Business

SOFTWARE DEFINED WIDE AREA NETWORK (SD-WAN)

G-Cloud 15: Service Definition Document

Date: January 2026

Issue number: 1

Contents

Brand Statement

Buyers entering into a Call-Off Contract will be contracting with Virgin Media Business Limited ("The Supplier").

On the 1st August 2025 Virgin Media O2 Business and Daisy Group merged to create a new B2B telecoms powerhouse – O2 Daisy.

O2 Daisy is fully consolidated by Virgin Media O2 with a 70/30 ownership structure with Daisy Group. The corporate brands Virgin Media O2 Business, Virgin Media Business and O2 Business remain.

For contracting purposes, customers of these brands contract with Virgin Media Business Ltd. Depending on the services to be provided, affiliate companies may act as billing and collection agents, such as Telefonica UK.

1.0 Overview

A Software Defined Wide Area Network (SD-WAN) is a network connectivity service that connects multiple Buyer sites and cloud services. It is implemented as a software overlay across multiple underlay options (Data Access types), for example: Ethernet, SOGEA, FTTP, 4G/LTE and even those provided by a third party.

The Supplier's SD-WAN service bridges the gap between the Internet and the Supplier's network, creating fluidity and agility, and capability that empowers Buyers to respond to disruption and embrace digital transformation.

The key benefits include:

- Improved network performance and visibility
- Improved support for real time applications and access to the cloud
- Improved network agility and automation
- Increased security

2.0 Buyer Needs Addressed

SD-WAN leverages software for the centralised design, control, and management of business networks. It is a revolution in wide area networks that is delivering increased network agility, greater saleability, more control, and clearer network visibility.

SD-WAN is delivered as software overlay, in order to form a wide area network, across any form of connectivity, to separate a normal network's control plane (as a software application) from its data plane. This software is implemented on a central control platform in the Supplier's network, giving it a low level and comprehensive view of everything around it. In having this high-level view of the whole network, the software platform can send automatic and dynamic instructions to the network devices in response to changing conditions such as network capacity and congestion, or application requirements and enables the Supplier to programme the software to further refine how the network operates.

Once deployed, Buyers can send data and run applications over the Virtual Private Networks and the Internet (where Local Internet Breakout has been enabled) just like a traditional private network. SD-WAN can be implemented over fixed lined connectivity, as well as 4G/LTE and 3rd party Internet circuits.

The SD-WAN service is a fully managed service, where the Supplier manages all elements of the service between the LAN ports of the CPE located on Buyer sites, the only exception being where the CPE is connected to a 3rd party (non-Supplier) provided circuit.

3.0 Service Scope

3.1 Infrastructure for SD-WAN Solution

Supply, staging, installation, configuration and activation of the infrastructure required for SD-WAN.

3.2 Incident resolution

This activity is a 24x7 service that is oriented on the quick resolution of the incidents reported by the Buyer or detected by internal alarms.

3.3 Problem resolution

This activity focuses on a Root Cause Analysis of the recurrent incidents, alarms, or any detected fault, to define a permanent resolution.

3.4 Changes/Requests

This activity ensures that proven and standardised methods and procedures are used for efficient and prompt handling of all changes and, that the Buyer network and equipment configuration is correctly identified, controlled and maintained.

3.5 Commitments

They are focused on essential indicators that reflect the quality of the service. These indicators are measured and monitored to detect and correct any divergence with the committed values and thresholds.

3.6 Performance reports

Relevant information and reports about the performance are obtained by processing the data collected by the monitoring tools and other mechanisms.

3.7 Management Service reports

Besides the performance reports, the service provides information about service regarding quality aspects.

3.8 Customer relationship tools

Buyers access a specific tool for customer relationship management to improve and assure a good experience.

3.9 WAN and LAN Interfaces Configuration and Management

Being the SD-WAN equipment an essential part of the Buyer's WAN and LAN, the service provides the Configuration and Management of the WAN and the LAN interface towards the Buyer's Network.

4.0 SD-WAN Features

4.1 Application Aware Routing (AAR)

Collects the characteristics of the network (packet loss, latency, jitters, among others) and tunnels between the Routers and uses this information to calculate optimal routes for data traffic. The ability to consider other factors in route selection, other than those used by standard routing protocols, offers numeral advantages for the Buyer.

4.2 CloudOnRamp for IaaS

It extends the overlay network into public cloud instances, allowing Buyer branches with Routers to connect securely and directly to public cloud applications. It is built using virtual edge CPEs. Two vEdge Cloud routers that as together as a gateway between the overlay network and the application provide the connection between the overlay networks and a public-cloud application.

4.3 CloudOnRamp for SaaS

It optimises the performance of Software as a Service cloud applications based on network loss and latency. Provides clear visibility to the Buyer of the performance of individual applications and automatically chooses the best path for each one.

4.4 Dynamic Tunnel

SD-WAN supports dynamic on-demand tunnels between any two SD-WAN spoke devices. This feature enables you to configure an Inactive state for tunnels between edge devices, reducing performance demands on devices and reducing network traffic.

4.5 Forward Error Correction (FEC)

It is a mechanism to recover lost packets on a link by sending extra packets for every group of packets. This technique is recommended for sites with just one transport because they cannot select between different transport networks the better one to send the packets with no packet loss.

4.6 L7 Health Check to Zscaler

This feature allows to monitor service performance based on an HTTP request and response and to failover to an alternate tunnel based on the results. It ensures traffic takes the best path when redundant paths are available.

4.7 Local Internet Breakout (LIB)

Internet connectivity can be provided to the site at a local level, without centralised aggregation. This is often described as Local Internet Breakout allowing CPEs to function as a local exit to the Internet safely, without having to invest in security devices. When implementing a Router, traffic can go directly to the Internet at a specific location (it works as a Layer 4 and NAT Firewall).

Alternatively, Centralised Internet connectivity is also supported where Local Internet Breakout is not desirable.

4.8 Packet Duplication

Provides correction and protection against packet loss technique and that consists in duplicate packets in multiple transport networks. If packet loss occurs in one link it takes the packet from the secondary one.

4.9 Per QoS VPN

When an SD-WAN device receives traffic belonging to different VPNs from the branch network, a QoS policy can be set up to limit the bandwidth that can be used by the traffic belonging to each VPN or each group of VPNs.

4.10 Per tunnel QoS

This feature applies a Quality of Service (QoS) policy on individual tunnels, ensuring that branch offices with smaller throughput are not overloaded by larger aggregation sites. This feature is only supported for hub-to-spoke network topologies.

4.11 Route Leaking VPN0

This feature segments the network using VPNs. Route leaking between the global or default VRF (transport VPN) and service VPNs allows Buyers to share common services that multiple VPNs need to access.

4.12 Segmentation

Network segmentation provides traffic isolation. Segmentation is implemented at the ends of the network and is maintained throughout the network, safely isolating data traffic within different segments. The most usual form of segmentation is VLANs, for Layer 2 and VRF solutions for Layer 3 solutions. The features enabled can segment by physical interface, VLAN or application profiles.

4.13 Service Side EtherChannel

allows to increase the bandwidth and resilience between SD-WAN routers and other devices such as routers, switches or servers connected in a network.

4.14 TCP Optimisation

By employing this feature, communicating nodes are protected from performance-limiting WAN conditions such as packet loss and latency. Furthermore, this technique allows nodes to use available network capacity and minimise the impact of retransmission more efficiently. The Router works as a TCP proxy between a Buyer initiating a TCP flow and a server that is listening for a TCP flow. This functionality is applicable for certain devices.

4.15 Traffic Steering

Provides the capability to create a “Service Chaining,” allowing the solution to create a list of network services and steer the traffic (using DPI) through a specific path. Also, it permits determine the set of services through which a particular flow of packets must pass on its way towards the destination. The service chaining allows for additional services such as: vFW and Web Security Gateway Service.

4.16 Zero Touch Provisioning (ZTP)

Enables a rapid deployment with a quick connectivity solution in new sites while the connectivity elements are being provided. A “plug and play” deployment model can be established; this helps to keep the delivery costs minimal by reducing onsite resource time.

5.0 SD-WAN Security Features

5.1 Advanced Malware Protection (AMP)

Provides continuous monitoring and analysis to help a Buyer’s security team detect threats, and it is a security solution that addresses the full lifecycle of the advanced malware problem. It also gives you the visibility, context, and control to rapidly detect, contain, and remediate threats if they evade front-line defences, all cost-effectively and without affecting operational efficiency.

5.2 Advanced Malware Protection (AMP) with Threat Grid

AMP with Threat Grid, permit file analysis feature. File Analysis is the process of submitting an unknown file to the Threat Grid (TG) cloud for detonation in a sandbox environment. During detonation, the sandbox captures artifacts and observes behaviours of the file, then gives the file an overall score. Threat Grid’s findings are reported back to the AMP cloud so that all AMP Buyers will be protected against newly discovered malware.

5.3 Enterprise Firewall Application Awareness

Uses a flexible and easily understood zone-based model for traffic inspection, by applying a localised security policy (firewall policies) that allows stateful inspection of TCP, UDP, and ICMP data traffic flows between zones. Examine the source and destination IP addresses and ports in the packet headers, as well as the packet's protocol. The Application Firewall inspects and blocks traffic based on applications or application-family.

5.4 Intrusion Prevention (IPS)/Intrusion Detection (IDS)

Intrusion Prevention/Intrusion Detection Systems (IPS/IDS) on SD-WAN is a deep-packet inspection-based solution that mitigates a wide range of network attacks, worms, and viruses by inspecting traffic passing in both directions. IPS inspects traffic flowing through a network and can block flows malicious. It usually uses a combination of traffic and file signatures and analysis of flows. IDS is similar to IPS but does not affect flows and only to monitor the network and determine whether or not an attack is in place.

5.5 SSL/TLS Proxy for encrypted traffic

Today more applications and data reside in the cloud. As a result, majority of internet traffic is encrypted. This may lead to malware remaining hidden and lack of control over security. The TLS proxy feature allows the Buyer to configure edge devices as transparent TLS proxy. TLS proxy devices decrypt encrypted TLS traffic going through the WAN and are inspected by UTD (Unified Threat Defence). TLS Proxy identifies risks that are hidden by an end-to-end encryption over TLS channels, being re-encrypted after a proper inspection and finally being sent to its final destination.

5.6 URL Filtering

Enables the Buyer to provide controlled access to Internet websites or Intranet sites by configuring URL-based policies and filters on the device. Allows and disallows access to specific URLs and webpages categories based on whitelists, blacklists, classes, and reputations.

5.7 5.7 IP Filtering

Enables to control IP traffic based on its attributes like IP reputation and geo-location.

5.8 5.8 File Filtering

File filtering feature can be configured to block the transfer of potentially dangerous files and types of files (files associated with specific applications), files associated with specific protocols, and files travelling in a particular direction.

5.9 5.9 DNS Filtering

Allows the Supplier to control access to websites, webpages, and IP addresses, to provide protection from malicious websites, such as known malware and phishing sites.

5.10 5.10 DOS Protection

A Denial of Service (DoS) attack is an attempt to disrupt network services and deny network access by overloading unnecessary traffic using multiple sources. To defend against such attacks, we configure DoS protection policy and profiles to detect and prevent zone-based or endpoint-based DoS attacks.

5.11 5.11 Antivirus

The antivirus software scans files received or transmitted in live traffic. When the last byte of a file is transmitted, the antivirus software extracts the file and scans common file types for viruses.

5.12 Zone-Based Firewalls (ZBF)

It is a type of localised data policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs in the overlay network. Grouping VPNs into zones allows establishing security boundaries in the overlay network so the Buyer can control all data traffic that passes between zones.

5.13 Stateful Firewall

The stateful firewall feature is optional feature and can be either enabled or disabled.

The firewall keeps track of the state of network connections (such as TCP streams or UDP communication) and can hold the significant attributes of each connection in memory. These attributes are collectively known as the ‘state of the connection’ and may include such details as: the IP addresses, ports involved in the connection, and the sequence numbers of the packets traversing the connection. Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated, so that filtering decisions would not only be based on administrator-defined rules, but also on context that has been built by previous connections as well as previous packets belonging to the same connection.

Security access policies classify network traffic and define rules that are triggered upon match conditions. A non-exhaustive list of classifications includes:

- Source or destination zone
- Source or destination address
- IP Headers
- Services (based on port/protocol)
- Domain names
- Source or destination geo-location
- Time of Day

There are two types of rule actions, these are:

- Logging: start, end, both, never
- Enforcement: allow, deny, reject

A total of 50 rules can be specified as standard.

6.0 SD-WAN VPN designs

The primary function of SD-WAN, when considering a replacement for more traditional MPLS VPN networks, is the ability to create VPN environments through which traffic can flow from site to site. The VPN functionality, often referred to as the overlay, is achieved by utilising tunnels from CPE to CPE over the connected Data Access Services, often referred to as the underlay.

The VPN overlay is facilitated by the Supplier's cloud-based controllers and control plane, which operates on a separate control tunnel between the CPE and the controllers.

6.1 Encryption

All VPN site-to-site traffic is encrypted as standard. To provide predictable service in terms of operation and performance a single suite is used and based on the 'Foundation' principles.

Foundation is a recommended cryptographic profile according to the National Cyber Security Centre (https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data).

This Foundation profile consists of an RFC-compliant implementation of IPsec with IKEv1 (RFC2408 and RFC2409 apply), without custom extensions, using Extended Sequence Numbers (RFC4304), Encapsulating Security Payload (ESP - RFC4303).

There are several overlay VPN topologies that the Supplier supports as part of the Supplier's solution. These are defined as follows:

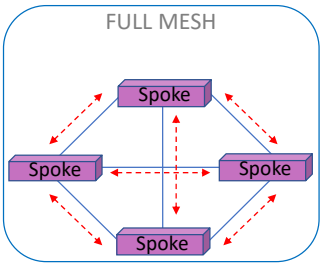
- Full Mesh (typical)
- Hub and Spoke
- Multi-Hub and Spoke
- Spoke Group Segregation

For each CPE deployed, the Supplier can configure the device to be either in a Full Mesh or a Hub or a Spoke configuration. When a spoke topology is requested, each site must specify a Spoke Group option which provides the Buyer with the options of defining the topology:

- Spoke to Hub Only
- Spoke to Spoke via Hub
- Spoke to Spoke Direct

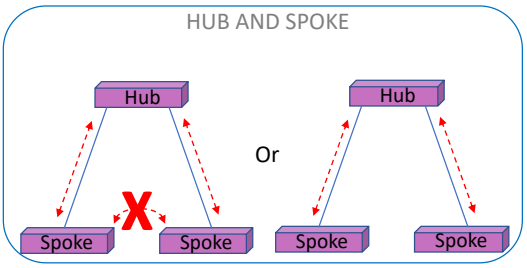
6.2 SD-WAN-Topology01: Full Mesh

The fully meshed VPN topology provides any to any connectivity between Buyer sites where devices build overlay tunnels to each other, as shown in the diagram.



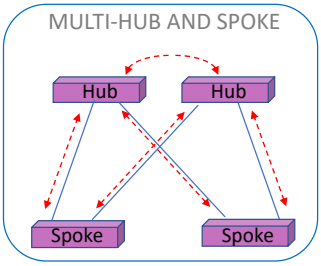
6.3 SD-WAN-Topology02: Hub and Spoke

The hub and spoke VPN topology has a single hub (for example a data centre) that has connections to each spoke (the remote sites). The spokes cannot route traffic directly to each other but can be configured to send traffic via the hub, as shown in the diagram.



6.4 SD-WAN-Topology03: Multi-Hub and Spoke

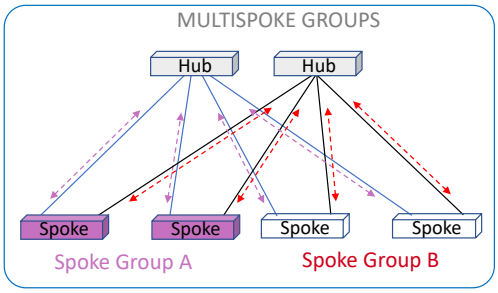
The multi-hub and spoke VPN topology can consist of multiple hubs (up to eight) each of which may have connections to each spoke (the remote sites). This topology enables hub overlay traffic to be load shared to prefer one hub over another but fail over to the other hub in a failure scenario or support an active standby scenario, failing over all overlay traffic from one hub to another, as shown in the diagram.



6.5 SD-WAN-Topology04: Multispoke Groups

The multispoke group VPN topology functions in a very similar way to a multi-hub and spoke topology but additionally enables groups to maintain data segregation by creating different spoke groups, as shown in the diagram.

There is also an option to define a community value that is associated to a spoke group and can be used in a similar manner to BGP communities to identify members of a spoke group. If this is not used, a community value is automatically created within the platform.



6.6 SD-WAN Access Connectivity Services

Access connectivity Services extend the network directly to the Buyer's premises and will be terminated by a network termination unit (NTU) and a Buyer Edge (CPE) router which will normally provide the demarcation point between the Supplier's network and the Buyer's.

In this scenario, the managed service domain from the Supplier only covers the CPE hardware and the software installed on it – see the below figure. At the Buyer's sites, the Buyer is responsible for the LAN and all applications.

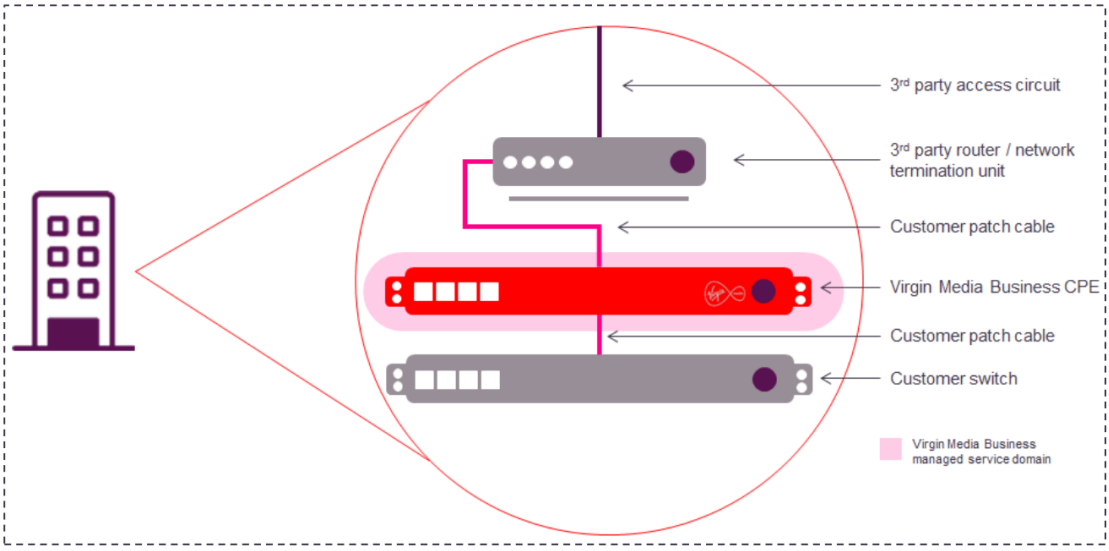


Figure 1: Supplier managed service domain, where a 3rd party connection is in use.

6.7 SD-WAN Virtual CPE (VCPE)

Access connectivity services may extend the network directly to the Buyer's public cloud environment.

The SD-WAN service supports Virtual CPE (vCPE) for deployment in Cloud service Provider (CSP) environments including Amazon Web Services and Microsoft Azure.

This allows you to bring your public cloud services direct into your SD-WAN – using the same range of routing and security functions as at physical uCPE, but in virtual form.

vCPE are also visible within SD-WAN Analytics and the SD-WAN Console.

vCPE are deployed by the Supplier into the buyer's cloud environment – with the buyer configuring the underlying compute function, foundation routing and security policies to enable the vCPE to be visible to the SD-WAN and provide access to the internal services.

In this scenario, the managed service domain from the Supplier only covers the software installed on the buyer's virtual platform.

The Buyer is responsible for all components relating to the CSP.

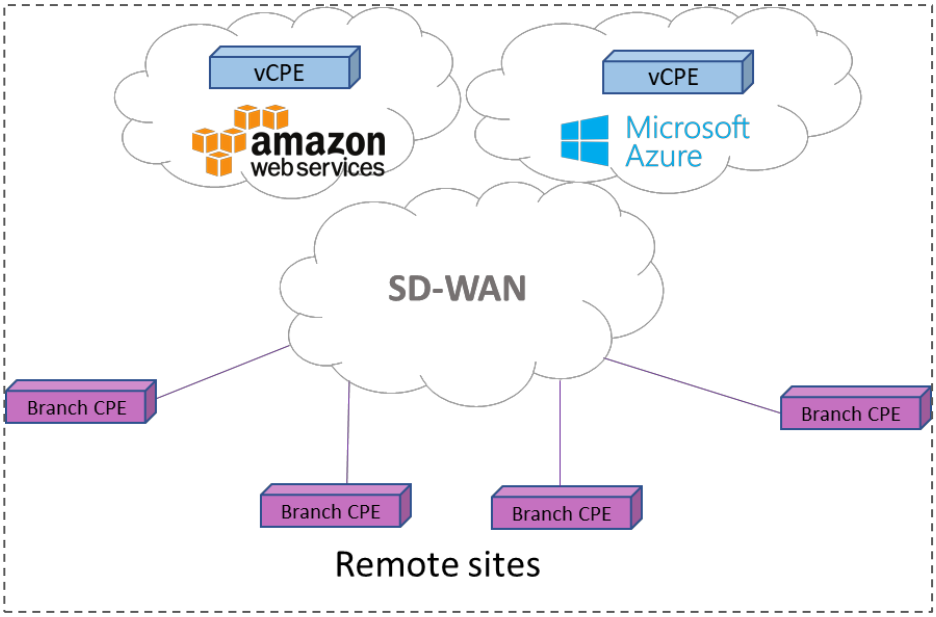


Figure 2 Supplier managed CSP environment with managed vCPE

7.0 SD-WAN Access Services

Resilience Services are not complete on their own, they must be purchased with the corresponding topology and service.

Sites are connected to the Managed SD-WAN Service by one or more Access Connections, typically 2 per site, however, can scale up to 4 access connections. A variety of Access Connection types and speeds are available, as set out in the Table below.

For diverse resilient services separation can only be assured when both circuits are provided by the Supplier and have been delivered as diverse circuits. Please note that on rare occasions geographic 'pinch points' can still occur, such as at the only bridge in the area where ducts may run along either side of the bridge to maintain separation.

Ethernet	FTTP	Cable	SOGEA
☑	☑	☑	☑

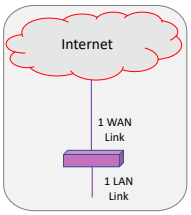
A variety of Access Connection types and speeds are available, as set out in Table below.

Table 1: Access Options

Access Connections		Description
Access	Ethernet	Up to 10Gbps
	FTTP	Up to 1Gbps
	CABLE	Up to 1Gbps
	SOGEA	Up to 80Mbps
	SOADSL	Up to 24Mbps
	LTE/4G	The Supplier provided cellular for primary or backup
Ethernet Fibre Access Resilience	Standard	Direct fibre access to the nearest PoP.
	Secure	Adds a second diversely routed access circuit to the same PoP
	Secure+	Adds a second diversely routed access circuit to a different PoP

8.0 Site Deployments

8.1 Non-Resilient



This Service delivers no resilience; a single Data Access Service connects the single Buyer CPE to the Internet via any single circuit type.

A single LAN connection is provided which is presented as an RJ45 Ethernet port. The LAN connection can support IEEE 802.1Q VLANs.

8.2 Dual access circuit, Single CPE

This Service delivers a resilience model that provides a single CPE with two data access circuits. A total of two access circuits will be used to connect to a single CPE. Permitted access types are LTE, xDSL, Hybrid Fibre Coax, GEA FTTA, EFM and Ethernet, any combination is permitted.

A single LAN connection is provided which is presented as an RJ45 Ethernet port. The LAN connection can support IEEE 802.1Q VLANs.

8.3 Dual access circuit, Dual CPE

This Service delivers a resilience model that provides Dual CPE with two data access circuits. A total of two access circuits will be used to connect to a two CPEs (one circuit per CPE). Permitted access types are LTE, xDSL, Hybrid Fibre Coax, GEA FTTA, EFM and Ethernet, any combination is permitted.

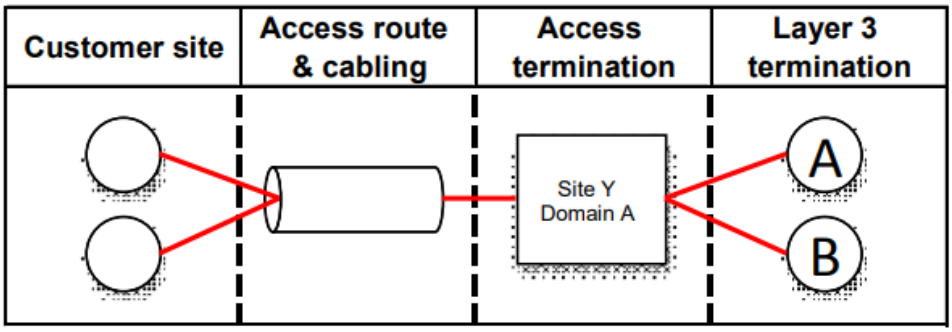
A single LAN connection is provided from each CPE which is presented as an RJ45 Ethernet port. The LAN connection can support IEEE 802.1Q VLANs.

8.4 Dual Ethernet access circuit, dual CPE- Partial Diversity

This Service delivers a resilience model that provides two data access circuits that connects the Buyer CPE to the Internet using two Ethernet fibre circuits, no other access type is permitted.

The CPEs are connected via an inter-chassis link (ICL) – an RJ-45 Ethernet connection between the two CPE devices. This connection can be direct over a single cable or over Buyer Cat-5e (or better) structured wiring (maximum 90m) but cannot be via a layer-2 network or layer-3 device.

This option is designed to protect against a network failure (such as a fibre break) away from the Buyer site (as the circuits may share a single duct until the nearest separation point). For example, where both circuits are provided by the Supplier, they may share a single duct until they reach the end of the street where one circuit turns left and the other right.

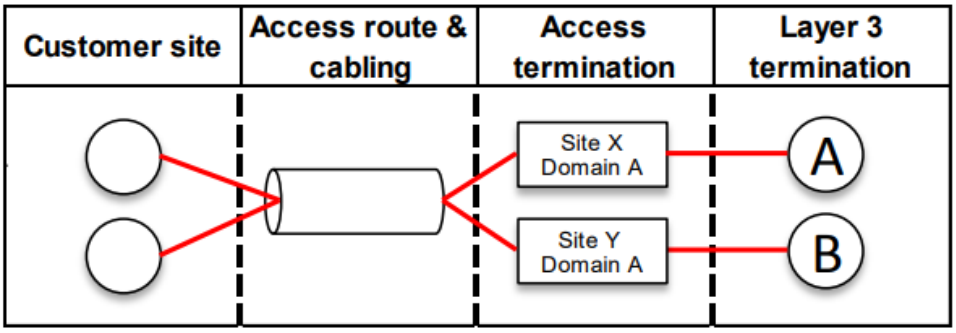


8.5 Dual Ethernet access circuit, dual CPE – Assured Diversity

This Service delivers a resilience model that provides two data access circuits which connect via two access termination points, the circuit connects the Buyer CPE to the Internet using two Ethernet fibre circuits, no other access type is permitted.

The CPEs are connected via an inter-chassis link (ICL) – an RJ-45 Ethernet connection between the two CPE devices. This connection can be direct over a single cable or over Buyer Cat-5e (or better) structured wiring (maximum 90m) but cannot be via a layer-2 network or layer-3 device.

This option is designed to protect against on-site equipment failure, an access termination failure and network failures (such as a fibre break) anywhere in the network away from the Buyer site as the circuits may share a single duct until the nearest separation point).

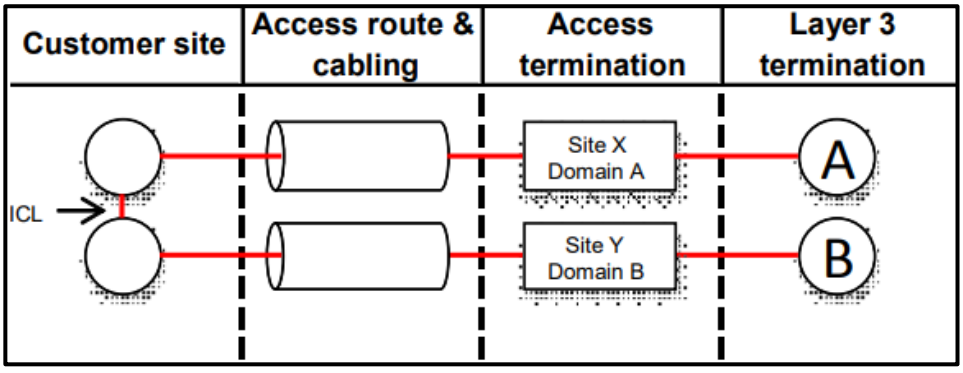


8.6 Dual Ethernet access circuit, dual CPE – Assured Separation

This Service delivers a resilience model that provides two separately routed data access circuits that connects the Buyer CPE to the Internet using two Ethernet fibre circuits, no other access type is permitted.

The CPEs are connected via an inter-chassis link (ICL) – an RJ-45 Ethernet connection between the two CPE devices. This connection can be direct over a single cable or over Buyer Cat-5e (or better) structured wiring (maximum 90m) but cannot be via a layer-2 network or layer-3 device.

This option is designed to protect against on-site equipment failure and network failures (such as a fibre break) anywhere in the network, even close to the Buyer site. The circuits will normally be in separate ducts and connected to the site separately, this option can provide the highest level of resilience and separation available.



8.7 Dual access circuit, Single CPE

This Service delivers a resilience model that provides a single CPE with three data access circuits. A total of three access circuits will be used to connect to a single CPE. Permitted access types are: xDSL, Hybrid Fibre Coax, GEA FTTA, EFM and Ethernet, any combination is permitted however three of the same access type may not be used, for example, LTE + LTE or xDSL + xDSL.

A single LAN connection is provided which is presented as an RJ45 Ethernet port. The LAN connection can support IEEE 802.1Q VLANs.

8.8 Triple access circuit, Dual CPE

This Service delivers a resilience model that provides Dual CPE with three data access circuits. A total of three access circuits will be used to connect to a two CPEs (one or two circuits per CPE). Permitted access types are LTE, xDSL, Hybrid Fibre Coax, GEA FTTA, EFM and Ethernet, any combination is permitted however two of the same access type may not be used, for example, LTE + LTE or xDSL + xDSL.

A single LAN connection is provided from each CPE which is presented as an RJ45 Ethernet port. The LAN connection can support IEEE 802.1Q VLANs.

9.0 SD-WAN Deployment Models

9.1 SD-WAN Private Deployment

SD-WAN in a private deployment model focuses on the benefits and service assurance of private transport and networking. This can be delivered across 1 or 2 edge devices to enable the buyer to take advantage of private SD-WAN which offers a more secure service with network path tunnel performance (SLA's) based on latency, Jitter, and packet loss to suit the specific business or critical application performance needs.

9.2 SD-WAN Hybrid Deployment

SD-WAN in a hybrid deployment model supports the use of both Public and Private transport connectivity at the branch sites. This can be delivered across 1 or 2 edge devices to enable the buyer to take advantage of the best of both transports to ensure optimum application performance for business-critical private applications whilst leveraging direct connectivity from the branch to the corporate cloud applications.

9.3 Public Connectivity Dedicated Internet Access

SD-WAN in a public deployment model is designed for "cloud first" Buyers leveraging the flexibility and accessibility of internet transport and cloud access from the branch sites. This can be delivered across 1 or 2 edge devices to deliver optimal access to the corporate cloud applications.

9.4 3rd Party Internet Access

For Buyers that have an existing Internet circuit or prefer to source the access themselves.

10.0 Customer Self-Serve Portals

10.1 ITSM

The Supplier's Service Operation uses a single service management tool across the SD-WAN Service. This service management system, allows Incidents, Problems and Requests to be raised on a single system, pushed to the correct resolving team, and allow all the service and support teams to see a single view of the ticket.

10.2 Self-Serve portal

The Supplier's ITSM system provides Buyers with a self-service portal offered as standard for our customers where dedicated customer service teams can raise (non-urgent) incidents as well as, update and check on the status of all the Incidents and Requests.

10.3 ITSM Integration (option)

Additionally, for Buyers that prefer a more automated service experience, we offer:

- Full API & integration between the Supplier's ITSM and Buyer's ITSM
- Email integration – the Buyer can be set up to receive emails

ITSM integration is optional, though recommended and incurs an additional cost to set up, test and activate.

10.4 SD-WAN Portal

SD-WAN offers the buyer access to a Next Gen advanced WAN monitoring & management platform used to perform various tasks and operational workflows, including provisioning, monitoring, managing, and reporting on the SD-WAN components. Up to ten Buyer elected users are offered READ ONLY access to their SD-WAN portal, which will present a set of pre-defined dashboards for SD-WAN observability, monitoring, assurance, and reporting.

10.5 SD-WAN Analytics Portal

SD-WAN Analytics Portal offers a comprehensive insight into application and network analytics, and enables users to generate reports on the fly or have them automated and delivered via email in either CSV or PDF format.

10.6 Concerto Self-Service Portal

Designed to enhance customer experience and autonomy, Concerto provides an intuitive, self-service platform that allows buyer to manage their SD-WAN environment with greater efficiency, flexibility, and confidence. Concerto provides a user-friendly interface that enables buyer to take charge of their SD-WAN environment with less dependency on external support. They can make changes, optimise network performance, and monitor their services in real-time.

Company Statement

All information contained in this proposal is subject to contract and, unless expressly stated to the contrary, to Virgin Media Business Limited's standard terms and conditions.

Registered office: 500 Brook Drive, Reading, RG2 6UU, United Kingdom

Brand Statement

Buyers entering into a Call-Off Contract will be contracting with Virgin Media Business Limited ("The Supplier").

On the 1st August 2025 Virgin Media O2 Business and Daisy Group merged to create a new B2B telecoms powerhouse – O2 Daisy.

O2 Daisy is fully consolidated by Virgin Media O2 with a 70/30 ownership structure with Daisy Group. The corporate brands Virgin Media O2 Business, Virgin Media Business and O2 Business remain.

For contracting purposes, customers of these brands contract with Virgin Media Business Ltd. Depending on the services to be provided, affiliate companies may act as billing and collection agents, such as Telefonica UK.


Virgin media
O2
Business