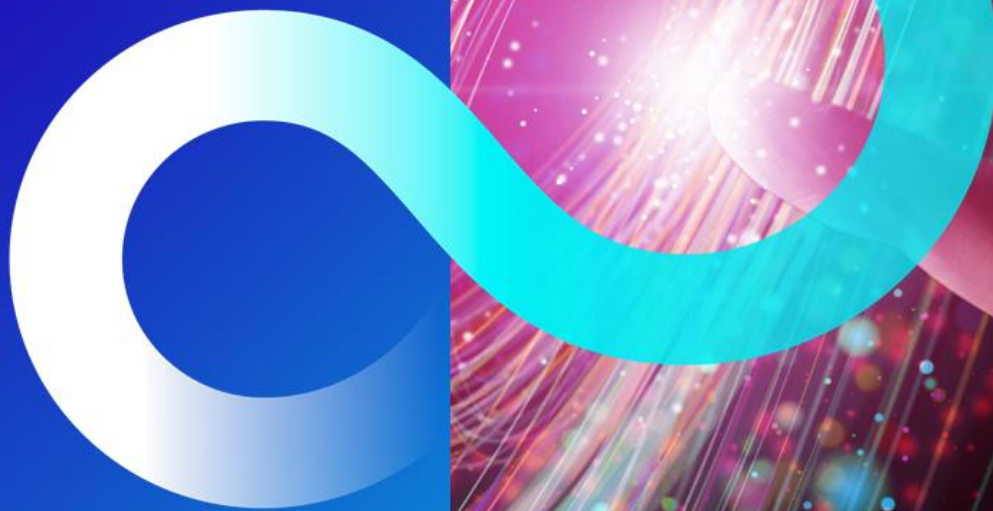


Service Definition

Fujitsu Software Defined Networking (SD-WAN) High Assurance

FUJITSU



G-Cloud 15

Commercial in Confidence © Fujitsu 2026

Contents

1: Introduction to Software Defined Wide Area Networking (SD-WAN) Technology.....	3
1.1: Fujitsu's SD-WAN Offerings.....	4
1.2: Hosting Charges	4
1.3: Licences and Capacity	5
1.4: Edge Devices.....	5
1.5: G Cloud Continuity Services.....	5
1.6: Statement of Work Purpose	5
1.7: Configuration Data Upon Expiry	5
2: Fujitsu SD-WAN Edge Devices	6
2.1: Cisco 8000 Series.....	6
2.2: Fujitsu uCPE Series.....	12
2.3: Ensemble Connector for uCPE devices.....	15
3: SD-WAN Managed Services.....	15
4: SD-WAN FSC UK Deployed solution.....	15
4.1: Solution overview	16
4.2: Multicloud Choice and Control	19
4.3: SD-WAN Cloud OnRamp for Multicloud	20
4.4: SD-WAN Cloud Hub.....	20
4.5: SD-WAN Cloud OnRamp for SaaS.....	21
4.6: Fujitsu SD-WAN Cloud Interconnect	22
4.7: Analytics and Insights.....	23
4.8: Fujitsu SD-WAN Software Subscription Licensing.....	24
4.9: Prominent Features.....	25
4.10: Support for Security and Information Assurance	26
4.11: Certifications.....	26
5: Service Delivery.....	26
5.1: Service Demarcation Responsibilities.....	27
5.2: Fujitsu Cloud Infrastructure Support.....	29
5.3: Fujitsu Capacity Management	29
6: Fujitsu SD-WAN Service Levels	30
6.1: Service Availability.....	30
6.2: Service Level Response Time.....	30
6.3: Edge Device SLAs	31
6.4: Service Desk	32
6.5: Service Reporting.....	34
Appendix 1 – Glossary of Terms	36

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

Software Defined WAN (SD-WAN uses software-defined networking concepts to distribute network traffic across a wide area network (WAN). SD-WAN offers a cost-effective way to connect offices to customers own datacentres, SaaS or cloud-based applications. An SD-WAN provides automation, centralisation and flexibility, which creates a more agile WAN environment for Public Sector organisations.

An SD-WAN architecture creates a virtual overlay that abstracts underlying private or public WAN connections, such as Multiprotocol Label Switching (MPLS), internet broadband, fibre, wireless satellite or 5G. This virtual overlay capability means the customer 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. With Fujitsu's solution 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.

Fujitsu's SD-WAN service, is based on Cisco Catalyst SD-WAN, positioned as an overlay capability where Fujitsu provides the customer with hosting infrastructure, software and edge device options to operate SD-WAN technology. For deployment, customers plug their WAN links into the edge deployed at a location see Figure 1.

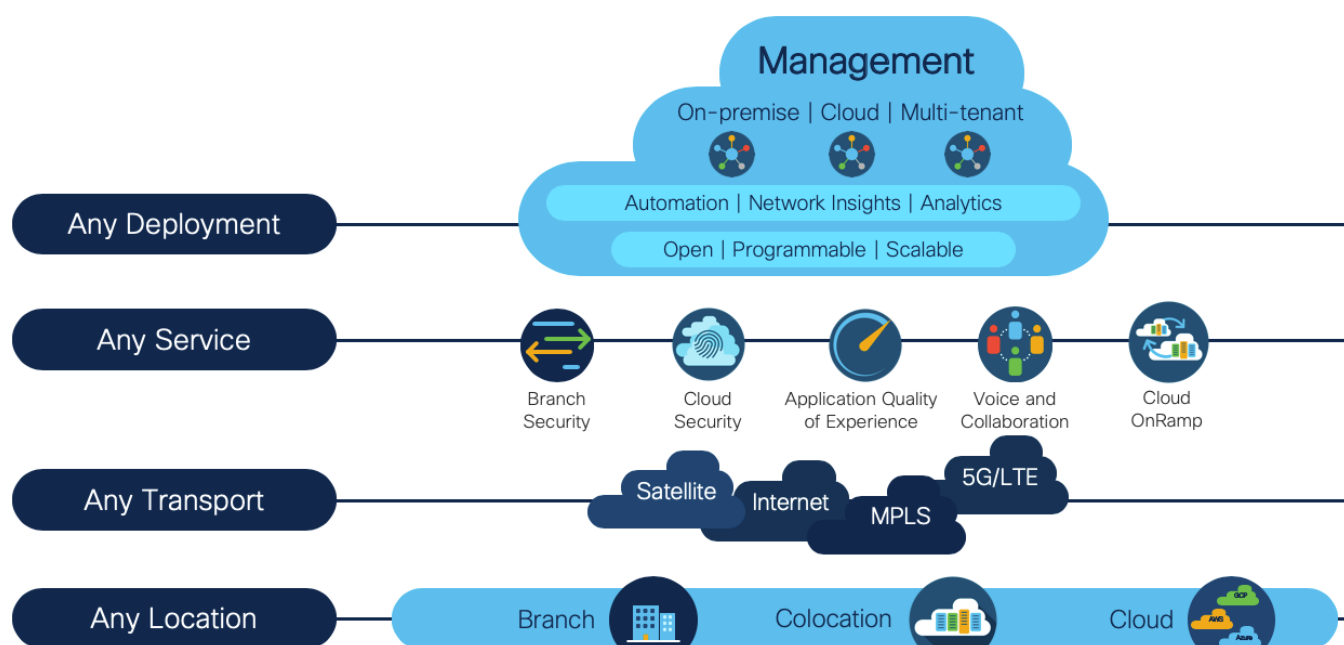


Figure 1: SD-WAN Schematic

The following sections provide a technical overview of the features functionality and service options using Fujitsu's Cisco Catalyst SD-WAN offerings. This document assumes the customer has a technical appreciation of SD-WAN technology. Customers 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 service is a fully deployed and certified subset of Fujitsu's wider Software Defined Networking services portfolio.

Fujitsu's SD-WAN G Cloud 15 service is delivered on a shared platform 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..

Fujitsu's SD-WAN offering uses best of breed vendor's technology providing customers a full catalogue of services and functionality which comprise of:

- A sovereign Cisco Catalyst SD-WAN supplemented with other Fujitsu services deployed in Fujitsu's Facility Security Cleared (FSC), certified datacentres. The certified datacentres are also certified as Police-Assured Secure Facility (PASF) facilities. The platform supports OFFICIAL with Caveat uplifts. The solution provides an assured and secure network overlay solution, complying with relevant high assurance requirements, NIST standards and current NCSC guidance.
- Managed Services, ITIL aligned services to support customer SD-WAN environments or other Cisco SD-WAN deployments, using Fujitsu tooling and procedures using catalogue charges (section 3).

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

The customer shall be responsible for the provision of all last mile connectivity to the SD-WAN Service, excluding any internet connectivity used by Fujitsu for SD-WAN management at its hosted locations.

Unless otherwise specified the customer shall perform end user management of the platform and edge devices using the portal provided. Alternatively, the customer may subscribe to itemised managed services from Fujitsu using the SFIA rate card (or day rate fractions thereof), the headline services provided by Fujitsu for SD-WAN services are detailed in section 3

Fujitsu's SD-WAN service extends into Cloud Service providers, with proven configurations detailed in the service descriptions (in association with the vendors).

The service is based on a Cisco Catalyst SD-WAN solution (using vendor recommended software [SD WAN](#) with integration into other platforms and applications using Fujitsu's own dedicated infrastructure with all Orchestrators and tooling deployed in the UK using certified datacentres and PASF and FSC Accredited facilities. The service is supported by Fujitsu UK (Defence and National Security) network operation centres (Offering support of OFFICIAL SENSITIVE infrastructure). All Fujitsu staff managing the service are at a minimum Security Cleared (SC). The service complies with relevant HM Government Information Assurance and Security guidance. This infrastructure will be monitored by Fujitsu for availability with the customer performing SD-WAN end user management.

Fujitsu operates pre-production environments aligned to the customer environment to support Fujitsu testing, patching and software updates supporting changes to recommended release software) and model office requirements. The Service aligns to Secure by Design and the published certification requirements of Police Digital Service (PDS) such as the service operates from Assured Secure Facilities (PASF).

Prior to award of any contract specialist SD-WAN solution architects will be assigned to work with the customer to define the functionality and to agree relevant Information Assurance requirements and any additional controls see section 1.6.

1.2: Hosting Charges

Hosting charges using Fujitsu's certified UK datacentres hosting and UK Facility Security Clearance (FSC) (or Police Assured Secure Facilities (PASF) certified UK datacentres facilities are detailed in the charging schedule

1.3: Licences and Capacity

Changes by Cisco for Catalyst SD-WAN licensing now enable greater flexibility in throughput capacity (the tier-based charging bands has been amended if purchased with Cisco hardware). For consistency the Fujitsu Catalyst SD-WAN license tier charges from previous G Cloud frameworks have been maintained in this G Cloud 15 service. The customer is responsible for specifying throughput requirements per edge device the service is to support. Upon deployment the SD-WAN solution will be configured to support that requested throughput for each edge device. Additional tier license charges will apply if the throughput is exceeded by the customer.

1.4: Edge Devices

The SD-WAN service requires edge devices or cloud (virtual license) software to be deployed at sites, or for cloud and datacenter environments. The service options from Fujitsu are:

- Provision of cloud Software for deployment on customer provided hardware.
- Rental from Fujitsu as an optional catalogue item billed monthly.
- Request Fujitsu manage edge devices provided by the customer for the term.

Edge devices currently supported by Fujitsu for the SD-WAN service are detailed in Section 2.

1.5: G Cloud Continuity Services

For customers using Fujitsu SD-WAN services (from G Cloud 13 or 14), Fujitsu will discuss with the customer changes required to the current configurations or services to use the G Cloud 15 SD-WAN service. All G Cloud 15 charges will apply for the new service ordered. Fujitsu's approach to existing G Cloud users is to support service continuity and an uninterrupted service when transitioning to a G Cloud 15 service. This will be summarised in the Statement of Work detailed in section 1.6 which will detail the difference from any existing Fujitsu G Cloud service to the new offering under G Cloud 15.

1.6: Statement of Work Purpose

The Statement of Work is a pivotal document created in advance of signing the Call Off contract in cooperation with the customer. The Statement of Work shall confirm for new or current G Cloud customers the operational requirements of the new service. This will include confirmation of Information Assurance requirements (and or for example OFFICIAL plus any applicable caveats) to be supported. Creating a Statement of Work is not a chargeable activity and reflects Fujitsu's commitment to establish suitability of the G Cloud SD-WAN service for the customer prior to contract award. All material created in the Statement of Work will remain the property of Fujitsu until a Call Off contract is signed.

The Statement of Work will also inform the creation by Fujitsu of the High-Level Design Document which shall follow upon award of call of contract and prior to deployment of solution. To aid the customer, all applicable charges associated with the SD-WAN (for services selected) will be summarised in the Statement of Work. Upon agreement of the Statement of Work, and award of any Call Off contract a detailed implementation plan and agreed milestone dates will be provided confirming timescales and deployment dependencies.

1.7: Configuration Data Upon Expiry

Where Fujitsu is managing and operating the configuration of the SD-WAN edge as agreed with the customer (section 3), the configuration data will be made available for a period of 30 days upon expiry of the agreement in a format to be agreed or specified in the transition plan, thereafter the data will be deleted. The export of customer data will be subject to additional professional charges, using the SFIA rate card.

Configuration data of Fujitsu hosted elements will not be available for export and remains the property of Fujitsu upon expiry of the agreement.

2: Fujitsu SD-WAN Edge Devices

The SD-WAN service from Fujitsu offers customers a wide choice of edge devices or licences to support their operating environment.

The customer may select Cisco or Fujitsu universal Customer Premises Equipment (uCPE) with optional secure builds on Fujitsu supplied uCPE for OFFICIAL Sensitive deployments together with appropriate Cloud (virtual) licenses for deployment on customer supplied hardware.

uCPE devices provided by Fujitsu may also be used for Fujitsu's Next Generation Network platform, the Graphiant Network as a Service.

2.1: Cisco 8000 Series

The following Cisco 8000 series edge devices 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.

2.1.1: Cisco 8100 Edge Router Series:

Cisco 8100 Series Secure Routers deliver secure networking. Powered by the all-new secure networking processor and the unified Cisco secure networking platform, Cisco 8100 Series Secure Routers deliver robust, platform-level security; advanced performance engineering via routing and SD-WAN; and on-premises, infrastructure-as-code, or cloud management flexibility that enables businesses to seamlessly scale and grow.

Purpose-built for branch deployments, Cisco 8100 Series Secure Routers deliver enterprise-grade security and high performance in a compact, energy-efficient form factor. With integrated next-generation firewall, zero-trust capabilities, and SASE-ready architecture, the 8100 Series empowers small sites to operate securely and reliably simplifying management.

Models and specifications supported in G Cloud 15 are:

- Cisco 8100 Series Secure Routers are 1 RU fixed form factor devices with four models.
- Cisco C8130-G2; C8140-G2; C8151-G2; and C8161-G2.

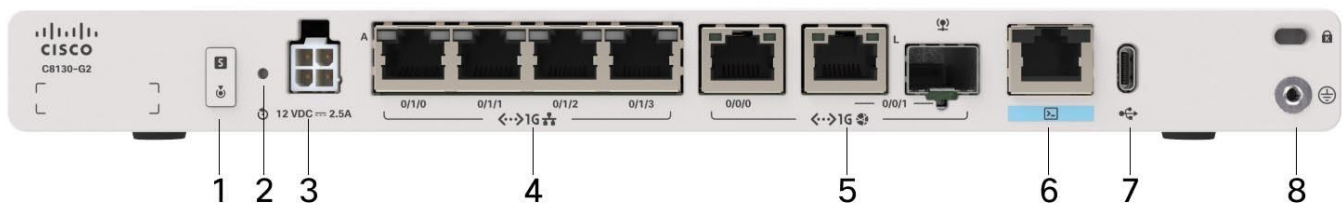


Figure 2: Front panel of Cisco C8130-G2 Secure Router

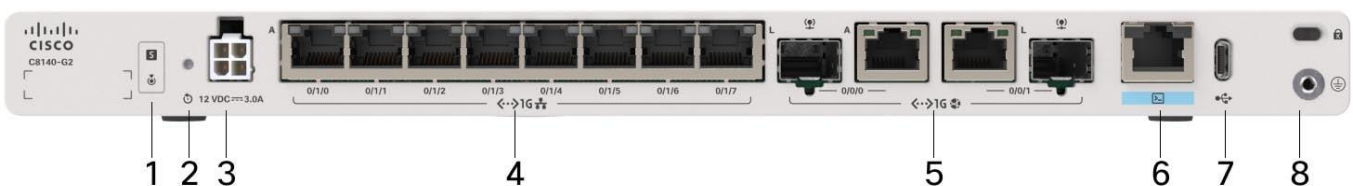


Figure 3: Front View of a Cisco C8140-G2 Secure Router

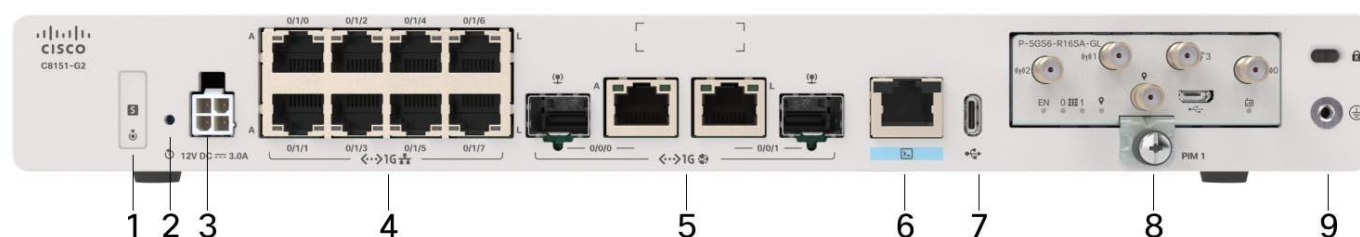


Figure 4: Front View of a Cisco C8151-G2 Secure Router

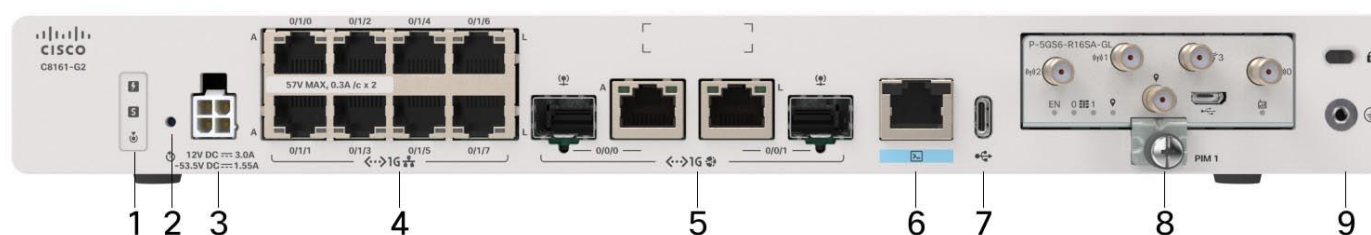


Figure 5: Front View of a Cisco C8161-G2 Secure Router

Technical specifications – Interfaces and Slots

	C8130-G2	C8140-G2	C8151-G2	C8161-G2
WAN Ports	1x 1GE RJ-45, 1x 1GE RJ-45/SFP Combo	2x 1GE RJ-45/SFP combo	2x 1GE RJ-45/SFP combo	2x 1GE RJ-45/SFP combo
Flex Ports	2 x GE RJ-45	2 x GE RJ-45	2 x GE RJ-45	2 x GE RJ-45
LAN Ports	2x 1GE RJ-45	6x 1GE RJ-45	6x 1GE RJ-45	6 x GE RJ-45 (4PoE/2PoE+) PoE output max power 80W
Cellular Slot	-		-	Optional Pluggable Module – CAT 7 or 5G
Management Port	1 x RJ-45 console			
DRAM	4GB RAM	4GB RAM	8GB RAM	8GB RAM
Flash	16 GB			
Storage	1 x USB Type-C 3.0 OOB management			
External Power Supply	30W/66W	66W	66W	150W
Typical Power	16W	20W	23W	25W

Table 1: Technical specifications

	C8130-G2	C8140-G2	C8151-G2	C8161-G2
Dimensions (H x W x D)	1.09 in x 7.8 in x 10.8 in	1.09 in x 6.9 in x 12.7 in	1.57 in x 8.5 in x 12.7 in	1.57 in x 8.5 in x 12.7 in
Rack Units (RU)	1RU (mounting options: rack mount, under desk, din-rail)			
Chassis weight	3.5 lb	3.57 lb	5.1 lb	5.1 lb
Temperature	Operating temperature: 0° C to 40° C (32° F to 104° F) at sea level, 1° C/1000ft derating from 40° C Non-operating temperature: -40° C to 70° C (-40° F to 158° F)			

Table 2: Mechanical specifications

Throughput	C8130-G2	C8140-G2	C8151-G2	C8161-G2
Forwarding (512B)	1.9 Gbps	5.6 Gbps	5.6 Gbps	5.6 Gbps
IPsec (512B)	1.5 Gbps	1.5 Gbps	1.5 Gbps	1.5 Gbps
SD-WAN* (512B)	-	-	900 Mbps	900 Mbps
Threat Protection** (EMIX)	-	-	1 Gbps	1 Gbps

Table 3: Throughput

2.1.2: Cisco 8200 Edge Router Series:

The Cisco Catalyst 8200 Series Edge Platforms are 5G-ready cloud edge platforms designed for Secure Access Service Edge (SASE), multilayer security, and cloud-native agility. The Cisco® Catalyst® 8200 Series Edge Platforms deliver Cisco's secure, cloud-scale SD-WAN and SD-Routing solutions to a branch.

The platforms are purpose built for performance and integrated SD-WAN services along with flexibility to deliver security and networking services together from the cloud or on premises. The Catalyst 8200 Series Edge Platforms are offered in two models: C8200L-1N-4T for the small branch with SASE-compliant, cloud-based security requirements, and C8200-1N-4T for the small to medium sized branch with requirements for higher throughput, scale, and service flexibility.

Models and configurations



Figure 6: Catalyst 8200 Series with 1 NIM slot and 4x 1 Gigabit Ethernet WAN ports

Model	Description	1G port density	Slots	Memory (DRAM) default	Storage (M.2 SSD) default
C8200-1N-4T	C8200 1RU w/ 1 NIM slot and 4x 1 Gigabit Ethernet WAN ports	4	1 NIM 1 PIM	8 GB	16 GB
C8200L-1N-4T	C8200L 1RU w/ 1 NIM slot and 4x 1 Gigabit Ethernet WAN ports	4	1 NIM 1 PIM	4 GB	No

Table 4: Platform specifications

Feature	C8200-1N-4T	C8200L-1N-4T
SD-WAN IPsec Throughput (1400Bytes)	Up to 1Gbps	Up to 500Mbps
SD-WAN IPsec Throughput with IQDF** (1400Bytes)	Up to 1Gbps	Up to 460Mbps
SD-WAN IPsec Throughput (IMIX*)	900Mbps	400Mbps
SD-WAN IPsec Throughput with IQDF** (IMIX*)	850Mbps	300Mbps
SD-WAN Overlay Tunnels scale	2500	1500

Table 5: Cisco Catalyst 8200 Series SD-WAN performance

2.1.3: Cisco 8300 Edge Router Series:

The Cisco Catalyst 8300 Series Edge Platforms are, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.



Figure 7: Cisco 8300 Routers

Cisco Catalyst 8300 Series Edge Platforms (Catalyst 8300) with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale Catalyst SD-WAN solution for the branch. The Catalyst 8300 Series is purpose-built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises.

Model	Description	10G port density	1G port density	Slots	Memory (DRAM) default	Storage (M.2 SSD) default
C8300-2N2S-4T2X	C8300 2RU w/ 10G WAN (2 SM and 2 NIM slots, and 2 x 10-Gigabit Ethernet and 4 x 1-Gigabit Ethernet ports)	2	4	2 SM 2 NIM 1 PIM	8 GB	16 GB
C8300-2N2S-6T	C8300 2RU w/ 1G WAN (2 SM and 2 NIM slots, and 6 x 1-Gigabit Ethernet ports)	-	6	2 SM 2 NIM 1 PIM	8 GB	16 GB
C8300-1N1S-4T2X	C8300 1RU w/ 10G WAN (1 SM slot and 1 NIM slot, and 2 x 10-Gigabit Ethernet and 4 x 1-Gigabit Ethernet ports)	2	4	1 SM 1 NIM 1 PIM	8 GB	16 GB
C8300-1N1S-6T	C8300 1RU w/ 1G WAN (1 SM slot and 1 NIM slot, and 6 x 1-Gigabit Ethernet ports)	-	6	1 SM 1 NIM 1 PIM	8 GB	16 GB

Table 6: Cisco Catalyst 8300 Series specifications

Feature	C8300-2N2S-4T2X (2RU w/ 10G WAN)	C8300-1N1S-4T2X (1RU w/ 10G WAN)	C8300-2N2S-6T (2RU w/ 1G WAN)	C8300-1N1S-6T (1RU w/ 1G WAN)
SD-WAN IPsec Throughput (1400Bytes)	Up to 18.8Gbps	Up to 17Gbps	Up to 2Gbps	Up to 2Gbps
SD-WAN IPsec Throughput with IQDF** (1400Bytes)	Up to 18.8Gbps	Up to 17Gbps	Up to 2Gbps	Up to 2Gbps
SD-WAN IPsec Throughput (IMIX*)	7.6Gbps	6.3Gbps	1.8Gbps	1.8Gbps
SD-WAN IPsec Throughput with IQDF** (IMIX*)	5.6Gbps	5.5Gbps	1.7Gbps	1.7Gbps
SD-WAN Overlay Tunnels scale	6000	6000	6000	6000

Table 7: Cisco Catalyst 8300 Series Catalyst SD-WAN performance

2.1.4: Cisco 8500 Edge Router Series:

The Cisco Catalyst 8500 Series Edge Platforms are high-performance cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence



Figure 8: Cisco 8500 Edge

Platforms and configurations

The C8500-20X6C platform allows all ports to be enabled simultaneously. It offers:

- 20x 1/10GE ports.
- 6x 40/100GE ports.

The C8500-12X4QC platform allows for a maximum of 240GE ports to be enabled simultaneously. It offers:

- 12x 1/10GE ports (can increase to 24x 1/10GE if using 4x10GE breakout from QSFP 40G ports when not in SD-WAN mode).
- 3x 40GE ports.
- 2x 40/100GE ports.

The C8500-12X platform offers 12x 1/10GE ports.

The C8500L-8S4X platform offers 4x 1/10GE and 8x 1GE ports.

Cisco Catalyst 8500 Series Edge Platforms (Catalyst 8500 and Catalyst 8500L) with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for aggregation sites.

The Catalyst 8500L Edge Platform features an x86 based platform architecture that is purpose built to continue delivering the same experience as an ASR1000 platform. The Catalyst 8500 Series Edge Platforms are compact 1RU or 3RU (Catalyst C8500-20X6C) devices with flexible interface options, including 1GE, 10GE, 40GE, and 100GE ports.

Platform	Description	Max 1GE ports	Max 10GE ports	Max 40GE ports	Max 100GE ports
C8500-20X6C*	20-port 1/10GE, 6-port 40/100GE	20*	20*	6*	6*
C8500-12X4QC**	12-port 1/10GE, 2-port 40/100GE, 2-port 40GE	12**	12**, ***	4**	2**
C8500-12X	12-port 1/10GE	12	12	0	0
C8500L-8S4X	4-port 1/10GE, 8-port 1GE	12	4	0	0

Table 8: Cisco Catalyst 8500 Series configurations and port density

Performance attribute	C8500L-8S4X
50% IQDF*+ 50% (DIA w. NAT + NGFW + IPS + URLF + AMP)	Up to 5.9 Gbps
DIA w. NAT + NGFW + IPS + URLF + AMP	Up to 4 Gbps

Table 9: Cisco Catalyst 8500L Series SD-WAN, Multi-layer security performance

2.2: Fujitsu uCPE Series

Fujitsu has developed secure edge devices using commercial off the shelf (COTS) products based on universal customer Premises Equipment (uCPE). Fujitsu’s uCPE enable customers 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 portfolio comprises of current uCPE devices for new installations and support of previous uCPE devices that remain supported by the manufacturer.

The uCPE devices offered are:

- COTS X86 hardware computing platform.
- Deployed with Optional NFVI (ADTRAN Ensemble Connector).
- Can be deployed with Optional SAT VNF hosting a vTA (Paragon service assurance).
- Can be deployed with Graphiant NaaS Service Chain.

2.2.1: Current Advantech Series



Figure 9: Advantech Series

Features

- Powered by single Intel® Xeon D-2700/D-2800 series processor up to 22C/44T with Intel® QAT and DPDK to boost performance.
- 4 x DDR4 up to 3200 MHz ECC UDIMM/RDIMM/LRDIMM support.
- 2 x NMC (Network Mezzanine Card) PCIE Gen4 slots for a wide range of 1G/10G/25G/40G/100G NICs and POE module expansion.
- Upgradable with interface for Advance-LTE/5G.
- 2 x 2.5" internal SATA HDDs/SSDs drive bay.
- 2 x M.2 2280 SSD/NVMe sockets.

		FWA-3051-8CA1R	FWA-3051-16A1R	FWA-3051-20A1R
Form Factor		1U Rack Mount	1U Rack Mount	1U Rack Mount
Processor System	Processor Core Count	Intel® Xeon® D-2832NT 8C/16T	Intel® Xeon® D-2876NT 16C/32T	Intel® Xeon® D-2896NT 20C/40T
	Base Frequency	2.1 GHz	2.0 GHz	2.0 GHz
	Chipset	N/A		
	BIOS	AMI UEFI		
Virtualization		Intel® VT-x, VT-d, SR-IOV		
Memory	Technology	DDR4 2667MHz DDR4 2933MHz		DDR4 2933MHz
	Max. Capacity	128 GB UDIMM / 256 GB RDIMM / 512 GB LRDIMM		
	Socket	4 x 288-pin DIMM		
	ECC Support	UDIMM / RDIMM / LRDIMM		
Networking	Controller	2 x Intel i210, 1 x Intel i350, Others via Intel SOC (Idaville HCC Ethernet)		
	1GbE	4 x 1GbE RJ45 via Marvell 88E1543 (w/ Advanced LAN bypass) 4 x 1GbE RJ45 via Intel i350-AM4 2 x 1GbE RJ45 via Intel i210-AT for management		
	10GbE	4 x 10GbE SFP+ via Intel SOC		
	LAN bypass	Two pair of LAN bypass		
Expansion Slot	PCIe x16	1 x PCIe x16 (Option: by project base)		
	NMC	1 x PCIe Gen4 x8 (Option: 1x Field-replaceable NMC-E02 POE by project base)		
IPMI		IPMI 2.0 and Redfish compliant		
Storage	2.5" bay M.2 (SSD)	2 x SATA HDD/SATA SSD 2 x 2280 M.2 M-key slot for SATA SSD or PCIe x4 Gen3 NVMe SSD		
I/O	Console	1 x RJ45 type console		
	USB	2 x USB 3.0		
	LED Indicator	1 x Power LED, 1 x Alert LED, 1 x Locate LED, 1 x Software-defined LED		
	Display	1 x VGA port		
	Button	1 x Power button, 1 x Software-defined button		
	Others	1 x dedicated 1GbE LAN for IPMI		
TPM		None (Option: Infineon TPM 2.0 module)		
LCD Module		None		
Power Supply	Power Type	AC Redundant CRPS (Option: DC Redundant CRPS)		
	Watts Input	300W AC: 100-240V~, 50-60Hz (Option: DC -48V, 800W by project base)		
	Connector	AC 3pin plug		
Environment	Operating Temperature	0 ~ 40 °C (32 ~ 104 °F)		
	Non-operating Temperature	-40 ~ 70 °C (-40 ~ 158 °F), 60 °C@95% Non-Condensing Humidity		
	Vibration Resistance (Operation)	5-500 Hz, 0.3 Grms, 3 axes, 1 hr/per axis		
	Shock Protection (Operation)	10 G, 11 ms		
Cooling		4 x System fans with smart fan feature		
Mechanical	Construction	SECC		
	Mounting	1U Rackmount		

	Dimensions (W x H x D)	438 x 44 x 420 mm (17.2" x 1.7" x 16.5")
	Weight (G.W)	8.23kg (18.14 lbs)
OS support		Linux (CentOS, Red Hat, Ubuntu, Fedora)

Table 10: Advantech Specifications

2.2.2: Supported DELL 4600 uCPE devices on Fujitsu SD-WAN service

The DELL VEP – 4600 supports a throughput of 3.0Gbps. The Dell VEP models support both High Availability (Dual Power and Active Active deployments) and Standard Availability (Single) designs.



Figure 10: uCPE (Dell VEP-4600)

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	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 11: DELL uCPE specifications

2.3: Ensemble Connector for uCPE devices

Fujitsu supports Ensemble Connector for its uCPE deployments. Ensemble Connector is a 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.

When combined with Fujitsu's SD-WAN LOSS orchestration service, this allows VNF service chains to be modified in the field without the need for a site visit or on-site configuration.

3: SD-WAN Managed Services

Fujitsu provides ITIL aligned specialist SD-WAN professional services calculated using the G Cloud SFIA rate card (or fractions thereof) as detailed in the charges. The optional services comprise of;

- 1) Provision of help desk services.
- 2) Network Operations Services, managing SD-WAN instances.
- 3) Provision of Protective Monitoring (enhanced).
- 4) Provision of Managed Firewall and Encryption Services.
- 5) SD-WAN moves adds and changes.
- 6) Management of customer provided connectivity (acting managing agent).
- 7) Design and deployment services.
- 8) Security Consultants.
- 9) Project Management.
- 10) Break Fix Services.
- 11) Transition Management Services.
- 12) Management of third-party SD-WAN infrastructure including residential locations (using the service headings above).
- 13) Use of Fujitsu FSC locations for platform management where specified.

Upon request and where not specified in the charges catalogue Fujitsu will calculate the services required using the SFIA rate card for additional professional services.

All Fujitsu staff associated with managing the SD-WAN service hold as a minimum NPPV3 and SC security clearance.

4: SD-WAN FSC UK Deployed solution

Fujitsu's SD-WAN is based on the Cisco Catalyst SD-WAN software, as a shared platform with Fujitsu enhancements to support Higher Information Assurance requirements. The service is hosted in Fujitsu's UK FSC and PASF Accredited facilities. All service management facilities are provided in the UK from Fujitsu Defence and

National Security facilities manned with staff who hold as a minimum SC and NPPV3 clearance supporting sovereign management requirements.

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 customer SOC capabilities as an optional service.

The customer is responsible for the end user management of the platform and edge devices using the portals provided. If a customer chooses to manage the platform it shall follow ITIL v4 or the equivalent standards.

The customer as an optional service can subscribe to a range of itemised ITIL based managed services from Fujitsu using the SFIA rate card detailed in section 3.

As a shared platform the features and functionality of the service may differ from published Cisco documentation even though it's based on Cisco Catalyst SD-WAN software. The functionality supported will be in accordance with Fujitsu's High Level Design Documents and advised software supported. This is guided by good practice for secure networks, NCSC guidance, any limitations imposed by Secure by Design for connecting applications and customer CISO guidance. Customers are advised to seek confirmation (using the Statement of Work see section 1.6) 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 customers 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.

4.1: Solution overview

The salient features of this service are:

- The data plane, the control plane, and the management plane traffic for each customer is fully isolated
- Each customer is allocated within the Fujitsu infrastructure a pod to manage the enterprise SD-WAN elements. This acts as a firewall from other SD-WAN users
- SD-WAN will always run on the latest star-marked release tested by Fujitsu
- Software-Defined AVC (SD-AVC) and web certificates are managed by Fujitsu
- The features and functionality of Fujitsu SD-WAN Service can be found using the following link [Feature Matrix](#).

Please see Figure 11 for a high level schematic of a deployed customer instance:

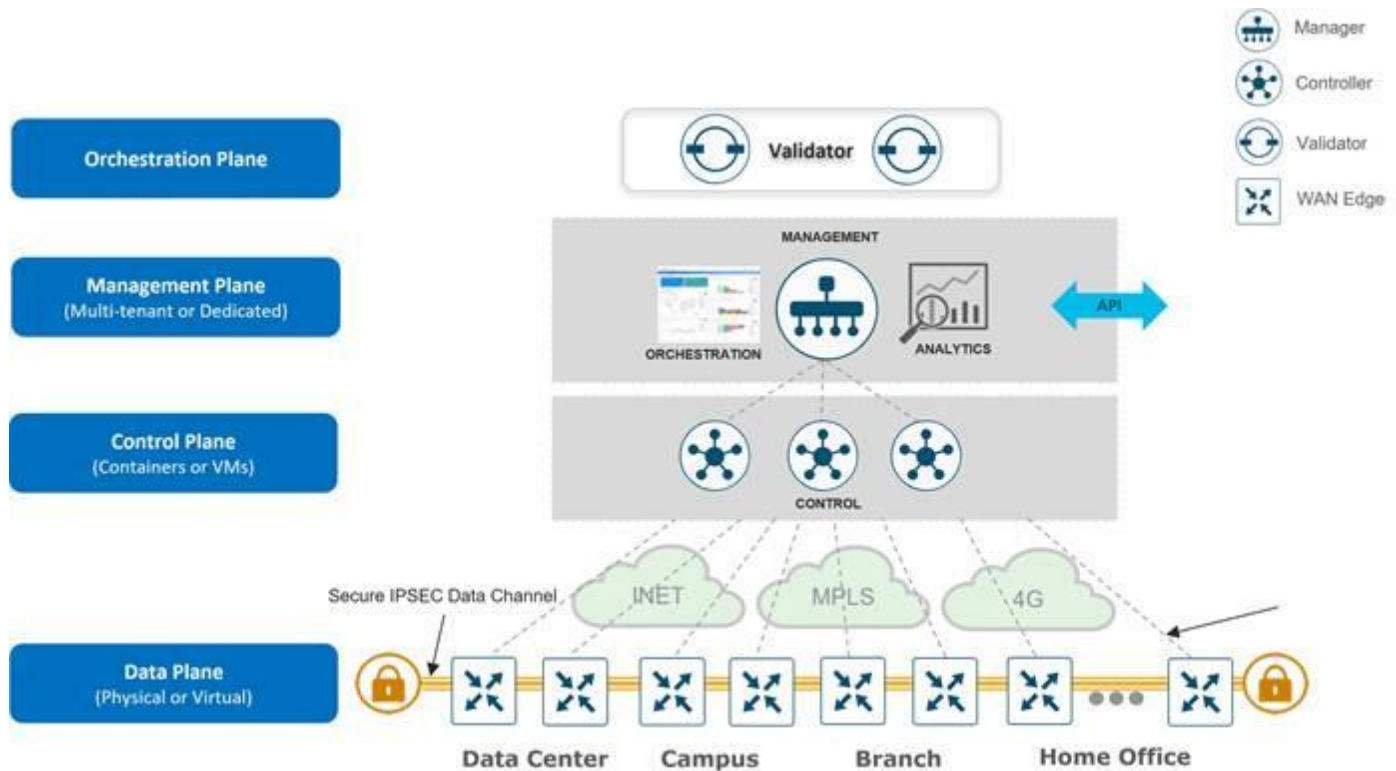


Figure 11: Overview of Fujitsu SD-WAN solution planes

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. See section 2 for available devices

Figure 12 demonstrates several aspects of Fujitsu's SD-WAN solution 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 the internet (this could also be MPLS etc).

In addition, the topology also includes cloud access to SaaS and IaaS applications using the customer connectivity and network.

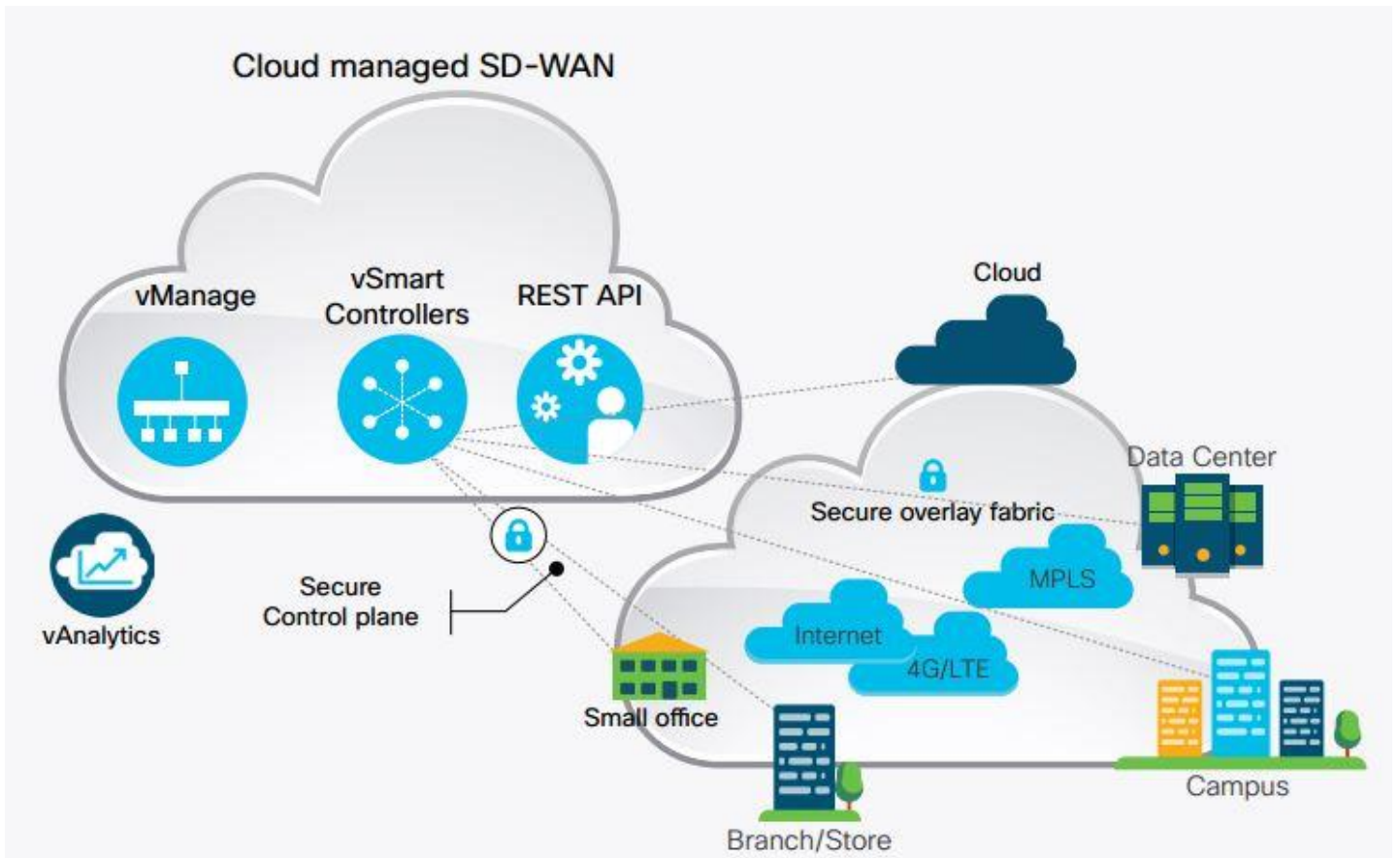


Figure 12: Example SD-WAN topology

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 on Cisco's 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 a full-stack multilayer security capability as an optional service via Cisco software uplifts which must apply to all licences deployed for the customer. To support a full stack multilayer security, additional devices may be required to reflect information assurance requirements, which shall be advised in the Statement of Work. Additional appliances or edge hardware can be added to the service catalogue by change note to reflect customer requirements. 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.

Using the SD-WAN Manager (see Figure 13) Fujitsu's SD-WAN simplifies IT operations with automated provisioning, unified policies, and streamlined management.

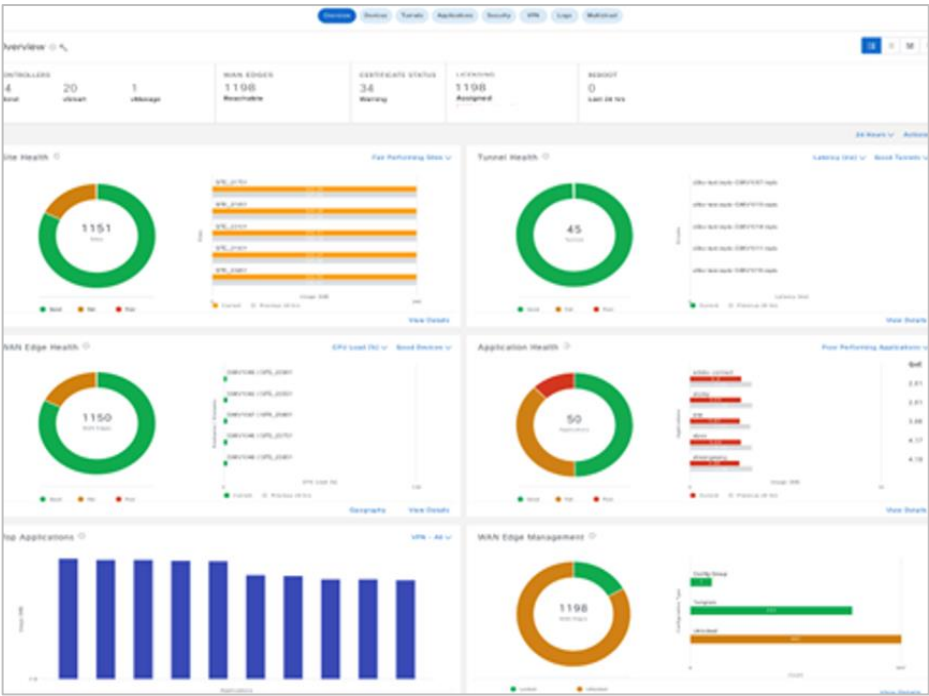


Figure 13: Fujitsu SD-WAN Manager dashboard showing network and application health

Fujitsu’s service provides a flexible architecture to extend SD-WAN to any environment (Figure 14).

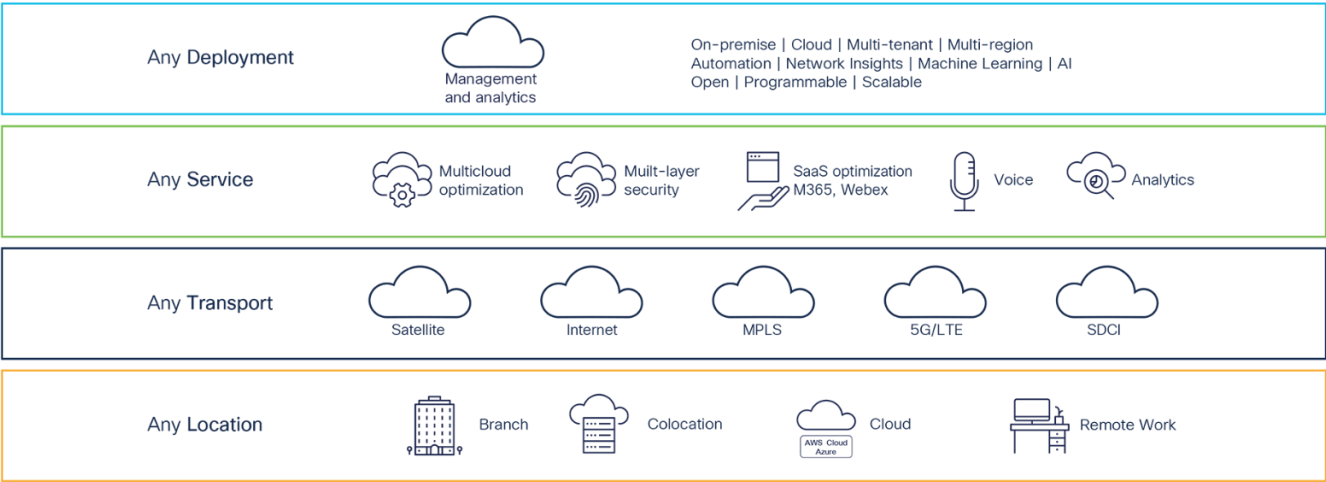


Figure 14: Flexible and scalable architecture for network transformation

4.2: Multicloud Choice and Control

Fujitsu’s SD-WAN provides the ability (subject to any restrictions imposed by the customer) to connect to multiple cloud platforms or other enterprise, enabling increased connection speeds and connection reliability. Fujitsu’s SD-WAN Cloud OnRamp creates a WAN extension for customer 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.

4.3: 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.

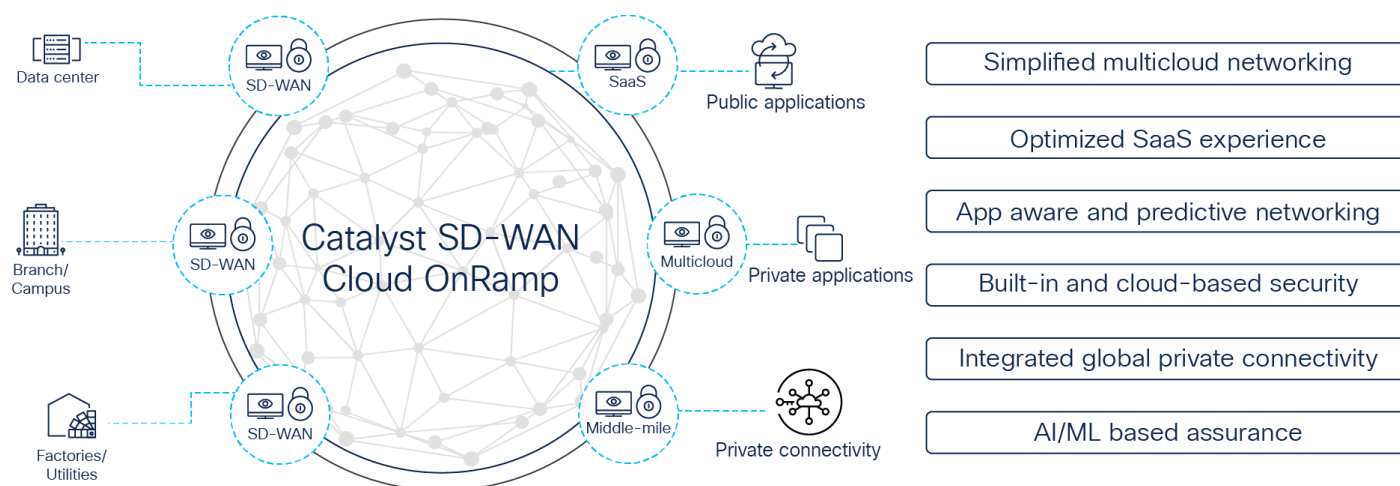


Figure 15: Fujitsu's SD-WAN Cloud OnRamp for IaaS, PaaS, and SaaS applications

4.4: SD-WAN Cloud Hub

Fujitsu's SD-WAN Cloud Hub leverages SD-WAN to interconnect branch sites, on-premises data centres, and the cloud using a public cloud service provider's backbone (AWS, Google Cloud, or Microsoft Azure) as an underlay. This network functionality will be subject to any restrictions imposed by the customer. 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 16). It should be noted customers will still be required to provide connectivity for the sites, and that connectivity will be used to access the cloud hub.

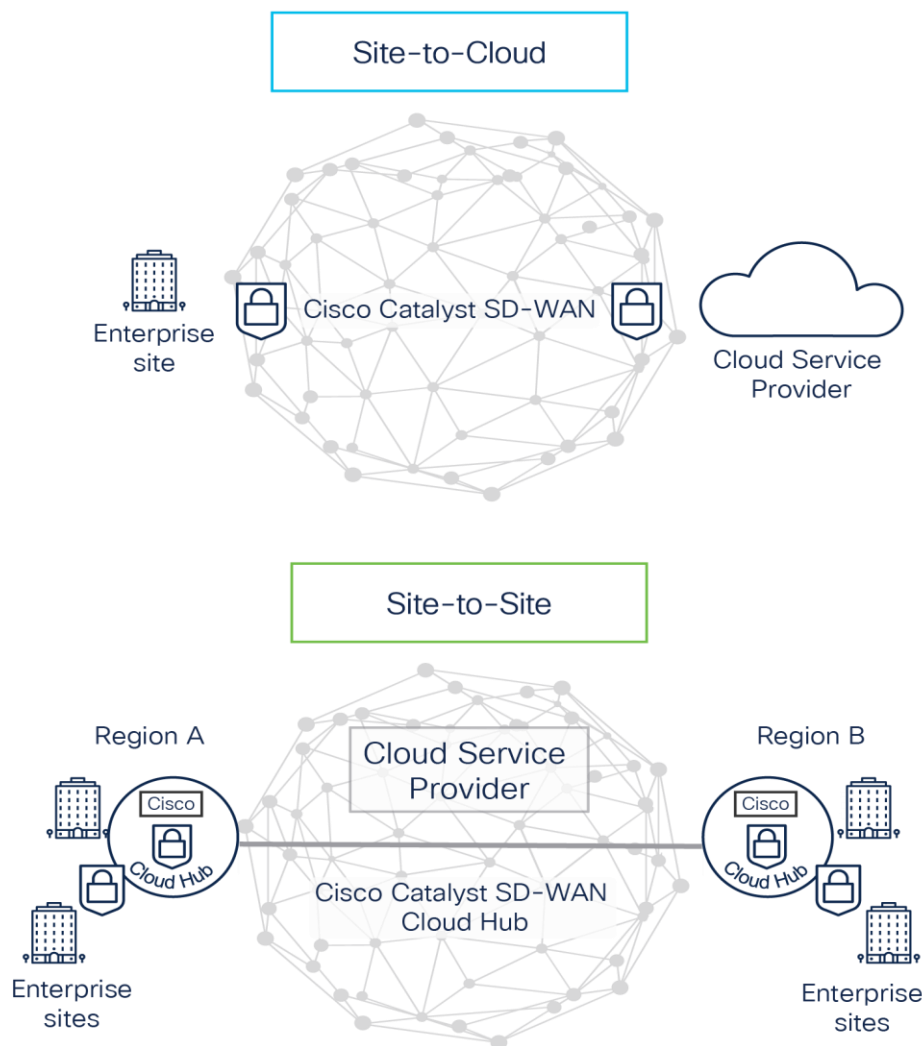


Figure 16: Fujitsu's SD-WAN Cloud Hub

4.5: SD-WAN Cloud OnRamp for SaaS

In addition to building application workloads in IaaS cloud environments, customers may 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 17), 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 customer 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 customers to enable Cloud OnRamp for SaaS capabilities with the application of their choice. 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.

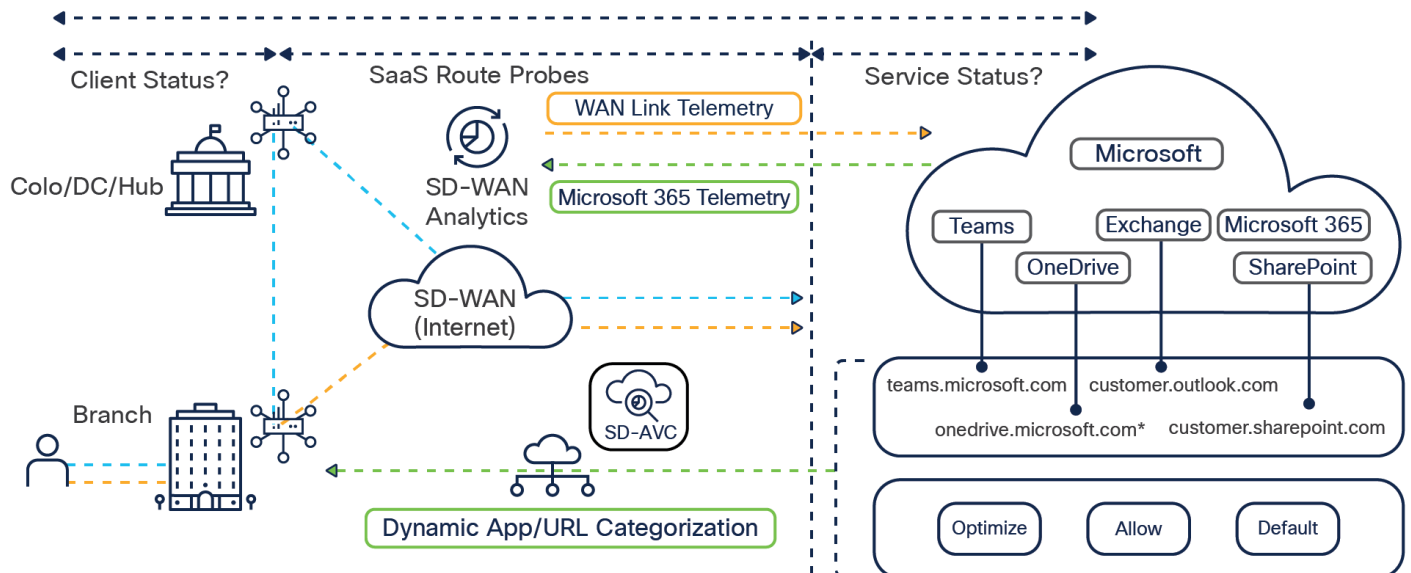


Figure 17: Fujitsu's SD-WAN Cloud OnRamp for SaaS

4.6: Fujitsu SD-WAN Cloud Interconnect

Fujitsu's SD-WAN Cloud Interconnect figure 18 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 supports an optional integration capability for customers 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. Subject to any restrictions imposed by the customer Cisco SD-WAN Cloud OnRamp, Cisco SD-WAN Cloud Interconnect can be 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.

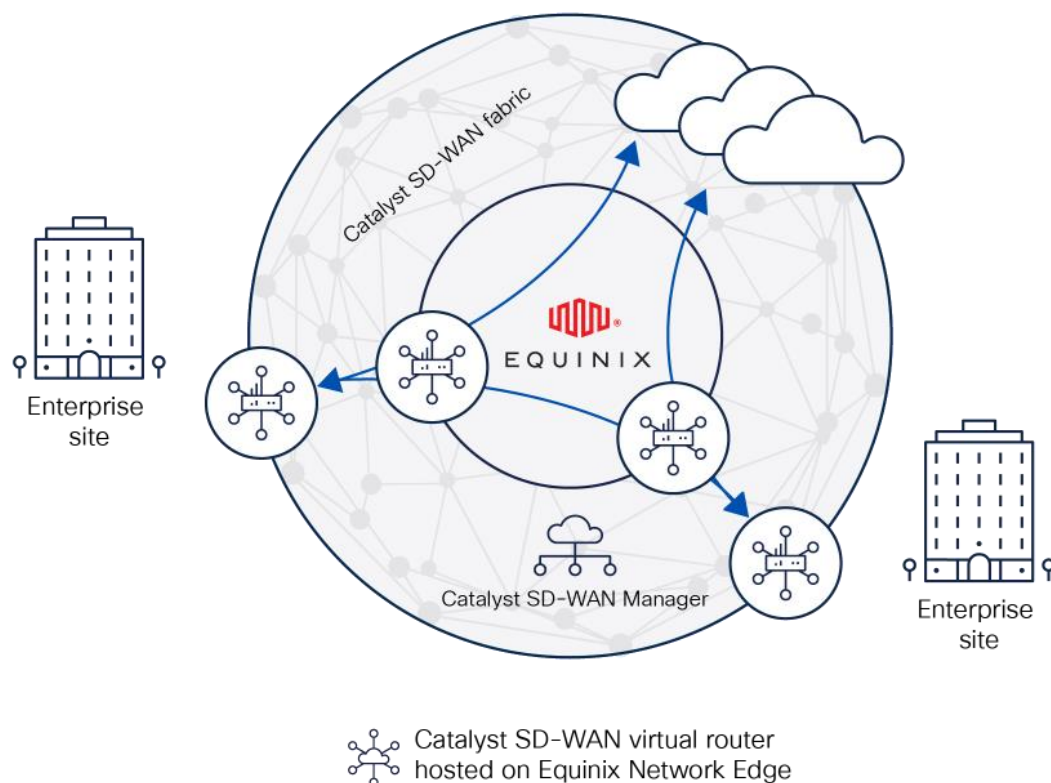


Figure 18: Fujitsu SD-WAN Cloud Interconnect

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 customer 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 customer 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.

4.7: 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 offers a UK deployed solution where any user data remains in Fujitsu's FSC environment. Figure 19 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 customers 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.

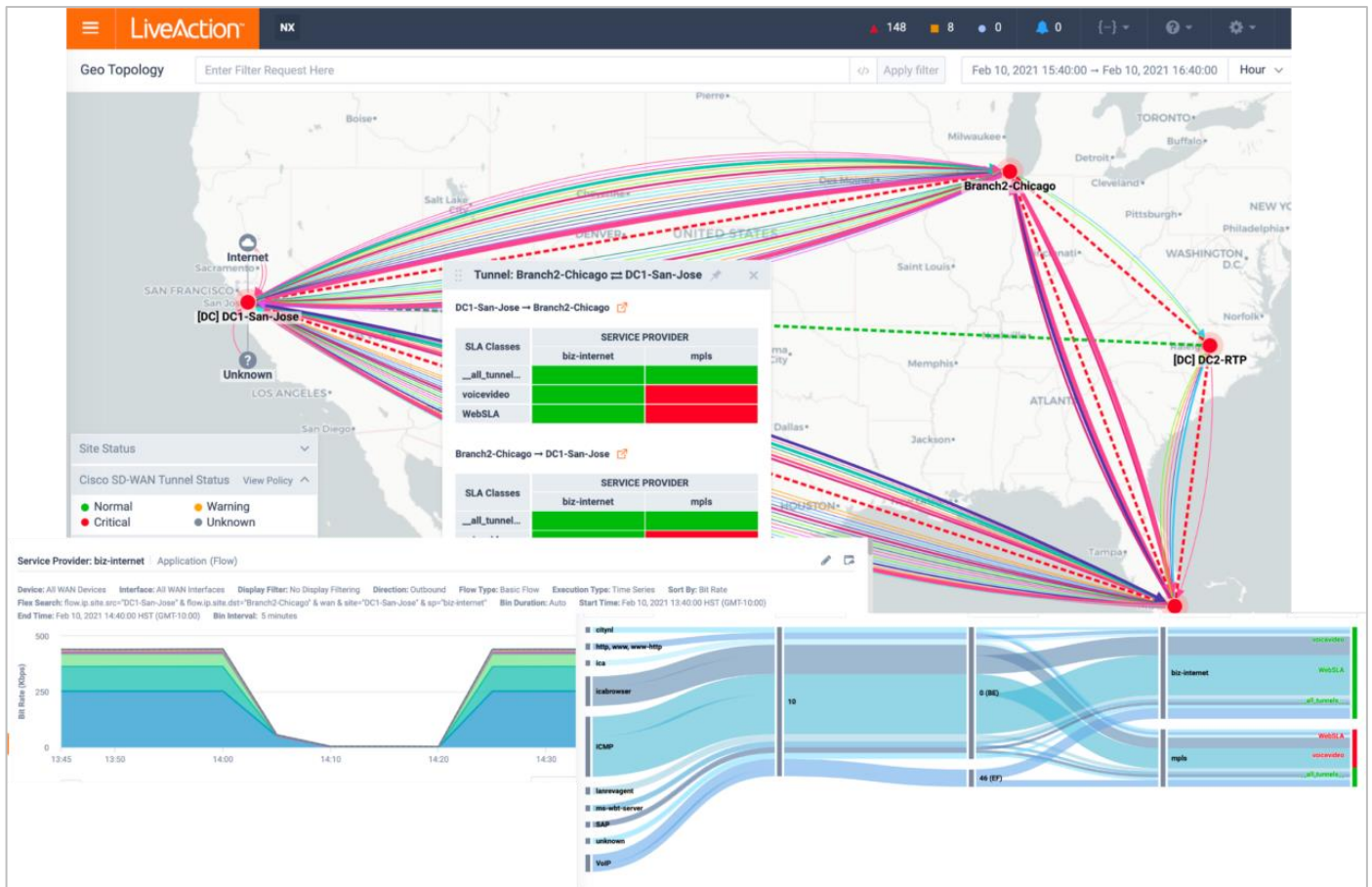


Figure 19: Fujitsu Live NX SD-WAN Analytics

4.8: Fujitsu SD-WAN Software Subscription Licensing

Fujitsu's SD-WAN Software subscription aligns to the Cisco Catalyst SD WAN licence model (with exclusions regarding tier throughput). By default Fujitsu deploys Cisco DNA Advantage. Use of SASE applications (such as NGFW etc) will be subject to additional charges and must be applied to all Cisco Catalyst SD-WAN licences deployed. 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.

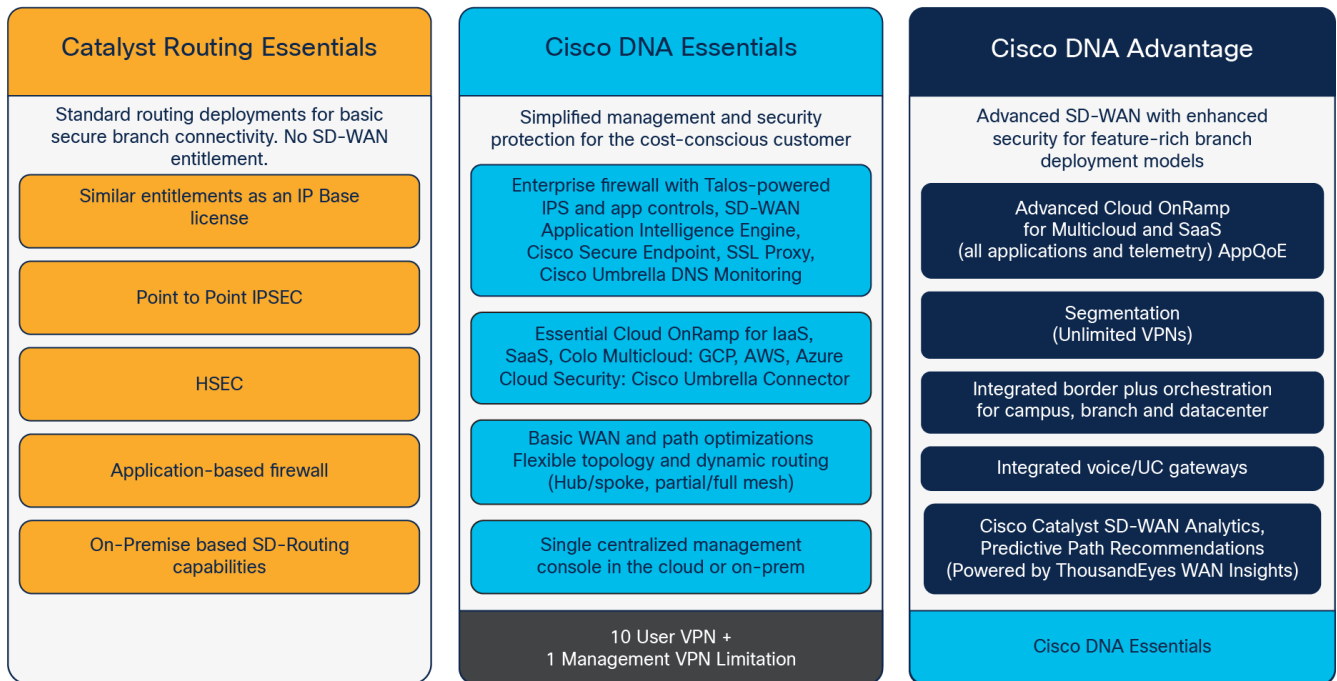


Figure 20: Cisco DNA Software subscription licensing for SD-WAN and routing

4.9: Prominent Features

- Vendor approved Software deployed after functional testing completed.
- Integrated security uplifts.
- Uplifts using software 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.
- IPv6 support (BGP, OSPF).
- Robust IP multicast support.

4.10: Support for Security and Information Assurance

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

4.11: Certifications

The Fujitsu SD-WAN, operations are certified ISO/IEC 27001 Certificate Number: IS 798357

The scope includes: The provision of design, integration and support of Software Defined Wide Area Network Services from Fujitsu offices and Data Centres in the UK for Fujitsu Customers. This is in accordance with Statement of Applicability version 2, 31st October 2024.

Fujitsu's Catalyst SD-WAN, for Cloud is certified Certificate Number: CLOUD 808326

Scope: The provision of design, integration and support of Software Defined Wide Area Network Services from Fujitsu offices and Data Centres in the UK for Fujitsu Customers. This is in accordance with Statement of Applicability version 1.3 dated 28/03/2024, in conjunction with ISO 27001 license IS 798357

Fujitsu implements the following best service and security practice:

- Established Data Protection Act program across Fujitsu's UK business.
- 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.

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.

5: Service Delivery

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.

5.1: Service Demarcation Responsibilities

The customer's attention is drawn to the Responsibilities Matrix in Table 12 below. This table details the extent of the operational management responsibilities of the customer 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. The table below provides the service demarcation points between the customer and Fujitsu further clarity will be provided in the Statement of Work if required:

Task	Fujitsu Hosted Cloud Catalyst SD-WAN Responsibility	Comments
The Customer shall where undertaking management duties of the service perform all ITIL service management functions of the Edge estate, notifying Fujitsu of any changes where appropriate with respect to Fujitsu monitoring	Customer	
Where the customer is performing management duties of the SD-WAN service. The customer shall manage all user access and administration processes) to the Portal (inc. Privileged access management (PAM, etc)	Customer	
Underlay Provision	Customer	customer responsible for all connectivity and bearer performance
CPE Environmental requirements	Customer	Provision of any suitable racking, power and operating environment as advised by Fujitsu will be the responsibility of the customer to provide. Customer shall provide upon request safety certificates for any infrastructure accessible by Fujitsu engineers.
Fujitsu will provision hosted controllers for SD-WAN overlay and Cisco SD-WAN Manager with access for the customer.	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 customer to report incidents and to raise service requests
Protective Monitoring of core infrastructure 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	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the customer to report incidents and to raise service requests

Elasticsearch, Kibana and Logstatsh stack.		
Customer responsible for edge device monitoring, firewall configuration connection of new devices or the monitoring of data traversing the network	Customer	A Fujitsu Service Desk will be provided to enable the customer to report incidents and to raise service requests
Customer 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 customer.	Customer	A Fujitsu Service Desk will be provided to enable the customer 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 customer 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 customer 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 customer 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 customer 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	Customer to manage Fujitsu to support	LiveAction (LiveNX) Analytics is by default onboarded for cloud-delivered Cisco Catalyst SD-WAN customers.

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 customer 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	Customer	
Accept external management of SA/VA and map tenant VA to customer's SA/VA	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the customer to report incidents and to raise service requests
Define configure and deploy device configuration templates and policies through Cisco SD-WAN Manager	Customer	Note customer 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	Customer	Note customer responsible for defining policies and resulting performance
Web server certificates	Managed by Fujitsu	A Fujitsu Service Desk will be provided to enable the customer to report incidents and to raise service requests
Edge serial sync with credentials	Customer	Cloud-delivered Cisco Catalyst SD-WAN customers 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	Customer	

Table 12: Service Demarcation Responsibilities

5.2: 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 any customer premises network into its cloud-hosted overlay network.

5.3: Fujitsu Capacity Management

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

6: Fujitsu SD-WAN Service Levels

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

6.1: 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)	99.9%	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 13: Service Availability SLAs

6.2: Service Level Response Time

Service Measure	Description	Support Hours	Target Response Time
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	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) Standard	Major business disruption: critical user or user group unable to operate, or an entire service experiencing significant reduction in system performance	24x7x365 days	2 hours
Priority 2 (Medium)	Partial service disruption to a live/production service.		3 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 14: Service Measure

6.3: Edge Device SLAs

High Availability Edge Sites UK Mainland

	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 15: Edge Device SLAs – High Availability Edge Sites

Standard Edge Sites UK Mainland

	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 16: Edge Device SLAs – Standard Edge Sites

Edge Device Replacement SLAs UK Mainland

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 17: Edge Device SLAs – Replacement SLA

All service levels have a target that 98% 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'.

6.4: 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	<u>Severe business disruption:</u> 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	<u>Major business disruption:</u> 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	<u>Minor business disruption:</u> 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	<u>Minor disruption.</u> 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	<u>Enquiry:</u> 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 18: Core Platform SLAs

6.4.1: Problem Management Priority Levels and Definitions

Ref	Definition	Resolution Target (1)	Performance Indicator
PM1	Level 1 (P1): The Problem poses significant risk to the customers business or operations in that the Incident or series of Incidents may result in significant adverse impact to the customer 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 customer 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 customer 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 customer that it has Resolved such Problem by completing the relevant sections of the relevant Problem Record.	95%	100%

Table 19: Problem Management SLAs

6.5: Service Reporting

Service Reporting encompasses the production and delivery of defined reports to accurately report against agreed Service Level Agreements.

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

Monthly Reporting

ITSM Monthly Service Reports (from ServiceNow)

- ITSM Service Reports are provided as part of the monthly service reviews and will generate the following pre-built reports monthly 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 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 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 status of the incidents.
Configuration Items (CIs)	List of CIs	Provide a list of all CIs within the estate

Table 20: ITSM Monthly Service Reports

Additional Monthly Reports

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

Quarterly Reporting

- Availability Reports.

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
CI	Configuration Items
CIR	Committed Information Rate
CLI	Command Line Interface
CPE	customer Premises Equipment
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
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
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
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
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
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

© Fujitsu 2026 | All rights reserved. Fujitsu and Fujitsu logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use. Subject to contract. Fujitsu endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same. No part of this document may be reproduced, stored or transmitted in any form without prior written permission of Fujitsu Services Ltd. Fujitsu Services Ltd endeavours to ensure that the information in this document is correct and fairly stated, but does not accept liability for any errors or omissions.