WHITE PAPER
2024

VMware SD-WAN for State, Local, and Education Sectors

vmware® by Broadcom

Table of contents

Introduction to VMware VeloCloud SD-WAN

Enterprises are embracing cloud adoption to optimize costs and to choose the most suitable solution for their applications. This means that data and applications are not just hosted within the on-prem data center but are also hosted on public, private or hybrid clouds. Remote and hybrid work has become a normal part of our work culture, and reliable WAN connections are required to securely access these applications. The availability and cost to operate and manage the WAN has become expensive, and the complexity of networks is increasing. Distributed users and data with current WAN architecture results in suboptimal traffic flows which results in added latency and poor user experience.

Software-Defined Wide Area Network (SD-WAN) addresses these critical issues and effectively transports branch and remote user traffic. VMware VeloCloud SD-WAN dynamically utilizes any available underlying WAN transport (private circuits, broadband, DSL, LTE, satellite, fixed wireless access, etc.,) to find the optimal delivery path for traffic across the entire network, thereby delivering an optimal user experience regardless of the location or access type.

Figure 1: WAN architecture before and after Velocloud SD WAN

VeloCloud SD-WAN Components and Architecture

VeloCloud SD-WAN consists of three components that provide enterprises a reliable platform to access data and applications securely while optimizing traffic and lowering operating costs.

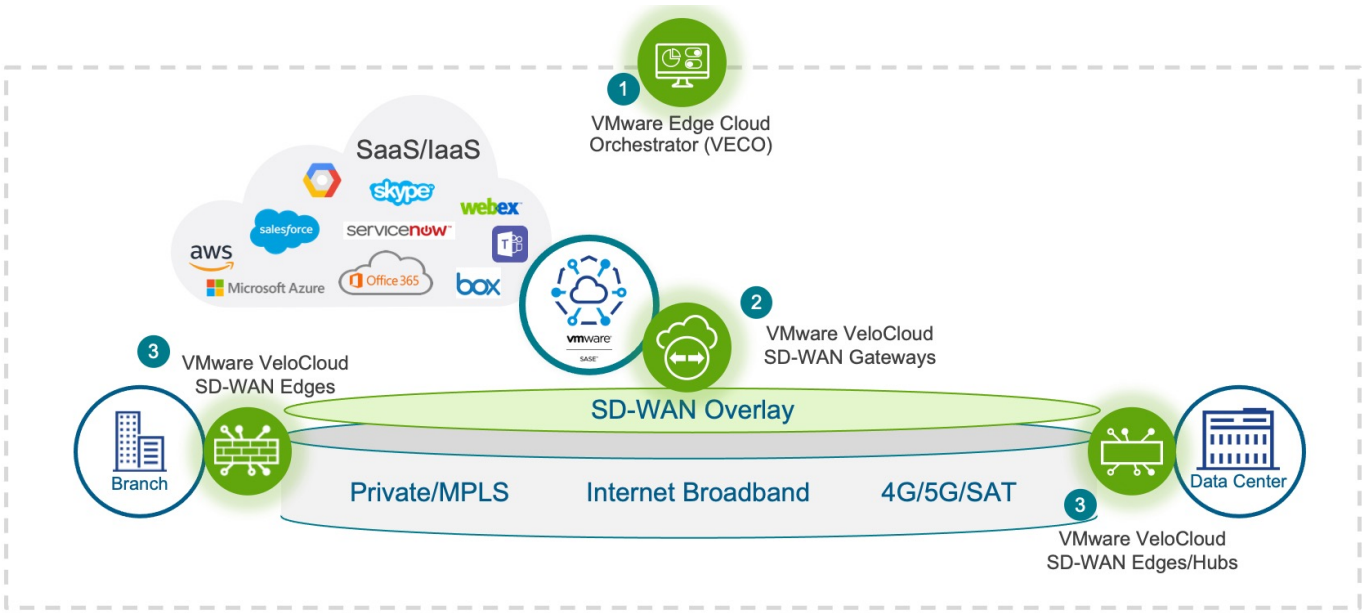

Figure 2: Velocloud SD WAN architecture

1. VMware Edge Cloud Orchestrator (VECO)

VECO is a cloud-delivered, multi-tenant portal that provides a simple web-based user interface for centralized management, configuration, monitoring, logging and reporting.

2. VMware VeloCloud Gateways (VCG)

The VCGs are deployed at top-tier network points of presence (PoPs) and in cloud data centers around the world, facilitating the full range of VeloCloud SD-WAN benefits. The gateways enable optimized access to applications in the cloud and data centers, as well as for accessing private network backbones and legacy enterprise sites. The gateways can be cloud-hosted or deployed on-prem. The gateways provide a scalable and distributed infrastructure resulting in quick, secure, high-quality, and direct on-ramp to cloud from any location.

3. VMware VeloCloud Edges (VCE)

The VeloCloud Edge appliances are easy to install at remote branches, data centers or home offices and provides a range of throughput and ports for WAN and LAN connectivity, integrated wireless LAN, and security firewall services. Both physical and virtual edge form factors are available. All policies and configuration will be pushed to the edges from the centralized VECO when the edges are activated.

There are three communication paths in a VeloCloud SD-WAN deployment, all secured with encryption:

- **Management plane** communication between the Edges and Orchestrator or Gateways and the Orchestrator uses TLS 1.2 over TCP 443
- **Control plane** communication between the Edges and Gateways uses VCMP tunnels over UDP 2426 and is encrypted with IPSEC AES 256 and SHA-256 with periodic key rotation
- **Data plane** communication between the Edges or Edges and Gateways also uses VCMP over UDP 2426 and is encrypted with IPSEC AES 256 and SHA-256 with periodic key rotation.

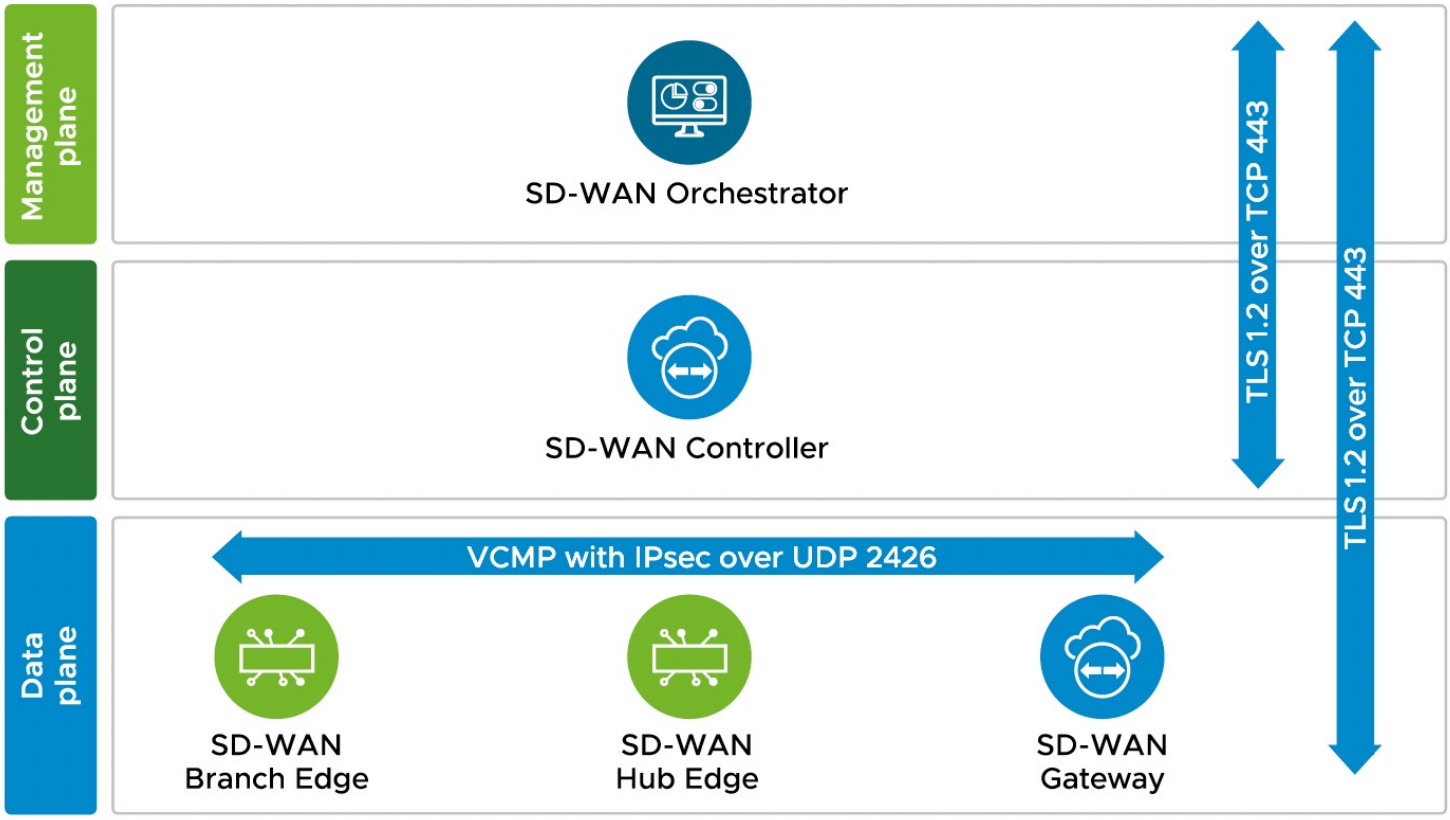

Figure 3: Communication between Velocloud SD WAN components

Appendix A contains more information on Security specific to SLED requirements.

VeloCloud SD-WAN deployment at state/local/education sites

Wide Area Networks (WANs) have undergone a significant evolution, transforming basic communication systems into complex global infrastructure that connects users and devices to applications—not just hosted within the enterprise data center but also extended to public, private and/or hybrid clouds.

Adopting SD-WAN is usually driven by the need to reduce networking costs, easily deploy sites while leveraging all underlying WAN transports, and optimize application performance. SD-WAN also enhances security by allowing for more granular control over network traffic and implementation of advanced security protocols.

There are different ways to design and deploy an SD-WAN solution. In the case of state, local and education organizations, it is largely driven by two factors:

- Traffic flow and segmentation requirements
- How the IT and network infrastructure is managed

In most cases, several state agencies or schools with varying traffic flow requirements are managed by a centralized state or education IT department. But in some cases, different organizations prefer to self-manage their network while still retaining a consistent "cookie cutter" deployment model across all organizations.

In a scenario where each agency or school heavily relies on a strong centralized IT team to deploy, configure, and monitor all sites with a turnkey solution that does not require each entity to manage their SD WAN sites, a single-tenant enterprise solution is a good fit.

In a scenario where each agency or school wants a high degree of independence in managing sites, network administrators, business policies, or security policies, a multi-tenant Managed Service Provider model solution would be better suited. In this case, the state IT department delegates the administration and management to the respective agencies, thereby reducing dependency on the central IT team.

This section dives deep into how each of these two use cases can be deployed using the VMware VeloCloud SD-WAN solution.

Single-tenant enterprise solution with segmentation

This is a good fit for state or education customers who want to:

- Centralize the control of their SD-WAN network within a single IT administrative team, rather than letting each agency or school manage their own SD-WAN
- Keep each agency/school traffic separate from other agencies/schools, with their own applications
- Allow all agencies/schools to access common applications at their data centers
- Minimize SD-WAN operational costs by leveraging VMware VeloCloud hosted orchestrator (VECO) and VeloCloud Hosted Gateways. When constrained by stringent security requirements, the state or education body may decide to deploy their on-prem VECO and VeloCloud Gateways to avoid the use of a shared VECO/VeloCloud gateway infrastructure.

This solution relies on a single tenant —for example, the state or the head campus — managed by a central network and IT administrative group, with different logical segments (more generally known as VRFs in the networking industry). This solution allows separation of traffic between different agencies within the state. or different schools within the education campus, while maintaining all control within a single network and IT central authority. It does not allow each state agency or school to be their own tenant with full administrative rights in their enterprise (discussed in the subsequent section, Multi-tenant Solution).

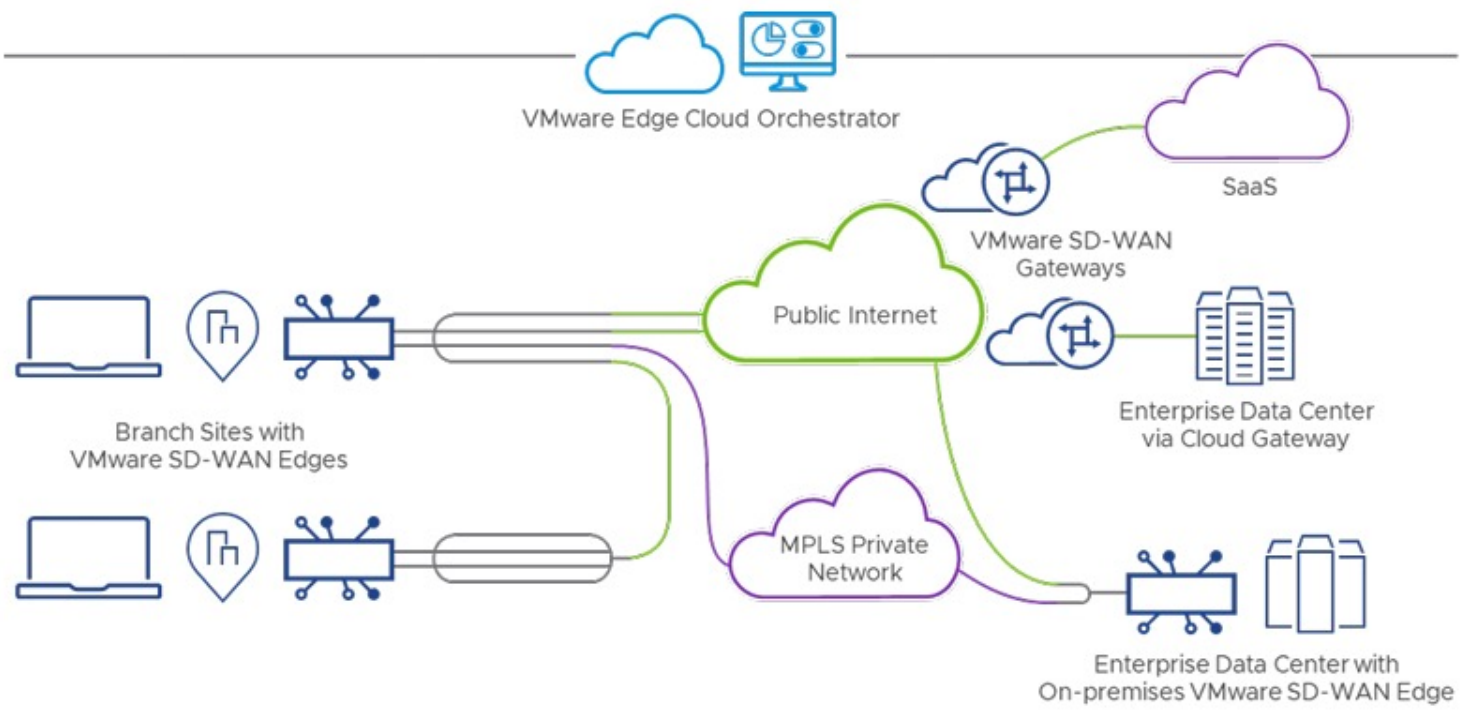

Figure 4: State SD-WAN solution in a traditional single-tenant configuration

Within that tenant (aka that enterprise), the state administrator may create several segments (up to 128) to isolate different state agencies or logical groups into discrete VRFs within the State enterprise network. Segmentation is the process of dividing the network into logical sub-networks called segments by using isolation techniques on a forwarding device such as a switch, router, or firewall. Network segmentation is important when traffic from different organizations and/or data types must be isolated.

The Orchestrator is typically hosted by VMware as a multi-tenant shared resource across enterprises. It is deployed and managed by VMware in Broadcom SASE PoPs. There is always a primary and disaster-recovery VECO.

Note that the VECO can be hosted dedicated to the state, in which case it is not shared with other VMware SD-WAN customers. However, that increases the cost of the solution because it calls for dedicated VeloCloud Gateways involved in control and the production plane.

In the segment-aware topology, different Virtual Private Network (VPN) profiles can be activated for each segment. For example, guest traffic can be backhauled to remote data center firewall services, voice media can flow direct from branch to branch based on dynamic tunnels, and any given agency segment can backhaul traffic to the data center to communicate with that particular agency's application servers, as represented in the next diagram.

Segmentation basically allows configuring discrete VRFs with complete isolation from one another, each with their own routing table. There is no route leaking between segments and, although not a best practice, different segments can actually have overlapping IP addresses.

This is a single-tenant enterprise model because all the agencies or logical segments are part of the same "enterprise" tenant with a central admin group managing all SD-WAN configuration elements (Edges, profiles, routing, policies, edge firewalls, Interfaces, etc.), troubleshooting and monitoring.

For example, a state could deploy the following segments:

- A global segment for over-arching services available across all agencies for access to common applications
- Department of Transportation
- Department of Corrections
- Department of Justice
- Guest Wi-Fi segment, which could be deployed at all agencies
- Department of Financial Services
- IOT segment which could be used for environmental sensors, road signs, surveillance cameras, where security rules are more stringent
- Department of Natural Resources, etc.

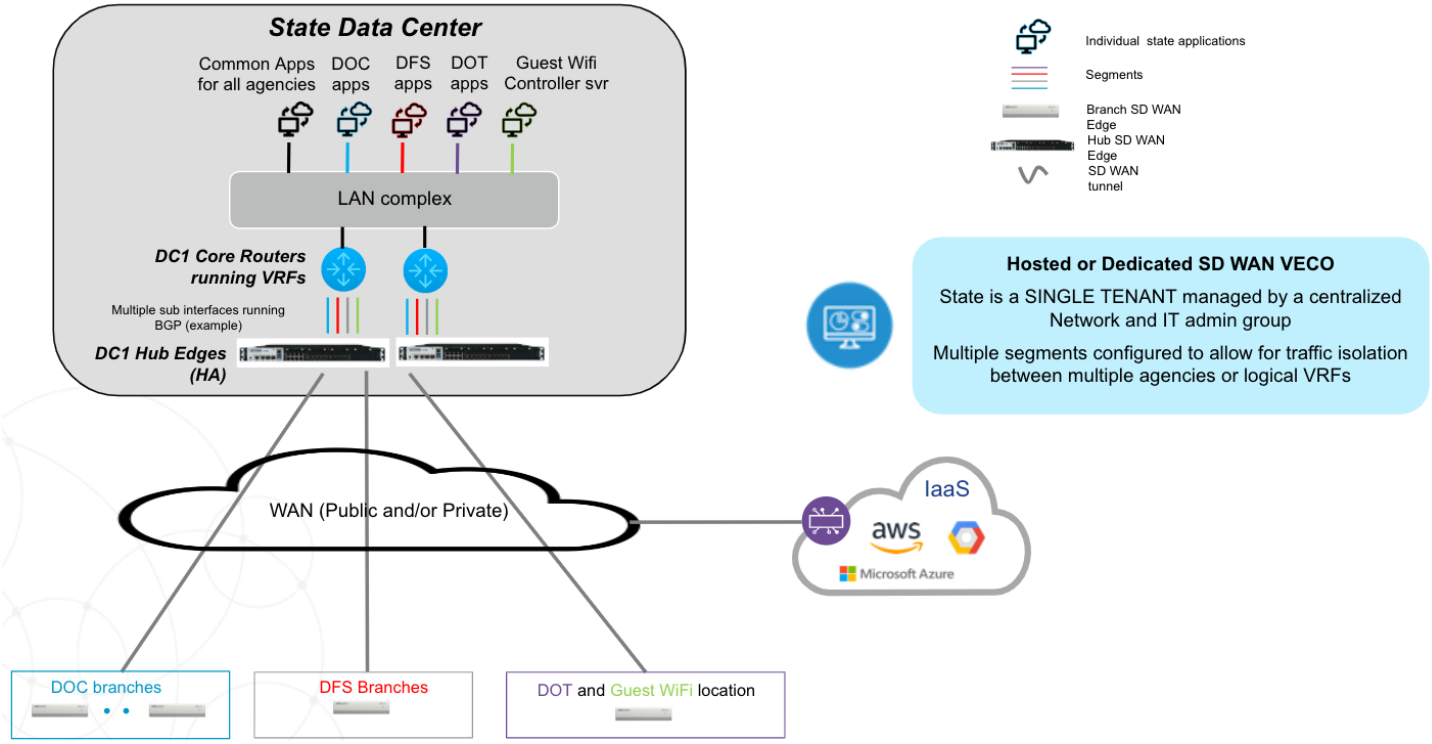

Figure 5: State SD-WAN solution segmentation example

- Line-of-business separation by departments for security and audit
- **User data separation:** guest traffic, Payment Card Industry (PCI) data, employee traffic
- **Mergers and acquisitions:** network segmentation is used to allow overlapping IP addresses and secure access to shared assets
- An external party such as partners or contractors needing access to a subset of information in the corporate data

VeloCloud SD-WAN segmentation has two layers:

- **Overlay delivery:** as packets enter the Edge devices, a segment ID is inserted into the Dynamic Multipath Optimization ™ (DMPO) tunnel header to isolate different segments as they traverse the overlay
- **Edge routing:** the Segment ID identifies a unique segment within the SD-WAN network whose routes are entirely isolated from the rest of the network

Each segment is treated as a separate configuration entity with its own cloud VPN, business policy, firewall, and QoS configuration elements. All of this is centrally managed through the VMware Edge Cloud Orchestrator.

As represented in the above diagram, all segments share common Hub Edges located at a state data center. Note there could be more than one state data center, and hub edge clusters could also be deployed at public cloud IaaS locations.

The challenge is to keep each segment logically separate from routing, security and business policy perspectives, especially at the hub sites or data centers where all segments converge into one campus. This is easily solved with VeloCloud SD-WAN segmentation technique which provides network isolation. Within a single tenant, segmentation isolates networks using a VRF-like concept to solve for the following use cases:

All VeloCloud Edge interfaces share a default Global Segment, and additional segments can be created and assigned to the interfaces. In the Orchestrator, multiple segments can be created, and those segments would be extended into the branch/data center Edge infrastructures and mapped to corresponding VLANs/VRFs.

VeloCloud SD-WAN supports network segmentation at a maximum for 128 isolated VPNs that can traverse the overlay fabric.

Typically, the Hub edges are configured with LAN Layer 2 interfaces DOT1Q trunk handoffs with multiple VLANs, each belonging to a separate segment as represented in the below diagram. The same logical separation can be achieved with multiple Layer 3 sub-interfaces instead.

When an Edge establishes an SD-WAN tunnel with another Edge with both edges participating in multiple segments, traffic from all segments is encapsulated into a single tunnel. There is no need for distinct unique tunnels per segment. Traffic is kept separate within the SD-WAN tunnel by use of a segment IDs, ensuring complete isolation between segments, as represented below.

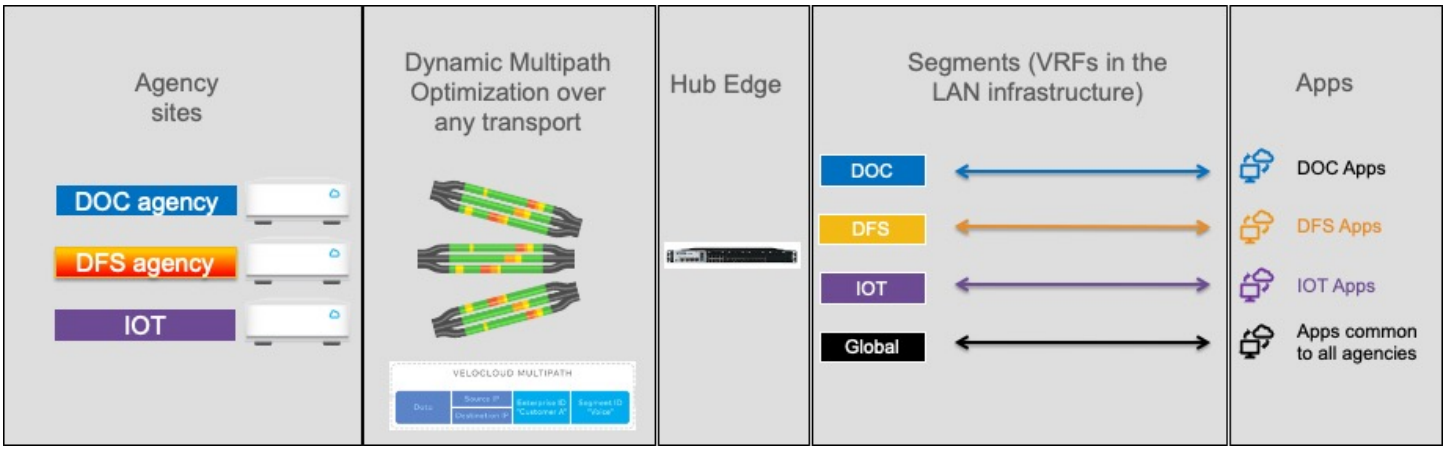

Figure 6: Segmentation mechanism within SD-WAN tunnels

Note that the **global** segment is always common to all Edges.

If a remote edge only participates in a **single** segment, users connected to that Edge will be able to send/receive traffic within that segment only and talk to hub resources configured in that segment.

Note that remote Edges can also be configured to handle multiple segments if need be, in the same way as a hub edge with Layer 2 dot1q handoff or separate Layer 3 interfaces allow a remote site to join multiple segments.

The segment type can be one of the following:

- **Regular:** The standard segment type.
- **Private:** Used for traffic flows that require limited visibility in order to address end user privacy requirements.
- **CDE:** VMware provides PCI-certified SD-WAN service. The Cardholder Data Environment (CDE) type is used for traffic flows that require PCI and want to leverage the VMware PCI certification.

Limitations of the segmented solution

- The number of segments is limited to a maximum of 128 per Enterprise
- Multicast and OSPF routing protocols can only run in the global VRF at this time
- Administrators have access to all segments

Multi-Tenant Managed Service Provider (MSP) Solution with Partner Gateway

Before we delve into multi-tenant MSP solutions, it is important to understand VeloCloud Gateway types. There are three different types of VMware SD-WAN Gateway.

1. **Cloud Hosted Gateways:** These are deployed and hosted by VMware globally in major Internet Exchanges, PaaS and Cloud PoPs. Cloud gateways are multi-tenant and serve as a control plane for the SD-WAN fabric and data plane for cloud on-ramp to SaaS and internet traffic flows. The hosted gateways can either be shared or dedicated.
2. **On-Premise Gateways:** These gateways are deployed and managed by enterprise customers within their own on-prem data centers. These gateways are not multi-tenant and function only as the controllers for the SD-WAN control plane connectivity.
3. **Partner Gateways:** These gateways are typically deployed by Service Providers/Telcos within their networking infrastructure to integrate SD-WAN branches with their SP's backbone network. Unlike the cloud hosted and on-prem gateways that have only one interface, Partner Gateways have 2 interfaces. Public Interface is connected to the internet and private interface is connected to the PE router for VRF or VLAN handoff. Private Interface is also referred to as a handoff interface for this reason.

The Partner Gateway deployment model is a multi-tenant solution where the State IT Department serves as a Managed Service Provider (MSP) for all the State Agencies.

This is a good fit for state customers that:

- Have multi-tenancy requirement at the headend to segregate traffic between the agencies
- Need Partner Gateways instead of Hub edges at their Data Center when the requirements exceed the Hub segment capacity (SD-WAN edges support a maximum of 128 segments)
- Wants to minimize the hassle of deploying and maintaining a separate hub edge for each agency
- Provide the state agencies ability to manage their respective SD-WAN network
- Has multiple tenants with overlapping IP addresses and needs isolation
- Provides some common services across some or all of their tenants

The State (MSP) can choose either of these two deployment models:

- Hosted VECO and On-Premise Partner Gateways where the Orchestrator is completely hosted and managed by VMware/ Broadcom
- On-Premise VECO and On-Premise Partner Gateways where the VECO and Partner Gateways are deployed at the State's Data Center and the State is responsible for managing this entire infrastructure.

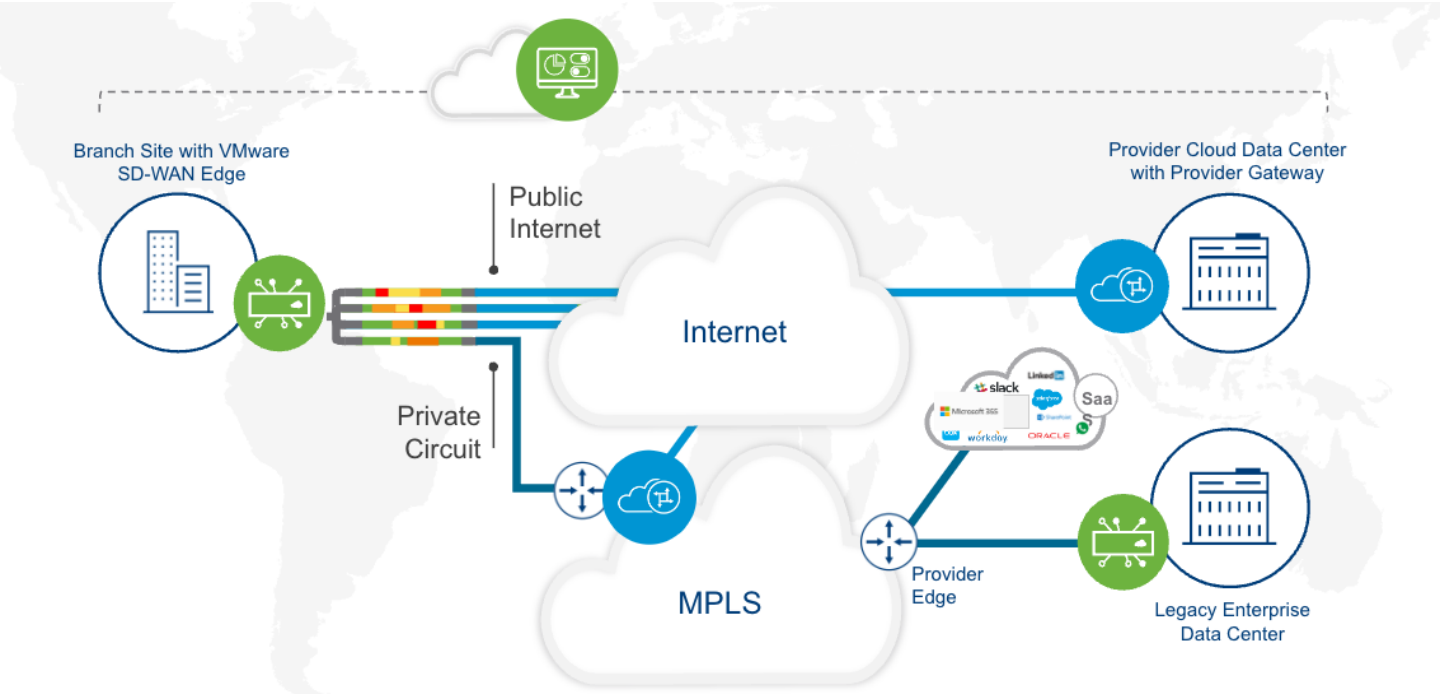

Figure 7: SD-WAN solution with Partner Gateway deployment at the State Data Center

The User Management feature within the VECO allows the State (MSP) to create users for every tenant/agency to allow them to manage their environment. The Orchestrator supports a 3-tiered hierarchy: Operator, Partners, and Customers.

The Operator tier is the highest level of management and control and the VMware/Broadcom ops team has this access. The State IT department is configured as a Partner and all agencies will be configured as separate Customers under the Partner tier. Each customer/enterprise has visibility and control into their own SD-WAN network, and is completely isolated from other enterprises. An Operator can create and assign MSP user accounts and roles; Similarly, the State (MSP) can create users and assign roles at the customer level.

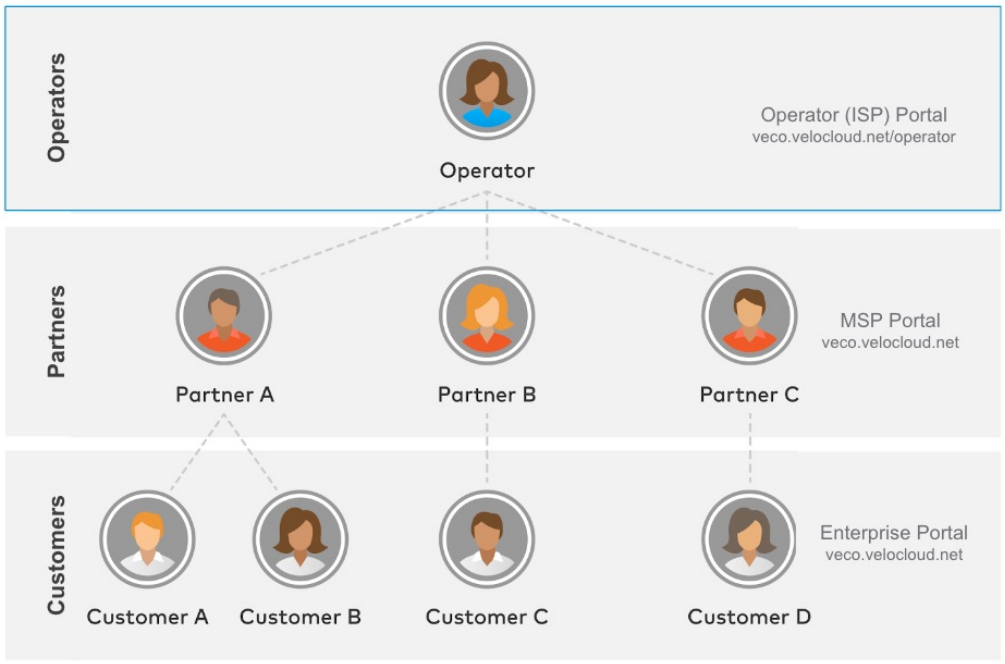

Figure 8: VECO Account management hierarchy

Partner Gateway configuration in the VECO:

To configure a gateway as a Partner Gateway, simply enable the “Partner Gateway” role once the gateway is created.

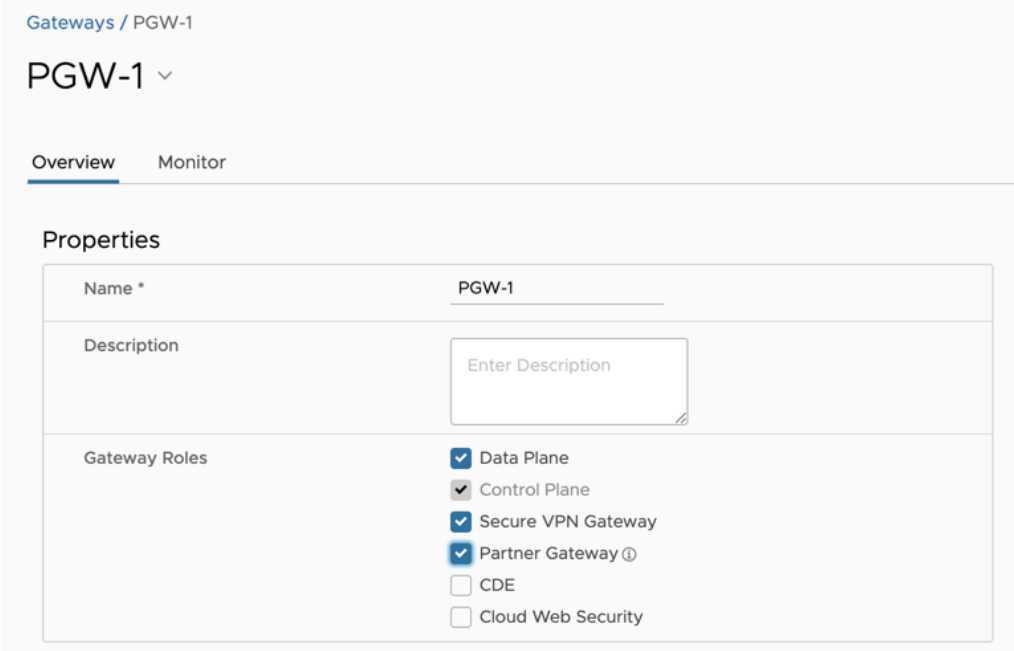

Figure 9: Enabling the Partner Gateway option in VECO

Routing, application and Internet traffic flow via Partner Gateways:

This is a “hub-less” design where the Partner Gateways themselves function as Hubs at the MSP data center. Apart from its role as a controller, the partner gateway will connect and forward traffic to the downstream core switches/routers which separates traffic from multiple tenants over a L2 VLAN or a L3 VRF.

The state (MSP) hosts tenant-specific services within their data center for all its agencies. These agencies will have visibility and administrative control to edges within their SD-WAN environment. When the edges are deployed at these agencies, partner gateways will be manually assigned to them. The clients/users within these state agencies that require access to applications will traverse the partner gateway within the state’s data center where these services are hosted. Communication between the edges within a tenant/state agency for branch-to-branch VPN and dynamic branch-to-branch VPN will all go through the partner gateway at the state data center. SaaS and internet traffic can either be sent split-tunnel directly from the tenant edge or backhauled to the state data center via the partner gateway.

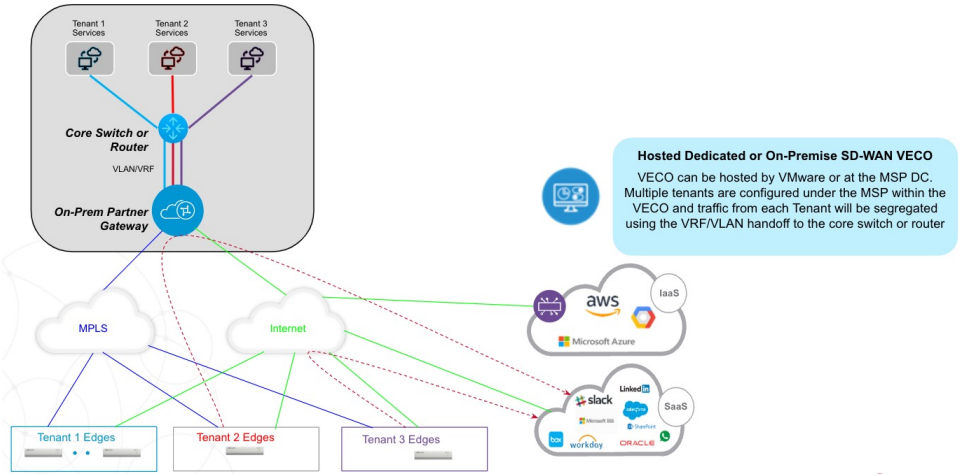

Figure 10: State SD WAN Partner Gateway deployment example

Within each tenant, end-to-end service separation can be provided using segmentation. For instance, we could completely isolate and forward voice, data, PCI and guest internet traffic over separate segments and configure business policies per segment to route specific traffic accordingly on a per-tenant basis.

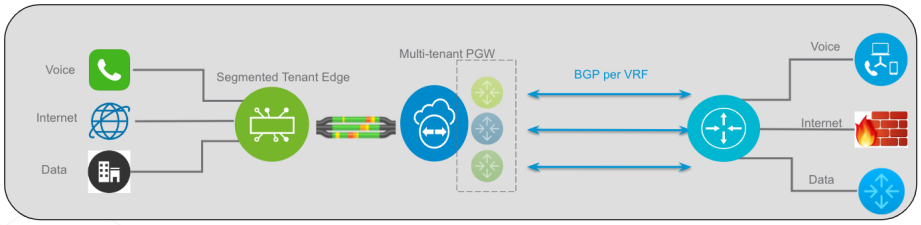

Figure 11: Segmentation with the Partner gateway solution

If there is a requirement to send PCI data, a separate PCI segment can be configured for the tenant. The Partner Gateway should also be assigned a CDE role to support the PCI functionality.

Business Policies

VeloCloud SD-WAN makes setting a policy as simple as a single click. In this solution, the state SD-WAN administrator providers can define business-level policies that apply enterprise-wide across many Edges, all through the centralized, cloud-based Orchestrator (VECO) with a different policy for each segment. For instance, multicast traffic may be prioritized as high in a Department of Transportation segment for near-real-time road sign updates, while a guest wireless segment may be rate-limited and classified as low priority. VoIP and video monitoring may be classified as real-time high class of service in a Department of Corrections segment with failover to wireless links, whereas in another segment, video might be forced to use wired links.

Link steering, link remediation, and QoS are all applied automatically based on those business policies; however, specific configuration overrides may also be applied. The centralized VMware Edge Cloud Orchestrator also provides an enterprise-wide view and configurability of routing in an overlay flow control table, eliminating complex node-by-node route configurations.

For the Partner Gateway deployment model, the business policies to classify and steer application traffic will be applied at each tenant's edge/profile level as the Partner Gateways are stateless devices.

Application and Internet traffic flow

In the overlay, Site-to-Hubs and Site-to-Site traffic is routed across SD-WAN tunnels using VeloCloud Control Routing Protocol (VCRP).

The underlay VMware SD-WAN solution fully supports all the standard routing protocols, including OSPF, BGP, Multicast PIM/IGMP, and static routing with IP SLA probes and responders. VMware employs static routing, OSPFv2, BGPv4 and BGPv6 to communicate with other network devices external to SD-WAN overlay, e.g., customer L3 switch, SP CE, or PE router. On both Gateways and Edges, BGP and OSPF are supported on a per-segment basis. The SD-WAN solution also carries the attributes of routing protocols over the SD-WAN overlay. For example, BGP path attributes such as AS-Path, local preference, and OSPF metrics are preserved and passed over the overlay to peer SD-WAN Edge. The Orchestrator provides a powerful and intuitive UI to configure BGP, OSPF, and multicast, so it's easier for an organization to decide on introducing SD-WAN into their existing network and defining policies to begin their WAN network transformation.

VECO maintains all the dynamically learned routes in an internal table called the Overlay Flow Control (OFC). The OFC table displays a summary view of all the routes in your network, including subnet, route type, preferences, etc.

Applications are automatically recognized and steered to the optimal link(s) based on business priority, built-in knowledge of application network requirements, and real-time link performance and capacity metrics. Dynamic per-packet steering can move a session, for example a voice call, mid-stream to avoid link degradation without any call drop or voice quality glitch. Single, high-bandwidth flows can utilize aggregated bandwidth for faster response times.

Internet traffic breakout can be offered in many ways with different methods per segment

- Local breakout directly out of the remote site broadband connection, with or without conditional backhaul failover to hub site if the local broadband connection is down
- Local SSE tunnel such as Symantec SSE for VMware VeloCloud or a third-party SSE provider, with or without conditional backhaul failover to hub site if the local broadband connection is down
- Backhauled centrally through the data center's hub firewalls with no local site breakout
- Backhauled to VeloCloud Gateways through SD-WAN optimized tunnels for SaaS traffic (requires premium license)
- A combination of the above with granular policies per application groups
- A Guest Wi-Fi segment could be created to only allow guests to access the Internet and not the state internal network. Cloud VPN would be simply turned OFF in the guest Wi-Fi segment and all traffic could be rate-limited to avoid over-consuming Internet bandwidth at smaller sites.

Summary matrix

As explained in the above 2 sections, there are many drivers that could push a SLED organization to adopt either a single tenant or a multi-tenant solution. This is a summary of the main differences between the two models:

	Multi-Tenant MSP solution	Single tenant Enterprise solution
Multi-tenancy	Y	N
Hub Edge required	N (function is served by Partner Gateway)	Y (function served by Edges)
Single Admin Group manages all edges	N	Y
Segmented traffic between agencies	Y	Y
SD-WAN sites to non- SD-WAN sites communication	Through Partner Gateway	Through Hubs or by using underlay routing
Partner Gateways required	Y	N
Ability for each agency to manage their edges	Y	N
Policy customization (QoS, Steering, remediation, Internet routing)	Y	Y
Enhanced Firewall Service on Edge add-on	Y	Y
VMware VeloCloud SASE by Symantec Cloud Web Security add-on	Y	Y

Resources

Both SD WAN solutions depicted in this document integrate seamlessly with the complete VMware VeloCloud SASE portfolio as follows:

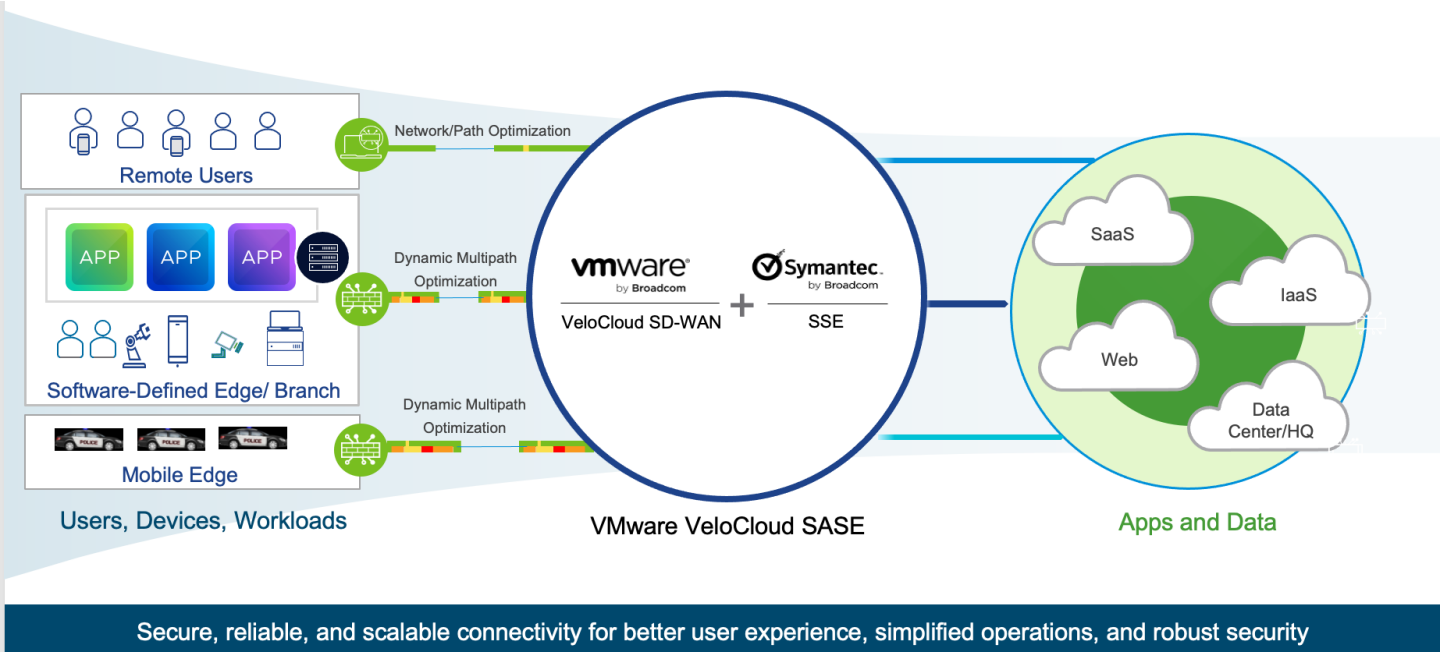

Figure 12: velocloud SASE architecture

- **VMware VeloCloud SASE, powered by Symantec:** Symantec's advanced cloud-delivered network security service enforces consistent web and cloud application security and compliance policies for all users, regardless of location and device.
- **VMware VeloCloud SD-Access:** a cloud-managed, secure, and high-performance remote access solution for today's distributed enterprise workforce. Based on zero trust network access (ZTNA), it replaces inflexible VPN infrastructure to enable work from anywhere and connect IoT devices.
- **Enhanced Firewall Service:** provide EFS security functionalities on VMware SD-WAN Edges. The NSX Security powered EFS functionality supports URL Category filtering, URL Reputation filtering, Malicious IP filtering, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) services on VMware SD-WAN Edges.
- **VMware Edge Compute Stack (ECS)** is an edge computing product portfolio that allows organizations to build, run, manage, connect, and protect edge-native applications at both the near and far edge locations. Typical examples in SLED would be compute services in road infrastructure (road signage, traffic sensors), environmental sensors (such as weather stations), or self-service kiosks. They can be orchestrated from the same VECO as SD-WAN.
- **VMware Velocloud SD-WAN datasheet** this is the specification document for the Velocloud SD WAN Edge hardware and software platforms, with details on performance capabilities, connectivity options and operating conditions. The document also includes a description of the solution and the license editions available to customers.

Appendix A - VeloCloud SD-WAN Security Components Description

All VMware SD-WAN components—including VMware Edge Cloud Orchestrator, VMware VeloCloud SD-WAN Gateways, and VMware VeloCloud SD-WAN Edges — meet PCI requirements. In addition, VeloCloud SD-WAN provides optional PCI-compliant points of presence (PoPs) with VMware Edge Cloud Orchestrator and VeloCloud SD-WAN Controller for customers who prefer to leverage the VeloCloud SD-WAN AOC to further simplify their PCI audits. VeloCloud SD-WAN will provide a PCI responsibility matrix upon purchase of the service.

In addition to security, VeloCloud SD-WAN offers multiple benefits including but not limited to improved appliance performance, simplified deployment, continuous visibility of network performance, cloud-scale at presence and easier management.

The table below shows the current state of VeloCloud SD-WAN compliance with common Security Frameworks.

FIPS 140-2 Strong Cryptography	SOC 2 Type 2 Controls at Service Organization	SOC 2 Type 1 Controls at Service Organization	Common Criteria Government Platform Security
Current	Current	Current	In-progress – 1QCY24
ISO 27001 ISO 27017 ISO 27018 Information Security	GDPR/DPA Data Privacy	PCI Payment Information Security	ICSA Firewall Commercial Firewall Security
Current	Current	Current	April, CY22

vmware® by Broadcom

Item No: bc-vmw-SLED-whitepaper-usletter 9/24