults fixed in 96 hours.
SOFTWARE	**P1**	Failure of All edge devices preventing site connectivity.	24x7x365	30 minutes	4 hours	98% of all faults (where remote support capable) fixed within 4 hours	100% of faults where remote support capable) fixed within in 8 hours.
	P2	Failure of a single edge device not preventing site connectivity.	24x7x365	30 minutes	8 hours	98% of all faults (where remote support capable) fixed within 8 hours	100% of faults where remote support capable) fixed within 24 hours.

Table 24: edge Device SLAs – High Availability edge Sites

11.4.2 Standard edge Sites

	Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1)	Performance Indicator only
HARDWARE	P1	Hardware failure of a single edge device preventing site connectivity.	24x7x365	30 minutes	12 hours	98% of all hardware faults fixed within 12 hours	100% of hardware faults fixed in 24 hours.
SOFTWARE	P1	Failure of a single edge device preventing site connectivity.	24x7x365	30 minutes	4 hours	98% of all faults (where remote support capable) fixed within 4 hours	100% of faults (where remote support capable) fixed within in 8 hours.

Table 25: edge Device SLAs – Standard edge Sites

11.4.3 edge Device Replacement SLAs

Service	Support Hours	Resolution Time	Resolution Target (1)
High Availability Sites	24x7x365	72 hours	100% of all hardware replacements delivered to site within 72 hours
Standard Sites	24x7x365	72 hours	100% of all hardware replacements delivered to site within 72 hours

Table 26: edge Device SLAs – Replacement SLA

All service levels have a target that 95% will be fixed within the SLA, subject to a minimum volume as advised.

The incident period is measured based on the timings from ITSM; from incident raised to the time at which the incident is set to 'resolved'.

Repeated Buyer provided hardware failure that exceeds published Meantime Between Failure performance will incur additional SFIA rate card charges as advised by Fujitsu.

11.5 Service Desk

Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1) (SLA)	Resolution Target (2)
P1	Severe business disruption: Any existing core servers are unavailable or unable to be managed. Loss of all network connections or firewalls at core datacentres	24x7x365	30 minutes	4 hours	98% of all hardware faults fixed within 4 hours	100% of hardware faults rectified in 8 hours
P2	Major business disruption: Application services are unavailable or unable to be managed.	24x7x365	1 hour	8 hours	90% in 8 hours	100% in 16 hours

Priority	Definition	Support Hours	Response Time	Resolution Time	Resolution Target (1) (SLA)	Resolution Target (2)
	Loss of a network or firewall connection at core datacentres Loss of core resilience but service to site operating					
P3	Minor business disruption: Authority unable to manage resources within the user portal	Monday to Friday 0800-1700hrs (Excluding Bank Holidays)	5 hours	3 working days	90% in 3 working days	100% in 6 working days
P4	Minor disruption. Single user or user group experiencing problems with the user portal or API, but with circumvention available.	Monday to Friday 0800-1700hrs (Excluding Bank Holidays)	1 working day	5 working days	90% in 5 working days	100% in 10 working days
P5	Enquiry: Single user or user group requiring assistance but with no direct impacts on business. Example: a request for information or change request.	Monday to Friday 0800-1700hrs (Excluding Bank Holidays)	2 working days	10 working days	80% in 10 working days	100% in 20 working days

Table 27: Core Platform SLAs

11.5.1 Problem Management Priority Levels and Definitions

Ref	Definition	Resolution Target (1)	Performance Indicator
PM1	**Level 1 (P1):** The Problem poses significant risk to the Buyers business or operations in that the Incident or series of Incidents may result in significant adverse impact to the Buyer operations. No Workarounds have been identified to Resolve the Problem.	10 Working Days	20 Working Days
PM2	**Level 2 (P2):** The Problem poses no immediate risk to the Buyer business or operations but may, if not Resolved, result in degradation in the performance of a Service. Workarounds are available to Resolve the Problem.	1 Month	40 Working Days
PM3	**Level 3 (P3):** The Problem poses no risk to the Buyer business or operations but may in the long term impact on the overall performance of a Service	6 Months	N/A
PM4	The percentage of all Problems occurring during the Service Measurement Period that Fujitsu has Resolved within the relevant Resolution Time for each Problem. Problems shall only be considered as validly Resolved if the service desk has Resolved the Problem and notified the Buyer that it has Resolved such Problem by completing the relevant sections of the relevant Problem Record.	95%	100%

Table 28: Problem Management

11.6 Service Reporting

Service Reporting encompasses the production and delivery of defined reports to accurately report against agreed Service Level Agreements. Excluding the Daily Service Update Report, which only provides volumetric data.

Fujitsu will provide the following reports on a Daily, Monthly and Quarterly basis:

- Daily Reporting

- Daily Service Update Report
  - Generate the Daily Service Update Report each Working Day with respect to the immediately preceding Working Day (Monday – Friday)
    - Information pertaining to Saturdays and Sundays to be included within Monday's report
  - Email the Daily Service Update Report to the SDM by 09:00 each day.

11.6.1 Monthly Reporting

ITSM Monthly Service Reports (from SCSM)

- ITSM Service Reports are provided as part of the monthly service reviews and will generate the following pre-built reports on a monthly basis generated from the ITSM toolset:

Report Area	Report Name	Description
Change Management	List of Change Requests	Provides a list of change requests within a certain time frame. The data in this report includes the current status, category, and user to whom the request is assigned.
Incident Management	Incident Resolution	Provides the number of incidents, including the number of incidents past their targeted resolution time and the average time to resolution. You can filter the data by day, week, month, quarter, or year.
Incident Management	List of Incidents	Provides a list of all incidents within a certain time frame. The data in this report includes the users to whom incidents are assigned, when the incidents were created, and the current status of the incidents.
Problem Management	List of Problems	Provides a list of all problems within a certain time frame.
Security Incident Management	List of Incidents	Provides a list of all security incidents within a certain time frame. The data in this report includes the users to whom incidents are assigned, when the incidents were created, and the current status of the incidents.
Configuration Items (CIs)	List of CIs	Provide a list of all CIs within the estate

Table 29: ITSM Monthly Service Reports

11.6.2 Additional Monthly Reports

- Forward Schedule of Change (derived via SCSM)
- Forward Schedule of Release (derived via SCSM)
- Patch Compliance Report/Statement of Conformance.
- SPLA Licence (Service Provider Licence Agreement) Report
- BRA07 Spares Pool Stock Report

11.6.3 Quarterly Reporting

- Availability Reports

11.6.4 Annual Reporting

Annual AccSec Audit/Reporting; Fujitsu provides the Buyer with access to records which tracks location and status of all security encrypted ACCSEC edge devices throughout its life and into its terminal state.

12 Licence Capacity

The Buyer shall be responsible for the selection of appropriate licences (for example tier capacity) detailed in the Supplier's Platform pricing document.

In the event the licence capacity exceeds 90% for 2 consecutive months, Fujitsu will, upon 30 days' notice, limit the capability to the stated licence tier (thus preventing any burst capability). Upon such notice the Buyer may request Fujitsu to upgrade to the next licence tier for which the Buyer will be responsible for the relevant licence cost (including any SFIA charges to deploy). Or accept the throughput will be limited to the maximum capacity of the licence tier ordered.

The Buyer should note changes to a licence tier may require an edge Device upgrade (throughput capacity), which will be advised by Fujitsu. Changes to edge Device will be subject to charges as detailed in the Supplier's Platform pricing document.

Appendix 1 – Glossary of Terms

ACL	Access Control Lists
Active / Active	High Availability dual configured devices deployed
AD	(Microsoft) Access Directory
API	Application Programming Interface
AppQoE	Application Quality of Experience
AVC	Application Visibility Control
BCDR	Business Continuity and Disaster Recovery
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BIOS	Basic Input-Output System
Broadcom	To Detect Packed Malware
CA	Certificate Authority
Catalyst SD-WAN	Cisco SD-WAN Software (previously Viptela)
CI	Configuration Items
CIR	Committed Information Rate
CLI	Command Line Interface
CPE	Customer Premises Equipment
Configuration Groups	Deployed on Cisco second generation (G2) edge devices replacing Fujitsu templates
DIA	Dedicated Internet Access
DNS	Domain Name System
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
DTLS/TLS	Datagram/Transport Layer Security
eBGP	External Border Gateway Protocol
EC hypervisor	Virtual Appliance and hypervisor
ECMP	Equal Cost Multi Path
edge	Site or Datacentre CPE device
EIGRP	Enhanced Interior Gateway Routing Protocol
Elastic	Used to support Search, Observability, and Security
ELS	Early Life Support
ESO	Ensemble Service Orchestration
FEC	Forward Error Correction
FSC	Facility Security Clearance
G2	Second Generation Cisco edge device
Gbps	Gigabit per second
GNSS	Global Navigation Satellite System
GRE	Generic Routing Encapsulation
HA	High Availability
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IaaS	Infrastructure as a Service
IKE	Internet Key Exchange
IP	Internet Protocol
IPS/IDS	Intrusion Prevention Detection or System
IPSec	Protocols used to set up encrypted connections
iSCSI	Internet Small Computer Systems Interface
ISE	Cisco Identity Services Engine
ISO	International Organisation for Standards
ISP	Internet Service Providers

ITHC	IT Health Check
ITIL	IT Infrastructure Library
ITSM	Information Technology Service Management
KVM	Kernel Virtual Machine
LAN	Local Area Network
LEC	Law Enforcement Community
LiveNX	Live Action Statics Collector
LOSS	Lightweight Operation Support System
LTE	4g or equivalent Mobile Network Connectivity
Mbps	Megabits per second
MPLS	Multiprotocol Label Switching
MSL	Master Site List
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NCSC	National Cyber Security Centre
NFVI	Network Function Virtualisation Infrastructure
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NNI / s	Network to Network Interconnects
NPIRMT	National Policing Information Risk Management Team
NPPV	Non-Police Personnel Vetting
NSS	Zscaler Nanolog Streaming Service
NTP	Network Time Protocol
OFFICIAL	HMG Security Handling Classification
OMP	Overlay Management Protocol
OSPF	Open Shortest Path First
OSS	Operational Support System
PASF	Police Assured Secure Facilities
PDS	Police Digital Service
PKI	Public Key Infrastructure
PLP	Packet Loss Priority
PM	Problem Management
PRIME	NCSC Encryption Standards
PSN	Public Services Network
PSNfP	Public Services Network for Policing
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Access Dial In User Service
RAM	Random Access Memory
RBAC	Roles Based Access Control
RDS	Remote Desktop Servers
SaaS	Software as a Service
SAL	Security Aspects Letter
SASE	Secure Access Service edge
SAT	Service Activation Testing
ServiceNow	ITSM Toolset for Service Management and Portal Access
SDM	Service Delivery Manager
SDN	Software Defined Network (holistic term of Suppliers services)
SD-WAN	Software-Defined Networking in a Wide Area Network
SFIA	Skills Framework for the Information Age
SIG	Secure Internet Gateway
SLA	Service Level Agreement
Smart Hands	Semi-skilled local person completing tasks as allocated

SME	Small Medium Enterprise
SOC	Security Operations Centre
SSE	Security Service edge
SSL	Secure Socket Layer
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
Tenable	Used for Security Scanning
TLOC	Transport Locator
Templates	Configuration details of SD-WAN routing tables deployed on Fujitsu edge devices
UC	Unified Communications
UCS	Unified Computing System
uCPE	Universal Customer Premise Equipment
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
Veeam	Used for Advanced Backup & Restore
VLANs	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function
VPN	Virtual Private Network
VRF	Virtual Route Functions
VRRP	Virtual Router Redundancy Protocol
vTA	Virtual Test Agent
Zabbix	Used for Network and Application Monitoring

About Fujitsu

As one of the world's leading IT companies, Fujitsu is at the forefront of pioneering technology in the UK since we made our initial investment over 40 years ago. As a key strategic partner we deliver essential services, from our secure hybrid IT which underpins critical national infrastructure to our investment in emerging technologies to boost national capability. Drawing on our Japanese technology expertise we provide bespoke digital transformation solutions. This unrivalled expertise has allowed us to specialise in emerging focus areas; Hybrid IT, AI & RPA, Data analytics, Agile application development/transformation and Security. Together, we offer a full package of solutions to support the UK as a long-term industry supplier.

We believe in realising the significant alignment between the UK and Japan in emerging technologies and in creating a UK-Japan 'Innovation Bridge' to support the UK's science and technology superpower objectives. We are committed to investment in UK skills and research and development, driving customer outcomes and promoting social value. We employ 124,000 people around the globe, including around 8,000 people across the UK, promoting diversity and inclusion as a DWP Disability Confident Leader. We are recognised as a Times Top 50 employer for Women since 2017, a Stonewall Top 100 Employer for 2023 and were awarded an EcoVadis Silver Rating, the world's largest provider for sustainability ratings.

Contact: government.frameworks@fujitsu.com