SIFY MANAGED SD-WAN SERVICES

**Technical Service Descriptor**

Table of Contents

[1.1 Revision History: 2](#_Toc530042049)

[1 Introduction 3](#_Toc530042050)

[2 Document scope 4](#_Toc530042051)

[3 What is SDWAN 4](#_Toc530042052)

[4 Services overview 7](#_Toc530042053)

[5 Service Components 8](#_Toc530042054)

[5.1.1 Components 9](#_Toc530042055)

[5.1.2 SD-WAN Edges 9](#_Toc530042056)

[5.1.3 SD-WAN ZTP server 10](#_Toc530042057)

[5.1.4 SD-WAN controller 10](#_Toc530042058)

[5.1.5 SD-WAN Manager 11](#_Toc530042059)

[5.1.6 SD-WAN Analytics 11](#_Toc530042060)

[5.1.7 Transport networks 12](#_Toc530042061)

[5.1.8 Sify aakaash (service portal) 12](#_Toc530042062)

[6 Service description 13](#_Toc530042063)

[6.1 SD-WAN Services 13](#_Toc530042064)

[ Multi-provider transport 13](#_Toc530042065)

[ Encrypted VPN 13](#_Toc530042066)

[6.2 Sify Managed services 19](#_Toc530042067)

[6.3 Transport connectivity 21](#_Toc530042068)

[7 Service delivery model 21](#_Toc530042069)

[8 Service differentiation – Analytics based data-driven WAN 22](#_Toc530042070)

[9 Deployment work flow 24](#_Toc530042071)

[9.1 Deploy control components 24](#_Toc530042072)

[9.2 Deploy SD-WAN edges 25](#_Toc530042073)

[9.2.1 Deploy SD-WAN edges as hardware box 25](#_Toc530042074)

[9.2.2 Deploy SDWAN Edges on Cloud (AWS only) 26](#_Toc530042075)

[9.3 Transport connectivity 27](#_Toc530042076)

[9.4 Configure WAN policies 27](#_Toc530042077)

[9.5 Service management 27](#_Toc530042078)

[10 Central control component design 28](#_Toc530042079)

[10.1 Central component design – Viptela 29](#_Toc530042080)

[10.2 Central control component design – Versa 31](#_Toc530042081)

[10.2.1 Model 1 - Sify DC centrally deployed for multi-tenant 35](#_Toc530042082)

[10.2.2 Model 3 - Customer, on-prem deployed for single-tenant 36](#_Toc530042083)

[11 Use cases 37](#_Toc530042084)

[11.1 Policy Change via AAKASH portal(roadmap) 37](#_Toc530042085)

[11.2 App-Aware routing- Blackout scenario 37](#_Toc530042086)

[11.3 App-Aware routing- Brownout scenario 38](#_Toc530042087)

[11.4 AppQoS 39](#_Toc530042088)

[11.5 End-End VPN Segmentation 39](#_Toc530042089)

[11.6 Any Transport Connect 40](#_Toc530042090)

[11.7 Firewall features Like Stateful, NextGEN and UTM 41](#_Toc530042091)

[11.8 Path Optimization 41](#_Toc530042092)

[11.9 Direct Internet Access 41](#_Toc530042093)

[11.10 Single pane of glass for all reports 42](#_Toc530042094)

[12 Solution sizing, hardware and software 42](#_Toc530042095)

[12.1 Viptela 42](#_Toc530042096)

[12.2 Versa 44](#_Toc530042097)

[13 Technology differences – Viptela and Versa 46](#_Toc530042098)

[14 Overhead calculation 48](#_Toc530042099)

[14.1 Viptela 48](#_Toc530042100)

[14.2 Versa 48](#_Toc530042101)

[15 SLA 49](#_Toc530042102)

[16 Appendix 51](#_Toc530042103)

## Revision History:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date** | **Revision** | **Author** | **Remarks/Modifications** | **Approver** | **Reviewer** |
| 24-09-2018 | 2.0 | Vivek Karthik S | Updated draft | Ramakrishna Kotha |  |

# Introduction

As enterprises transform their business processes to embrace greater digitization, cloud and mobility are combining to rapidly shift the application and data traffic profile within the enterprise. More enterprise applications are being delivered from the cloud, and more enterprise users are mobile and require anytime/anywhere access to applications. The network delivering application data to users must evolve. In distributed enterprises, such as those with several branches and remote workers, it is the wide area network (WAN) that requires an urgent transformation.

WAN transformation for a distributed Enterprise needs to address a diverse set of connection types, dispersed locations with different bandwidth needs, and the need to access applications both within the network and through the cloud. At the same time WAN transformation needs to look at simplifying networks, enhancing control, improving performance, visibility and driving efficiency.

Software-defined wide area network (SD-WAN) provides a solution to the WAN transformation. SD-WAN solution promises the enablement of:

* Optimization of modern application delivery costs through the WAN in the face of future application traffic profile change and growth
* Greater flexibility and efficiency of network transport via cost-effective alignment of network connectivity options and bandwidth with application criticality
* Improved branch IT agility and efficiency through automated and agile service provisioning and reduced complexity
* Better customer engagement By enhancing cloud application reliability, availability, performance, and security
* Secure data traffic for all applications especially those hosted in the cloud

Sify’s Managed SD-WAN service provides risk free WAN transformation service for Enterprises by offering

* A Hosted service to ease the costs of adoption.
* Experts guided Network deployment and migration.
* Orchestrating the network to meet the desired objectives of application performance.
* Transport services that enable a true Hybrid network.
* Better performance to the cloud hosted applications
* Comprehensive network management and monitoring.
* Service backed by comprehensive SLAs
* Leverage all Strategic and technical benefits that come from using Managed SD WAN

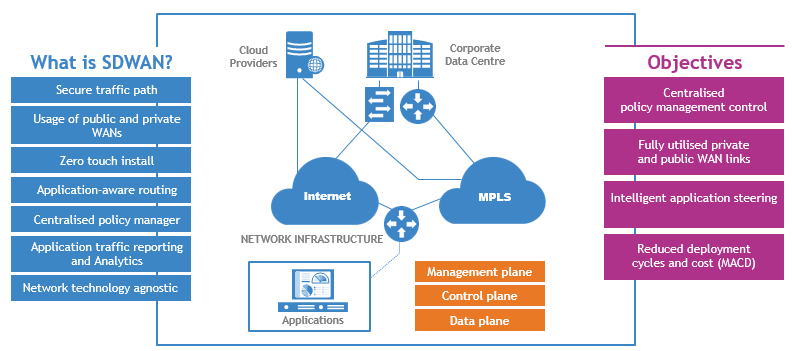
# Document scope

The scope of this document is to define Sify Managed SDWAN services leveraging Versa networks as a platform. The document covers:

1. Service description
2. Service architecture
3. Service features
4. Service delivery mechanisms
5. Service level agreements

The document is for Product Management, Solution architects, Provisioning, NOC and Delivery teams to understand the complete service offering to conduct all operations relevant to the product.

# What is SDWAN



Businesses are increasingly under pressure to respond to the ever-increasing demand from end-users and employees, who demand more from computer systems, networks, and mobile devices than ever before. As a result, businesses are constantly exploring ways to keep up with fast evolving technology trends, business and end-user requirements, and to provide innovative applications and services with faster time to market. "Business Agility" is the buzzword in this new world where providers are expected to provision and roll out services rapidly.

Software Defined Networking provides a new paradigm that attempts to respond to the new requirements of business agility and improved user experience. Many cloud-computing environments operate in an application-centric world, where virtualized applications are hosted within a public or private cloud. As a result, users can access their applications from anywhere, on any device, at any time. Instantiating a Virtualised application instance takes minutes whereas networks remained rigid, hardware centric and protocol heavy.

To create agility and flexibility in networking, the Open Network Foundation (ONF) defines Software-Defined Networking with the below characteristics

* Separation of the forwarding from the control plane
* Implementation of the forwarding plane
* Use of a protocol (typically open flow) to connect the control and forwarding or data plane.

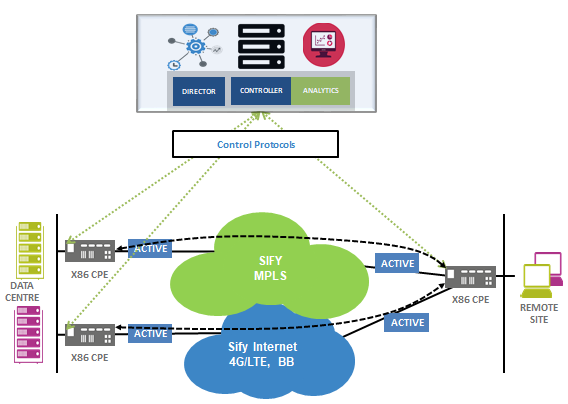
These characteristics are very narrowly tailored to fit into datacentres, cloud networking where SDN got its start. However, for wider adoption and to work with a huge deployment based on legacy networks and protocols, broad benefits of SDN have been pursued. For the desired benefits following are the essential characteristics of SDN to any enterprise

* Focus on automation for provisioning, activation and verification or combined into a single word orchestration
* Update of Network elements with modern programmable interfaces like REST, NETCONF/YANG from legacy interfaces such as CLI and SNMP.
* Use of policy to simplify control of the network and align to a business centric network than a device centric network.

The Software-Defined Wide Area Network (SD-WAN) is a specific application of Software-Defined Networking (SDN) technology across a WAN. The SDWAN borrows the characteristics of centralised control and overlays from SDN as seen in the data centre or cloud and combines them with the characteristics as seen for an Enterprise implementation.

With the controller being centralised, Enterprises can now orchestrate their WAN, apply policy and manage their networks from a single console without involving in the complexities and intricacies of every device. The centralised controller works on the new programmatic interfaces with the devices to enable agility.

Similarly with overlays, the underlay is abstracted to manage application paths, measure and manage performance across any network. Our Managed SDWAN leverages SDWAN technology to deliver a WAN transformation with the technology benefits to our customers.



SIFY AAKASH

# Services overview

Our Managed SD-WAN services comprises of the following 6 key elements. We believe all the 6 elements are essential for a customer to leverage the complete benefits of SDWAN and enable a successful WAN transformation.

1. SDWAN as a service including all feature sets as delivered by the SDWAN platform including IP routing, encryption, Application aware performance routing and Security.
2. Transport underlay could be Sify Siteconnect, Expressconnect or options to support bring your own Transport [BYOT] such as third party MPLS, Internet, Broadband or LTE.
3. Supply of Hardware Customer premise Equipment against the site bandwidth and functional requirements from a chosen OEM through a subscription or outright purchase model.
4. Implementation and Migration services.
5. Lifecycle management through our Proactive network managed services.
6. Self-service through Sify Aakaash portal to manage policy, view network insights through analytics and get service support.

Sify Managed SD-WAN services are offered using two SD-WAN vendor platforms –

1. **Versa networks**
2. **Viptela**

Feature set of Viptela and Versa based SD-WAN platforms would differ based on individual capabilities of each SD-WAN platform and will be considered during solutioning based on customer requirements. Both the vendor solutions are exclusive of each other and enterprises can be deployed and managed with a single SD-WAN vendor solution.

# Service Components

SD-WAN as a service consist of following below components:

* **Control, configuration and management plane components** – deployed in Sify cloud with capabilities supporting multi-tenancy
* **Data plane components** – SD-WAN edge devices are deployed in every customer site where customer apps are hosted either in VM or Hardware based model
* **Transport networks** – Provides last mile network connectivity to CE’s that establishes connection towards SDWAN Infra for Control plane communication and data plane between Branch devices
* **Cloud** – Applications hosted in on-prem or cloud (public/private/hybrid)
* **Service management portal** – a single pane of glass for complete service lifecycle management (Until the portal is completely live Versa director and Viptela vManage will be used for the same)

Below is the architecture of Sify Managed SD-WAN services.

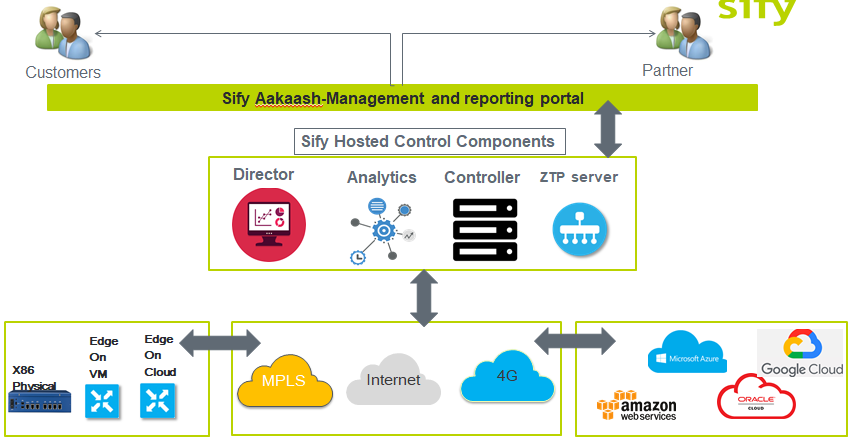


Figure 1 Managed SD-WAN services architecture

Service architecture of Sify’s Managed SD-WAN services makes use of creating a service layer on top of SD-WAN vendor provided solution components and provides that as service management interface to end users – Sify MS-NOC, SD-WAN customers and partners.

Sify aakaash is the self-service management portal which performs complete lifecycle management process of SD-WAN services. Integration between SD-WAN components and service portal is through standard API (REST).

### Components

SD-WAN component name and functionality may vary between Viptela and Versa based SD-WAN solution, this document consists Sify’s terminology from the perspective of managed SD-WAN services and also includes relevant component name of Viptela and Versa SD-WAN. Below are the components involved:

* SD-WAN Edges
* SD-WAN ZTP server
* SD-WAN Controller
* SD-WAN Manager
* SD-WAN Analytics
* SD-WAN Gateway
* Transport network
* Sify aakaash (Self-service portal)

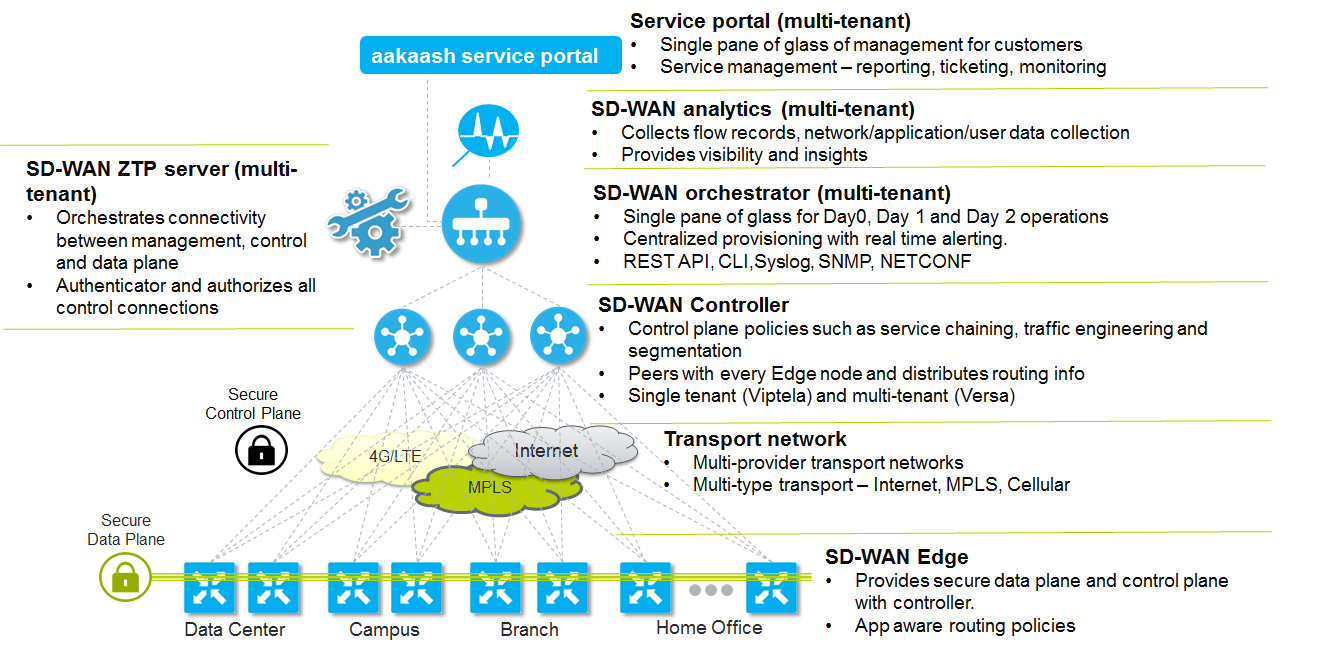
****

Figure 2 SD-WAN solution components

### SD-WAN Edges

SD-WAN edges are customer premise equipment placed at every customer premise. SD-WAN edges terminate WAN connectivity from single or multiple service providers including various WAN technology types (MPLS VPN, Internet, 4G/LTE, DSL). SD-WAN edges are available as hardware box or as virtual network function (VNF) instantiated over x86 based compute based on KVM or VMWare ESXi or cloud based deployments

SD-WAN edges are delivered as part of Sify’s managed SD-WAN services and will be configured and managed by Sify MS-NOC. Edges create overlay secure tunnels between other edge devices using all possible WAN transport links (underlay) as references and measure real-time network performance to determine the ideal best path for application traffic.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sify SD-WAN parameter | Viptela SD-WAN | | Versa SD-WAN | |
| SD-WAN edge | vEdge |  | | Versa FlexVNF |
| Supported deployment options – Day 1 on customer premise/Cloud | Hardware box as supplied by Sify |  | | Hardware box as supplied by Sify |
| VNF based SD-WAN edge support on case to case basis |  | | VNF based SD-WAN edge support on case to case basis |
| Cloud based VM deployment on AWS/Azure Platforms |  | | Cloud based VM deployment on AWS/Azure Platforms |

### SD-WAN ZTP server

Ease of bringing up enterprise sites and automatic configuration with minimal or no truck load is one of the values of SD-WAN. This is achieved using a process called Zero touch provisioning (ZTP). A dedicated component is responsible for ZTP functionality in SD-WAN. Below are the functionalities of ZTP server:

* Initial authentication and subsequent multi-factor authentication of SD-WAN edges before authorized to join SD-WAN overlay network
* Provide initial information and facilitate inter-communication between SD-WAN components (controller, Manager and analytics) information and SD-WAN edges and vice-versa
* As per Sify deployment dedicated ZTP servers hosted in our DC will be used for this purpose

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sify SD-WAN parameter | | Viptela SD-WAN | | Versa SD-WAN | |
| SD-WAN ZTP server |  | | vBond | | Versa Controller | |
| Supported deployment options – Day 1 |  | | vBond as VNF  vBond as hardware box | | Versa controller as VNF | |

### SD-WAN controller

SD-WAN controller is the central intelligent element and plays a key role in underlay abstraction. Below are the functionalities of SD-WAN controller:

* Acts as central control plane component for both routing and security information collection and distribution
* Establishing secure communication session with all SD-WAN edges, ZTP server, Manager and analytics
* Acts as a common reflection point from control plane to all SD-WAN edges
* Enables communication from SD-WAN edges to other control components (Manager and analytics)
* Controls SD-WAN policy information distribution

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sify SD-WAN parameter | | Viptela SD-WAN | | Versa SD-WAN | |
| SD-WAN Controller |  | | vSmart | | Versa Controller | |
| Supported deployment options – Day 1 |  | | vSmart as VNF | | Versa controller as VNF | |

### SD-WAN Manager

SD-WAN Manager is the service management component which provides following functionalities:

* Service fulfillment – configuring and activating SD-WAN services from a single console including service, security and policy enforcement
* Configuration management of all SD-WAN edges including support of template based configuration – routing, WAN, LAN, policies
* Device management – management of all SD-WAN edges, controller, ZTP server including serial number, model details, software version
* Orchestrates SD-WAN policy engine as defined by user with the support of various templates and other direct SD-WAN edge configuration options
* Integrates with SD-WAN analytics and provide a common GUI platform for visibility and reporting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sify SD-WAN parameter |  | Viptela SD-WAN |  | Versa SD-WAN |
| SD-WAN Manager |  | vManage |  | Versa Director |

### SD-WAN Analytics

SD-WAN analytics is a component responsible for gathering and collecting various data from SD-WAN edges, controller and ZTP server and provides correlated insights to end user. SD-WAN analytics can be a separate component or can reside on Manager itself. Irrespective of this, SD-WAN analytics provides below functionalities:

* Collects network information from all SD-WAN edges including LAN, WAN, overlay tunnel including performance value of each tunnel
* Collects application information from all SD-WAN edges using DPI and flow based technology
* Protocols used in the collection of Data from Edge routers are IPFIX,Netflow and TWAMP
* Collects end user information from all SD-WAN edges – either based on IP details or integrating with LDAP/AD
* Collects various other alarms and events from all SD-WAN edges, controller, which includes SNMP MIB, SNMP traps, Syslog information
* Correlates collected information and provide analytics insights including network usage, application usage, network performance details
* Provides forecasting and trending reports based on collected data and correlation engine

|  |  |  |  |
| --- | --- | --- | --- |
| Sify SD-WAN parameter | | Viptela SD-WAN | Versa SD-WAN |
| SD-WAN Analytics |  | vAnalytics in Viptela cloud | Versa Analytics [hosted as part of central control components] |
| Supported deployment options – Day 1 |  | vManage as VNF  vAnalytics as SaaS subscription, only supports multi-tenant | Versa Analytics as VNF |

### Transport networks

Transport networks provide inter-connectivity among sites of enterprise WAN. Sify’s Managed SD-WAN services can support multiple transport types including MPLS VPN, Internet, DSL and 4G/LTE. MPLS VPN links can be from single or multiple transport providers. As MSP, Sify owns provider governance of all transport networks by managing on behalf of enterprise networks. This is a common component to both Viptela and Versa.

* *Sify Recommends customer to get Internet links from SLA backed Internet service provider for optimal network performance for business critical traffic*

### Sify aakaash (service portal)

Customer self-service portal is the single point of contact for complete lifecycle management of managed SD-WAN services provided to enterprises. Sify aakaash is the self-service portal configured as single pane of glass for all managed services of Sify. Self-service portal integrates with SD-WAN Manager and analytics, retrieves relevant information of particular customer WAN metrics and provides visibility into end customer. REST API based integration of self-service portal with SD-WAN components. Self-service portal provides the following functionalities:

* Service management – incident and problem management, configuration management, inventory management, helpdesk
* Monitoring and reporting – SD-WAN edge health, transport health, overlay health
* Visibility – applications and sub-applications, users, top applications, top users, top sites by bandwidth and app usage
* Configure and manage WAN policies based on business and application needs **(In roadmap)**

# Service description

Legacy networking technology has become increasingly expensive and complex and it cannot scale to meet the needs of today's multisite enterprises. Sify Managed SD-WAN, which is based on time-tested and proven elements of networking, offers an elegant, software-based solution that reduces the costs of running enterprise networks and provides straightforward tools to simplify the provisioning and management of large and complex networks that are distributed across multiple locations and geographies. This is an enhanced version of existing PNMM services with SD-WAN as technology. Thus functionalities supported on managed SD-WAN services including traditional PNMM related services, Transport services and services specific to SD-WAN.

Sify Managed SD-WAN services comprises of three components:

* SD-WAN Services
* Sify Managed services(PNMM)
* Transport services (Sify MPLS, Internet and OSP links)

## SD-WAN Features overview

Sify SDWAN service support following key features. This feature set varies depending on SD-WAN solution vendor – Viptela or Versa.

### Control communication Overview-Viptela

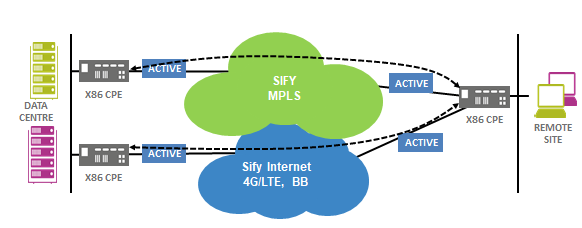
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Local device |  | Remote device |  | DTLS/TLS |
| **vSmart** |  | vManage |  | DTLS/TLS, permanent |
| **vSmart** |  | vBond |  | DTLS, permanent |
| **vSmart** |  | vEdge |  | DTLS/TLS, permanent |
| **vSmart** |  | vSmart |  | DTLS/TLS, permanent |
| **vEdge** |  | vBond |  | DTLS/TLS, temporary |
| **vEdge** |  | vManage |  | DTLS/TLS, permanent |

### Control communication Overview-Versa Networks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Local device |  | Remote device |  | Protocols |
| **Controller** |  | SDWAN Edge |  | IPSEC/UDP and BGP(Versa Private) |
| **Director** |  | Controller |  | Netconf, SSH, RPC |
| **Director** |  | SDWAN Edge |  | Netconf, SSH , RPC |
| **Analytics** |  | SDWAN Edge |  | TCP |
| **Director** |  | Analytics |  | Rest-API |

### SDWAN services

* Multi-provider transport– SD-WAN creates a unified overlay fabric over many underlay transport networks, so enterprise WAN can connect over many transport networks like Internet, MPLS VPN, cellular, DSL but able to communicate across its enterprise sites, cloud and internet hosted applications. This gives the flexibility to select mix of various types of transports based on availability of the geographical location.

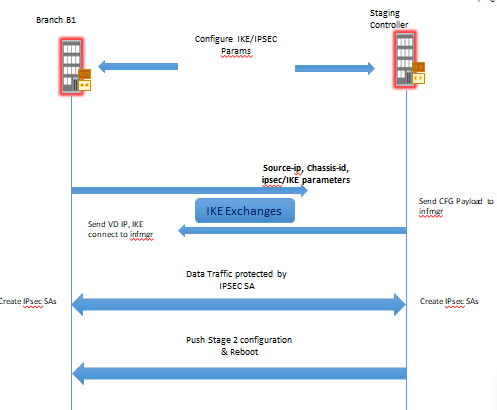


* **Zero Touch Provisioning**

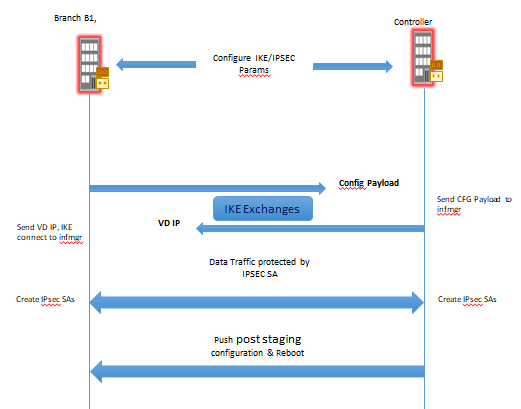
**Versa:**

Staging is done in 2 stages:

1. Pre-staging (For stage 1, IKE is over VNI interfaces)
2. Post-staging (For stage 2, IKE is over loop back interfaces (TVI interfaces)
3. Pre-staging-
   1. Branch device comes pre-loaded with staging server configuration. IPSec configuration profile has staging server FQDN/IP Address as remote IP address.
   2. IKE session is started between branch and staging server. Once the IKE session comes up, staging server assigns an IP address to the branch.
   3. IKE is over VNI interface. Traffic to branch is controlled through implicit filters in controller.
   4. Versa Director IP address is notified to branch. Branch installs reverse route to VD.
   5. Notification is sent to VD that the branch device has come up.
   6. Versa Director pushes stage 2 configurations to branch device through the staging server and reboots the branch device.



1. Post-staging-
   1. Branch device comes with stage 2 configuration – Controller’s IP address is the remote IP in IPSec config.
   2. Establishes IKE session with controller.
   3. Controller assigns an IP address to the branch device and generates a notification to Versa Director.
   4. VD IP address is notified to branch.
   5. Branch installs reverse route to VD.
   6. VD pushes the post staging configuration to branch device over the IKE session and reboots the branch device.



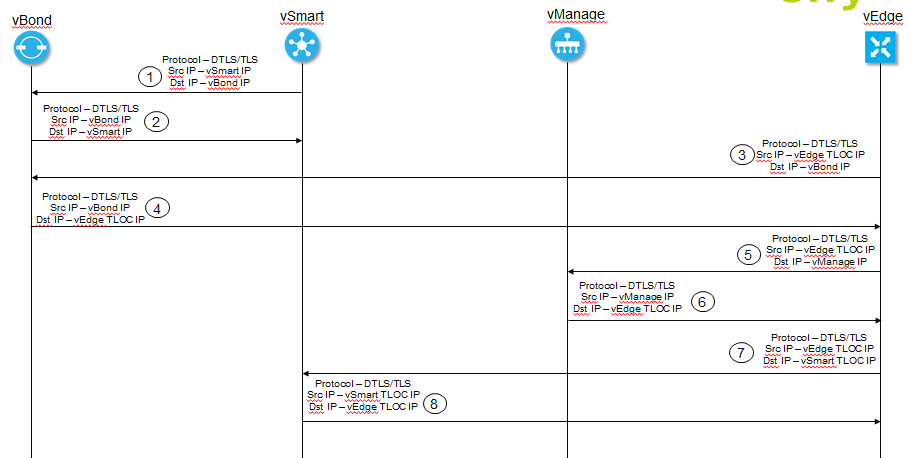
Post reboot successful IKE is established towards the controller and establishes Versa-private BGP and downloads routing information and ipsec sa about the connected topology and the Controller advertises this node’s details to other devices via bgp update

VD establishes a permanent Netconf based session with the CPE

* **Viptela:**

In Viptela based solution the ZTP happens with Vbond which initimates, vSmart about a new node turn up and vManage

* vEdge knows details about vBond in local configuration – IP address or domain name of vBond
* Two-way authentication process, initiated by vEdge
* Serial number (extracted from vEdge authorized list), organization name (extracted from certificate) and challenging handshake are used for mutual authentication process
* Temporary DTLS connection is established between vEdge and vBond
* Success authentication causes vBond to send below details vEdge
  + Serial number and IP address of vSmart(s) in the domain
* Success authentication causes vBond to send below details vSmart
  + Announce new vEdge is entered in the domain
* DTLS connection is tear down once vEdge starts direct session with vManage and vSmart



Post successful validation a permanent DTLS session is established with vSmart and vManage nodes which triggers OMP update between edge and vSmart carrying service side prefixes, tloc and ipsec sa details. vSmart advertises these OMP details to other vEdge and vSmart in the domain

* Encrypted VPN– SD-WAN enables any-to-any, IKE-less and route-based IPSEC VPN between SD-WAN edges. SD-WAN support standard IPSEC protocols such as ESP and AH to provide encryption, authentication and integrity of data packets between SD-WAN edge devices. Support of standard IPSEC parameters including AES-256 bit encryption, SHA-1/SHA-2 based integrity is supported. Support of flexible IPSEC VPN topology based on business application needs can be defined (full mesh, hub and spoke, partial mesh). In case, encryption is not required between SD-WAN edge devices, this can be disabled and replaced with VXLAN encapsulation.
* **Effective WAN path selection** – SD-WAN enables effective utilization of all available paths between two SD-WAN edge devices. Supports per-packet and per-flow based traffic load balancing.

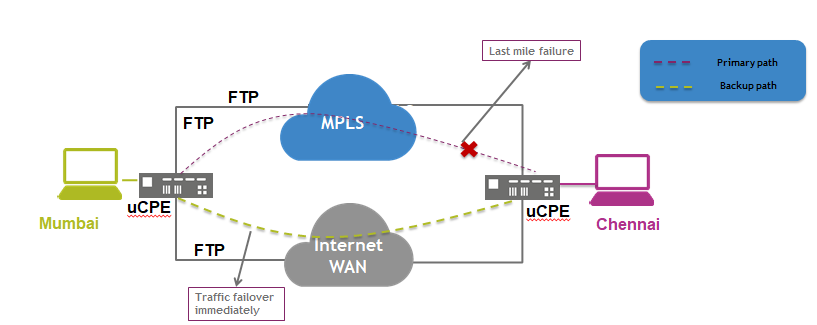
***Note****: Per packet load balancing is only support in Versa.*

* **Network performance measurement** – SD-WAN measures the network performance end to end across all available paths between 2 sites over all available underlay transport networks. This metrics are used to identify the best possible path and route traffic end to end between two SD-WAN sites. Supported metrics include
  + forward and reverse delay measurement,
  + forward and reverse drop rate,
  + delay variation (jitter)
  + mean opinion score (MOS)(only in Versa)

\*\*\*Versa uses Y.1731-modified variant for performance monitoring and default poll interval is 2s and loss threshold time is 3 this means it waits for 6 seconds to declare a wan path non-sla compliant and also relies on re-compute interval for reliability.

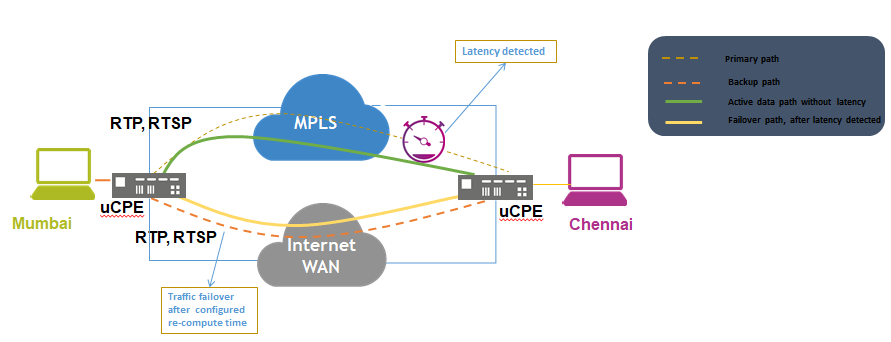
\*\*\*Viptela uses custom BFD for performance measurement by default, the poll interval is 10 minutes. With the default BFD Hello packet interval at 1 second, this means that information from about 600 BFD Hello packets is used in one poll interval to calculate loss, latency, and jitter for the tunnel. The poll interval is user-configurable

**App-Aware routing- Blackout scenario**



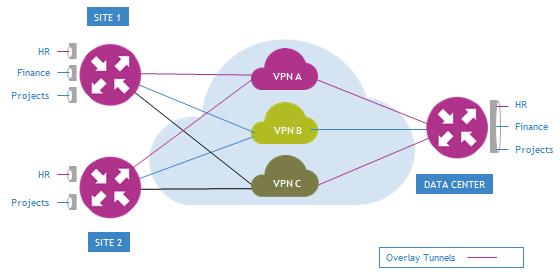
* Customer’s traffic is benefited from traditional brownout scenario where traffic once traversing through MPLS link fails, then the session gets disconnected as the end user application has to re-initiate the session to the remote host
* SDWAN enhances this failure scenario by maintaining the session table within the box, which seamlessly fails over the traffic to the next best available path without the Application traffic getting affected
* Post recovery of the primary path the traffic is preempted back to the active link without any manual intervention

**App-Aware routing- Brownout scenario**



* In traditional WAN network, MSP’s and customer’s use IP-SLA’s to detect path failure for any SLA measurement and trigger a reactive step using EEM. But this scenario has a drawback with some amount of manual intervention required to revert the traffic to the primary link after the performance has improved, this causes a lot of manual time to understand the log pattern and take reactive steps.
* With the SDWAN now the similar behavior is achieved in a more enhanced way by CPE’s automatically enabled for full-mesh or HUB-SPOKE SLA measurement model as per the network design
* Now traffic is shifted to the next best available path based on the configured SLA value in the sdwan policy framework which is based on the following parameters like loss, latency, Jitter and interface bandwidth utilization(rx/tx)
* SDWAN CPE detects the failure in the path performance and shifts the traffic intelligently and also detects flaps to understand if it’s intermittent loss or active loss with features like SLA dampening and re-compute time and steers the traffic back to original path after performance is improved on primary path

**End-End VPN Segmentation**



* VPN segmentation is done on SDWAN Overlay network, requires no additional configurations/resource allocations on underlay transport network for adding new VRFs.
* This significantly reduces the complexity when compared with traditional MPLS network where new Vlans/VRFs need to be provisioned on MPLS PE routers as well.
* VPN Segmentation enables segregation of different business traffic within the same organization CPE, restricting communications with each other.
* No configuration required in the underlay network for adding VPN Segments
* Different topologies available for every VPN segment Example:
* Voice and video (full-mesh)
* HR (hub-and-spoke)
* Finance(Hub n Spoke)
* BYOD
* Guest WIFI

Customer’s such as service aggregators who buy bulk bandwidth pipe from Service providers and provide managed network services to cater their customers e.g. DC customer’s and other enterprise businesses

* **Application centric and policy driven WAN (app aware routing)** – SD-WAN has in-built DPI engine across all SD-WAN edges. Any application being accessed is identified using DPI engine including app and sub-apps. Once apps are discovered, SD-WAN provides a mechanism of defining policy to determine the desirable network performance metrics of apps and selects the best path based on measured network performance, security and business needs.

***Note****: Home grown and custom application will be identified using TCP/UDP Port numbers, currently Versa supports custom app identification using port numbers, this feature is in roadmap for Viptela.*

* **Cloud centric (IaaS and SaaS)** – SD-WAN solution supports applications hosted on cloud including IaaS (public and private clouds - AWS) and SaaS (O365, Skype, Salesforce etc)
  1. For IaaS, SD-WAN supports instantiating SD-WAN edge devices in AWS VNF and configure as gateway for workloads in cloud
  2. For SaaS, SD-WAN computes QoE value (Quality of experience) of SaaS applications using custom HTTP ping probes across available paths and selects the best path **(Available only in Viptela)**
* **Routing** – SD-WAN supports traditional routing protocol like OSPF, BGP and static. This can be configured to operate with traditional routing devices on LAN and WAN side during transitioning of traditional WAN design to SD-WAN design.
* **LAN –** Supports traditional technologies such as configuring SD-WAN edges as DHCP server/client/helper, VRRP to support two edge devices configured for high availability.
* **Direct Internet Access**

Traditional networks require the Internet traffic from Spokes to breakout to internet via secure access via the HUB/DC firewall, this design has a drawback with both the HUB and spoke internet Bandwidth getting consumed. SDWAN solution supports both format of Internet breakout i.e.

1. Local Internet breakout
2. Secure Internet breakout( Zscalar, Managed URL proxy by Sify)

Customer benefits of having branch specific security policies for filtering outside threats and at the same time regular browsing traffic can exit locally with optional parameter to enable URL filtering locally or customer can subscribe to Industry standard URL proxy solutions for secure breakout

* **NAT** – Local internet break-out, static and dynamic translation, one to one, many to one, local inbound port forwarding and full cone NAT.
* **Security –** SD-WAN natively supports encrypted transport across overlay fabric between two SD-WAN edge devices. Encryption is using IPSEC standard headers including ESP and AH. In addition to encrypted VPN, below are additional security features supported:

1. **Statefull firewall**:-
   * + The statefull firewall provides a mechanism to enable full visibility of the traffic that traverses through the firewall and also enforces fine grain access control on the traffic.
     + To classify the traffic, the statefull firewall verifies its destination port and then tracks the state of the traffic and monitors every interaction of each connection until it is closed.
     + The statefull firewall grants or rejects access based not only on port and protocol but also on the packets history in the state table. When statefull firewall receives a packet it checks the state table for an established connection or for a request for the incoming packet from an internal host. If nothing is found then  the packets access is subject to the access policy rule

**Classification types**

Each security access policy comprises of one or more rules and each rule consists of match criteria and the enforcement action. Use one or more of these traffic attributes to specify the match criteria:

* + - 1. Source Zone
      2. Destination Zone
      3. Source Address
      4. Destination Address
      5. IP Headers
      6. Services (based on port/protocol)
      7. Time of Day
* A rule is considered a match when all match criteria’s defined in the rule matches. All rules in the security access policy are evaluated in a top-down order. The first rule that matches is selected and the corresponding security actions are enforced.

**Action**

* + - Allow—Allows the sessions matching the configured rule to pass.
    - Deny—Drops the sessions matching the rule.
    - Reject—Drops the session and sends the RST packet for a TCP session and ICMP port unreachable packet for a UDP session.

1. **DOS Protection**

A Dos protection profile provides detailed control for Denial of Service (DoS) protection policies. A DoS protection profile specifies the threshold rate of incoming packets and the action the firewall takes to protect against the DoS attack. The DoS protection profile is attached to the DoS protection policy rule which establishes the matching criteria for packets that are subject to Deny, Allow, or Protect actions.

A DoS policy allows you to control the number of sessions between interfaces, zones, addresses and region. You can configure the DDoS protection profile to define the flood thresholds for these protocols:

* TCP
* UDP
* ICMP
* Other IP
* SCTP
* ICMPv6

The DoS protection profile specifies:

1. Maximum number of sessions.
2. Profile Type—Aggregate or Classified
3. Classification Key—this is defined for a classified profile. You can specify one of these as the classification key:
4. Source IP Address
5. Destination IP Address
6. Source and Destination port numbers (TCP/UDP)

Set the classification key to source and destination IP address to monitor the thresholds based on a per-source and destination IP address basis. The rate at which packets are received is tracked per-protocol, per-source-and-destination-IP-address.

Use Classified DoS profile to defend against DDoS attacks targeted against specific endpoint hosts, based on the destination IP address or to narrow down the source of the DDoS traffic to a few source IP addresses

1. **Next-Gen Firewall**
   1. The Next Generation Firewall (NGFW) policy includes all the match criteria of a Statefull Firewall policy in addition to Layer 7 match criteria like application and URL category and assign an action on them based on the match condition
   2. The application for a session is automatically determined based on various identification methods like applying signatures, heuristics, statistical identification, etc
   3. Versa NGFW supports more than 2600 predefined applications and 83 predefined URL categories, as well as custom applications and custom URL categories
   4. NGFW policy rules can be created based on predefined and/or custom application/URL categories

In addition to providing L7 filtering options for web and application based traffic, these are the broad classification of features supported under Nextgen Firewall:

1. ***URL Filtering*** –

Filter Internet or Intranet browsing control using the following parameters

* 1. Pre-defined
  2. Custom URL type creation or white-listing/blacklisting URL’s
  3. URL-Reputation based filtering

1. ***IP Filtering****-*
2. When traffic passes through the network there is a huge possibility of certain IP addresses are associated with bad reputation and may cause security risk to your network. Versa Firewall provides IP filtering to control IP traffic based on its attributes like IP reputation and geo-location.  This ensures that the traffic that passes through the Versa Security gateway blocks all such bad reputation IP addresses as part of the IP filtering inspection and policy enforcement.
3. IP filtering based on reputation associated with IP address and its geolocation.
4. The Versa FlexVNF software provides capability to enforce filtering of traffic based on IP Address metadata (Geo-Location) and IP Reputation. Versa provides IP Reputation feed that is updated both daily, and real time. You can also additionally populate the IP Filtering Profile with blacklists and/or whitelists of IP Addresses by the user

* Versa provides a list of predefined IP reputation based on which you can block predetermined bad reputed IP traffic.

These are Pre-defined IP based filtering profiles:

1. Block DoS.
2. Block Bad Traffic.
3. Block Bots.
4. Block Scanners.
5. Block Spam.
6. Block Windows Exploits.
7. Web Protection
8. ***Http/HTTPS Proxy****-*

SDWAN CPE inspects the HTTPS traffic without decrypting the connections. Even though the HTTP content of an HTTPS session is encrypted, the SSL certificate is transmitted without encryption. Versa FlexVNF provides the ability to inspect the various attributes of the SSL certificate and enforce policy based on the inspection

There are 2 types of Decryption types

* 1. SSL Forward Proxy

This is a transparent proxy that can decrypt and encrypt the SSL/TLS traffic between the client and the server. This is a transparent proxy and neither the client nor the server would know about the proxy’s presence. The Proxy acts as server towards the client and as a client towards the server.

* 1. SSL Full Proxy

*This proxy service works in 2 modes*:-

***Explicit***:-This processes the SSL/TLS traffic destined to a particular IP address and a port. End user must configure the clients with the proxy IP and the port as that of the SDWAN CPE

* + - 1. The Client connects to the configured proxy IP and port and sends HTTP CONNECT request.
      2. The SSL full proxy parses the received HTTP CONNECT and extracts the domain that the client wants to connect to. It uses that along with relevant L3/L4 parameters to find a decryption policy, if it finds a decryption policy, based on the action set in that policy the SSL connection will either be decrypted or bypassed. If there is no policy configured then, the decryption will be bypassed.
      3. The SSL full proxy responds with 200 OK to the CONNECT and waits to the Client Hello. Upon receiving the Client Hello, if the policy decision was to decrypt, the SSL proxy will respond with Server Hello and the rest of the handshake message get exchanged between the client and the proxy.
      4. After the handshake is complete, the client does a GET or a POST on that connection.
      5. The proxy parses the HTTP request and extracts the domain name and port from the URL and does DNS resolution of that domain and opens a connection towards the resolved IP, it uses the source IP and port from the configured SNAT pool from the HTTPs proxy profile.
      6. Once the connection is successful, the proxy initiates the SSL handshake with the server, after that it forwards the HTTP request to the server.
      7. All the other services in the service chain like IPS/IDS, AV get to examine the decrypted stream for any threats and may drop the packet based on the outcome of their examination.

***Transparent****:-* This processes the SSL/TLS traffic designated to any IP but to a particular port. The DNS resolution happens at the client and the client opens the connection to the actual server IP. The same steps as explained above for the explicit proxy are applicable to transparent proxy as well, except for the DNS resolution. Since the destination IP is that of the actual server, the proxy skips the DNS resolution. It just does the source NAT using the configured SNAT pool in the HTTPS proxy profile.

1. ***UTM***

Versa includes unified threat management capabilities, which can be turned on by configuring the threat profiles in the Next Generation Firewall (NGFW) policy rules. FlexVNF supports the following threat profiles:

1. Anti-Virus
2. Vulnerability (IDS/IPS)
   * + 1. ***Anti-Virus***

Versa has a built-in antivirus engine to scan the live traffic. The antivirus engine waits till the last byte of the file is received and then process entire file at runtime. You must configure at least one antivirus profile to enable scanning of files for viruses

To scan the files for virus, you must configure the antivirus profile to extract files on certain protocols in a specific file transfer direction.

* + - * 1. Based on protocols like http, ftp, smtp, imap, pop3, MAPI
        2. Virus scanning based on various file types

The anti-virus profile follows these rules while scanning files for virus:

* + - * 1. If the file type of the extracted file matches one of the configured file types in the antivirus profile then the entire file is extracted and buffered in Versa FlexVNF.
        2. If the file type does not match any of the configured file types then the file extraction is aborted.
        3. If the file size is less than 512KB then the file is buffered in memory.
        4. If the file size exceeds 512KB or if there is not enough RAM available then the file is stored in either the hard disk or the RAM disk depending on the configured storage profile settings.

When a file is extracted and buffered (to either RAM or storage), the file data is forwarded to the destination except for the last data packet. A virus scan is performed on the entire file after the entire file is received and buffered in Versa FlexVNF. If the file contains a virus, then the policy action is enforced on the packet/session based on the configured action of the antivirus profile. If no virus is detected, the last packet held by Versa FlexVNF is forwarded to the destination.

* + - 1. ***IDS / IPS***

Versa’s IDS/IPS solution is Integrated solution with detection of network anomalies based on various threat vectors detected over the recent years including various APT based attacks, customer gets the benefit of turning on this feature to enhance network security over various threat landscapes.

Vulnerability profile provides a list of pre-defined vulnerabilities based on which network scan’s for vulnerabilities, all these profiles gets constant update using SPACK(service pack update)

Provisioning of IDS/IPS rules can be done based on predefined list of vulnerability criteria which contains various types of match conditions based on different attack levels as listed below:

* All Anomaly Rules—This profile loads all the anomaly signatures.
* All Attack Rules— This profile loads all attack signatures.
* Client Protection— This profile loads all client-side attack detections.
* Database Profile—This profile loads the oracle database server vulnerability signatures.
* ICS Profile—This profile loads the Industrial Control System (ICS) vulnerability signatures.
* Linux OS Profile—This profile detects all attacks specific to Linux OS.
* MAC OS Profile—This profile detects all attacks specific to MAC OS.
* Malware Profile—This profile detects all antivirus attacks.
* Server Protection—This profile  detects server side attack detections.
* Windows OS Profile—This profile detects attacks attacks specific to all windows OS.
* Versa Recommended Profile

Additionally user can create own Vulnerability rule matching various threat identifiers for a given vulnerability profile, based on these criteria:

* Year
* Rule Set
* Severity
* Reference
* Confidence
* Classification Type
* Rule Type
* Rule Default Action
* Direction
* CVSS Score
* OS
* OS Version
* Product
* Product Version
* Application

And based on the rules mentioned, enforcement actions can be defined like Rule default action,Allow,Alert,Drop PacketDrop Session,Reject,Reset Client,Reset Server, Packet Capture

***Note****: These are versa specific features; a separate firewall components to be built centrally to support this features in Viptela.*

* **Quality of service –** supports quality of service on WAN ports on SD-WAN edges
  1. Classification – IP precedence and DSCP based, 5 tuple based [src ip, dst ip, src port, dst port, protocol], application based
  2. Re-Marking – IP precedence and DSCP
  3. Scheduling – scheduling based on bandwidth percentage
  4. APP-QOS
  5. Adaptive QOS- Congestion management ( Versa only)
* **WAN optimization** – Supports optimization functionalities on the usage of WAN bandwidth and mitigates network performance degrade including
  1. TCP optimization – configure SD-WAN edges as TCP proxy between client and server and increase TCP performance
  2. FEC – To recover lost packets over lossy transports\* effective only for media related loss. This can give protection only over a configured window interval of 4(recommended) which implies out of 4 if 1 packet is lost it can be recovered. **(Consider Engineering recommendation before proposing to customer)**
  3. Packet replication and packet striping – Duplicate incoming packets and replicate them on all available WAN paths, This method is used to overcome lossy transport paths and avoid out of order delivery of packets
  4. Full-fledged WAN optimization functionalities like packet de-duplication, caching, compression are not supported(Versa/Viptela)
* **High availability –** SD-WAN services support high availability on control plane components and data plane components. Control plane components are deployed and managed centrally in geo-redundant regions of Sify. Data plane HA includes deploying 2 SD-WAN edges in a site using VRRP on LAN.
* **Configuration management –** Configuration management of SD-WAN services reside on central management plane component supporting below:
  1. zero touch provisioning (ZTP) using device authentication and multi-factor authentication for SD-WAN edge on-boarding to VPN
  2. template based configuration of SD-WAN edges, with site specific variables to configure WAN, LAN, VPN and other features
  3. configuration backup of SD-WAN edges
  4. configuration changes lock and device changes lock
* **In-depth visibility and analytics of network and application performance** – SD-WAN CPE are exporting traffic and application flows to central analytics component. This analytics makes use of big data technology to gather all flows and provides contextual analysis in terms of network and application performance.
* **Multi-tenancy –** This is a functionality which is benefiting MSP like Sify. This function enables Sify to manage multiple enterprise WAN networks using a common configuration, management and analytics components deployed in central location. Each enterprise is identified as a tenant and managed independently though use of common network resources (IP address of WAN and LAN) can be the same.
* **Single pane of glass for management –** SD-WAN enables complete management of enterprise WAN network on a single pane of glass. This is common for both Sify MS-NOC resources and enterprise users. End to end lifecycle process including configuration, monitoring, analytics; inventory of enterprise WAN network can be managed through this common portal.

Below are the feature matrix of Viptela and Versa:

|  |  |  |
| --- | --- | --- |
| Parameters | Viptela SD-WAN | Versa SD-WAN |
| Transport type support | MPLS VPN, Internet, DSL, 4G/LTE (to be tested) | MPLS VPN, Internet, 4G/LTE (to be tested) |
| Encrypted VPN | Secure DTLS, TLS  Encryption: AES-256  Authentication: ah-sha1-hmac, sha1-hmac, | Encryption: 3DES, AES128, AES256  Authentication: MD5, SHA1, SHA256, SHA384,SHA512 |
| ZTP | ZTP with certificate based authentication [PKI] | * ZTP with certificate based authentication [PKI] and URL based authentication * Multi-factor authentication – SMS and e-mail |
| Path selection | * Per flow * ECMP and non-ECMP | * Per flow, per packet * ECMP and non-ECMP |
| Network performance | Synthetic probes (BFD) - Latency, loss and jitter | Synthetic probes (Y1731) – latency, loss and jitter  In-line loss (Data plane loss) |
| App identification | DPI and cFlowd support  App and sub-app support of 2500 apps  Custom app fingerprinting – not supported | DPI  App and sub-app support of 3000 apps  Custom app fingerprinting supported |
| App aware routing | Supported, define SLA class and map to application, selection of path based on complied SLA path per application | Supported, define SLA class and map to application, selection of path based on complied SLA path per application |
| Cloud support | Supported in AWS  Supports measurement of vQoE of SaaS apps | Supported in AWS |
| Routing | Supports OSPF, BGP and static on LAN and WAN interface | Supports OSPF, BGP and static on LAN interface |
| LAN technologies | VRRP – master, slave, priority, tracking of WAN link  DHCP client, server and relay | VRRP – master, slave, priority, tracking of WAN link  DHCP client, server and relay |
| NAT | * NAT on WAN interface – static and dynamic, one to one, many to one * NAT on LAN interface – static and dynamic, one to one, many to one * Supports NAT traversal | * CGNAT – one to one, many to one, static and dynamic NAT pools * Supports NAT traversal |
| Port forwarding | Supported | NA |
| Security | Integration with Cisco Umbrella  Statefull Firewall(Roadmap), URL-Filtering | URL filtering  Statefull firewall  Anti-virus/anti-malware  IDS/IPS  SSL inspection and decryption |
| Quality of service | * Classification – 5 tuple (src/dst IP and port, protocol), application, IP PREC, DSCP * Scheduling – bandwidth percentage with WFQ * Congestion avoidance – tail drop, RED * Policing – single rate two color * Hierarchical shaping – parent and child classes | * Classification – 5 tuple (src/dst IP and port, protocol), application, IP PREC, DSCP * Scheduling – bandwidth percentage with WFQ * Congestion avoidance – tail drop, RED * Policing – single rate two color * Hierarchical shaping – parent and child classes |
| Optimization | * TCP optimization (on vEdge 1000 and vEdge 2000 platforms only) | * FEC * Packet cloning and striping * External Riverbed Service Chaining |
| IKEv1/IKEv2 with 3rd party devices | Supports IKEv1 and IKEv2. Tested with Cisco, Fortinet and HPE | Supports IKEv1 and IKEv2. Tested with Cisco, Fortinet and HPE |
| Multicast VPN | Supported – PIM sparse mode, auto-RP | In Product roadmap |
| CPE | vEdge as physical appliance, as supplied by Viptela  vEdge cloud as VM – supported on ESXi and KVM | FlexVNF as physical appliance, as supplied by Versa certified ODM  Direct ODM x86 appliance supported  FlexVNF as VM – supported on ESXi and KVM |
| CPE Mode | Routing, bridging | Routing, bridging and tap (mirroring] |
| Local internet breakout | Supported | Supported |
| SD-WAN gateway | * vEdge as SD-WAN gateway. * Deploy non-SD-WAN sites on service side and SD-WAN sides on transport side | * FlexVNF as SD-WAN gateway. Supported BGP/MP-BGP in exchanging prefixes from non-SD-WAN sites and exchanges with SD-WAN sites. * Configure two different VRF which part of SD-WAN and non-SD-WAN respectively. * Route-leaking with SD-WAN gateway as next-hop to enable communication between disparate underlay and SD-WAN and non-SD-WAN sites |
| High availability | Control components HA;   * vSmart – Active-Active * vBond – Active-Active * vManage – Active-Active   2 x vEdges on site – Active-Active, Active-Standby | Control components HA:   * Versa Controller – Active-Active * Versa Director – Active-Standby * Versa Analytics – Active-Active   2xFlexVNF on site – Active-Active, Active-Standby |

## Sify Managed services

Below table lists functionalities and description related to managed SD-WAN services:

* Monitoring & reporting
* Configuration management
* Incident management
* Problem management
* Performance management
* Change management
* Inventory management
* Vendor management
* Provider governance
* Helpdesk
* SLA reporting
* Implementation services
* Transition services

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Functionality | | | | | Description | |
| Monitoring & Reporting |  | | |  | * 24x7 pro-active monitoring of network, user and application related metrics and reporting on common dashboard and metric specific dashboard * Ability to view real-time and historic reporting | |
| Configuration management |  | | |  | * Archiving of current configuration of SD-WAN edges, controller, ZTP server, manager and analytics * Configuration audit for compliance | |
| Incident management |  | | |  | * Ticketing – customers can use Sify aakaash as single portal for managing incidents. Sify MS-NOC manages logs and record actions taken on the ticketing tool in aakaash * MS-NOC prepares RCA for incidents raised by customer and on-request * Fault and performance management – this would based on logs, events and data retrieved from central components | |
| Change management |  | |  |  | | * MS-NOC manages all changes to be executed in customer WAN – MACD based on requests from customer and proactively * Changes are carried out on online module in aakaash * Customer would be providing approval for every change based on detailed POA prepared by MS-NOC |
| Inventory management |  | |  |  | | * Managing inventory of customer devices within the scope of managed SD-WAN services – network wide and site wide * Managing logical resource of customer network – IP address (WAN and LAN), VLAN, customer site contact information details etc |
| Vendor management | |  | |  | * MS-NOC co-ordinates with SD-WAN vendors to work on issues related to managed SD-WAN services | |
| Provider governance | |  | |  | * MS-NOC owns the complete transport provider lifecycle management. This includes identifying transport providers in each customer site, coordinating with transport providers for any issues | |
| Implementation and transition services | |  | |  | * This is covered as separate section – Section 7 service engagement model | |
| SLA reporting | | | |  | * Sify MS-NOC is the single owner for all enterprise network connectivity of managed SD-WAN services. Sify aakaash is the common portal for managing end to end SLA between SD-WAN edges which includes transport network, hardware and software, central component etc | |

## Transport connectivity

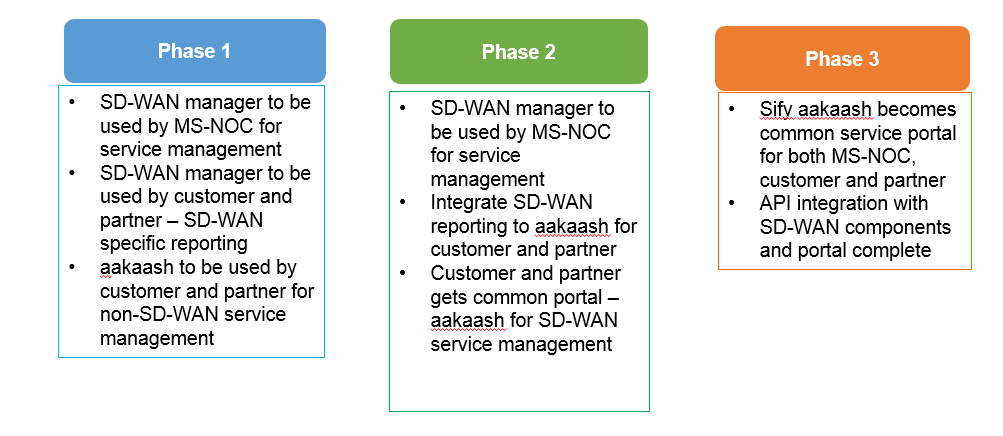
Transport connectivity enables inter-communication across SD-WAN edges, between SD-WAN edges and control components and between control components. Transport can be of any type – MPLS VPN, Internet, DSL and 4G/LTE. MPLS transport can be from multiple providers. Sify as part of managed SD-WAN services manages transport networks of all types and from multiple providers. As soon as SD-WAN edges are shipped and installed in customer premise, it will be connected to one of available transport network to start communicating with control components.

# Service delivery model

This section explains how managed SD-WAN services are delivered. Delivery model consists of how services are delivered internally by Sify team (MS-NOC) and externally to customers. End state of service model makes use of Sify aakaash by both Sify MS-NOC, customers and partners. This requires API integration of all SD-WAN components with sify aakaash service portal. This model is common to both Viptela and Versa based managed SD-WAN services.

Service delivery model is divided into three phases as below:

(Roadmap)



Phase 1 (Day1):

* This is the initial phase of managed SD-WAN service delivery
* Sify MS-NOC uses SD-WAN vendor based Manager and Analytics platform for configuration, fault, performance and inventory management
* Customer and partner are given access to SD-WAN vendor based platforms for SD-WAN specific reporting
* Customer and partner are given access to Sify aakaash for service management including incident, problem, helpdesk, inventory and other managed services

Phase 2:

* This is the second phase of managed SD-WAN service delivery
* Sify MS-NOC uses SD-WAN vendor based Manager and Analytics platform for configuration, fault, performance and inventory management
* Reporting from SD-WAN vendor based Manager and Analytics are integrated with aakaash through API
* Customer and partner are given access to sify aakaash as common portal for complete managed SD-WAN service management

Phase 3:

* This is the third and final phase of managed SD-WAN service delivery
* SD-WAN vendor based Manager and Analytics platform are integrated with Sify aakaash for complete service management including functionalities as required by MS-NOC
* Sify aakaash becomes a single console used by MS-NOC, customer and portal for complete managed SD-WAN service management **(Roadmap)**

# Deployment work flow

Managed SD-WAN services working can be divided into the following phases:

## Deploy SD-WAN edges

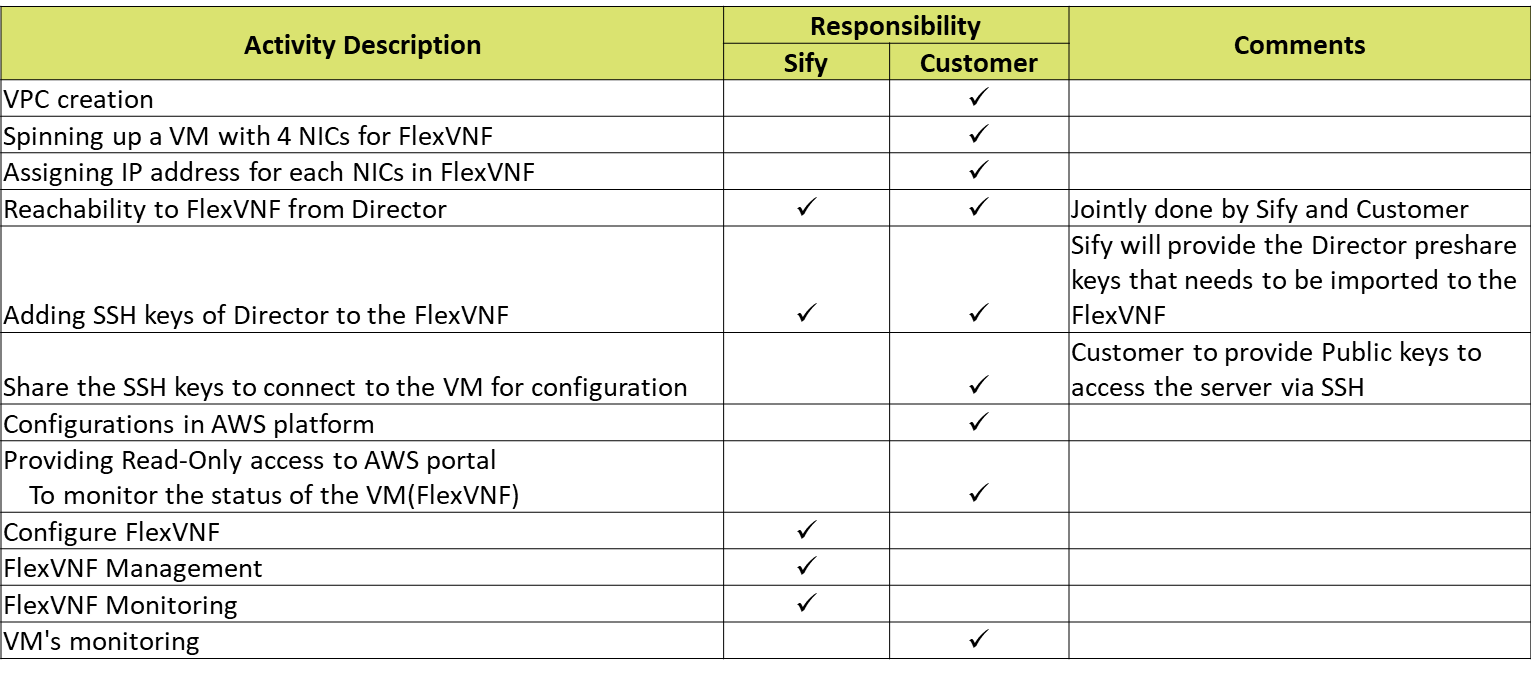
SD-WAN edges are customer premise equipment which is deployed in customer branches including hub, spokes, DC, DR, private cloud and public cloud (AWS). SD-WAN edges are shipped to customer locations with following minimal configuration called staging, below would be the process,

* Deploy SD-WAN edges as hardware box/Virtual machines

Note: *ZTP script Varies for Versa and Viptela, RSDE will be provided with both the scripts.*

* Deploy SDWAN Edges on Cloud (AWS only)

**SDWAN Cloud CPE responsibility matrix**



## ZTP

Below are the processes when a new tenant is on-boarded on control components:

* Create authorized serial-number (and chassis number in case of Viptela) on Controller, Manager and ZTP server. This serves as authorized SD-WAN edges which are allowed to be on-boarded on a tenant network
* Installation of certificates as required on all control components – Viptela
* Once SD-WAN edges establish communication and authenticates itself with ZTP server, controller and manager, then controller establishes control plane session and manager pushes relevant configuration of SD-WAN edge (as per initial template based configuration)

## Transport connectivity

Transport connectivity enables inter-communication across SD-WAN edges, between SD-WAN edges and control components and between control components. Transport can be of any type – MPLS VPN, Internet, DSL and 4G/LTE (sim/dongle based). MPLS transport can be from multiple providers. Sify as part of managed SD-WAN services manages transport networks of all types and from multiple providers. As soon as SD-WAN edges are shipped and installed in customer premise, it will be connected to one of available transport network to start communicating with control components.

*Note: Sify MPLS Transport and internet is the preferred Model.*

## Configure WAN policies

Once SD-WAN edges retrieve configuration from central manager and controller, WAN policies specific to branches can be configured and pushed to all SD-WAN edges. This can include the following:

* Define network SLA parameters – latency, loss, jitter
* Define application class – applications and sub-application, application family
* Define application aware routing – define desired SLA parameters for identified applications
* Security – functionalities include Statefull/NextGen Firewall, URL filtering, IDS/IPS, anti-virus etc.(Only Versa if local breakout required)
* High availability – VRRP within LAN
* Routing – OSPF and BGP on LAN and WAN side

## Service management

This is the final phase of managed SD-WAN services. Sify aakaash is the service management portal of Sify managed SD-WAN services. This is the portal which will be used by customers of Sify managed SD-WAN services for complete lifecycle service management. Service management layer integrates with central control components of SD-WAN to gather relevant information like FCAPS and integrates with billing systems. Service management includes the following functionalities:

* Incident and problem management
* Ticketing
* Configuration management
* Asset management
* Change management
* Fault and performance management
* SLA management

# Central control component design

Sify MS-NOC will setup a central infrastructure on geo-redundant locations to deploy and manage central components of managed SD-WAN services. Central components are multi-tenant capable (as applicable), wherein each tenant on-boarding would require enablement of tenant specific configuration in central components. Wherever the central component is only supporting single-tenant, then a new instance of central component would be instantiated and integrated with other central components of the tenant (connectivity specific to tenants).

Central component of managed SD-WAN services consists of the following:

* SD-WAN ZTP server
* SD-WAN controller
* SD-WAN Manager
* SD-WAN analytics
* Service portal

Below are the equivalent terminology of Viptela and Versa against Sify’s terminology and multi-tenant capability:

|  |  |  |  |
| --- | --- | --- | --- |
| Sify SD-WAN parameter | Viptela SD-WAN |  | Versa SD-WAN |
| SD-WAN ZTP server | vBond, multi-tenant |  | Versa Controller, single-tenant |
| SD-WAN controller | vSmart, single-tenant |  | Versa Controller, multi-tenant |
| SD-WAN Manager | vManage, multi-tenant |  | Versa Director, multi-tenant |
| SD-WAN analytics | vAnalytics, multi-tenant |  | Versa Analytics, multi-tenant |
| Service portal | Sify aakaash, multi-tenant |  | Sify aakaash, multi-tenant |

Deployment and delivery of central components to tenants of managed SD-WAN services varies between Viptela and Versa. Sify supports the below three deployment model of central components:

* **Model 1 - Sify cloud, centrally deployed for multi-tenant**
  + This is the default model of managing central components for both Viptela and Versa. Infrastructure is setup to deploy central components on day-1
  + As and when new tenants are on-boarded, tenant specific instances are created on the underlying infrastructure and connectivity to each tenant transport network is established.
  + Underlying infrastructure [compute, virtualization, storage] are managed by Sify MS-NOC
  + In Viptela case, this can be on SIFY cloud regions – Mumbai and Chennai
  + In Versa case, this is on Sify IP/MPLS cloud – Chennai and Mumbai DNS DC
* **Model 2 - Sify / AWS cloud, centrally deployed for single-tenant**
  + This model is followed when customer has specific requirement of needing dedicated instance of control component dedicated to his network and hosted in Sify cloud.
  + In this case, only when new tenant is on-boarded, respective infrastructure is setup and control components instantiated and connected to tenant transport network
  + Underlying infrastructure [compute, virtualization, storage] are managed by Sify MS-NOC
  + In Viptela case, this can be on AWS regions – Mumbai and Singapore
  + In Versa case, this is on Sify IP/MPLS cloud
* **Model 3- Customer, on-prem deployed for single-tenant**
  + This model is followed when customer has specific requirement of needing dedicated instance of control component dedicated to his network but hosted in any of their on premise location.
  + In this case, underlying infrastructure [compute, virtualization, storage and networking] would be managed by customer but instantiation and management of SD-WAN control components are managed by Sify MS-NOC
  + In Viptela case, this is not applicable
  + In Versa case, this is applicable

## Central component design – Viptela

* Sify hosted central control component design is adopted for Viptela based managed SD-WAN services
* Two regions are selected – Mumbai and Chennai to deploy central components in geo-redundant locations
* Supported model are model 1 and model 2
* Model 3 is not supported [installing in customer on-prem]

Below are the HA mode supported for Viptela central components:

|  |  |  |
| --- | --- | --- |
| Central component |  | Deployed HA mode |
| SD-WAN ZTP server – vBond |  | Active-Active, geo-redundant location |
| SD-WAN controller – vSmart |  | Active-Active, geo-redundant location |
| SD-WAN Manager – vManage |  | Active-Active, geo-redundant location |
| SD-WAN analytics - vAnalytics |  | This resides in Viptela cloud as on today. There are no two instances of vAnalytics deployed but data are consistently backed up and used to be activated in other AWS region during failure of active AWS region |
| Service portal – Sify aakaash |  | Active-Active, geo-redundant location |

1. **Sify Cloud, centrally deployed for multi-tenant**

This is the default mechanism in which all tenants of Managed SD-WAN services are delivered. Sify MS-NOC will setup vBond and vManage on multi-tenancy mode in Mumbai and Chennai. For each new tenant on-boarding, below actions are performed by MS-NOC:

* Dedicated instance (VPC) is setup in AWS Mumbai region which consists of vManage, vSmart and vBond in multi-tenant mode
* Create new tenant specific instance in vManage and install certificates
* Create new tenant specific instance in vBond and install certificates
* Bring up new instance of vSmart container
* Appropriate network connections between vBond, vSmart and vManage are configured
* SD-WAN Analytics (vAnalytics) is hosted in Viptela cloud and will be integrated with SD-WAN Manager
* Underlying infrastructure to host this central components are managed by MS-NOC with AWS support team

## Central control component design – Versa

* Versa controller plays the role of SD-WAN controller and ZTP server in Sify Managed SD-WAN service components.
* Communication between SD-WAN edges (Versa FlexVNF) and other control components (Versa Director and Versa Analytics (VAN and VSN) flows through Versa Controller, thus placed at the data path.
* Two instances of control components are deployed in geo-redundant locations of Sify – Chennai Tidel and Mumbai Airoli DC
* Dedicated infrastructure are deployed to support this control component infrastructure
* Compute, virtualization, storage and networking are managed by Sify MS-NOC
* Central control components are placed behind DNS Firewall and Router
* DNS firewall will have respective firewall policies opened, as per call-flow defined in previous section
* Routing between geo-redundant locations happen over VRF extended between DNS routers over Sify IP/MPLS

Below are the HA mode supported for Versa central components:

|  |  |  |
| --- | --- | --- |
| Central component |  | Deployed HA mode |
| SD-WAN ZTP server – Versa Controller |  | Active-Active, geo-redundant location |
| SD-WAN controller – Versa Controller |  | Active-Active, geo-redundant location |
| SD-WAN Manager – Versa Director |  | Active-Standby, geo-redundant location |
| SD-WAN analytics – Versa Analytics |  | Active-Active, geo-redundant location. Consists of two components within Analytics – Versa analytics node (VAN) and Versa Search node (VSN) |
| Service portal – Sify aakaash |  | Active-Active, geo-redundant location |

Below are available NIC in control components and its functionality:

|  |  |  |  |
| --- | --- | --- | --- |
| Control component | Production NIC | OOB NIC | Other NIC [transport NIC / internal NIC] |
| Versa Controller | * Used to communicate with Versa Director and Analytics * VD communicates to FlexVNF for configuration and monitoring through this NIC * VA communicates to FlexVNF for analytics log collection | * Default routes on this NIC for external access * Used to communicate with Versa Director and Analytics for OOB | Transport NIC   * Per tenant transport connectivity * Equal to number of transport per tenant * Each transport NIC belongs to unique VR within Versa Controller |
| Versa Director | * Used to communicate to FlexVNF. This happens through Versa Controller * Used as source to configure and monitor FlexVNF and FlexVNF PTVI5 is destination | * Default routes on this NIC for external access * Data retrieval with VD happens over this NIC * Used to communicate with Versa Controller and Analytics for OOB | NA |
| Versa Analytics Node | * Used to communicate to FlexVNF. This happens through Versa Controller * FlexVNF uses this NIC as destination IP to export logs to analytics node | * Default routes on this NIC for external access * Data retrieval with VD happens over this NIC * Used to communicate with Versa Controller and Analytics for OOB | * Used to connect to versa search node |
| Versa Search Node | * Not a mandatory NIC | * Default routes on this NIC for external access * Used to communicate with Versa analytics node | * Used to connect to versa analytics node |

**Versa Control component call-flow**

**Call-flow 1: FlexVNF to Versa Controller**

* This is the basic and critical call flow
  + Controller acts as a route reflector between FlexVNF to distribute network and policy information.
  + It acts as a central component in facilitating communication between FlexVNF and other central components [Versa Director, Versa Analytics (VAN, VSN)].
* Versa Controller has following virtual routers configured:
  + Transport VR – this is equal to number of transport per tenant networks
  + Tenant Control VR – Control VR similar to FlexVNF but specific to a tenant
  + Provider Control VR – Control VR similar to FlexVNF but global to all tenants and communicates with other control components
  + Global VR – part of OOB interface for device management purposes
  + There is no LAN VR concept in Controller
* In Versa Controller, PTVI of all FlexVNF branches are present in tenant control VR and exported to provider control VR
* From provider control VR, all PTVI of FlexVNF are exported to other control components – versa director and versa analytics
* Connectivity to DNS-Firewall in the above diagram is with provider control VR and facilitates communication to geo-redundant control components over this

**Call-flow 2: Versa Controller to Versa Director**

* Versa director has static route configured for all tenant FlexVNF PTVI interfaces towards versa controller over production NIC
* Any communication between Versa Director and FlexVNF happens over this call flow
* Versa Director pushes configuration and monitoring to FlexVNF over production NIC
* Versa Director and Versa Controller communication happens over OOB NIC – management traffic

**Call-flow 3: Versa Controller to Versa Analytics**

* Versa analytics has static route configured for all tenant FlexVNF PTVI interfaces towards versa controller over production NIC
* Any communication between Versa Analytics and FlexVNF happens over this call flow
* FlexVNF exports logs over this call flow to Versa analytics node through versa controller
* Versa Analytics and Versa Controller communication happens over OOB NIC – management traffic

**Call-flow 4: Versa analytics node to Versa search node**

* Versa search node need not have any NIC on production
* No communication happens from versa search node to other components.
* Only communication required is with versa analytics node
* Versa search node holds all data of analytics [events, logs, flows] and retrieved by versa analytics node as and when required

### Model 1 - Sify DC centrally deployed for multi-tenant

This is the default mechanism in which all tenants of Versa Managed SD-WAN services are delivered.

In Sify architecture, all the control components will be deployed in Sify Infra DC. To ensure high availability of control components, it will be deployed in 2 different locations (Chennai and Mumbai) Versa Director, Versa Analytics and controllers are deployed on Bare metal, Versa Director & Versa Analytics will be deployed in DMZ zone which is behind DC firewall. Versa controller will be deployed as CE prior to DC Firewall.

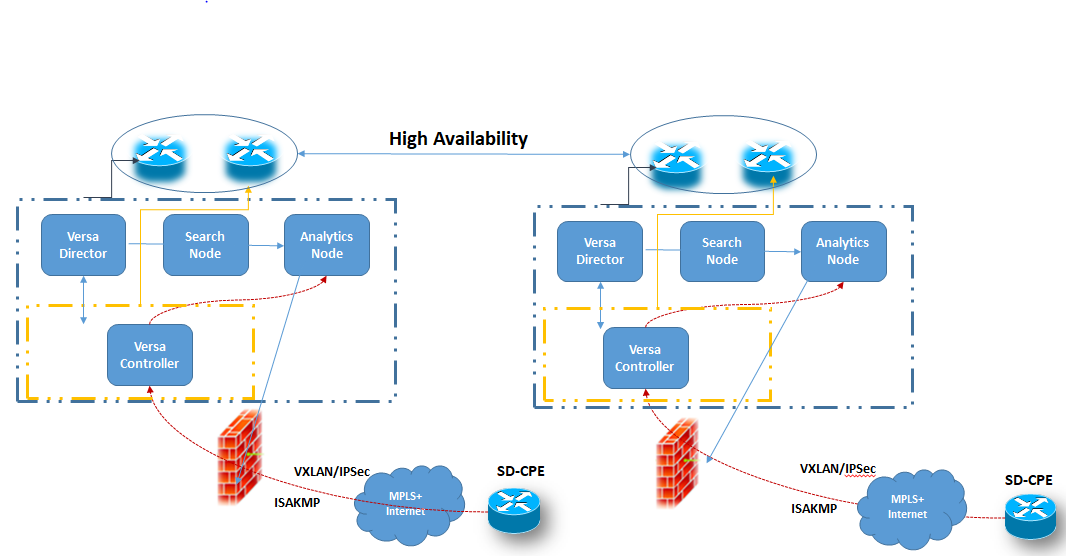
All the control components will have 2 interfaces in common; OOB / MGMT interface – used for communication within control components as well as management access, Network Control interface – used for communication between Flex-VNF and Control components, Network control interface of VC extended to VPE and run the BGP as last mile protocol for high availability. Network control interface of VD & VAN extend to FW and further extend to PE and Run static as Last mile protocol.

DC PE will be the common point for all the control components communications. DC PE will have 2 different VRF as below for Versa SD-WAN.

**SD-WAN-MPLS-VRF** – It is used to enable reachability between Flex-VNF & Controller. All the SD-WAN customers who are requesting for MPLS will be configured under this VRF.

**SD-WAN-Global** – This will be used for reachability between FlexVNF & Controller, all the cpe’s connecting via Internet will be accessed through this link.

**SD-WAN-CONTROL-VRF** – It is used for enable communication between all the control components. VD, VAN & VC network control interfaces are extend to this VRF at both locations.



**On-boarding customer**

* + - Create new tenant specific instance of Versa Controller in both Chennai and Mumbai
    - Connect newly instantiated Versa Controller to all transport networks of this new tenant
    - In Versa Director and Versa Analytics, configure respective reverse routes of new tenants towards newly instantiated versa controller
    - Routing of newly created tenant routes configured between Chennai and Mumbai DNS router over VRF
    - Respective configuration of tenant is executed on Versa Director and Versa Controller to start on-boarding FlexVNF
    - Underlying infrastructure to host these central components is managed by MS-NOC team.

### Model 2 - Customer, on-prem deployed for single-tenant

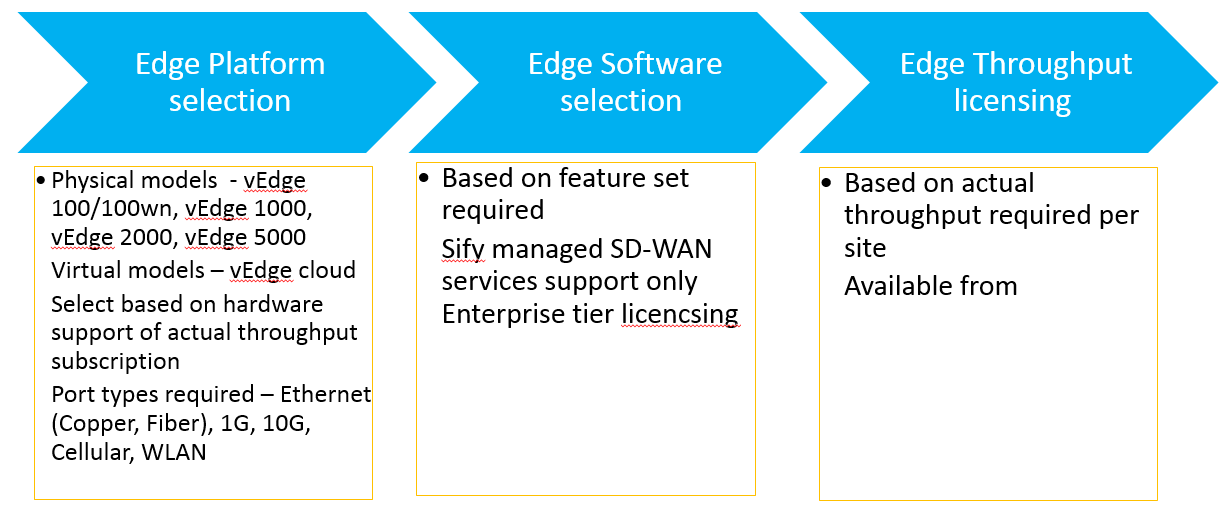
This mode is supported when customer wants to host central components of managed SD-WAN services on-prem in his DC/DR or sites for compliance and regulatory reasons. In this case, the underlying infrastructure to support central components (x86 compute, hypervisor, storage and networking) will be designed and deployed only for this specific purpose and managed by Sify MS-NOC. Below are actions performed by MS-NOC:

* Sify MS-NOC will design and deploy underlying infrastructure required to support this central components – x86 compute, hypervisor, virtual switch, networking, storage
* Dedicated infrastructure is setup in customer on-prem locations on geo-redundant locations
* Follow the design in Model 1 for this deployment.
* Bring up new instance of Versa Director, Versa Analytics [VAN, VSN] and Versa Controller on top of infrastructure [compute, virtualization, storage]
* Create respective NIC – production, OOB and internal on control components
* Connect newly instantiated versa controller to respective transport network of this new tenants
* Establish routing between control components for this teannt
* Routing of newly created tenant routes configured geo-redundant locations are managed by MS-NOC
* Respective configuration of tenant is executed on Versa Director and Versa Controller to start on-boarding FlexVNF.
* VD need at least 120GB Hard disk, 2 Socket 8Core per socket Intel Xeon 64 bit processor, 32GB RAM and 4 \* 1GE Interface.
* VA need at least 1TB Hard disk, 2 Socket 12Core per socket Intel Xeon 64 bit processor, 64GB RAM and 4 \* 1GE Interface.
* VC need at least 120 Hard disk, 1 Socket 18Core per socket Intel Xeon 64 bit processor, 8GB RAM and 4 \* 1GE Interface.

# Solution sizing, hardware and software

SD-WAN Edge platforms are CPE’s placed at each site of enterprise WAN including branch, HO, DC, DR and cloud sites. Sizing of any SDWAN solution works based on the following:

* Step 1 – Select hardware platform to support actual throughput subscription requirement at each site
* Step 2 – Select software licensing based on feature required
* Step 3 – Select throughput licensing based on actual throughput subscribed



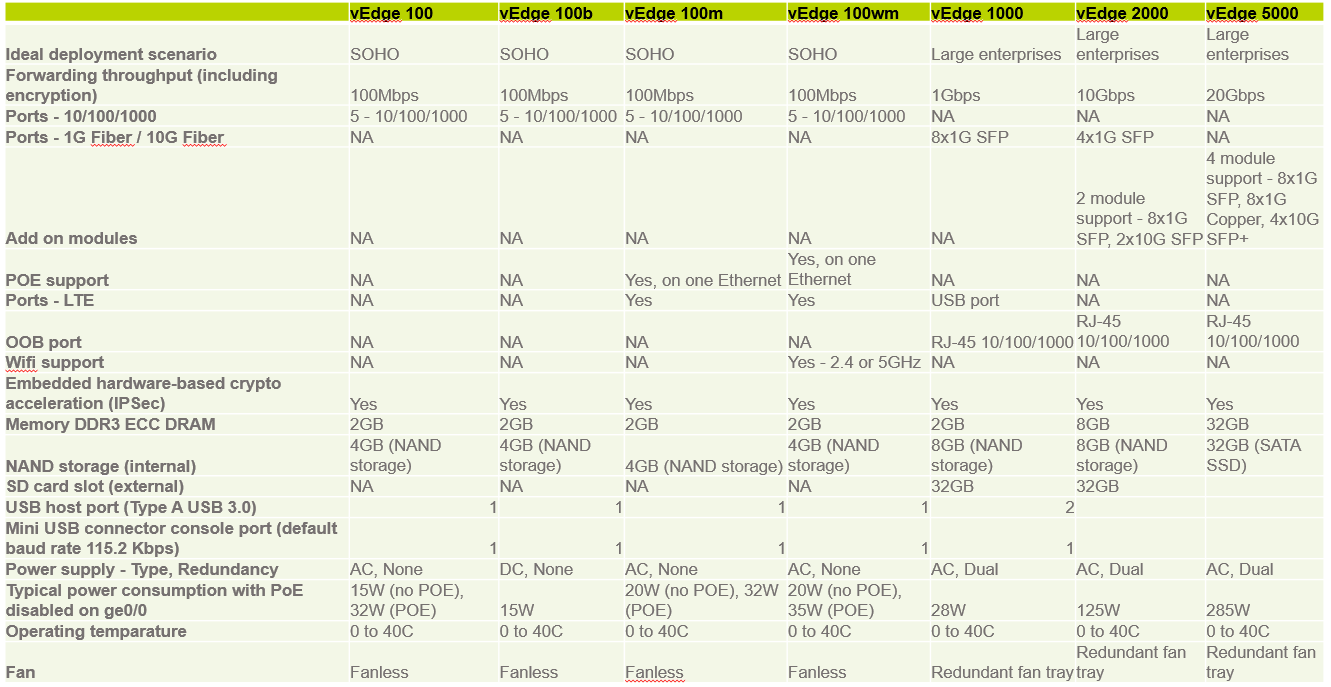
## Viptela

1. **SD-WAN vEdge platforms**

Viptela Edge routers can be deployed in 3 modes

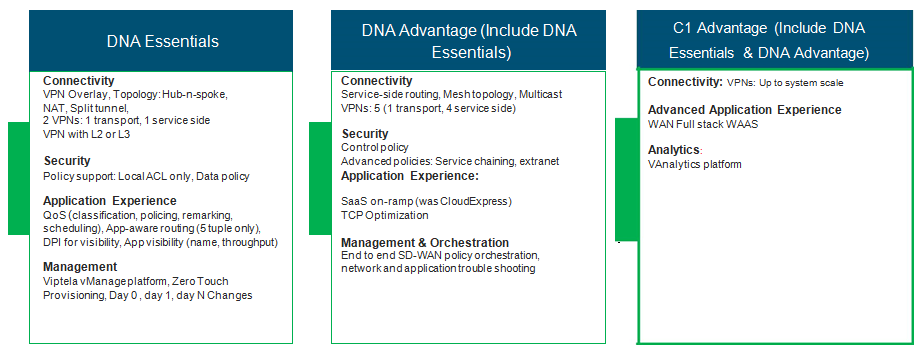
1. Hardware platforms
2. Virtual platform based on KVM or ESXi
3. Cloud based Edge routers is supported in AWS cloud

Hardware vEdges are available as per the table below:



1. **SD-WAN edge software**

Viptela has a total of 4 feature set supported today. Base feature set (Plus) supports basic SD-WAN functionalities and further top tiers support additional functionalities. Top software tier is called Enterprise which has got all available SD-WAN functionalities.



1. **SD-WAN throughput licensing**

Throughput licensing is required to be activated at each SD-WAN edge device and it’s based on actual throughput subscription required for customer per branch. This will be charged based on throughput and recurring charge per quarter. Throughput licensing is available in below bandwidth slabs for enterprise tier software. Below are the mechanism of selecting throughput licensing:

* In case of 1 SD-WAN edge device at a site, total cumulative WAN throughput (multiple WAN links) are considered for SD-WAN edge device
* In case of 2 SD-WAN edge device at a site configured as Active-Active, total cumulative WAN throughput (multiple WAN links) are considered for each SD-WAN edge device
* In case of 2 SD-WAN edge device at a site configured as Active-Standby, total cumulative WAN throughput (multiple WAN links) per SD-WAN edge device are considered for each SD-WAN edge device respectively
* The above method is common for physical vEdges, virtual vEdges (vEdge cloud), vEdge cloud hosted in AWS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bandwidth Tiers | License type | | | Hardware variant |
| vEdge-Plus-10M | DNA Essentials  (**Bronze**) | DNA Advantage  (**Silver**) | C1  Advantage  (**Gold**) |  |
| vEdge-Plus-20M |  |
| vEdge-Plus-50M | vEdge 100, 1000, 2000 & 5000 |
| vEdge-Plus-100M |  |
| vEdge-Plus-1G |  |

## Versa

Versa routers can be deployed in 3 modes

1. Hardware platforms
2. Virtual platform based on KVM or ESXi
3. Cloud based Edge routers is supported in AWS cloud
4. **SD-WAN edge platforms**

SD-WAN edge platforms are CPE placed at each site of enterprise WAN including branch, HO, DC, DR and cloud sites. This can be hardware platforms or virtual machine based platforms. VM based platforms are called cloud CPE’s and supported on ESXi and KVM hypervisors. In addition to that SD-WAN edge platforms are deployed on public cloud – AWS and AZURE

1. **SDWAN Feature bundle**

SDWAN feature bundle for versa is categories in to Bronze, Silver, Gold and Platinum.

Note: *In addition to selecting the feature tier, bandwidth has to be selected based on aggregate or physical link bandwidth per CPE*

**Bronze**

This Category includes following features,

VRRP, (DHCP),Routing Policies, PBF,MP-BGP, OSPF, VRF, VLAN, QoS, HQoS, Route reflector, External Service Chaining and ZTP.

**Silver**

This categories includes all the features of Bronze Categories additionally below feature will be included,

Dos Protection, Statefull firewall, CGNAT, SD-WAN Traffic Management & shaping, Multiple Active Links, Dynamic IPsec overlay, SD-WAN controller and IPSEC Transport.

**Gold**

This categories includes all the features of Silver Categories additionally below features will be included,

Application Policy Forwarding, Application QoS, Traffic Shaping and Application ID/Visibility, MOS, Path conditioning

**Diamond**

This categories includes all the features of Gold Categories additionally below features will be included,

Antivirus, IDS-IPS, SSL, TLS Decryption, User, Group Access Ctrl, IP Reput. & Filtering and Application Access Ctrl

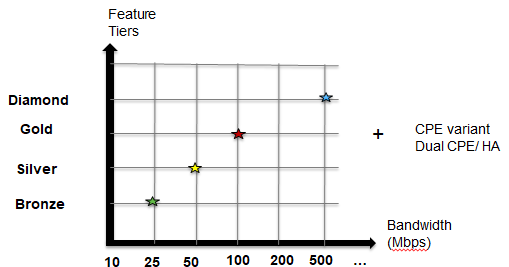
***Note: IDS-IPS and AV is under evaluation***

1. **Sify White box Appliance Models**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Part Code** | **Item Description** | **CPE Type** | **Max Bandwidth**  **(Diamond)** | **Max Bandwidth**  **(Gold**  **or lessor)** | **Branch Type** | **Available ports** |
| **MSDWAN-P1-OnPrem** | Managed SD WAN Platform 1 On Premise | v110  2.4 GHz, Intel Rangeley Atom C2558, **4 Cores, 8GB** | 100Mbps | 220Mbps | Branch offices | 2**x Mgmt ports + 4x Cu GE Ethernet routed ports** |
| v110  2.4 GHz, Intel Rangeley Atom C2558, **4 Cores, 8GB** | 100Mbps | 220Mbps | Branch offices | 2x Cu or SFP WAN port selectable interfaces  **4x Cu GE (via 4 Ethernet switch ports embedded)** |
| V110 (LTE)  2.4 GHz, Intel Rangeley Atom C2558, **4 Cores, 8GB** | 100Mbps | 220Mbps | Branch offices | 2x Cu or SFP WAN port selectable interfaces  **4x Cu GE (via 4 Ethernet switch ports embedded)** |
| V110 (LTE + WIFI)  2.4 GHz, Intel Rangeley Atom C2558, **4 Cores, 8GB** | 100Mbps | 220Mbps | Branch offices | 2x Cu or SFP WAN port selectable interfaces  **4x Cu GE (via 4 Ethernet switch ports embedded)** |
| **v120/v520**  **2.4 GHz, Intel Rangeley Atom C2758, 8 Cores, 16 GB** | 250Mbps | 550Mbps | Branch offices | 2x Cu or SFP WAN port selectable interfaces  4x Cu GE (via 4 Ethernet switch ports embedded)  \***Optional hardware variant for ordering CPE with 5 routable ports** |
| **v810**  **2.0 GHz, Intel Xeon D-1548, 8 Cores, 64GB** | 500Mbps | 900Mbps | DR/Hub/Large Branch offices Location | 2x 10GE SFP+, 5x Cu GE Ethernet ports |
| **v1000**  **2.6 GHz, Intel Xeon E5-2697v3, single socket, 14 cores, 64GB** | 1Gbps | 1.6Gbps | DC/DR locations | 2x 10GE SFP+, 4x cu GE Ethernet ports |

1. **SD-WAN throughput licensing**

Throughput licensing is required to be activated at each SD-WAN edge device. This is based on customer actual throughput subscription required. This will be charged based on throughput and recurring charge per quarter. Throughput licensing is available in below bandwidth slabs for enterprise tier software. Below are the caveats of selecting throughput licensing:



* In case of 1 SD-WAN edge device at a site, total cumulative WAN throughput (multiple WAN links) are considered for SD-WAN edge device
* In case of 2 SD-WAN edge device at a site configured as Active-Active, total cumulative WAN throughput (multiple WAN links) are considered for each SD-WAN edge device
* In case of 2 SD-WAN edge device at a site configured as Active-Standby, total cumulative WAN throughput (multiple WAN links) per SD-WAN edge device are considered for each SD-WAN edge device respectively
* Each feature tier base SKU includes 25 Mbps bandwidth by default.
* Licensing for Feature tiers with vary based on the following bandwidth slab 1Mbps, 2Mbps, 5Mbps, 10Mbps, 25Mbps, 100Mbps, 200Mbps, 500Mbps, 1Gbps and 2Gbps.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Bandwidth Tiers | License type | | |  | Hardware variant |
| 10 M | Base-SDWAN  (**Bronze**) | Standard SDWAN  (**Silver**) | Advanced SDWAN  (**Gold**) | Advanced secure SDWAN  (**Diamond**) | u100, 110, 120/520, 810, 1000 |
| 25 M |
| 50 M |
| 100 M |
| 200 M |
| 500 M |
| 1 GB |
| 5 GB |
| 10 GB |

# Technology differences – Viptela and Versa

|  |  |  |
| --- | --- | --- |
| Parameter | Viptela | Versa |
| Control plane | Makes use of DTLS/TLS between vEdge and control [vBond, vSmart and vManage] | Makes use of traditional IPSEC between FlexVNF and Versa Controller. [Further communication to Versa Director and Versa Analytics happens through Versa Controller] |
| Data plane | IKE-less IPSEC. vSmart acts as RR and facilitates exchange of data plane and security related attributes  OMP is the protocol | IKE-less IPSEC. Versa Controller acts as RR and facilitates exchange of data plane and security related attributes  Extended BGP address family “Versa-private” protocol is used |
| ZTP server | * Dedicated control component, played by vBond * Do not support URL based ZTP | * Versa Controller plays the role of ZTP server as well. 3 modes of staging – pre-staging, staging and post-staging. Pre-staging is optional and staging and post-staging are mandatory * Supports URL based ZTP |
| CPE | * Supports only vEdge hardware as supported by Viptela * No support of 3rd party x86 hardware * Supports on VM – ESXi and KVM | * Supports only FlexVNF hardware as supported by Viptela’s certified OMD partners * Support of 3rd party x86 hardware * Supports on VM – ESXi and KVM |
| Controller | vSmart is single-tenant | Versa Controller is multi-tenant |
| Control HA | CPE is multi-homed with redundant vSmart controllers | CPE is multi-homed with redundant controllers |
| Transport links | All transport links are part of same VPN instance [VPN 0] in vEdge. This limits duplicate WAN numbering across all tenants in multi-tenant environment | Each transport link is part of different VR in FlexVNF. This do not post any limit of duplicate WAN numbering across all tenants in multi-tenant environment |
| IPSEC source Interface | IPSEC is sourced from WAN interface. This limits duplicate WAN numbering across all tenants in multi-tenant environment | IPSEC is sourced from virtual loopback interface [PTVI 4 and PTVI 5]. This decouples WAN numbering from IPSEC source endpoints |
| Performance measurement | BFD extension is used for measuring link performance between vEdge routers  Does not support MOS and inline loss measurement(Dataplane) | Modified Y1731 probes are used for link performance measurement Supports MOS and inline loss measurement(dataplane) |
| Service chaining | Supports service chaining | Supports both external and Internal service chaining |
| Security | Supports ACL and basic security filtering | Supports statefull, nextgen firewall services and supports 3rd party VNF service chaining(Fortigate, palo alto) |

# Overhead calculation

## Viptela

|  |
| --- |
| **Outer IP 20 bytes** |
| UDP 8 Bytes |
| SPI 4 Bytes |
| Sequence Number 4 Bytes |
| MPLS 8 Bytes |
| Padding Length 1 bytes |
| Next Header 1 bytes |
| IPsec Authentication Data 16 bytes |
| Customer Data |

**Viptela**: Total 58 bytes of overhead

## Versa

|  |
| --- |
| **Outer IP 20 bytes** |
| UDP 8 Bytes |
| VXLAN 8 Bytes |
| ESP 40 Bytes |
| MPLS 8 Bytes |
| Customer Data |

**No Encryption**: 44 Bytes

* + MPLS header+ VXLAN + UDP + Transport IP

**With Encryption**: 84 Bytes

* + MPLS header+ ESP+ VXLAN + UDP + Transport IP

**Note**: Encryption of “ESP 40 bytes” based on aes256 –sha256 encryption may vary based on encryption selection type

**SDWAN Overhead table**

|  |  |  |
| --- | --- | --- |
| **Packet-Size(with L2 headers)** | **Over Head %**  **without encryption** | **Over Head %**  **with encryption** |
| iMIX1 | ~14% | ~20% |

**IXIA Tested IMIX pattern:**

**IMIX1** - *64, 594 and 1518 byte packets in 7:4:1 ratio*

# SLA

**SLA measurement methodology**

Versa uses standard Y.1731 based probes encapsulated within SDWAN overlay tunnels per access circuit ‘Network Control’ queue to measure the path SLAs.

1 probe packet is sent every ‘1s’ and measurements are aggregated over 5 mins and exported to Analytics using IPFIX.

Viptela uses BFD variant of SLA probes within SDWAN overlay Tunnels per access circuit to measure the path SLA

1 probe packet is sent every 1s and measurements are aggregated over 5 mins and exported to V-Manage

|  |  |
| --- | --- |
| **SLA Parameter** | **SDWAN** |
| RTD | Measure of Delay between pair of sites is calculated based on the probe time-stamp i.e. difference between sent vs received timestamp. The  aggregated reports can be viewed via the charts under sdwan metrics - **Delay** |
| Jitter | Measure of Jitter is calculated between par of sites is based on the variation in the time for the probes sent and received accounts to the Jitter. The aggregated reports can be viewed via the charts under sdwan metrics: **1. Forward Delay Variation 2. Reverse Delay Variation** the total jitter is **Maximum of either(Forward Delay Variation, Reverse Delay Variation)** |
| PDR | PDU Loss is calculated by no. of synthetic SLA probes dropped during the probing interval, The aggregated reports can be viewed via the charts under sdwan metrics - **PDU Loss Ratio** |

**SLA for Customer using Sify’s Network:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **For Customer's using Sify's Network** | | | | **Comments** |
| **Sr. No.** | **Service Features** | **Specifications** | **PNMM - Bundle CPE** |
| **NBD** |
|  | Service Availability Guarantee - Link | (Tier 1/Tier 2/Tier 3) | > 99.9 / > 99.5 / > 99% | **These will apply as per Sify Site connect SLA Design considerations**  **Manual unplugging at customer premise will also be not considered under this SLA cat** |
|  | Service Availability Guarantee – Device | (Tier 1/Tier 2/Tier 3) | > 99.9 / > 99.5 / > 99% | * **Service Availability on Device will be provided for branch range appliances like v110, 120(1 PSU) only if customer has dual power source** * **For Hub ranges appliances like v8xx and v1000 are provided with dual PSU. The Customer should provide power redundancy on-premise by connecting different power sources to meet this SLA** |
|  | Service portal |  | 99.99% | AAKAASH availability |
| Availability |  |
|  | Mean Time to Resolve (MTTR) | for severity 1/2/3 | 4 hrs / 4 hrs / 24 hrs |  |
|  | Mean Time to Respond | for severity 1/2/3 | 15mins/ 30 mins/ 60 mins |  |
|  | Incident Response Rate |  | 99.90% |  |
|  | Hardware Replacement Time | Replacement of Faulty Hardware according to  Tier 1/Tier 2/Tier 3 | NBD/2 Business days/2 Business days |  |
|  |

# Appendix

1. *SLA co-referenced with the* ***SiteConnect L3VPN SLA*** *parameters, subject to changes as per customer ask on case to case basis*

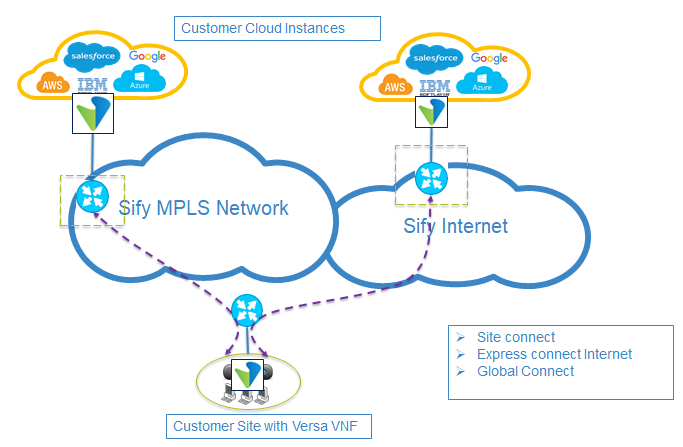
****

1. ***SiteConnect*** *service will be used for Sify provided MPLS circuits delivered across Tier1, Tier2 and Tier 3 locations*
2. ***SDWAN*** *CPE supports only Ethernet handoff and on select cases Fiber*
3. ***SDWAN*** *hardware will be supplied to the customer only by Sify*
4. *Customer can bring their own transport links for WAN connectivity, the condition being its SLA backed for optimal network performance*
5. Script based **ZTP** is the preferred mode of CPE on-boarding
6. *Multi-tenant SDWAN is the preferred mode of deployment, on-prem or dedicated SDWAN deployment should be discussed on case to case basis*
7. *SDWAN interface, CPE and WAN networks naming convention will be captured in Configuration and Provisioning guide document*
8. *SDWAN overhead should be considered for customer Bandwidth provisioning, Please refer to sec* [*SDWAN Overhead table*](#_Overhead_calculation)
9. *QOS/APP-QOS still maintains the same as* ***SiteConnect QOS*** *offering, with only exception customer needs to provide application names to be added for per queue servicing*
10. *While provisioning or discussing SDWAN CPE on Cloud refer to the section* [**SDWAN Cloud CPE responsibility matrix**](#_Deploy_SD-WAN_edges)

***Cloud Connectivity and Cloud Centric Data approach***

*DC’s are migrating to the cloud for the robustness of service scaling and ease of management of their servers, with this approach customers loose the visibility of type of traffic and accelerated call flow from the company users to the respective Servers. These services are already enhanced with our cloud connectivity offerings, SDWAN based cloud Edge generates a new stream for business and enhancing customer experience by introducing SDWAN-on-Cloud*

*SDWAN Edge routers will be deployed in customer specific cloud provider regions of AWS/Azure and connectivity from customer branch to Cloud branch can be extended via* ***Global connect*** *and Internet based access services.*



**Use cases for the customer**:

1. Deterministic routed MPLS path to the nearest cloud connectivity exit using ***Global connect*** *service*
2. Traffic steering and traffic acceleration during link degradation over non-deterministic Internet path from branch’s to the Cloud
3. Security on the Cloud with SD-Security use cases like statefull firewall, Next-gen firewall and UTM for enhanced security from branch till the cloud
4. On the cloud security features for corporate users accessing DC’s apps over public Internet and helping customers mitigating threats using AV and IPS
5. Application/Link utilization reports for cloud based applications and effective load sharing and High-availability of DC App’s within one cloud region
6. GRE based IPSEC connectivity from Remote Cisco branch routers till Cloud SDWAN gateway for secure connectivity over IP underlay
7. Complete end-end management of Cloud Edge CPE, Global Connect links will be provisioned and managed solely by Sify MS-NOC

---------------------------------------------------Document Ends-------------------------------------------------------------------