Colt SD Wan

External Service Guide – Customer Reference

Contents

1. Overview

Colt's Software Defined WAN (SD WAN) is a managed service offering towards deploying and managing Enterprise network connectivity and providing several integrated functionalities to transform customer's digital network experience. It gives Customers the ability to combine multiple access connections types (MPLS, Internet, 3G/4G) with application-based policy forwarding and advanced security functions to create a software defined network capable of delivering on changing business needs and capacity challenges.

Colt SD WAN incorporates various software images of Virtual Network Functions (VNFs) deployed on commodity hardware for routing, security, WAN and application optimization and analytics. Colt SDWAN makes use of underlay connectivity (private MPLS and public Internet) to establish a secure, encrypted overlay VPN. Customers can use it to quickly create and deploy a network that offers services like business-grade IP VPN, secure broadband Internet or application-aware routing with full security and QoS over WAN connections. Traffic can be automatically and dynamically (manually) forwarded across the most appropriate WAN path based on network conditions, quality-of-service (QoS) requirements, usage requirements and cost. This combined feature set offers higher network service availability and increased network performance.

In addition, SD WAN allows Customers to optimize the use of their bandwidth through load balancing over multiple Internet uplinks over broadband, 3G/4G (with an Ethernet handoff) in addition to traditional MPLS connections. SD WAN also allows to connect to Cloud service providers and SaaS providers to extend their WAN edge to Cloud.

Colt has further enhanced its SD WAN service with the launch of its universal customer premises equipment (uCPE) solution at the network edge. The Colt SD WAN service now provides 3pp unmanaged VNF hosting functionalities like CheckPoint Firewall offered as an additional VNFs on the uCPE with Versa SDWAN VNF. It further puts the control of network in the hands of the customer, giving them the flexibility to license, manage, monitor functions with the choice of network options. This capability is bringing the benefits of cloud computing from data centres to edge computing at the customer premises and branch sites, representing a paradigm shift in how enterprises consume connectivity services.

Colt also offers a Wholesale SD WAN solution that provides a flexible approach that offers not only an alternative to an existing vendor, but also the instant ability to a fast time to market when no SD WAN solution is in place for them.

This solution consists in offering our current Versa solution to them, with some clear adaptation (customizable portal, branding and further hierarchy levels, systems and processes modification, etc) that allows the end-customer to benefit from a top-quality SD WAN service without any reference to Colt, as if our Wholesale customers were offering it directly.

Perfect match will come for those who haven't developed an owned solution, proactively looking for some partner who could cover that gap and offer a turnkey solution with no upfront investment or development time, assuming certain limitations because of the resale environment and the vendor restrictions, that will be covered throughout the document.

Colt can help to engage this digital enrolment, helping to integrate our existing SD WAN service so that the Wholesale customer can resell it to their end customers, with little visibility about who is actually providing the service in backstage and with full functionality towards them.

There are specific considerations along the processes, that will be covered during the following sections.

2. Benefits

2.1. Available Anywhere

Colt SD WAN service is available to virtually any business address worldwide (basic connectivity pre-requisite) in a fully meshed or hub-and-spoke network configuration options.

SD WAN allows connectivity between SD WAN and Non-SDWAN (traditional IPVPN) sites.

2.2. Quick Deployment

New locations can be turned up in as little as minutes with zero touch provisioning ("bringing" the device into the network). Customers will be able to manage their own service, add new branch sites in hours, or upgrade bandwidth real-time. The customer will be provided with Common off the Shelf (COTS) server, Colt uses pre-configured CPE devices which are as easy to setup as a home WiFi router.

2.3. Security

Secure end to end connectivity using IPSEC encryption, this ensures that the transit of an Customer's proprietary data is fully protected and inaccessible beyond the intended origination and destination points. Colt SDWAN provides an integrated firewall with SDWAN which provides secure local internet breakout, provides DDoS protection and ability to create firewall policies and rules required as per customer specific requirements.

2.4. Connectivity Flexibility

Colt SD WAN services can be provided over public internet - broadband Internet and business internet - dedicated internet access (DIA) connectivity (using any and all transport technologies like xDSL, wireless 3G/4G/LTE (only available in EU for Colt provided SIMs, no limitation for customer-owned), Ethernet or traditional MPLS regardless of whether Colt is providing that underlying connectivity or not. Local breakout is available, if desired, so that only certain traffic is forced through the SD WAN network.

Ideally MPLS should be from Colt. MPLS circuit is from Colt or from Colt's existing MPLS NNI partners. Any new MPLS provider needs an MPLS NNI to be setup first (see connectivity constraints for Carrier's provided MPLS legs)..

2.5. Application Performance

Based on Customer requirements, Colt SD WAN service ensures that it always provides the best available connection for traffic flows based on jitter and latency requirements. In addition, Customers are in complete control of steering traffic over specific preferred links through the use of layers 3, 4 and 7 based access control lists and policies that can be implemented via the self-service portal.

2.6. Self-Service Portal

Colt SD WAN portal allows dynamic management of network based on Customer requirements, with policy control and visibility, traffic data reporting is also available for visibility of throughput (peak/average) and traffic volume for a selected duration.

For Wholesale service, both Carrier and end-customer will benefit from a customized look and feel, setting your own logo, background image, links and contact details, so that your end-customer experience doesn't differ from the rest of your services offered.

2.7. Service Reliability

Multiple points of presence, bidirectional metro rings, and a fully redundant network core support ensures service availability and that customer data gets to where it needs to go.

2.8. Redundancy and High Availability

Colt SD WAN service can be deployed in a redundant and highly available manner, supporting link level and device level redundancy to eliminate single point of failures. In addition, the back-end control and provisioning systems are redundant as well to ensure service availability is not affected by any single point of failure.

2.9. Cost Efficiency

Colt SD WAN provides the ability to manage and optimize traffic over multiple infrastructure links and maximize the use of bandwidth thereby lowering costs. Customers can use it to top up existing IP VPN bandwidth by using the Internet in addition to existing IP VPN bandwidth; another use case would be an Internet only version which can be used where dedicated leased line cannot be justified due to cost reasons.

2.10. Control (Changing Traffic Patterns)

SD WAN gives the ability for customers to route their traffic for specific application based on a number of parameters. Traffic policies (MPLS vs internet) will be set during the initial deployment and will be based on basic business rule settings (IP address/subnet, protocol and/or port number, pre-loaded applications), these can be changed any time via the self-service portal.

2.11. Analytics

Near real time, interactive dashboards that enable Customers to keep an pulse on the health of a network and applications – continuously monitor traffic flows, enabling the identification of and response to business impacting events. Visualization of application performance, network security and Firewall, and utilization – allowing organizations to analyse issues at the site level, application layer, or individual user level.

2.12. Multi-cloud

With SD WAN Multi-Cloud, customers are able to connect their branch sites directly to all their cloud-based SaaS and IaaS and manage this connectivity centrally via the Colt SD WAN portal. It brings together a single cohesive view of the enterprise network, tying together WAN sites, IaaS/Cloud sites, and traffic towards SaaS cloud – all easily viewed and managed via the Colt SD WAN portal. It extends the SD WAN benefits of security, analytics and optimization to connectivity to the CSP and provides an end-to-end SLA for all connectivity types (MPLS, Internet, Wireless and Cloud) for enterprise networks.

Multi-cloud solution uses gateways hosted in the Colt network with dedicated connectivity into the Cloud (AWS Direct connect, Azure ExpressRoute or Google Cloud Interconnect (GCI)).

Today, Colt SD WAN Multi-Cloud supports AWS, Microsoft Azure, and Google Cloud and is currently only available in Europe; however, availability of this feature in Asia is in the roadmap, currently for Q4 2020/Q1 2021.

2.13. Support for IPv6

Internet Protocol version 6, is a new addressing protocol designed to incorporate whole sort of requirement of future internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on Network Layer (Layer-3). IPv6 provides larger addressing space and simplified header. Colt SD WAN supports use of IPv6 addressing on LAN interface.

2.14. Support for VoIP & Sip Trunking

Colt SD WAN brings the benefits of VoIP over SD WAN to deliver Colt SIP trunking solution for Colt countries. For VoIP Performance Monitoring, SDWAN sites use real-time flow monitoring and SLA probes to provide visibility of network performance between all sites. VoIP Traffic can be dynamically routed over Internet or MPLS based on Packet Loss, Latency, Jitter, or MoS thresholds. VoIP over SD WAN provides an integrated solution for connecting Internet and MPLS sites to benefit from hybrid connectivity.

2.15. WAN Optimization

SD WAN with WAN optimization provides customer an enhanced user experience as it improves the network performance and reliability over multiple wan links for a site. It alleviates the effects of latency that maximize bandwidth utilization and relieves network congestion. The advantage of SD WAN with WAN optimization is that it is aware of other network traffic on the same link and can intelligently manage all flows overcoming the problems of TCP retransmission.

We utilize following traffic optimization techniques

- **Forward Error Correction (FEC):** Allows missing data packets to be recreated at the destination without adding latency or jitter
- **Packet Cloning (Replication):** Mirrors packets between two or more paths – if one packet is lost, the mirrored packet will still be delivered

3. Service Design

3.1. Transport agnostic Application driven WAN

Colt SD WAN ensures Customer WAN network is designed to provide efficient application performance irrespective of the underlying transport (MPLS or Internet). The service enables and implements application routing policies and also allows for load balancing of default traffic in order to ensure that all available WAN capacity is optimally utilized.

3.2. Site design types – SD WAN Service Pack (Multiple WAN Links)

Colt SD WAN supports multiple access types to suit individual site requirements; these can include dedicated Ethernet, Direct Internet Access, cost-effective broadband DSL connectivity or 3G/4G/LTE.

The way in which you order Colt SD WAN services has changed. Up until now, Colt SD WAN has been sold as a mixed configuration solution with several non-standard elements, with personalised designs being built for every customer order.

The new approach significantly simplifies the process by offering new standardised packages which customers can mix and match to meet the requirements for each of their sites. This presents a number of benefits, both internally and externally.

Below is a table summarising the new standardised packages that are available for your customer to order per site.

Example site use case	Branch Office			Edge Data Centre		Core Data Centre	
	XS	S	S Plus	M	M Plus	L	L Plus
WAN							
Internet Link (excl. LTE	1	2	2	2	4	2	4
MPLS	1	1	2	1	2	1	2
Max Total (Max per Device)[1]	1	2	2(1)	2	4(2)[5]	2	4(2)[2]
LTE Option[2]	X[3]	X[5]	X[4]				
Single or Dual CPE	Signal	Signal	Dual	Signal	Dual	Signal	Dual
Link Diversity per CPE	-	X	X	X	X	X	X
CPE Diversity	-	-	X	-	X	-	X
Bandwidth							
up to 150Mbps (Versa 150)	X	X	X				
up to 250Mbps (Versa 120)	X	X	X				
up to 1Gbps (Versa 810)				X	X		
up to 3Gbps (Versa 1000)						X	X
Fibre Handoff Option	-	-		X	X	X	X
AC or IDC Power	AC	AC	AC	AC/DC	AC/DC	AC/DC	AC/DC
SLA (for on-net circuits)	99.90%	99.90%	99.95%	99.90%	99.95%	99.90%	99.95%

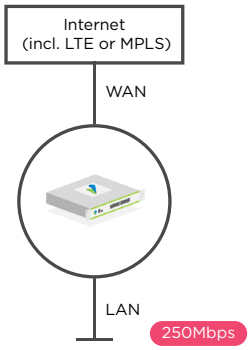
Each size package varies in the type and number of WAN uplinks, number of CPEs, bandwidth, diversity, and service assurance.

To build a new SD WAN solution, simply work with your customer to mix and match these 'sizes' to meet the requirements for each site.

1 Any combination of Internet and MPLS uplinks up to the max supported and not exceeding maximum for each type.
2 LTE as substitute or in addition to any fixed Internet connections.
3 LTE substitutes the fixed WAN Uplink
4 Dual LTE not supported in combination with Fixed MPLS or Internet uplinks. Single LTE uplink is on primary CPE when combined with 2 fixed uplinks.
5 Max 1 MPLS per CPE. Single MPLS is always on primary CPE.
6 For 2 Internet uplinks LTE substitutes the second Internet uplink

To illustrate these site size packages further, see the example use cases below:

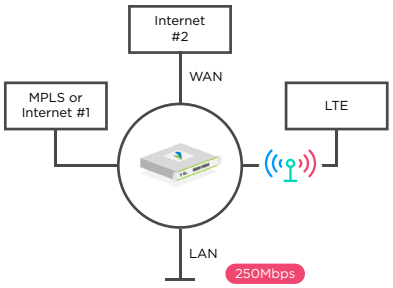
XS - Retail Store



XS package is the entry level connectivity option for customer sites to be connected using a single CPE with a single WAN uplink (either MPLS or Internet, including LTE). There is no redundancy in the solution design, and the CPE used will be the V120, allowing a maximum BW of 250Mbps.

S package provides two WAN uplinks using a single CPE with link diversity. It supports access redundancy with both lines in an active-active configuration, allowing total available bandwidth to be used under normal traffic conditions. Important to note that both uplinks should have the same nominal bandwidth to optimize the results of the active-active usage of both access lines and best path routing and traffic selection path. The CPEs used will be either the V510 for BWs up to 150Mbps, or the V120, allowing a maximum BW of 250Mbps.

S - Small Branch Office

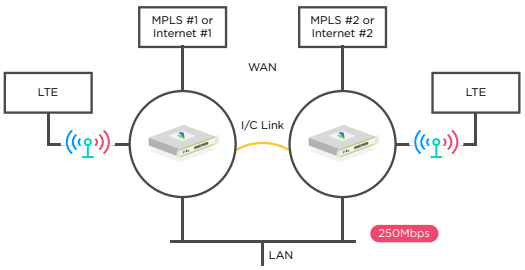


S plus package is useful for customers requiring a higher resiliency level, providing CPE diversity.

Two CPEs are deployed with back to back connectivity, with a maximum of one WAN uplink per each CPE

The CPEs used will be either the V510 for BWs up to 150Mbps, or the V120, allowing a maximum BW of 250Mbps.

S Plus - Production facility



M/L packages are a perfect fit for large office sites that require multiple WAN links but no CPE resiliency.

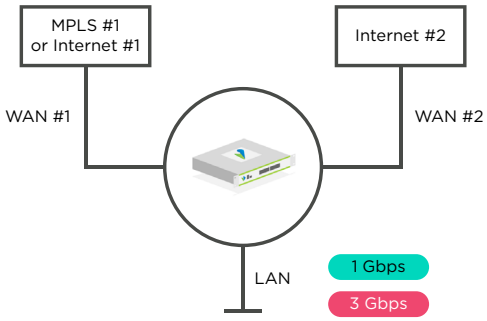
Both provide a maximum of two WAN uplinks, that can be either two internet (no LTE) or one internet plus an MPLS leg.

The CPE model used in M package will be the V810, offering a maximum BW of up to 1Gbps.

The CPE model used in L package will be the V1000, offering a maximum BW of up to 3Gbps.

Both support fibre handoff option.

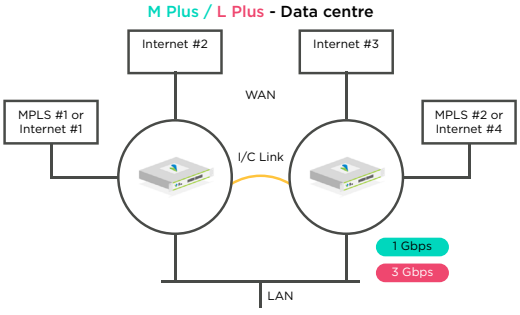
M / L - Large office with no resilience required



M/L plus packages are a perfect fit for data centre sites that require multiple WAN links but with CPE resiliency as well.

Both provide a maximum of four WAN uplinks (two per CPE), that can be either two internet (no LTE) or one internet plus an MPLS leg per CPE.

M Plus / L Plus - Data centre



The CPE model used in M package will be the V810, offering a maximum BW of up to 1Gbps.

The CPE model used in L package will be the V1000, offering a maximum BW of up to 3Gbps.

Both support fibre handoff option.

There are numerous key benefits, that can be separated either from a customer's perspective or internal:

For Customers, it means:

- Faster time to live SD WAN service vs competitors
- Simpler planning and deployment, no overengineering
- More efficient use of their backbone network – options can be mixed and matched to optimise the use of each site over their existing network (creating potential cost savings of 20-50% savings for retail, 30-40% for manufacturing)\
- More flexibility and greater choice with greater automation capabilities in ordering and delivering their service
- More resilience options to meet SLA requirements of their business
- Greater cost transparency

For a Colt employee, it means:

- Reduces bespoke designs, saving time and effort
- Customer network simplification – operationally less complex to build and maintain
- Communicating with your customer is simpler and easier
- Happy customers! Time to deliver is reduced from months to weeks

Common attributes for all site types:

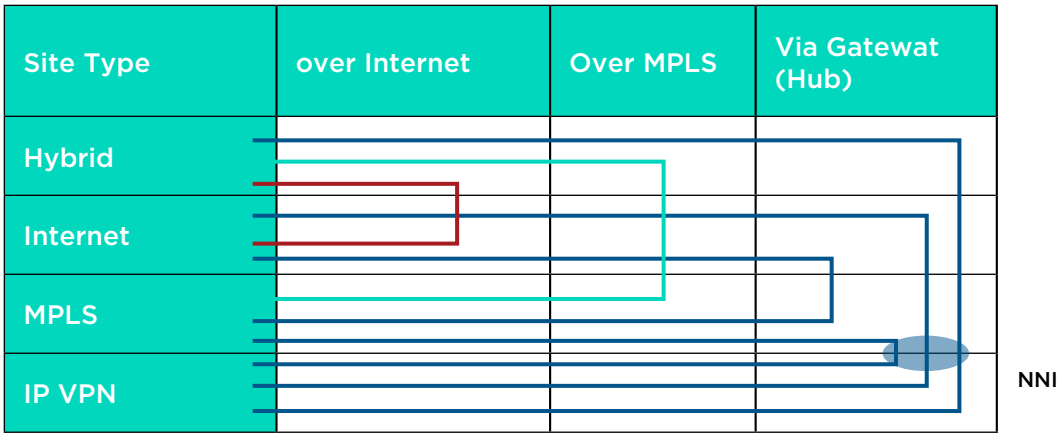
- Underlay to establish IPSec tunnel/MP-BGP and run data traffic directly between SD WAN and non-SD WAN sites.
- IPSec tunnels between all sites.
- Customer traffic load shared across the links.

Product approval for design is needed for all SD WAN orders above 250 sites.

At the moment this guide was written, new CPEs were being standardised to fulfil expectations of those customers who require higher bandwidth demands. Once they become available, the guides will be updated accordingly.

3.3. Traffic flows

The customer may have a mix of sites – IP VPN on-net sites (connected directly to Cisco based MPLS network) or SD WAN hybrid sites (OLO MPLS and Internet lines, Versa based) or SD WAN Internet only (Versa based) or SD WAN MPLS-only site.



*Backup Path not shown

Below table provides the overview of the traffic flows with regards to how SD WAN gateways and Encrypted tunnels are involved (Versa uses IPSec but combined with other protocols)

Site Type	MPLS + Internet	MPLS Only	Internet Only	IP VPN
MPLS + Internet	Encrypted	Encrypted	Encrypted	IPSec till one end of SD WAN Gateway, and then Normal IP VPN on the NNI from Gateway to PE from the other leg
MPLS only	Encrypted	Encrypted	Encrypted (via Gateway)	IPSec till one end of SD WAN Gateway, and then Normal IP VPN on the NNI from Gateway to PE from the other leg
Internet only	Encrypted	Encrypted (via Gateway)	Encrypted	IPSec till one end of SD WAN Gateway, and then Normal IP VPN on the NNI from Gateway to PE from the other leg

SD WAN Gateways provide the following functions 1) they act as a transit gateway between the encrypted SD WAN VPN and a normal IP-VPN and 2) They act as a hub for connecting SD WAN sites on disjoint networks e.g. a site connected to MPLS only and a site connected to Internet only. SD WAN Gateways are implemented on a region by region basis to reduce the latency caused by backhauling tunnels

3.4. Application aware connectivity

Colt SD WAN service delivers path control for application-aware routing and forwarding across the WAN. It supports, dynamic selection of the best path for application-based business policies and application-based load balancing across paths for full utilization of bandwidth with improved network availability.

3.5. Encryption

- Encryption method: Advanced Encryption Standard AES-128 and AES-256 supported.
- Authentication Method: Secure Hash Algorithm SHA2.
- Internet Key Exchange (IKE): IKEv2.
- PSK: As standard, pre-shared keys will be used to authenticate between IPSec peers.

(Colt owns & manages the keys).

3.6. Customer Information Protection

It is Colt's policy to protect all confidential information related to its business activities, as well as confidential information on customers, partners and others. The Information Security Policy standards are designed to ensure that information assets are protected from all types of security threats and that highly reliable services are provided. To this end, the Information Security Management System (ISMS) is established and will be enforced. Continuing efforts will be made to improve the system.

Summary of Colt's Security certifications (ongoing):

- BS7799
- MC is accredited with ISO 27001*

* ISO 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

4. Features

Colt SD WAN is an evolving product line, this is primarily because the industry is still evolving with ongoing developments (Colt product offering is mature as committed). Colt will continue to improve and add new product features and they will be added in this guide as they are released (please refer to roadmap for details).

4.1. Customer Portal

Colt SD WAN Portal is a self-service portal (does not support service provisioning and ordering – for now) available for both Carrier and end customer. It enables network services to be used, modified and orchestrated on real-time and on-demand basis - as is typical for cloud services. As it is 'software defined/controlled', the WAN transforms into an agile, flexible network enabling a Customer to be in control of its network.

In summary, the portal gives the Customer the ability:

- To map applications to specific WAN uplink (eg., MPLS and/or Internet)
- To choose when an application needs to switch to the secondary path

The portal is intuitive and easy to navigate with below features:

Portal Pages	Page Details
Dashboard	• Gives an overview of all provisioned sites on a geographically accurate map • Dashboard allows regularly used graphs or reports to be pinned to the Dashboard view. • Status of Pending orders are listed
Policy Management	• per site traffic steering policy rules • per site add, delete, edit and back-up traffic policies • map traffic to WAN uplinks on multiple parameters like source and destination IP Address, source and destination port/socket, protocol and applications (more than 2,500 applications supported) • define policy to switch between WAN links based on latency, jitter, packet loss, traffic Rx/Tx thresholds • Multiple metrics per policy can be added • Bulk copy pushes policies to multiple sites by single button click

Portal Pages	Page Details
Firewall Management	• per site firewall rules overview • per site add, delete, edit and back-up firewall policies • Policies applied to Internet and SDWAN for both inbound and outbound traffic • Create firewall rules based on multiple parameters like source and destination IP Address, source and destination port/socket • Create Application layer inbound and outbound Firewall policies with source/destination IP addressing • Create DNAT for LAN and DMZ zone rules by IP address and port number • Bulk copy pushes policies to multiple sites by single button click • default policy deny all
Firewall analytics	• lists all active firewall rules • top 10 (or more) applications with sessions, traffic Tx/Rx and bandwidth used • historical view by day, week, month or custom time frame
Interface Analytics	• delay, jitter, loss ratio, traffic in/out and number of sessions on per interface basis • historical view by day, week, month or custom time frame
Application Analytics	• application bi-directional bandwidth utilization • top application information pertaining to sessions, and traffic utilization (Rx/Tx) • Application view can be filtered or selected per application • historical view by day, week, month or custom time frame
DDOS	• create DDOS attack profiles and suspend actions • historical view by day, week, month or custom time frame of DDOS attack analytics associated with attack profiles.
Device	• detailed CPE hardware information • self CPE diagnostics, including ping and traceroute • Data synchronization icon to re-synchronize the Portal and SDWAN bases. • WAN interface details including MAC, status, IP address, speed, traffic Rx/Tx and QoS policies • LAN interface details including MAC, ARP information, IP address, speed, and routing policies

4.2. SD WAN Wholesale Customer Portal specifics

Colt SD WAN Portal for the Wholesale segment can have a personalized branding and domain, and therefore there are some requisites the Carrier needs to fulfil.

All the required information needs to be captured by Sales teams and shared to Portal team to set up Reseller's SD WAN portal.

At the same time, special flag within the EoF will remind the user that this requirement needs to be taken care of prior to service delivery.

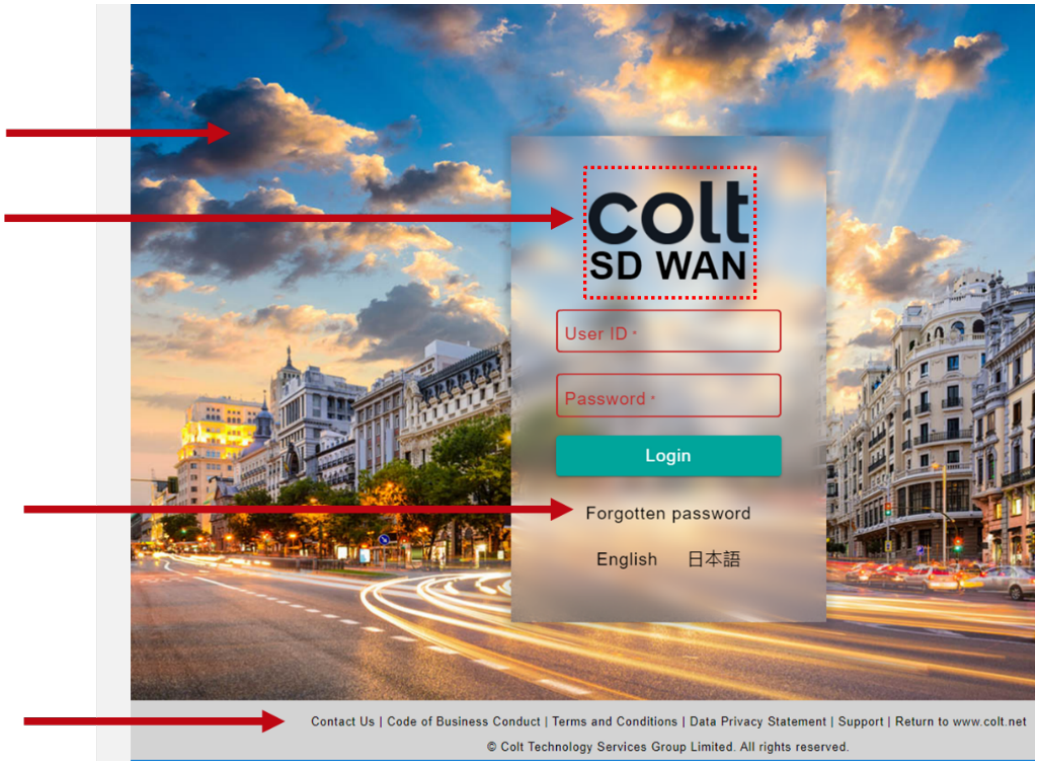
Main requirements:

- Select a domain name for the branded version of the portal (e.g. sdwan.reseller.com)
- Update the Carrier's own DNS records to associate this domain name with the Colt production portal, either:
  - as a CNAME record pointing to sd-wan.colt.net or
  - as an A record pointing to the colt-owned IP address: 217.111.165.33
- Obtain an SSL certificate to secure web traffic to this domain.
  - The associated private key for this SSL certificate should be a minimum of 2048 bits long.
  - The certificate should be signed by a widely trusted Certificate Authority – e.g. Verisign
  - The certificate expiry date should be a minimum of 365 days from the date of issue
  - Neither the key nor the certificate should be password protected
- Using the following pages as a starting point, collect content that the Carrier wants to be shown on the branded portal.
  - Not all content is mandatory (e.g. a login logo), but if it is not supplied, then the corresponding area of the screen will default to blank
  - Image sizes and other constraints apply
- Send the certificate, the private key and the branding information to the SDWAN Portal team (Novitas)
- For testing purposes, a Colt Demo portal can be set up as well with the customized look and feel (it can take up to two days to put it into production).
- Carrier is responsible for end-customer credentials and password management, that would be created within their user access to the portal (tenant management). End-customer will not be able to manage his credentials, only to ask for a reset to Carrier.

4.2.1. SD WAN Wholesale Customer Portal branding

In order to customize the specific branding for each Reseller, this information needs to be captured from Customer:

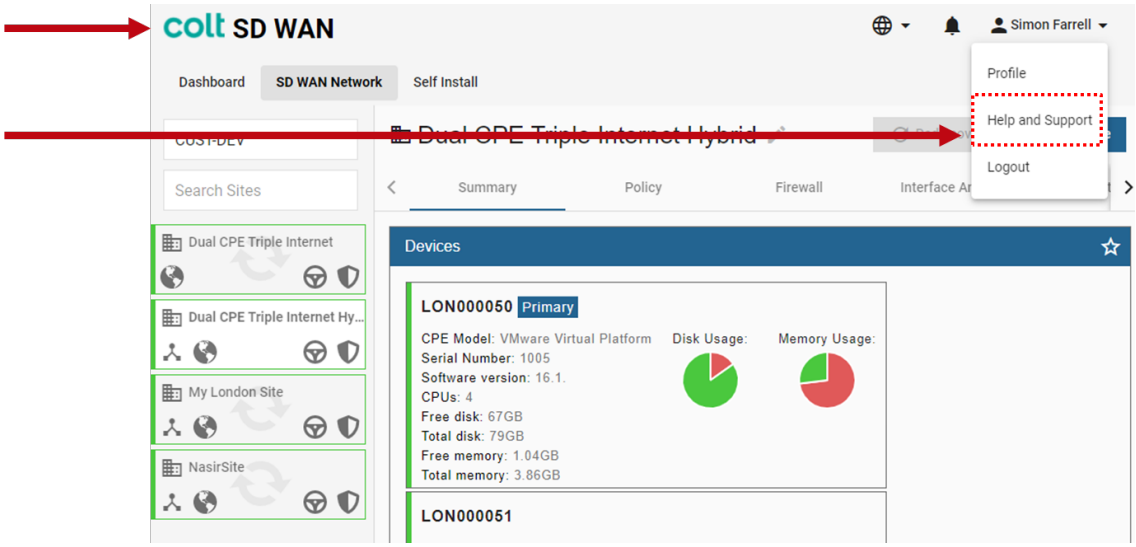
- Splash screen background image
  - Min 1920px wide, 1440px high, PNG or JPG format
- Login dialog logo
  - Max 250px wide, 200px high, PNG or JPG format
- Forgot password link (required)
  - URL only (text will be unaltered)
- Footer HTML (required)
  - HTML inside a DIV element, maximum 2 lines high. elements will be separated by vertical bars



Once in the SD WAN Network Dashboard, there are some other items that can be customized as well:

- Application logo
  - Max 250px wide, 32px high, PNG or JPG
- Help link (required)
  - URL only (text will be unaltered)

- NOT SHOWN:
  - Web page title (text only)
  - FAVICON.ICO icon to show in the address bar (48x48 px or 24x24 px, icon format)



In case the customer doesn't want to customise the landing page or the SD WAN dashboard logos, Colt can also offer the possibility of not showing any logo instead.

Anyhow, technical details as registered domain, SSL certificate or even the Help and support & Forgot password links are mandatory.

Note: Pease refer to Portal Guide document for further details

4.3. Dynamic traffic steering

Dynamic multi-path traffic steering is a real-time portal driven feature that helps Customers utilize both MPLS and Internet uplinks in a redundant or load sharing configuration. In addition to detecting pre-configured applications, traffic can be routed through IP address, protocol and/or port (socket) numbers.

To help quick site deployments, as a bespoke Colt can capture initial/service start-up policies through the order form and provision the CPE before shipping them to the Customer sites; however, Customers can choose to do (add/edit/delete) all their policy configurations anytime via the secure Colt SD WAN portal.

Colt SD WAN platform measures jitter, packet-loss, round-trip delay, traffic utilization TX/RX in all the paths between branches or between branch-to-hub. Please see portal appendix for policy configuration details.

4.4. Analytics

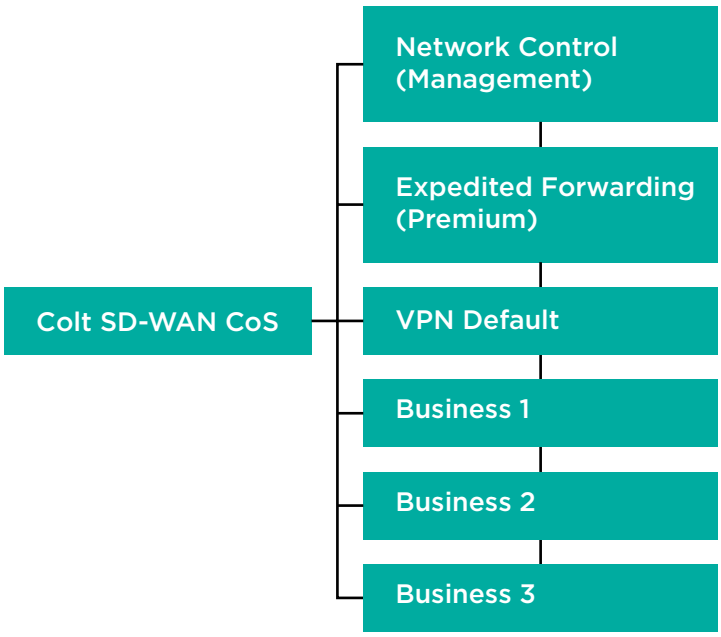
Supported for interface, firewall and applications. These are on near real-time basis with based on logs sent from branch sites and stored in the analytics database . Historical views are also supported along with deeper granularity. Please see portal appendix for details.

4.5. Class of Service (CoS)

Five classes available (similar to Colt IPVPN service). The network control queue is the first queue served in the priority order, this is to ensure that there is no limit to packets originated from Versa CPE locally.

QoS is only applied on MPLS transport provided by Colt.

Premium class is policed at the configured bandwidth and excess traffic will dropped (even if there is no congestion). All other classes - B1, B2, B3 and Default – are guaranteed the minimum bandwidth in case of congestion but can send excess traffic if bandwidth is available.



Service bandwidth applied after Premium bandwidth rate-limit.

4.6. Routing between Colt managed CPE and customer LAN

Both static and dynamic routing supported. Static, BGPv4 and OSPFv2 routes are all supported on SD WAN CPE for routing towards the customer LAN.

4.7. DHCP

DHCP requests from local clients are forwarded to Customer owned/managed central DHCP server (applies for IP addressing on the Customer LAN, not static or DHCP config in the WAN if customer is providing own Internet). Colt SD WAN CPE adds its own information to the request to identify the site (to enable the central server to allocate address from appropriate pool). DHCP server can be delivered as a bespoke on customer special request.

4.8. IP Address Management

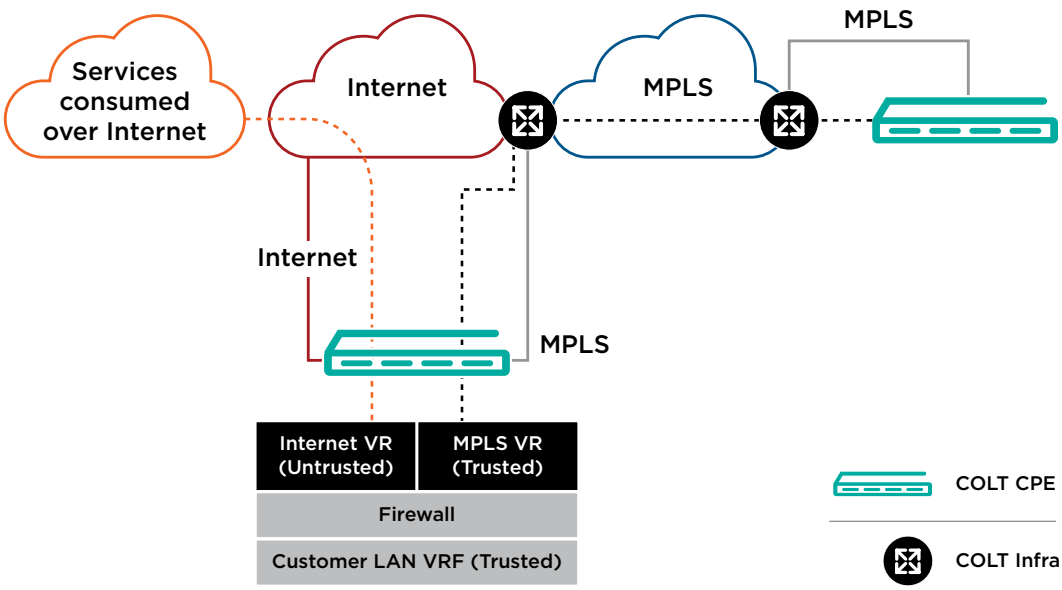
Customer IP addresses may be private or public as the service treats the addresses relevant only to the particular customer VPN.

As per DHCP, it applies for IP addressing on the Customer LAN, it not refers to the WAN if customer is providing own Internet.

- IPv4 & IPv6 are supported
- By default static routes shall be used for all the addresses for each site. As an option, routing protocols may be enabled as well at the time of ordering the service.

4.9. Local Internet Breakout

Local Internet breakout feature essentially allows 'to/from' internet traffic to utilize an SD WAN site's local internet connection rather than going through the central network gateway. Any traffic other than which is destined for SD WAN sites will 'break' from the local SD WAN CPE to the Internet via the 'local' internet connection. This helps reduce the customer's bandwidth needs across Colt SD WAN platform. By default a Deny-All rule is applied for traffic between the LAN and Internet in both directions. The customer can then add rules to selectively allow traffic towards and from the Internet.



Local Internet breakout is a default Colt SD WAN service feature, if an Customer, for any specific reasons, wants central internet breakout (central gateway) then it will be handled as a bespoke request and would need a modification order.

Highlights:

- Default option
- Will be on the first internet connection (more than one internet connections possible)
- Available on all site types that have an internet connection
- With dual internet, the local internet breakout will be on an active/standby basis (could be load balancing if requested by customer)
- With dual CPE, internet breakout will only be on the internet attached CPE
- With MPLS/internet, breakout will only be available on internet connection at that site

4.10. Standard Firewall

Colt SD WAN platform comes equipped with an L4 Stateful firewall (Versa FlexVNF Stateful FW feature on CPE). It supports rules around source and destination IP addresses, source and destination port and/or protocol numbers. When a customer site is first activated, the default firewall policy is to allow all traffic between SD WAN sites and "deny all" in both directions between the customer LAN and Internet. As an additional option, SD WAN firewall can be enabled which extends the default "deny all rule" to traffic between SD WAN sites Firewall policy rules can be modified using the SD WAN portal.

Complete firewall functionality is to be managed by the Customer, Colt has no control over security policies once the CPE is shipped.

Firewall rules are standard and based on simple allow, deny or reject commands on any of the 5 parameters highlighted above. Rule can be applied to a single or multiple CPEs.

The firewall feature is integrated with the Colt SD WAN solution and makes use of the stateful firewall feature embedded in the Versa FlexVNF software. This avoids the need for a separate firewall solution.

Highlights:

- Control – add, delete, modify and prioritize rules
- Back up – switch to any previous (saved) configuration version
- Analytics – there will be user friendly graphical analytics allowing users to view the number of allow and deny logs per rule.

Please see portal appendix for details.

4.11. Advanced Firewall

Colt SD WAN Advanced Firewall feature set is ideal for Customers needing protection against modern web-based security threats like malware attacks, targeted attacks, application-layer attacks; these attacks exploit weaknesses in applications, rather than weaknesses in networking components and services which are traditional attacks and can be prevented by a stateful firewalls.

Colt SD WAN platform uses an integrated Next Generation firewall that offers advanced firewall capabilities integrated with SDWAN router, the functionality can be configured via Colt SDWAN portal. Advanced firewall allows customer to connect separate LAN and DMZ networks to the SD WAN CPE and is used in combination with the local Internet breakout feature.

Colt also offers The Denial of Service (DoS) protection feature with SDWAN. It is used to protect services on the customer LAN or DMZ that are exposed to the Internet e.g. web servers, mail servers. It is only supported in combination with the DMZ / destination NAT feature for the traffic from the Internet towards the LAN/DMZ.

Features Currently Not Supported by default but part of roadmap:

- Firewall rules with match based on URL category
- User-based Firewall Rules incl. Integration with Microsoft AD and LDAP
- SSL decryption
- IDS/IPS security profiles to detect vulnerabilities from external sources
- Anti-virus capability

4.12. Dual CPE (High Availability Site)

For additional resiliency, two SD WAN CPEs are provided in high availability mode, (similar to IP VPN plus dual CPE) where VRRP is used to ensure that if either SD WAN CPE fails traffic will be routed to the other. By default not all traffic is rerouted, there could be application exception policies set to have a specific application to avoid Internet or MPLS network. Dual CPE form a high availability site with an aggregated total site throughput shared by both CPEs.

Dual CPEs can be in a same location or different locations, however, they have to have an additional interconnect (in addition to being connected via LAN (for VRRP), this additional interconnect is used to appropriate WAN routing.

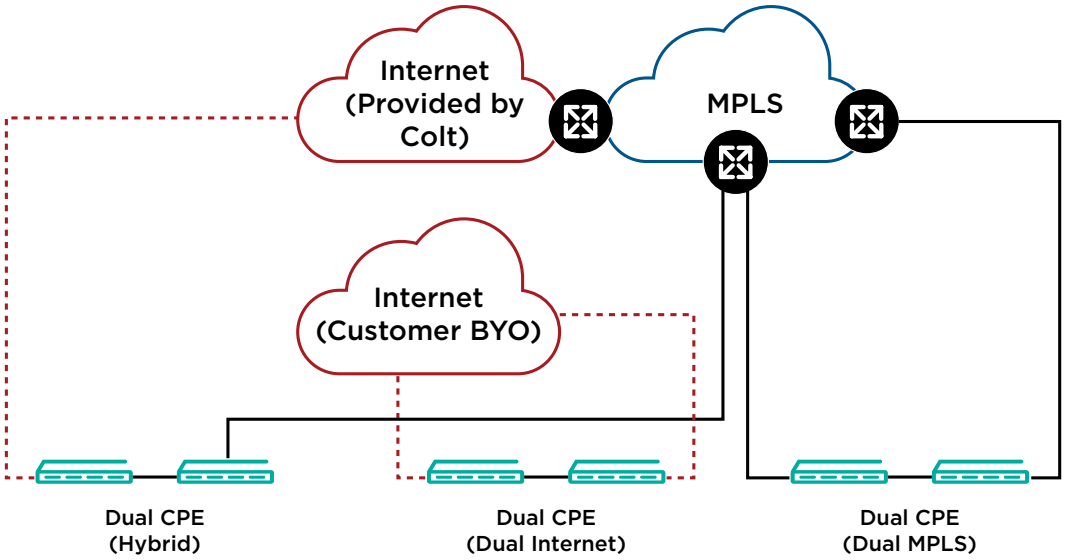
For the back to back connectivity between this two CPEs, the customer can decide whether they need an electrical or optical port ("B2B Connector Type" field in EoF, optical will be delivered by default).

In standard delivery internal cabling can include up to 5 metres, above that needs to be quoted in a case by case scenario.

In those cases when customer wants to use their existing cabling, Colt will not be responsible for any malfunctioning caused by this cabling, and therefore committed availability SLA will not apply for that site.

Dual CPE is available in three combinations:

- Dual CPE (Hybrid): Primary CPE with MPLS + Secondary CPE with Internet
- Dual CPE (Dual Internet): Primary CPE with Internet + Secondary CPE with Internet
- Dual CPE (Dual MPLS): Primary CPE with MPLS+ Secondary CPE with MPLS



4.13. CPEs

Versa FlexVNF can be deployed on either a Colt uCPE (not available yet for Wholesale segment, still in roadmap) or a Versa Certified Whitebox appliance (Baremetal), which are Advantech x86 network appliances, both installed on the customer premise. The following appliance types are used based on bandwidth and feature requirements:

Versa - Certified Whitebox Appliances

Model	Description	Bandwidth	Uplink	Deployment
Versa 510	Advantech FWA-2320 Intel Atom C2558, 4 core, 8GB RAM	Up to 150Mbps	GbE (Cu)	Small Branch
Versa 120	Advantech FWA-1010, Intel Atom C2758, 8 Core, 16GB RAM	Up to 250Mbps	GbE (Cu/ SFP) + LTE	Small Branch (with LTE)
Versa 220	Advantech FWA1012VC. • FWA-1012VC-8CA1V (Versa 220 without LTE) • FWA-1012VC-8CA1VR (Versa 220 with LTE modem for EMEA) • FWA1012VC2006-T (Versa 220 with LTE modem for APAC)	Up to 800Mbps	GbE (Cu/ SFP) + LTE	Small Branch (with LTE)
Versa 810	Advantech FWA-3260, Intel Xeon D-1548, 8 core, 64GB RAM	Up to 1Gbps	GbE (Cu/ SFP)	Medium Branch
Versa 1000	Advantech FWA-5020 Intel Xeon E5-2697, 14 core, 64GB RAM	Up 3Gbps	10GbE (SFP+)	Hub / Data Centre
Versa 1800	Advantech FWA-5070 Intel Xeon Gold 6212U, 24Core, 96GB RAM	Up to 7.5Gbps	10GbE (SFP+)	Hub / Data Centre

Versa 510

Versa 510 Specifications

Vendor Model	Advantech FWA-2320-01E
Processor	Intel C2558 4 Core CPU
Memory	4GB
Disk	64 GB SSD
Interfaces	4 x GbE Cu (WAN/LAN), 2 x GbE Cu Mgmt
Power	100W AC internal PSU
Cooling	1 x smart FAN maximum 37.5dB(A). Front to Back airflow
Physical Format	1RU rackmount device
Dimensions	426 x 44 x 318mm
Weight	4.5Kg

Versa 120

Vendor Model	Advantech FWA1012VC. Versa Builds: • FWA-1012VC-8CA1V (Versa 220 without LTE) • FWA-1012VC-8CA1VR (Versa 220 with LTE modem for EMEA) • FWA1012VC2006-T (Versa 220 with LTE modem for APAC)
Processor	Intel Atom C3758 (8 core), 2.2 Ghz
Memory	16GB
Disk	128 GB SSD
Interfaces	4x copper GbE via Marvell 88E1543, 2xSFP & 2x copper GbE via I350
LTE	Sierra/EM7455(EMEA) / MC7430 (APAC) Advanced-LTE module(Cat.6) with related antenna , SMA, screws
TPM	TPM1.2 Module
Power	12V 5A, 60W external adaptor
Cooling	2x system FAN with smart FAN
Physical Format	Tabletop device (optional rackmount kit FWA-1012VC-RMK)
Dimensions	250 x 44 x 193.04 mm (9.8” x 1.7” x 7.5”)
Weight	2.4 Kg

Table 4 : Versa 120 Specifications

Modem Name	AMER, EMEA: Sierra Wireless MC7455 APAC: Sierra Wireless MC7430
Performance	Cat-6 (peak down-link: 200 Mbps, up-link: 50 Mbps)
Wireless Standards	4G-LTE, 3G (WCDMA) Frequency Bands: MC7455: B1, B2, B3, B4, B5, B8 Frequency Bands: MC7430: B1, B5, B6, B8, B9, B19
FRU	No
Geo-Location	GPS, Glonass, Beidou, Galileo
SIM Card Access	Externally accessible
Antenna	External Antennas that attach to the device are included. Antenna extension (wall mount/roofmount) is also possible. The antenna must have dual SMA male connectors and max 5dbm insertion loss. Example parts include Poynting 4G-XPOL-A0001 (Omni-directional) and 4G-XPOL-A0002 (Directional)

Table 5 : Versa 220/120 - LTE Modem Specification

Versa 210

Vendor Model	Advantech FWA1012VC. Versa Builds: • FWA-1012VC-8CA1V (Versa 220 without LTE) • FWA-1012VC-8CA1VR (Versa 220 with LTE modem for EMEA) • FWA1012VC2006-T (Versa 220 with LTE modem for APAC)
Processor	Intel Atom C3758 (8 core), 2.2 Ghz
Memory	16GB
Disk	128 GB SSD
Interfaces	4x copper GbE via Marvell 88E1543, 2xSFP & 2x copper GbE via I350
LTE	Sierra/EM7455(EMEA) / MC7430 (APAC) Advanced-LTE module(Cat.6) with related antenna , SMA, screws
TPM	TPM1.2 Module
Power	12V 5A, 60W external adaptor
Cooling	2x system FAN with smart FAN
Physical Format	Tabletop device (optional rackmount kit FWA-1012VC-RMK)
Dimensions	250 x 44 x 193.04 mm (9.8" x 1.7" x 7.5")
Weight	2.4 Kg

Table 6 : Versa 220/120 - LTE Modem Specification

Versa 810

Vendor Model	Advantech FWA-3260
Processor	Intel Xeon D-1548(8 core), 2 GHz
Memory	64GB Memory
Disk	256GB SSD
Interfaces	6 x 1GbE, 2 x 10GbE SFP+, Optional expansion module NMC-1004-10E with 2 x 10G SFP+ with Intel 82599ESx
LTE/WiFi	N/A
TPM	TPM1.2 Module
Power	Redundant 1+Dummy 300W AC PSU. Optional DC PSU
Cooling	4x system FAN with smart FAN. Front-to-back airflow
Physical Format	1 RU Rackmount Device
Dimensions	430 x 44.2 x 500 mm
Weight	15 Kg

Versa 1000

Vendor Model	Advantech FWA-5020
Processor	Intel Xeon E5-2697v3 14 core, 2.6 GHz
Memory	64GB
Disk	512GB SSD
Interfaces	6 x 1GbE, 2 x 10GbE SFP+ Optional expansion module NMC-1004-10E with 2 x 10G SFP+ with Intel 82599ESx
LTE/WiFi	N/A
TPM	TPM 1.2
Power	Redund 650W AC PSU
Cooling	4x smart FAN. Front-to-back air flow
Physical Format	1 RU rackmount
Dimensions	1 RU (438 x 44x 625 mm) (17.24” x1.732” x24.61”) (W x H x D)
Weight	15 Kg

Versa 1800

Vendor Model	Advantech FWA-5070
Processor	Intel Xeon Gold 6212U, 24C, 2.4GHz
Memory	96GB
Disk	2 x 512GB SSD
Interfaces	9 x 1GbE, 8x10GbE SFP+, Optional expansion module NMC-1004-10E with 2 x 10G SFP+ with Intel 82599ESx
LTE/WiFi	N/A
TPM	TPM 1.2
Power	Redund 650W AC PSU
Cooling	3x smart FAN. Front-to-back air flow
Physical Format	1 RU rackmount
Dimensions	1 RU (438 x 44 x 550 mm) (W x H x D)
Weight	20 Kg

4.14. Universal CPE (only for Enterprise segment)

FlexVNF can also be deployed on the ADVA Ensemble Connector OS and certified uCPE appliances. See the Universal CPE solution guide for further details

Colt uCPE consists of following components

Component	Details
Hardware	1. Advantech FWA-3260 2. Advantech FWA-2012
Virtualization Layer	ADVA Ensemble Cloud Suite
VNF	1. Versa SD WAN 2. Checkpoint Unmanaged Firewall

4.15. Multi-VPN (Multi-VRF)

Multi-VPN feature allows a single SD WAN CPE to be used to deliver upto 9 sub-VPNs (10th is used for uCPE inbound management). On the LAN side, either a separate physical interface or 802.1q logical sub-interface is configured per service instance, and it is placed in the corresponding VRF. On the WAN interface, it's segregated using VPNv4 addresses. Unlike traditional MPLS VPN-based solutions, multi-VPN does NOT require separate logical circuits on the WAN for each sub-VPN. The SD WAN overlay provides the separation between each VPN

4.16. SNMP RO

SNMP Read-only access allows the customer to poll the MIBS on the Colt SD WAN CPE device from their own network management server. The customer server can be located on the local LAN or on another SD WAN site. SNMPv3 is supported using SHA/MD5 and AES ciphers for authentication and privacy. The type of encryption (privacy) can be: DES/3DES, or AES128

Customers who would like to use this feature need to provide authentication details like: username used in the SNMP requests, authentication password, privacy password. SNMP Traps are not provided by the CPE to the LAN, they are provided from SD WAN controller.

4.17. Advanced traffic steering (application based traffic steering)

Traffic Steering allows application traffic to be intelligently forwarded across different paths between SD WAN sites e.g. Internet or MPLS. By default traffic is load-shared across available paths or the customer can define application based policy. Capability to create traffic steering/forwarding policies based on 3000+ pre-defined applications pre-loaded on on-premise SD WAN CPE. Only the pre-loaded applications are in scope, user defined applications, applications groups and filters are not supported.

4.18. Advanced analytics (Versa Analytics) (only available for Enterprise segment, in roadmap for Wholesale)

Advanced analytics for applications by sessions, bandwidth, and access circuit on each branch, including bandwidth consumed by each application. It is accessible through Colt Online, and therefore limited for Colt's direct customer, not Carrier's end-customer. Please see appendix for details.

4.19. Self-Install CPE (Zero Touch Provisioning)

At the moment when this document was elaborated, the feature was under further development and only available for Colt EU countries, and for a limited number of sites.

(Only available for Enterprise segment, in roadmap for Wholesale)

A simplified way for Customers to enable Colt SD WAN service globally without having to have technical resources on site. As part of this service, a CPE with basic configuration is shipped to end site where any site personnel (even non-technical) can connect it to the network and complete activation to start consuming the services.

Simple workflow:

- CPE received on site
- Connected to the Internet (to access Colt SD WAN Controller)
- On-site personnel connects a PC to the CPE and accesses a URL provided by Colt
- Colt SD WAN Controller checks the serial number against the URL and if there is a match the post staged customer configuration is downloaded to the CPE and it is launched and connected to Customer subscribed Colt SD WAN service.

Once the connectivity service has been confirmed (whether provided by Colt or the customer), the customer will receive shipment info email with following details.

- Site address details to which the CPE will be sent
- List of requirements for the service to be set-up (e.g. connectivity type, Ethernet interfaces etc.)
- Shipment content (e.g. 10/100 Mbps Managed Optical Demarcation Compact CPE Device, TP-TX/FX-SM1310/PLUS-ST, w/ AC Adapter, Quick Start Guide)

In case of failed self-installation, customer can request the services of an on-site technician. Customers shall incur a service charge at the professional installation rate if the technician determines the failure is directly related to customer equipment, inability or unwillingness to complete the self-installation process or mistakes customer made during the self-installation process.

4.20. SD WAN Multi-Cloud

For customers looking for cost-effective, direct connectivity into multiple cloud environments, SD WAN Multi-Cloud is the optimal solution. It offers private MPLS and/or Layer 3 connectivity into multiple cloud providers in a single solution, combined with end-to-end performance backed by a SLA, end-to-end security, and end-to-end analytics. With this solution, customers are able to combine management of their SaaS/IaaS cloud, WAN, and branch site connectivity into a single intelligent platform. SD WAN Multi-Cloud provides high performance, inexpensive, and secure cloud connectivity directly into the Cloud Service Providers (CSPs) - Amazon AWS, Microsoft Azure, and Google Cloud. Following are the main benefits:

Direct and secure Branch to Multi-Cloud connectivity and common policy management
Most companies with connectivity to the cloud are working, not just with a single cloud, but with multiple cloud service providers. There is a growing need for a simple, straightforward way to manage multi-cloud infrastructures. With SD WAN Multi-Cloud, customers are able to connect their branch sites directly to all their cloud-based SaaS and IaaS and manage this connectivity centrally via the Colt SD WAN portal.

SD WAN Multi-Cloud also offers the ability for customers to manage common policies across their branch sites, SD WAN fabric and multi-cloud environment – further increasing the ease of control over their network.

SD WAN-powered dynamic path selection with SLA
With SD WAN Multi-Cloud, cloud-based applications are intelligently and dynamically routed to the best available path – minimising risk of performance disruption caused by unpredictable cloud traffic and resulting in an overall improved end-user experience and increased productivity.

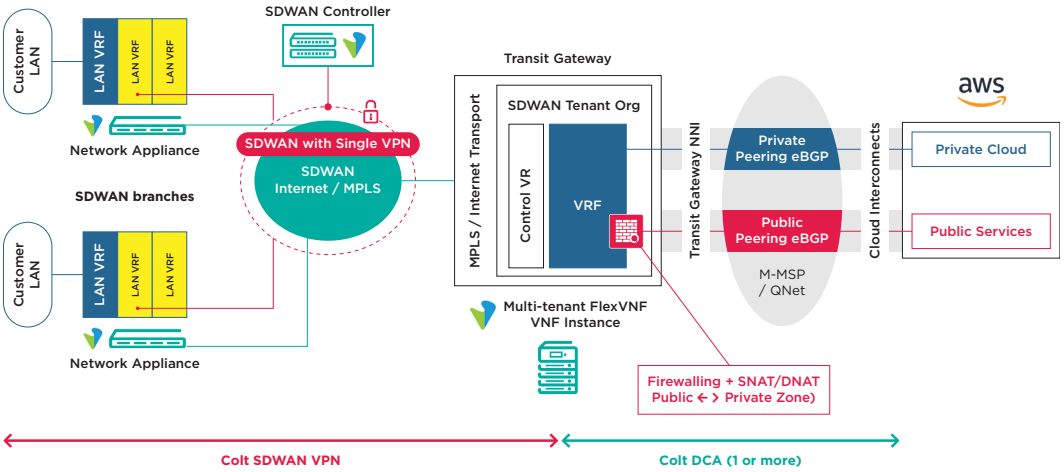
Performance visibility across WAN and Cloud, powered by SD WAN analytics
Customers are in full control of their network with Colt SD WAN Multi-Cloud, which provides comprehensive visibility of network performance across both WAN and Cloud. Having this visibility enables customers to monitor, troubleshoot, and make decisions to improve performance across their network.

Support of Cloud-to-Cloud communication
In many cases, customers' data will travel through multiple cloud environments. Rather than sending that traffic from branch site to one CSP and backhauling to a data centre or SD WAN gateway to reach another, traffic is routed over dedicated tunnels from one CSP's environment to the other. This means reduced latency and optimised performance for the end-user.

Security (Firewall/NAT) between Public and Private Cloud domains
Security remains a top concern for enterprises, particularly in adopting new technologies like Multi-Cloud. With the security features available with SD WAN Multi-Cloud – including Firewalls and NAT (Network Address Translation) – customers can be assured that customer network is secured from the cloud public domain.

4.20.1. SD WAN Services into Amazon (Amazon Web Services)
Connectivity to Amazon Web Services can be added towards the SD WAN network. Connectivity to AWS can be added to an existing SD WAN network, or ordered as part of a new SD WAN deployment.

In both cases, connectivity towards AWS from/to the SD WAN network goes via a Cloud Gateway in the Colt IQnetwork.



Colt support both the 'hosted' AWS Direct Connect option and the 'dedicated' AWS Direct Connect port option into Amazon. It supports both connectivity to the "private" Amazon domain and "public" domain of Amazon.

For hosted connections customers can choose bandwidth from 10-500Mbps. For dedicated connections bandwidth from 10Mbps up to 1Gbps are supported, please find an overview below:

AWS Direct Connect Hosted	
Colt Service Bandwidth	CSP Bandwidth
10 Mbps	50 Mbps
50 Mbps	50 Mbps
100 Mbps	100 Mbps
200 Mbps	200 Mbps
300 Mbps	300 Mbps
400 Mbps	400 Mbps
500 Mbps	500 Mbps

AWS Direct Connect Dedicated	
Colt Service Bandwidth	CSP Bandwidth
10-500 Mbps	1 Gpbs
1 Gpbs	1 Gpbs

The existing maximum capacity per Cloud Gateway per customer is 2Gbps. Bandwidths >2Gbps can be supported by distributing connections across 2 or more Cloud Gateways.

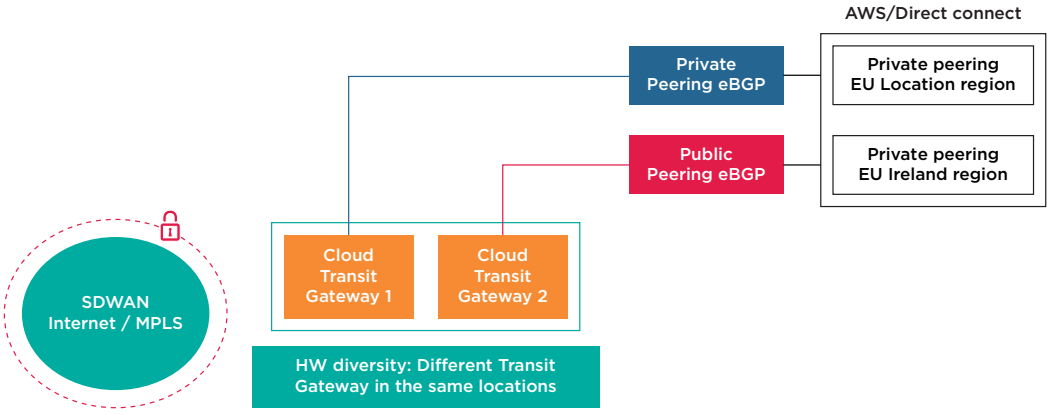
The Cloud Gateway supports features like NAT and firewall (for enhanced security).

The Cloud Gateway is currently only available in Europe, by Q1'-'21 the service will also be available in Asia (Tokyo and Singapore).

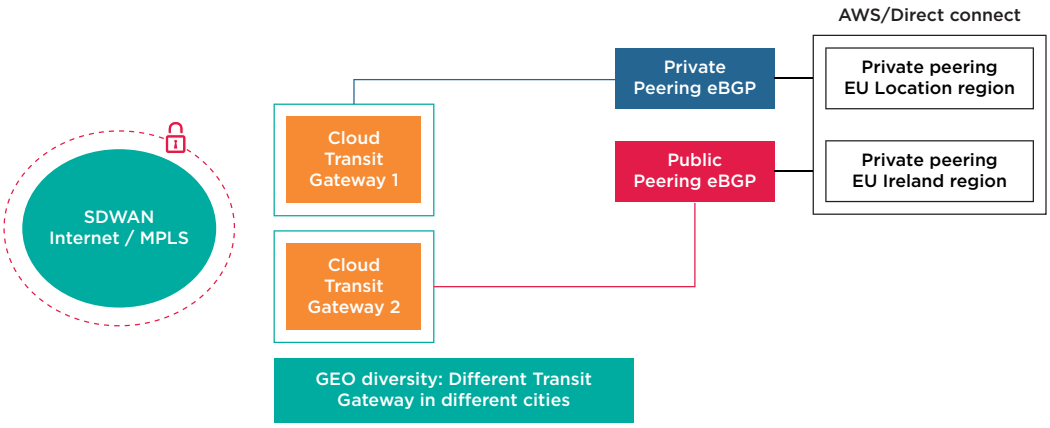
SD WAN solution into AWS by default supports Cloud-to-Cloud communications between different CSP's, which means that traffic between CSP's does not have to enter the SD WAN network which reduces latency.

Customers can order connectivity to any AWS location/region, connected by Colt. In case customers require diverse connectivity into AWS, Colt offers two options on the Cloud Gateway platform:

- Cloud Gateway Hardware diversity: Secondary AWS service will go through a different Cloud Gateway (located at same location).



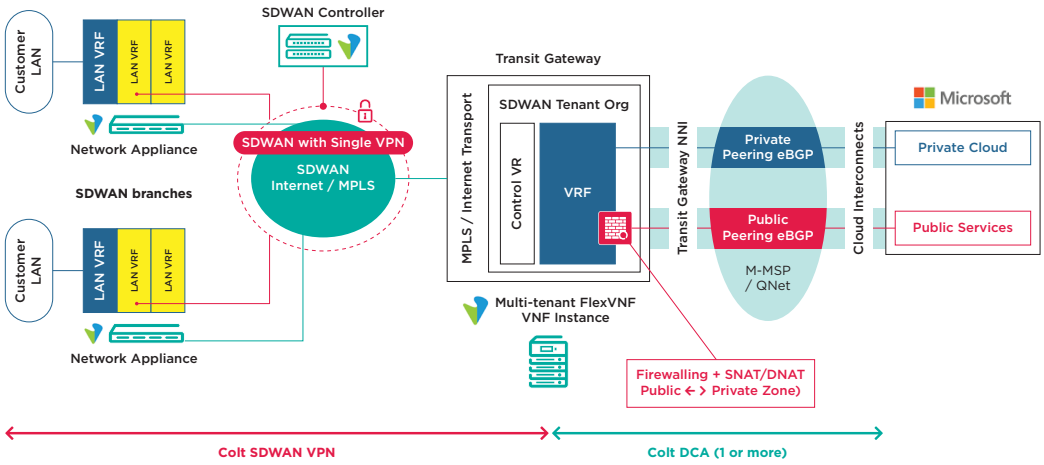
- Cloud Gateway Geo diversity: Secondary AWS service will go via a different Cloud Gateway in different cities.



4.20.2. SD WAN Services into Microsoft Azure (ExpressRoute)

Connectivity to Microsoft Azure ExpressRoute services can be added towards the SD WAN network. Connectivity to Microsoft Azure can be added to an existing SD WAN network, or ordered as part of a new SD WAN deployment.

In both cases, connectivity towards Microsoft Azure from/to the SD WAN network goes via a Cloud Gateway in the Colt IQnetwork.



Colt support 'hosted' Microsoft Azure ExpressRoute into Microsoft. It supports both connectivity to the "private" Amazon domain and "public" domain of Microsoft.

For hosted connections customers can choose bandwidth from 10Mbps – 1Gbps, please find an overview below:

Microsoft Port Size	Colt service bandwidth
50Mbps	50/100Mbps
100Mbps	100Mbps
200Mbps	200Mbps
500Mbps	500Mbps
1 Gbps	1 Gbps

The existing maximum capacity per Cloud Gateway per customer is 2Gbps. Bandwidths >2Gbps can be supported by distributing connections across 2 or more Cloud Gateways.

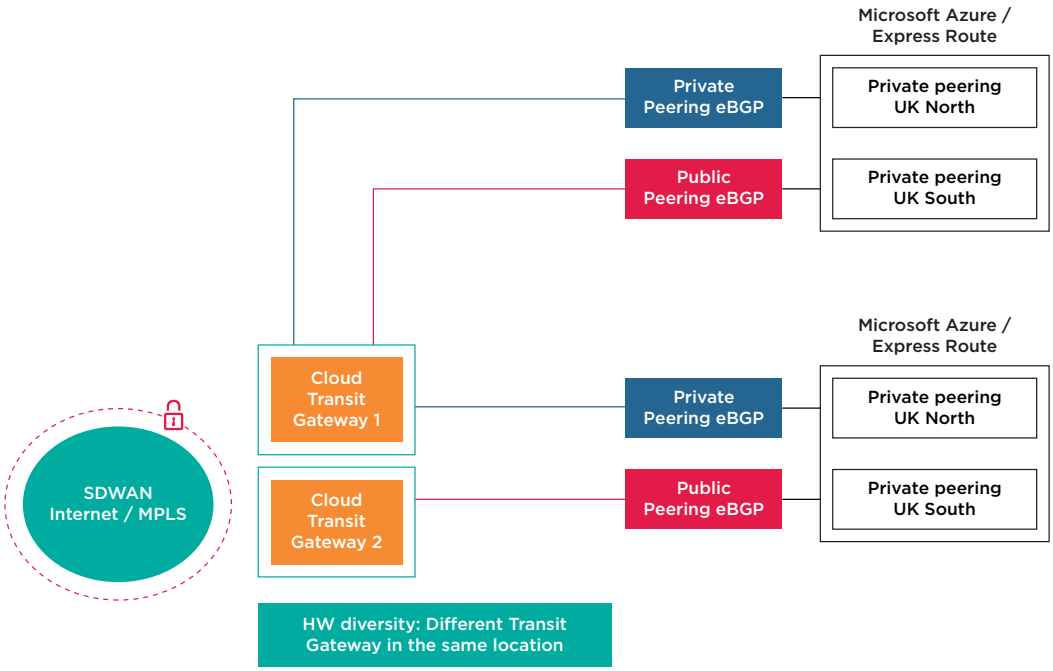
The Cloud Gateway supports features like NAT and firewall (for enhanced security).

The Cloud Gateway is currently only available in Europe, in Q1'-'21 the service will also be available in Asia (Tokyo and Singapore)

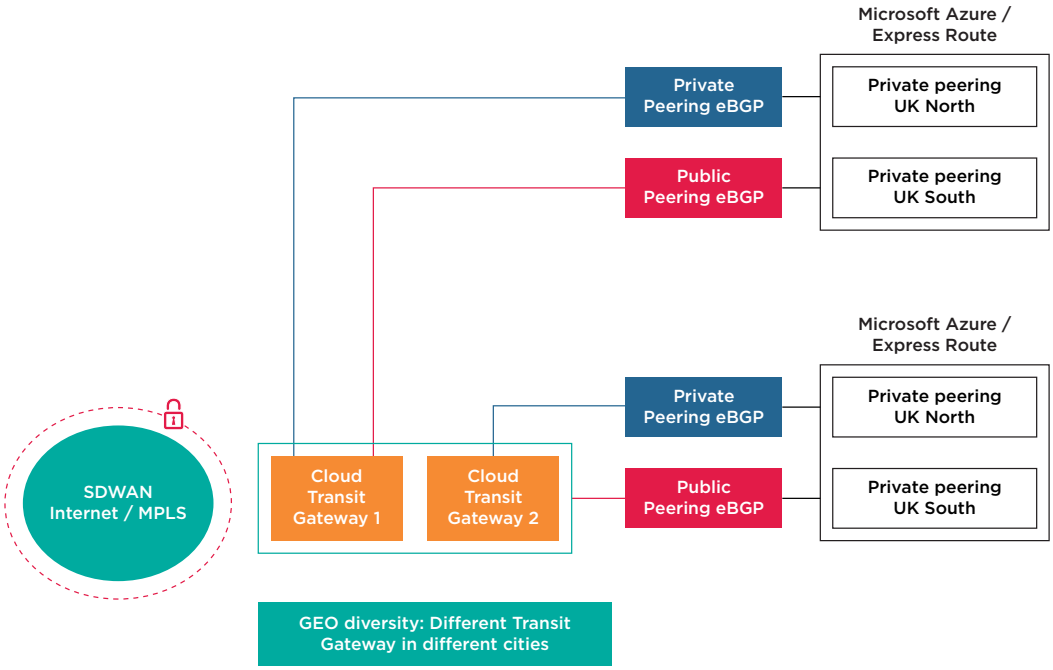
SD WAN solution into Microsoft Azure by default supports Cloud-to-Cloud communications between different CSP's, which means that traffic between CSP's does not have to enter the SD WAN network which reduces latency.

Customers can order connectivity to any Microsoft Azure location/region, connected by Colt. In case of Microsoft Azure ExpressRoute, diversity is a mandatory requirement, and Colt offers two options on the Cloud Gateway platform:

- Cloud Gateway Hardware diversity: Secondary Microsoft Azure service will go through a different Cloud Gateway (located at same location).



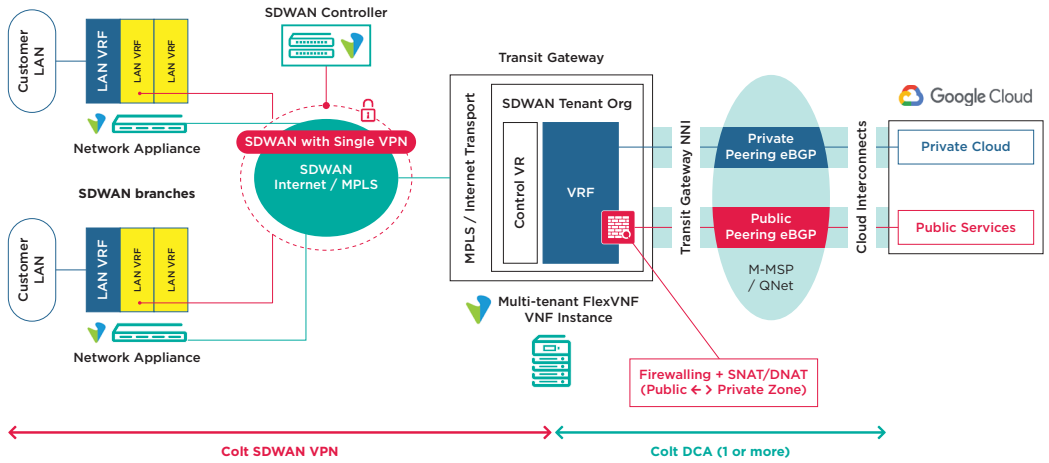
- Cloud Gateway Geo diversity: Secondary Microsoft Azure service will go via a different Cloud Gateway in different cities.



4.20.3. SD WAN Services into Google Cloud Interconnect (GCI)

Connectivity to Google Cloud Interconnect Services can be added towards the SD WAN network. Connectivity to Google Cloud Interconnect can be added to an existing SD WAN network, or ordered as part of a new SD WAN deployment.

In both cases, connectivity towards Google Cloud Interconnect from/to the SD WAN network goes via a Cloud Gateway in the Colt IQnetwork.



Colt support the 'GCI partner / hosted' Google Cloud Interconnect option into Google Cloud. It supports connectivity to the "private" Google Cloud domain.

For hosted connections customers can choose bandwidth from 10Mbps – 1Gbps., please find an overview below:

Google Cloud Interconnect Partner	
Colt service bandwidth	**CSP Bandwidth**
10Mbps	50Mbps
50Mbps	50Mbps
100Mbps	100Mbps
200Mbps	200Mbps
300Mbps	300Mbps
400Mbps	400Mbps
500Mbps	500Mbps
1 Gbps	1 Gbps

The existing maximum capacity per Cloud Gateway per customer is 2Gbps. Bandwidths >2Gbps can be supported by distributing connections across 2 or more Cloud Gateways.

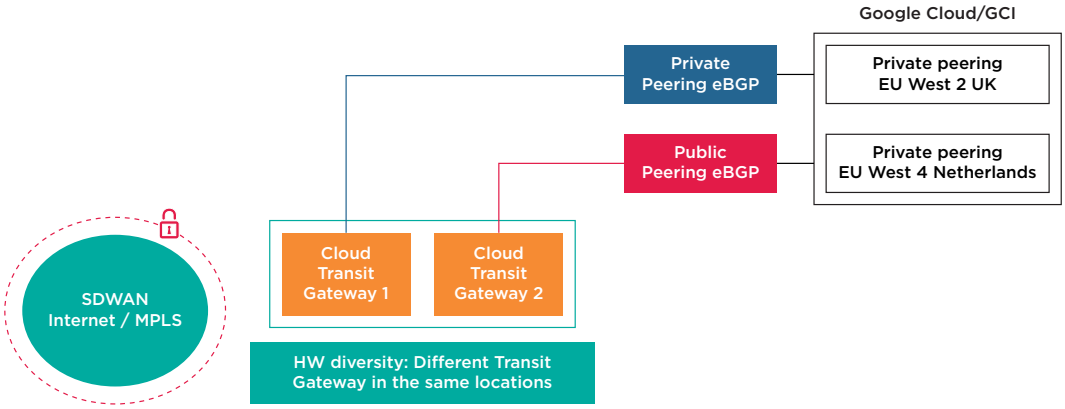
The Cloud Gateway supports features like NAT and firewall (for enhanced security).

The Cloud Gateway is currently only available in Europe, Q1'-'21 the service will also be available in Asia (Tokyo and Singapore).

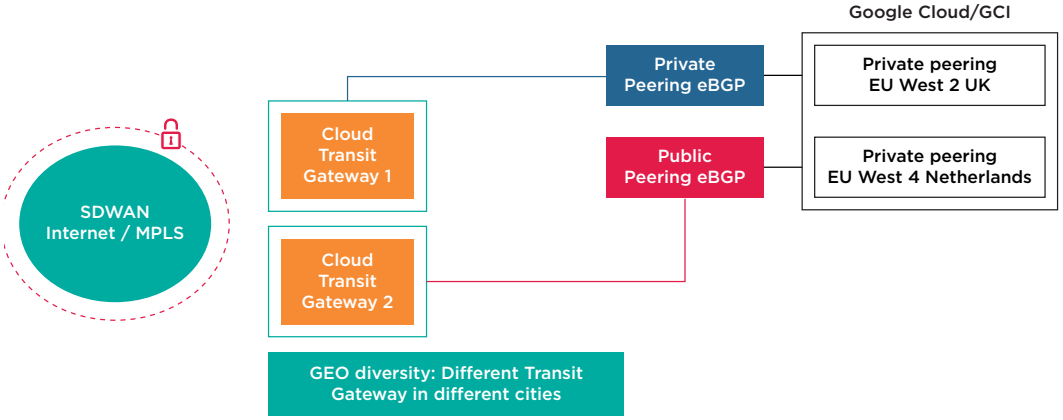
SD WAN solution into Google Cloud Interconnect by default supports Cloud-to-Cloud communications between different CSP's, which means that traffic between CSP's does not have to enter the SD WAN network which reduces latency.

Customers can order connectivity to any Google Cloud Interconnect location/ region, connected by Colt. In case customers require diverse connectivity into Google Cloud Interconnect, Colt offers two options on the Cloud Gateway platform:

- Cloud Gateway Hardware diversity: Secondary AWS service will go through a different Cloud Gateway (located at same location).



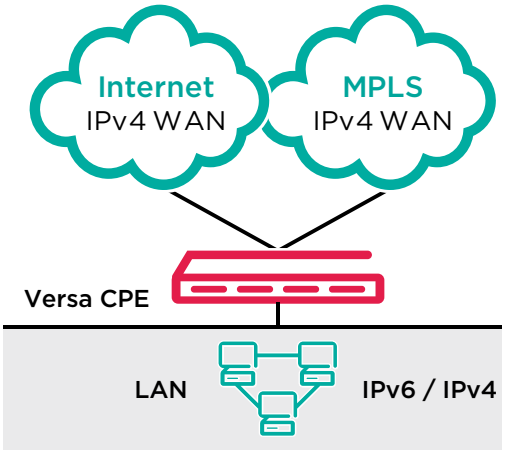
- Cloud Gateway Geo diversity: Secondary AWS service will go via a different Cloud Gateway in different cities.



'Today, we are monitoring proactively our Cloud Gateway infrastructure, we are also working to develop a solution to monitor the connectivity to the 3rd party cloud providers at an application level.'

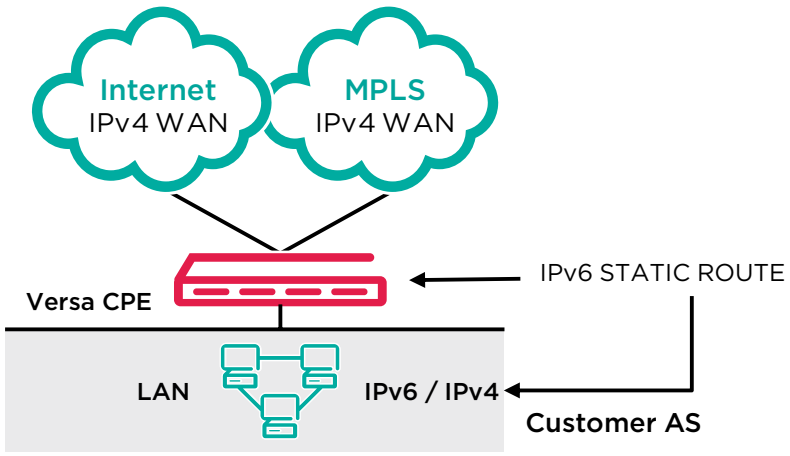
4.21. IPv6 support on LAN

IPv6 is supported on LAN to LAN communication for the customer (note that Internet Breakout for IPv6 is not supported). This has to enable IPv6 Static address in LAN VNI port of Versa CPE with the option to have both IPv4 & IPv6 towards the support of dual stack function in future.



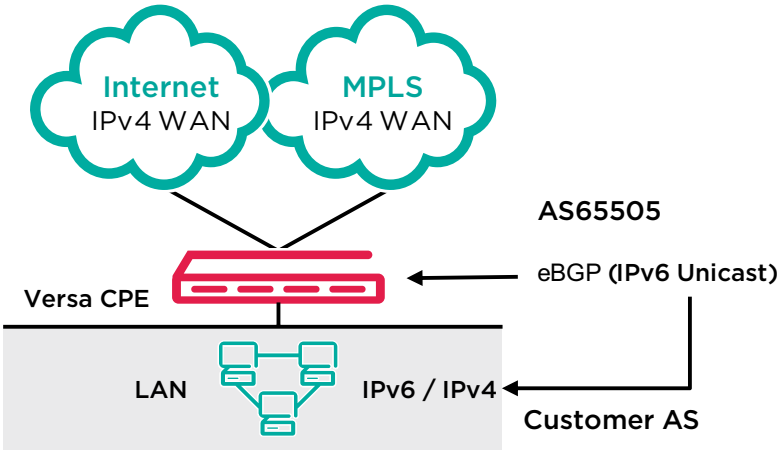
Customers are allowed to provide their IPv6 address and gateway address to Colt, similar to IPv4.

- **LAN IPv6 Static Routing**



IPv6 route shall be added along with tag numbering using Versa director keeping the next-hop as IPv6 address according to customer's requirement. At the initial release Colt SD WAN will not be supporting the self-service portal based IPv6 static routing by customer, however it shall be considered into future release scope.

- **LAN IPv6 Dynamic Routing**



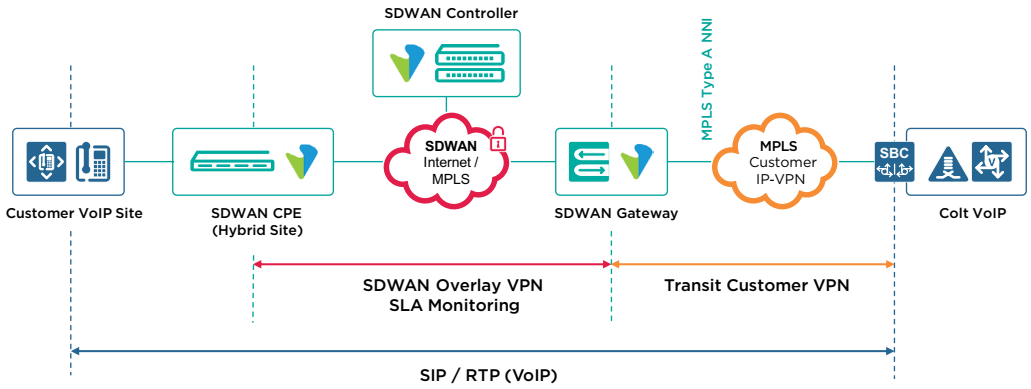
As a first release of Dynamic routing support in IPv6 Colt SD WAN will be supporting the customer to enable eBGP with IPv6 address family identifier between their Versa CPE and customer LAN device in native IPv6 address. It will be possible to filter the routes and redistribute the prefixes to remote destination using routing policies. Similarly It will be possible to display the BGP received and advertised routes via self-service portal.

The BGP parameters of the customer device will be provided by the customer similar to the Dynamic routing IPv4 currently in production.

- Customer Local AS Number
- Neighbour IPv6 address
- BGP Password
- Routing Policy requirement

4.22. VoIP over SDWAN

For SDWAN sites, VoIP Traffic must breakout via an SDWAN gateway to reach the VoIP POPs. A transit IP-VPN is required for each customer between SDWAN Gateways and VoIP POPs. Customer Connectivity terminates on an SBC in the VoIP POP connected to the transit IP-VPN. The transit VPN can be a customer's existing IP-VPN (used to connect traditional IP-VPN sites) or created specifically for VoIP breakout from SDWAN.



A customer VLAN and /27 IP range is configured on each SBC the customer is connected to. The /27 range is advertised via BGP over the transit VPN and redistributed into the customer SDWAN overlay on the SDWAN gateway

SDWAN gateways redistribute customer SDWAN routes into the customer transit VPN to ensure end-to-end reachability between customer sites and VoIP POPs

The SDWAN gateways are connected to the transit VPN via existing MPLS Type A NNIs to the Colt IP/MPLS network

In case a customer has sites connected to multiple SDWAN nodes (multi-node deployment), the NNI must be configured on SDWAN gateways in each node

SDWAN supports class of service over MPLS transport. VoIP signalling should be assigned to the Business-1 class and is marked AF31, VoIP media should assigned to the Premium and is marked EF. DSCP markings are preserved end-to-end. Over the encrypted SDWAN overlay DSCP markings are copied to the outer IP header so that traffic can be prioritised if the underlay network supports it.

QoS is also applied on the SDWAN gateway NNIs and 40% of the aggregate bandwidth allocated to premium class. Premium bandwidth utilisation should be monitored to ensure no premium traffic is dropped.

Traffic Steering Policy

Real-time VoIP Traffic is sensitive to network latency, jitter and packet loss. For hybrid SDWAN sites it is possible to create steering rules that match VoIP traffic (SIP/RTP) and route calls over a preferred path e.g. 1st choice MPLS, 2nd choice Internet. SLA Thresholds can be set for round-trip latency, packet loss, and jitter metrics that once exceeded cause calls to re-route onto another SLA complaint path if available.

Versa also supports MOS based path selection. A MOS score is computed for each path periodically, based on RTP analysis. SLA thresholds can be setup for MOS, similar to how packet loss, jitter or delay based SLA thresholds are specified.

However, MOS score feature is only available for those sites that have requested the feature before its deployment, and needs to be requested per site, not per VPN.

If any site previously deployed needs to be included in dynamic routing policies according to MOS thresholds, a request to activate the feature needs to be raised.

Therefore, it is recommended to activate the MOS Score feature in every new site by default, even if it is not requested by the customer, so therefore can be activated with no extra configuration.

It is important to mention VoIP Traffic is subject to the default per flow load-balancing inherent to the SDWAN solution so VoIP calls (SIP and RTP flows) to and from sites with multiple transports will be load-balanced across the available paths which might lead to inconsistency in call quality. To override this behaviour the customer needs to manually define traffic steering policies first for their sites that are using VoIP and secondly in the Gateway to ensure symmetric behaviour. This can be done by customers via the Colt Self Service Portal and it´s advisable to use the MPLS transport whenever available.

NetFlow & IPFIX

NetFlow is used for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches. It analyzes network traffic flow and volume to determine where traffic is coming from, where it is going to, and how much traffic is being generated. NetFlow-enabled routers export traffic statistics as NetFlow records which are then collected by a NetFlow collector. The collector does that actual traffic analysis and presentation to the user and can take the form of a hardware appliance or software. In our case we use software.

Now as a new feature development, using SDWAN CPE, sending log data to Analytics nodes and to third-party NetFlow collectors, which perform data analysis and provide required reports and data visualization. SDWAN devices export log data in IPFIX and syslog format.

To enable SDWAN devices to send log data to Analytics and third-party collectors, we enable the log export functionality (LEF) on the device. To export log data from the devices to a NetFlow collector, we configure a NetFlow collector, group and a profile, and we then configure which data to export.

Customer can request flow in IPFIX format for their NetFlow collector through SDWAN portal. IPFIX feature will be enabled for all the Customers in SDWAN portal. Customers need to configure collectors for selected sites/CPE to enable flow monitoring. IPFIX feature will be enabled at site level with capability to copy the IPFIX relevant configurations for some/all the sites in SDWAN Portal.

Following information needs to be captured in the Portal. Up to 5 collectors will be supported per site with following config per collector.

- NetFlow collector IP address– Max 5 (Only IPv4 address is supported by Versa)
- Port ID
- Protocol – TCP/UDP
- VRF instance (By default LAN-1 VRF)
- Frequency of flow record
- Match condition – L4 prefix/Application filter

Customer can choose the frequency at which the flow record will be updated based what is supported on their collector.

- Start of flow – log data at the start of each session
- End of flow - log data at the end of each session
- Start and End - log data at the start and end of each session

Every 1 minute - log data every 1 minute while the flow is active. (Supported in 20.2)

Logging

- No additional logging for Colt Analytics has been introduced through this development and no change to existing logging to Colt log servers.
- Flow logs (traffic monitoring) will be sent directly from CPE to Customer NetFlow collector only.

Software release and license

- Available with existing software release and license.
- Some feature functionality available with 20.2 release. (1 minute frequency)

Only following Versa verified NetFlow collectors are supported

- Solarwinds;
- Cisco Stealthwatch;
- CA Technologies NetFlow

URL Filtering

To address the customer demand on ever growing SDWAN space, besides other features such as firewall, AAR etc. It is imperative need for customers to use web safely for business needs. URL filtering is one of best features available in the market which is provided by many vendors such as Versa, Zscaler, Fortinet, Barracuda and Palo Alto etc.

URL filtering is mainly used for blocking certain URL from loading on company's network, If an employee would attempt to visit this URL, either by entering it manually or clicking a link in a search engine, they will be redirected to a page notifying the content is blocked. URL filtering relies on filtering databases that classify URLs by topic; each topic in this system is either "blocked" or "allowed."

Administrators are capable of setting up blocklists for individual URLs, blocking specific websites they know to be dangerous or harmful. More broadly, administrators can block entire URL categories, block listing entire groups of websites at once.

The Colt SDWAN URL filtering solution is a powerful next generation firewall feature that is used to monitor and control how users access the web over HTTP and HTTPS. This feature can be used to gain complete visibility and control of the traffic that traverses your firewall and will be able to safely enable and control how your users access the web. We use versa URLF NG firewall service to enable URLF feature in which it can perform URL categories and reputation including customer-defined, Cloud-based lookups, Policy trigger based on URL profile (blacklist, whitelist, category and reputation) action include allow, alert, block and Captive portal response including customer defined actions include block, ask, Override and justify by URLF profile.

Sales to capture the URL filtering requirement in EOF at site level and URLF feature is enabled for all the Customers in SDWAN portal. Customers can configure URL rules for selected sites/CPE to enable URLF under firewall.

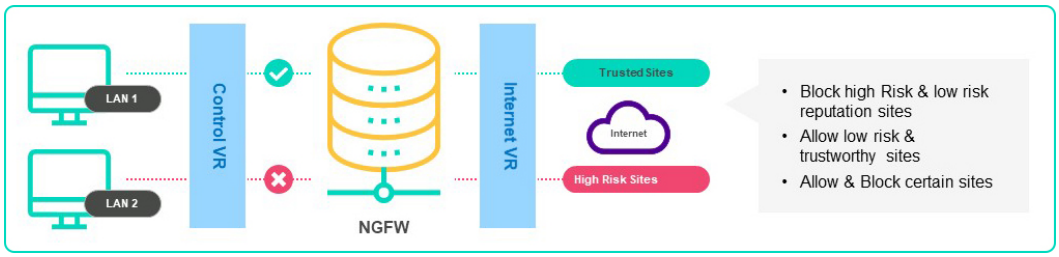
- Category Based Filtering

  Security access rule with URLF profile for ex. allowing Social sites category and blocking job sites.

- Reputation Based Filtering

  Security access rule with URLF profile for ex. allowing Trustworthy & Low risk reputation sites and blocking high risk and suspicious reputation sites

URL Filtering Setup



Topologies supported.

Please find the various single CPE topologies supported with standard deployments as mentioned below,

- Internet Only Single CPE (INT)
- Internet Only Single CPE (LTE)
- Hybrid CPE Single CPE (INT & MPLS)
- Hybrid CPE Single CPE (LTE & MPLS)
- Dual Internet Single CPE (INT & INT)
- Dual Internet Single CPE (INT & LTE)
- SINGLE-CPE-DUAL-INTERNET-HYBRID-LTE (New MWL)

Please find the Dual CPE topologies supported with standard deployments as mentioned below,

- Dual Internet Dual CPE (INT & INT)
- Dual Internet Dual CPE (INT & LTE)
- Hybrid Dual CPE (INT & MPLS)
- HYBBRID Dual CPE (LTE & MPLS)
- DUAL-CPE-DUAL-INTERNET-HYBRID-LTE-PRI (New MWL)
- DUAL-CPE-DUAL-MPLS-HYBRID-LTE-PRI (New MWL)
- DUAL-CPE-TRIPLE-INTERNET-LTE (New MWL)
- DUAL-CPE-TRIPLE-INTERNET (New MWL)
- DUAL-CPE-DUAL-INTERNET-HYBRID (New MWL)
- DUAL-CPE-DUAL-MPLS-HYBRID (New MWL)
- DUAL-CPE-DUAL-HYBRID-DUAL LTE (New MWL)
- DUAL-CPE-QUAD-INTERNET (New MWL)
- DUAL-CPE-TRIPLE-INTERNET-HYBRID (New MWL)

5. SD WAN Remote Access

Today, enterprises are faced with the following reality:

- **Digital Transformation :** has accelerated the migration of enterprise applications and workloads from an enterprise datacentre to a variety of public clouds and/or SaaS services.

- **Users are connecting from everywhere :** COVID-19 has changed the workplace to a new normal where employees Work from Anywhere, and the employee's home is the new office.

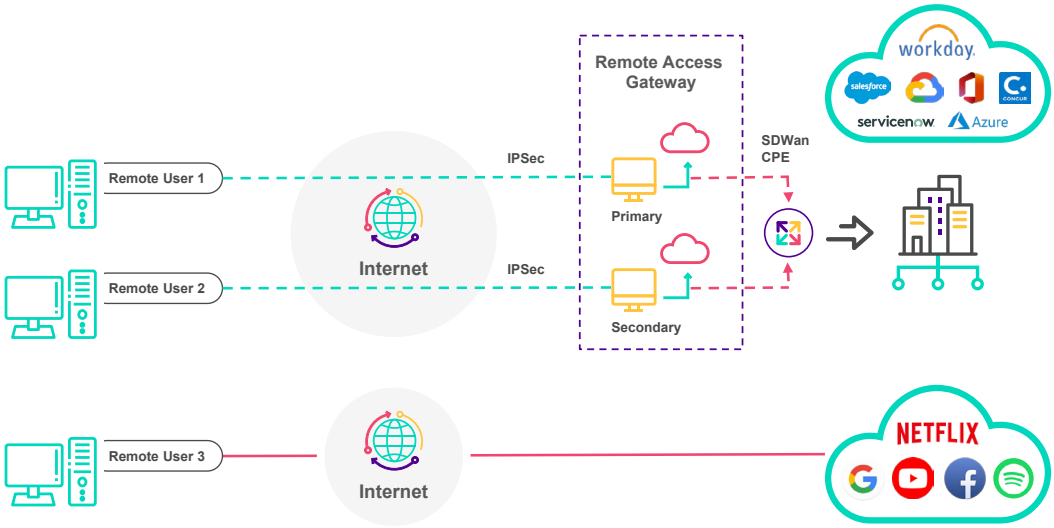
- **Moving to SASE :** Flexibility with a cloud-based infrastructure, where a customer can implement and deliver security services such as threat prevention, web filtering, sandboxing, DNS security, credential theft prevention, data loss prevention

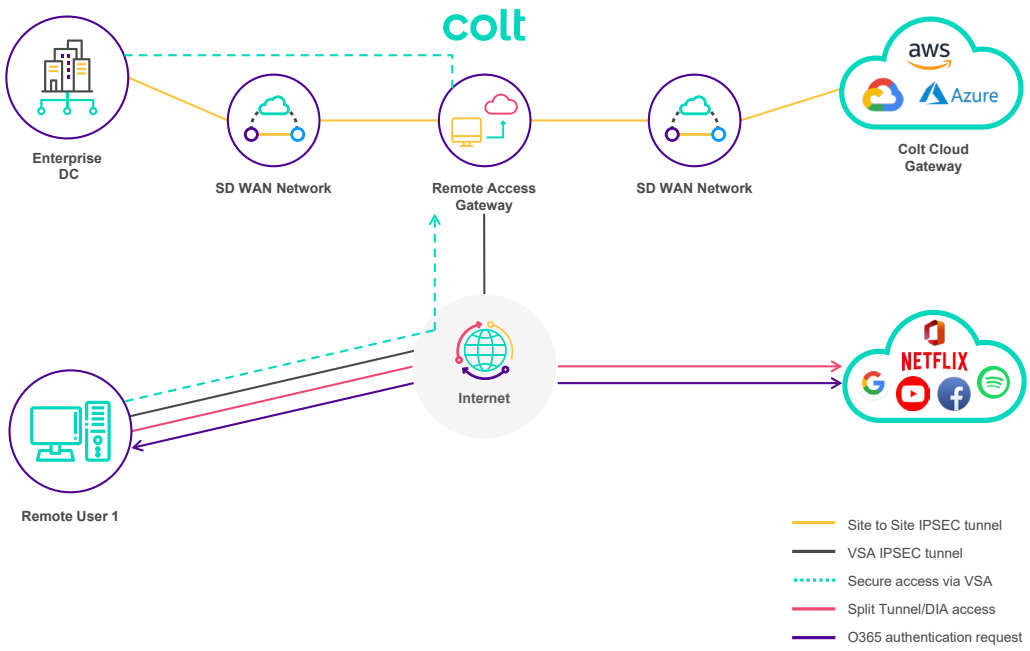
To meet customer demand and Part of adopting SASE (future), Colt uses Versa Secure Access as a feature of SD WAN. Colt's SD WAN Remote Access is the one of the industry's first solution to deliver the leading Secure SD-WAN services and private connectivity for remote employees. With this solution, employees can now securely connect to applications in both the private and public clouds as part of Remote Access Service Edge services.

With entire workforces connecting remotely through different devices during Covid 19 created an immediate demand for remote working solutions that can

- Scale
- Include security.
- Deliver traffic steering and conditioning.
- Offer easy to setup, manage and operate solution.
- Provide visibility and insight to network performance.

A new network model is needed to deliver remote working that is scalable, flexible, agile, and secure over a resilient and reliable network. With users remotely trying to access cloud-hosted applications, on-premises applications, VoIP, Virtual desktop applications, together with SaaS application such as Salesforce and Office365, security and performance demands skyrocket.





Service Components

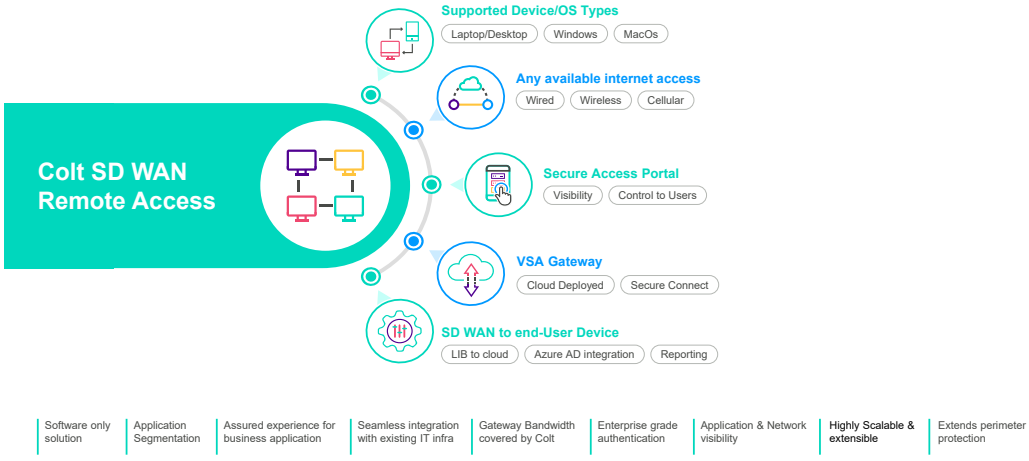
Remote Access is a distributed solution to connect distributed users to enterprise applications. The applications can be distributed across private cloud, enterprise data centers and public cloud. The Secure Access Solution consists of:

Remote Access Gateways are based on FlexVNF/VOS platform. They are globally distributed to provide distributed secure on-ramps for access to enterprise applications. Gateways authenticate users, authorize the application access and secure the enterprise network from external threats.

Remote Access Client is software agent/application that runs on and extends SDWAN to client devices (i.e.: Windows, MacOS computers). Remote Access Client creates a secure and encrypted connection from remote device to the Versa Cloud Gateway

Remote Access Portal provides enterprise administrators the ability to monitor the service and provides real-time and historical reporting at a network, application, and user level leveraging big database Analytics platform.

Benefits



High Level Activities

- Home users (End user) – installs RA client.
- The RA client creates IPsec tunnel to RA Gateway (GW)
- The RA Gateway will have statically configured IPsec tunnels to an SD WAN CPE.
- SD WAN CPE will act as an additional site on de customer SD WAN.
- The CPEs in DC are not in resilient mode, they act separately.

Gateway Locations.

- EU
- APAC – HK
- APAC – JP (upcoming)
- APAC – SNG
- US – East
- US - West

Customer responsibilities

- Customer IT admin is responsible for handling end user issues
- Customer IT admin to raise trouble ticket with Colt not end user
- Customer is responsible having the client OS for seamless performance.

6. Proof Of Concept (PoC) only available for Enterprise segment, or directly for Carrier auto-consumption (in roadmap for SD WAN Wholesale)

Reference documents for PoC:

- Standard SOW (statement of work)
- Standard T&C (PoC specific terms and conditions)

Test environment specification:

- Number of sites: 3 sites
- Site Type: SD WAN Hybrid site (MPLS + Internet), Internet Only or MPLS only
- MPLS: 100Mb, on-net;
- Internet: Public Internet provided by customer
- CPE: Preconfigured from available test pool
- PoC support window: EU local business hours only

Resources:

Standard resources

- Service Delivery is included in standard price
- Project Manager/ Technical Solution Manager: Only Project Management light (Silver) will be offered
- Product (OS) – Internal support for overall Solution

Dedicated resources (“Only upon request”)

- Resource model: Dedicate POC specialist not random resource from a pool
- SD WAN delivery engineer: Ensures POC configured correctly and support TSM when required

PoC charges:

- € 1200, it covers installation and three months maintenance cost (NRC € 450 and MRC € 250 x 3) + connectivity costs. If POC is part of the bigger deal and deal is won, PoC NRC is waived.

Test period"

- Up to 12 weeks only

Success criteria

- As stipulated in SoW.

7. Service Delivery

Service delivery consists of the following:

- New service order
- Modifying an existing service
- Out-of-hours changes
- Cessation or cancellation of service
- Demarcation point

7.1. New Service Order

Every service starts with a signed order (document capturing Customer specific requirements and deliverables).

7.2. Modifying an Existing Service

Modifying an existing service consists of the subsequent enabling or disabling of service features, functions and interfaces as well as service changes following initial installation. Service modification orders may have commercial impact, either in the form of one-off/NRC or on-going/MRC.

Modification orders can be grouped under following categories: A, B and C.

- Category A
  - modifications falling under this category need physical changes to the equipments on which the services are delivered.
  - examples include, local access bandwidth upgrade, CPE upgrade to a different version etc.,

Most category A modifications are regarded as new provision in terms of lead times and installations.

- Category B

Include remote configuration changes:

  - Option 1 (B1) refers to service requests that can be completed within 12 working hours. If a request cannot be handled within 12 working hours, then the delivery time is five working days.
  - Option 2 (B2) refers to service requests that can be completed within five or 10 working days.

A committed lead time can only be given for ≤ 25 sites. Please contact a Colt Account Executive if there is a requirement involving >25 sites

- Category C modifications
  - Emergency configuration changes can be requested at any time and have a target implementation time of one hour (depends on the change requested) from acceptance of order.

7.3. Out-of-hours Changes

Category B changes can also be requested out-of-hours. Out-of-hours changes must be scheduled and approved in advance, and there is a lead time of 10 working days. There is a charge of €200/hour per scheduled session with a minimum charge of €500 per session.

7.4. Cessation or Cancellation of Service

Request for cessation of service may be subject to a charge in accordance with Colt standard terms and conditions. Should the customer cancel their order during installation, Colt reserves the right to charge for the remaining contract term.

7.5. Demarcation Point

The demarcation point for Colt SD WAN site is Ethernet LAN port on the Colt provided CPE.

8. Service Assurance

Colt provides a high level of service assurance:

- The core network is proactively monitored
- A local language help desk is available 24 hours a day, seven days a week
- Colt Online provides a web-based portal that enables customers to view bills and trouble tickets

Note that this help desk and web-based portal is offered to Colt's direct customer, not Carrier's end customer for SD WAN Wholesale. Operation and commercial relationship towards Carrier's end customer is not part of Colt's responsibility.

Service assurance includes:

- Customer service
- Service Level Agreement
- Colt Online
- Service monitoring
- Planned maintenance

8.1. Customer Service

Colt has a high quality fibre network that enables the provision of an annual target service availability. The target availability depends on the service taken and the location of customer sites. The fault help desk is available 24 hours a day, seven days a week. Customers can report a fault at any time by contacting the Customer Service Centre and speaking to a representative in their local language.

When the service is provisioned, customers are issued with a unique service reference for each circuit that should always be used when reporting faults. The contact number for fault reporting is specified in the service handover pack.

8.2. Service Level Agreement

Colt offers a comprehensive service level agreement, which pays compensation if agreed targets are not met. Colt's own global fibre network enables it to provide customers with an annual service availability of up to 99.99%.

Colt's Terms and Conditions (T&Cs) only apply for our direct customer (Carrier), same for our offered SLAs.

End-customer's T&Cs and end-customer committed SLAs are Carrier's responsibility.

Colt Generic T&Cs are specified depending on the type of contract, Enterprise or Reseller. Please consult document Colt Generic T&Cs.

Ask a Colt Account Executive for more information about our SLAs.

8.3. Colt Online

Colt Online is an intuitive, user-friendly application enabling new and existing Colt customers to interact with Colt via a secure Internet connection without the need to speak to a Customer Service Agent or Account Executive.

Note that Colt Online is only accessible for Colt's direct customer.

For SD WAN Wholesale, Carrier's end customer will not have access to it, in any case.

All features only accessible through Colt Online, as Versa Analytics, wont' therefore be available to them.

Every Colt Online customer is provided with an administrator account for a defined user within their organisation. This administrator has full access to the available features for all their customer accounts and sub accounts, including:

- Search and view any bill from the previous six months in .pdf format*
- View the status of any order in the delivery process
- View the status of any ticket (covering faults, enquiries, service requests) in real-time
- Search and view all live services
- View an account dashboard, summarising the four features above

* Not available in Switzerland due to data protection legislation

8.4. Service Monitoring

The Colt backbone network is proactively monitored and maintained which facilitates prompt and efficient remedial action upon any fault detection. Proactive ticketing is delivered as a standard feature. Customers are proactively informed of Colt opening tickets.

Note that in SD WAN Wholesale, Carrier's end customers will not receive ticketing information originated from Colt, only Colt's direct customer (Carrier).

8.5. Planned works and maintenance

In order to ensure performance and security for all customers, Colt occasionally performs maintenance works that may cause customer's service being unavailable. Colt will endeavour to ensure that such works have minimum impact on Customer's service. Typically, planned works occur after 20:00 GMT on weekdays.

When planned works are required, customers will normally be notified in advance as per the following timelines:

- When service affecting planned works are necessary, the customer will be notified ten (10) calendar days in advance. Colt will endeavour to ensure that such works will occur during non-working hours, unless a critical intervention is required to maintain network stability.
- For any emergency work, no advance notification will be issued.
- If there are planned works to be undertaken by third parties, Colt will aim to give five (5) calendar days' notice, dependent on when Colt itself is made aware of the work.

The date and time for planned maintenance cannot be changed or cancelled by the customer.

Colt is not responsible for failure to meet SLA, where such failure is due to a planned maintenance works outage.

For SD WAN Wholesale, Carrier will be responsible for notifying any planned work that may affect their end-customer and ensure they can be carried out.

9. SD WAN Wholesale specifics

9.1. Intro

The aim of the SD WAN Wholesale service that Colt offers is to provide a flexible approach such that we are not limited to expansion when choosing the correct provider, but also scalability where we have the range of equipment we can increase a customer's environment when required.

Those customers that don't have an own SD WAN solution and want to cover that gap with a whitelabel choice, can find the perfect match in Colt's SD WAN Wholesale.

Colt provides the service in a multinational environment, including the equipment, shipment, installation and basic configuration of the devices according to the Carrier instructions during the initial deployment, and will maintain the devices provided (RMAs), together with the connectivity and management plane.

The subsequent management of the service and control platform will be performed by the Carrier/end customer, as for their services and operational model.

9.2. Responsibility split diagrams

The SD WAN Wholesale product is aimed at new or existing wholesale customers.

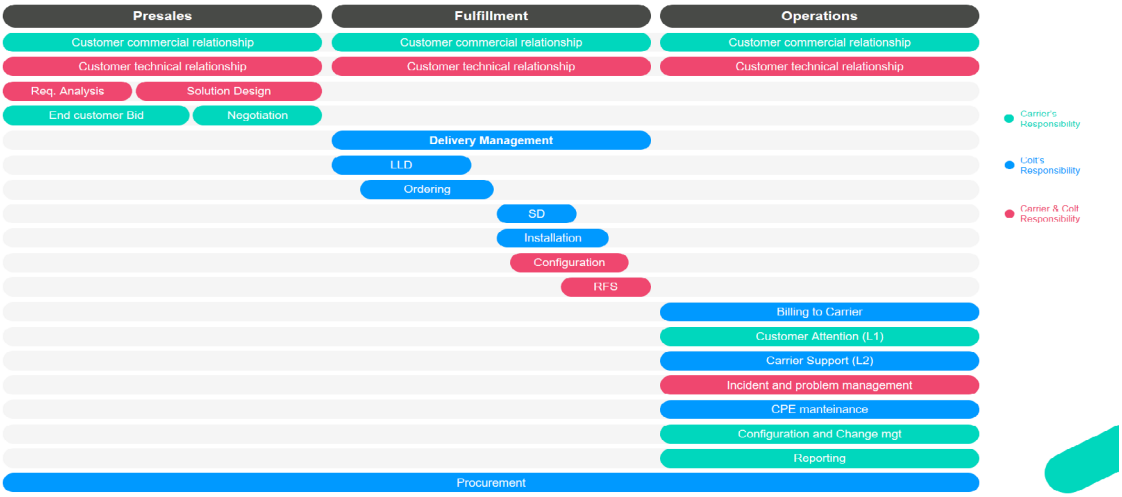
The Wholesale customer will be looking for an SD WAN product that can be sold to their end customers as a white-label product, as if they were providing the product by themselves.

The SD WAN portal can be either personalized with the Carrier look&feel or simply provided with no Colt logo or references, this is Carrier's choice.

The following diagrams show the main responsibilities of each entity, as:

acquisition (sale and support)	– See diagram below
service transition	– See diagram below
service operations	– See diagram below
billing	– See diagram below (only invoicing to Wholesale customer, not end-customer)
service cancellation	– See diagram below
change of circumstances	– See diagram below
claim	– See diagram below
renewal	– See diagram below

As per Wholesale segment nature, there needs to be some responsibility split. Here is a proposition for the main tasks and processes:



BSS	BSS Carrier	Carrier
	BSS Colt	Colt
OSS	OSS SD Wan	Carrier
	OSS SD Wan Portal	Carrier or Colt
	Carrier Tools	Carrier
Presales	Commercial Management	Carrier
	HLD	Carrier
	Support for HLD	Colt
	Bid and negotiation towards end customer	Carrier
	Request/order/purchase Underlay	Carrier
	Request/order/purchase Overlay	Carrier
Deploy-ment	LLD (design with End Customer)	Carrier
	LLD (Templates and configuration)	Carrier or Colt
	Management and control platform	Colt
	Supply, Installation, CPEs	Colt
	Configuration of initial tempaltes/policies	Colt
Manage-ment	CPEs maintenance	Colt
	RMA detection	Carrier
	Portal Management	Carrier or Colt
	L0, L1	Carrier
	L2, L3	Colt
	Change (request, notification to and customer)	Carrier
	Risk Analysis	Carrier
	Changes execution	Carrier or Colt
	Supply	Colt
	Installation	Colt
Fullfilment	Basic Configuration per site	Colt
	Underlay configuration	Carrier or Colt
	Underlay Network Monitoring management	Carrier or Colt
	Failures management	Carrier or Colt
	OSS Underlay	Carrier or Colt

For further details of the different responsibilities, please contact a Colt Account Executive.

10. Commercials

10.1. Contract period

The standard contract term is between one year and five years.

10.2. Billing

Colt offers a range of billing options including monthly billing. Bills are available on paper or on CDROM. Each bill contains summary sheet and further reports detailing the following charge types:

- Site installation and rental charges
- Any other charges and credits
- Discounts by service, if applicable

Charges will be billed on a per site basis as each site is provisioned. Bills are calculated on a pro rata daily basis. Bills will be raised for the entire network in the country in which the service was contracted.

Billing is only meant for direct customer (Carrier in the Wholesale segment). Billing towards end-customer is Carrier's responsibility.

There will not be any prebill set for that purpose.

10.3. Installation Charges

Installation charges are billed after the service has been installed at a site.

10.4. Rental Charges

Rental charges are billed in advance.

11. Colt Professional Services

Colt Professional Services is a team of highly focused experts dedicated to designing and managing solutions which support business transformation for our customers.

Our consultants are available to:

- Conduct thorough reviews of current and future communications requirements
- Design complex projects to exacting standards
- Manage project implementations
- Ensure the service is being delivered to customer expectations

Colt has expertise in four areas:

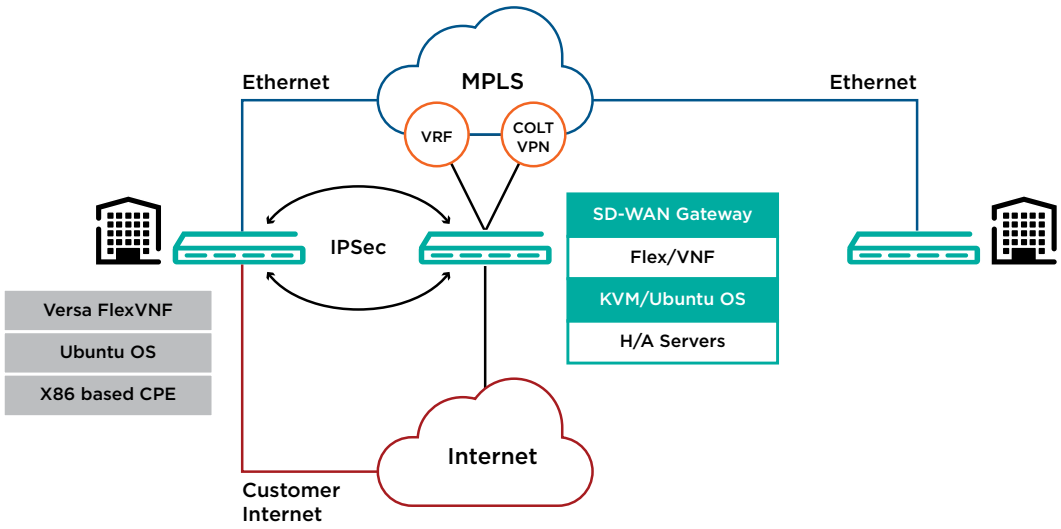
- Project Management
- Service Delivery
- Consulting Services and
- Design Services

For full details of the services available, please contact a Colt Account Executive.

12. Appendix

12.1. Colt SD WAN Network Architecture

SD WAN architecture consists of following components:



- Versa Director:

  This is Virtual Networks Function (VNF) manager that manages a set of FlexVNF software instances running on general purpose servers. Versa Director provides a single pane for provisioning, configuration, and management of FlexVNFs. The Versa Director will also perform the functionality of a Staging Server. A Staging Server is a registration and staging entity for deployment of all Branch FlexVNFs.

- Versa Analytics (only available for Enterprise segment, in roadmap for Wholesale):

  Versa Analytics is a big data solution that analyses logs, events, and provides reports, analytics as well as feedback loop capabilities. FlexVNF at various Branch-sites continuously provides monitoring data relating to link, network-path and services to the Versa Analytics server. This data can be used for dynamic application based traffic steering, capacity planning, and security forensics.

For SD WAN, the Versa Analytics supports historical and real time data reporting for:

  - Application usage based on total sessions, volume, bandwidth
  - Application performance based on latency, jitter, packet loss
  - Performance of various paths between any two Branches
  - Utilization of the different access circuit of Branches

- Versa SD WAN Controller:

The Versa SD WAN Controller plays a key role in the solution and serves as a primary attachment point to the Virtual Private Network (VPN). The SD WAN Controller provides a central control-plane entry point for zero-touch deployment of Branches. The Controller authenticates the Branch FlexVNF instances using PKI certificates as part of an IKE exchange. The secure channel established using IKE provides a transport-channel between a Branch node and the SD WAN Controller for transport of routes, policy, and configuration. A single SD WAN Controller can serve as the attachment point for VPNs belonging to several different customers.

Once a secure IP Sec tunnel is established it establishes MP-iBGP session with the branch CPE's over the IP Sec tunnel.

The Controller will act as a route reflector and reflect routes between branches between each customer sites.

- VNF Gateway:

  The VNF gateway is used when the SD WAN sites need to communicate to Colt MPLS Sites for Hybrid solutions. VNF gateway is capable of hosting Multi Tenancy which is an important feature as a part of the solution. The VNF gateway will connect to Colt PE router as Type A NNI circuit. FlexVNFs as a service appliance at VNF gateway node, will be provisioned as virtual machines on KVM or on x86 CPE's running any Ubuntu OS.

- Versa FlexVNF CPE:

  On the customer site, the Versa FlexVNFs will be deployed on bare-metal x86 servers, running Ubuntu OS.

  A Branch FlexVNF can be used for providing intelligent secure connectivity (e.g. secured connectivity, Support for multiple tenants and multiple VRFs, Intelligent load-sharing of traffic over various access circuits, SLA monitoring of multiple paths between various Branches of Routing Protocols (BGP/OSPF), VRRP, Static, QoS and CGNAT).

  A Versa FlexVNF can be deployed in either of the below high availability (HA) modes:

  - Inter-VNF redundancy or
  - Intra-VNF redundancy

  Note: Only those features, which are mentioned in the feature section of this document, can be offered to customers.

12.2. Colt SD WAN Portal Overview

The Colt SD WAN platform (available at the following URL: https://SD-WAN.colt.net/) allows Customers to check all the services that have been requested, and the status of each of these services. Customers can use the portal to edit traffic forwarding (over MPLS and/or Internet), set forwarding thresholds, view and edit firewall policies and see firewall, interface, DDOS and application analytics.

The portal is being continuously improved under Colt's agile programme and will be updated without notification, customer functionalities won't be impacted by these changes.

Please note that the portal only supports modern browsers such as Chrome, Firefox and Edge, but not legacy browsers such as Microsoft Internet Explorer.

Although the portal is a standalone web service, it uses the same authentication credentials as Colt Online; therefore, to access the portal you will need a Colt Online user account with a valid SD WAN role assigned.

In case of SD WAN Wholesale, it provides two layers of capability as shown below.

- SDWAN Reseller
- SDWAN End Customer

These two capabilities come with their own self-management portals to allow the administration of the service including for resellers and their end customers. The reseller portal view provides all the same functions as to the end customer portal but allows the end user to manage the addition and deletion Portal users from their end customers.

The capabilities of the reseller and the end user are shown will be detailed in the sections below. This guide can be split into four parts: general Information, key information, the reseller and end user guides. The key differences are that the Reseller Portal is Colt branded but the end user portal can have some splash screen and logo added to the page views for reseller branding.

As the Portal is in constant evolution, for updated and detailed information please consult the Portal User Guide available in the intranet (links below, for both Enterprise and Wholesale views)

12.2.1. Portal Specifics for SD WAN Wholesale

Please consult 4.2 section for Wholesale specifics, together with SD WAN Portal Guide Wholesale.

13. References to external documents

References and links to other documents mentioned throughout the ESG:

Secure Network Gateway (Zscaler)

3rd Party Internet Access and SLA Tiers

Regulatory Tracker

Encryption Restrictions Worldwide

DCG Internal Service Guide

DCG External Service Guide

DCG Deployment Guide

SD-WAN Deployment Guide

uCPE External Service Guide

PoC SoW

PoC Terms and Conditions

SD WAN Portal Guide Enterprise

SD WAN Portal Guide Wholesale

SD WAN Feature Matrix

For more information,
please contact us on:

+44 (0)20 7863 5510
sales@colt.net
www.colt.net