WHITE PAPER – **MARCH 2019**

GO MAINSTREAM WITH SD-WAN: MIGRATION BEST PRACTICES

vmware® | velocloud™ Now part of VMware

Table of Contents

Over the last couple of years SD-WAN technology has matured into a mainstream solution. Yet, the most appropriate migration path is not always clear. While there are many considerations to balance during a migration, the enduring benefit of an SD-WAN architecture is simplification: branch design, data center design, routing, edge platform choices, security choices, management.

To ensure an understanding of the fundamental concepts, let's quickly discuss the architecture and components of SD-WAN, and then move on to cover the best practices of various aspects of an SD-WAN migration.

Architecture and Components

If you're still new to the SD-WAN world, the essence of an SD-WAN comprises transport independence (broadband, LTE, MPLS, hybrid links), a secure overlay (flexible placement of firewalling, cloud security service insertion), dynamic path selection (continuous link measurements, deep application recognition) and a cohesive management structure (zero-touch provisioning, ReST APIs). Overall security is key, as is application performance. The overlay architecture is crucial: never having to rip and replace any part of your existing network during the migration.

The SD-WAN concept rests fundamentally on the separation of the control, data and management planes in the network. This separation allows significant flexibility in how and where services and functions can be deployed and how easily they are managed. There are three major components of an SD-WAN network to consider during a migration.

- **Edge**: Deploy branch, cloud and data center edges with a purpose-built hardware appliance, a virtual appliance, or a Virtual Network Function (VNF) running on a generic services platform.
- **Gateways**: This component is unique to the VMWare SD-WAN by VeloCloud solution giving optimized and secure access to cloud applications.
- **Orchestrator**: The all-in-one management station manages, monitors and troubleshoots the entire SD-WAN network. It can be deployed as part of the enterprise network, or hosted in a multi-tenant configuration by a service provider.

Key Considerations and Deployment Options

VMware SD-WAN offers great deployment flexibility. The enterprise can own and operate all the components on-premises, or you can choose a hosted solution where a service provider operates the gateways and orchestration, leaving only the branch devices in your care. These branch devices can be physical or virtual, and can be purchased or paid for using a subscription model. This provides not only deployment flexibility, but also budgeting (CAPEX vs. OPEX) flexibility.

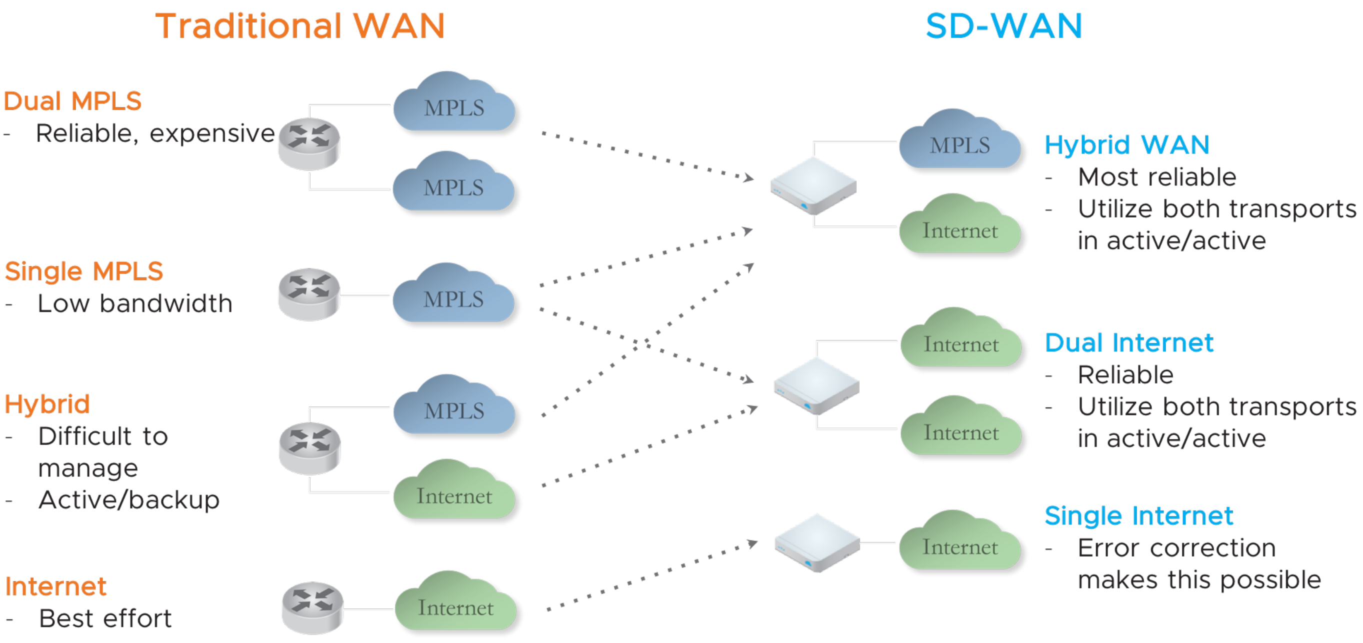
There are four key considerations when developing a migration plan.

- Where the components run, and who owns and operates them
- Site-type Migration
- Service Insertion
- Routing Strategy

Choosing the most appropriate model for your network determines where and how components are deployed.

COMPONENT	HOSTED (OPEX) MODEL	DIY (CAPEX) MODEL
SD-WAN Management	Eliminates management and maintenance overhead.	Full control by the enterprise. Requires ongoing maintenance.
SD-WAN Gateway	Leverages SD-WAN provider cloud infrastructure.	Sets up a hosting facility, or leverages a public cloud.
SD-WAN Edge	The edge function is available as subscription (hardware and/or software).	Edge function is purchased. Licensing may apply.

Map your traditional WAN site types to the most appropriate SD-WAN site type. SD-WAN architecture is an over-the-top overlay and transport-independent. These characteristics offer secure transport over public Internet links and superior application performance over any type of link leveraging SD-WAN features such as dynamic path selection, link sharing, and on-demand remediation.



Manage Complexity to Simplify Migration

Complexity leads to failures: complex systems result in complex failures. Assess your network to extract as much complexity as possible.

Assess the complexity in your network

Make sure you have a good understanding of the following issues.

- What is deployed: network diagrams; links and costs per site; IP addressing.
- The pain points: slow applications; site reliability concerns; sites with bandwidth constraints.
- Corporate initiatives: cloud migration; cost reduction; security policies.
- Obsolete technologies that should be replaced.

Determine which functions to move out of the branch

Centralize what you can; keep local what you must.

- Consider a Cloud Access Security Broker (CASB) for security functions
- Voice calling functions may move to a hosted VoIP provider
- Storage may use IaaS or be centralized in the data center
- Computing may use IaaS
- Localized applications may use IaaS or SaaS

With VMware SD-WAN's zero-touch provisioning and moving security firewalling and application hosting to the cloud, you could run zero-IT staff branches. Branch WAN optimization may no longer be needed and VMware SD-WAN does automatic load balancing, link monitoring and remediation. These changes provide significant branch cost-savings and simplification.

IP Addressing

Assign a meaningful address space to easily identify traffic origins, while also keeping enough free IP address space for future growth. VMware SD-WAN Overlay Flow Control (OFC) routing shows a unified view of all the subnets the SD-WAN has recognized.

Using a unique IP address space for each site is the most common deployment model. This practice allows branches to easily communicate via an overlay VPN. Alternatively, using overlapping address space in the enterprise is less common but a feasible deployment model. In this case, use segmentation to ensure segments of sites have a unique address space: all segments with no address space conflicts are VPN-capable.

DHCP, DNS and NTP

Your CPE device can be configured as a DHCP server for larger branches. For small branches you can use static IP addresses. A site can also use DHCP relay from a remote server if that is a more appropriate choice in your network.

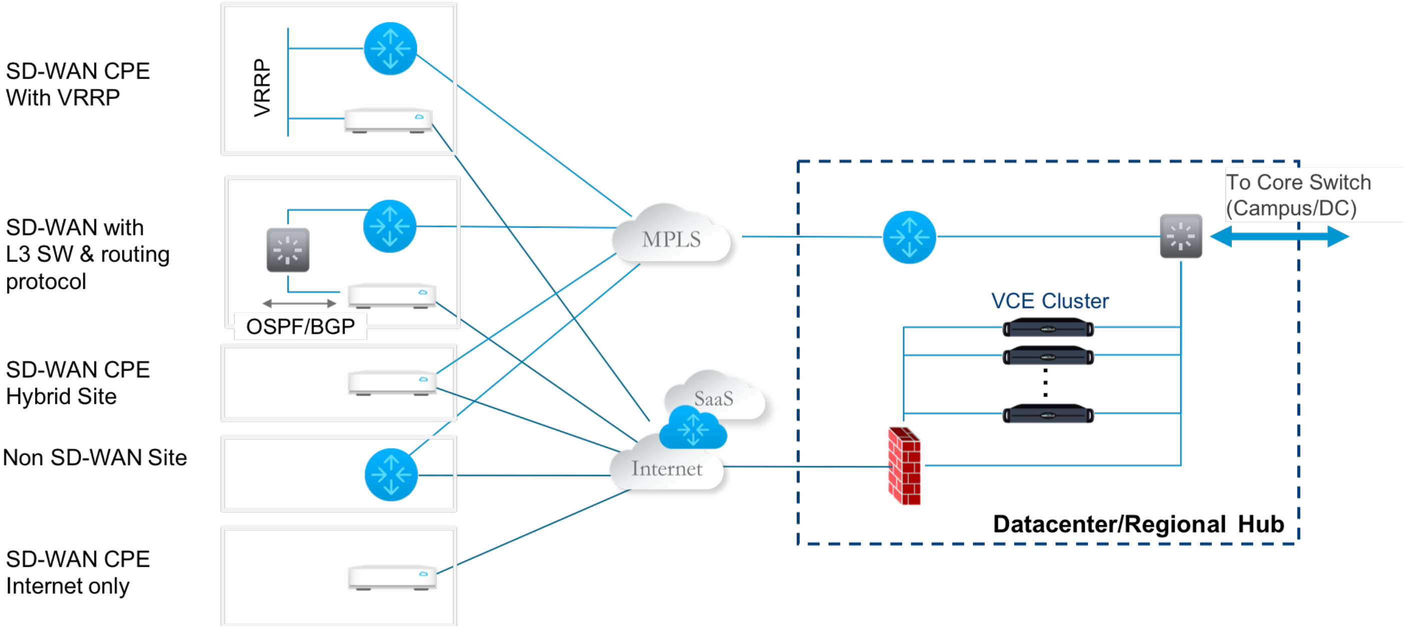
Use service provider-agnostic DNS servers for consistent treatment across sites in the enterprise. It is best to use public DNS or a private DNS server at the enterprise level (not the branch level).

NTP time synchronization is important to have a cohesive view at the Orchestrator of the sequence of events and statistics in your network. Edges automatically sync to public NTP servers. You may need a private enterprise NTP server for sites unable to reach a public server, for example, at sites with only an MPLS link and no Internet access.

Branch Design

Edge infrastructure with a VMware SD-WAN is highly flexible. You may deploy a physical hardware CPE device, or a software CPE device (VNF) running on a hypervisor, or a software-only cloud Marketplace subscription offering (e.g. Azure or AWS). You could also choose a hosted or an on-premises solution.

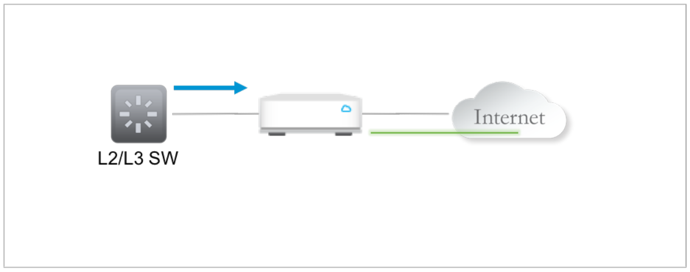
It is best to standardize branch design as much as possible. Smaller sites may require a different deployment model from larger sites, or the connectivity at a site (Internet or MPLS or both) may dictate the most appropriate model. There are several deployment models to choose from.



The VMware SD-WAN CPE can augment the branch; it does not have to replace your existing installation: it may run behind the Layer 3 router, or you could pair it with the CE router and run static routing, or any traditional routing protocol such as OSPF/BGP.

It is recommended to have at least two separate connections for sites with Internet-only connectivity; in the best case the links should be of diverse technologies and from different providers. If an LTE link is used as an active link (i.e. not for standby), control traffic consumes bandwidth on this link even if the SD-WAN overlay is configured not to use the link for data-plane traffic.

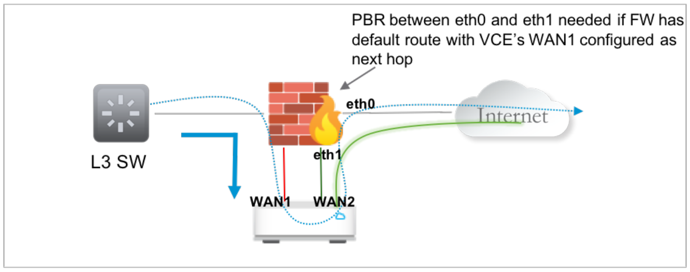
A site with Internet-only connectivity can be configured as either in-path or off-path. There is no particular best practice, both models have pros and cons.



Edge is in path and the default gateway for all traffic

Pro: Simple. Recommend & common when branch has only L2/L3 switch

- Easy if branch uses DHCP so readdressing is simple
- Traffic will stop if the VCE fails. Propose HA or VRRP if availability is a concern
- Internet traffic should be backhauled or filtered through Cloud Web Security (CWS). Split-tunnel Internet traffic should only be allowed with local firewall presence

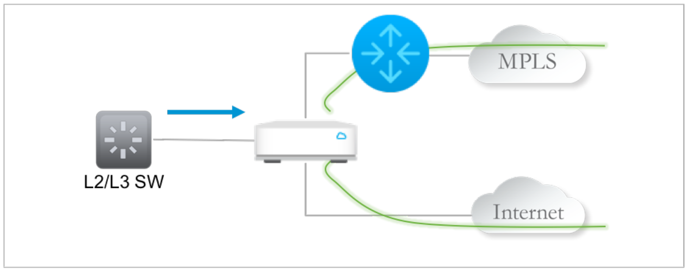

PBR between eth0 and eth1 needed if FW has default route with VCE's WAN1 configured as next hop

Edge is off path and is the default gateway for FW

Pro: Automatic fallback when VCE fails. HA not required for survivability

- FW or L3 SW redirects traffic to SD-WAN overlay - using OSPF, BGP, or IP SLA with static route)
- Redirection stops if VCE fails and traffic follows original path
- Bi-directional PBR needed on the FW to prevent looping of split-tunnel Internet traffic
- Internet traffic forwarded to VCG (via Business Policy) on WAN2 not visible to FW

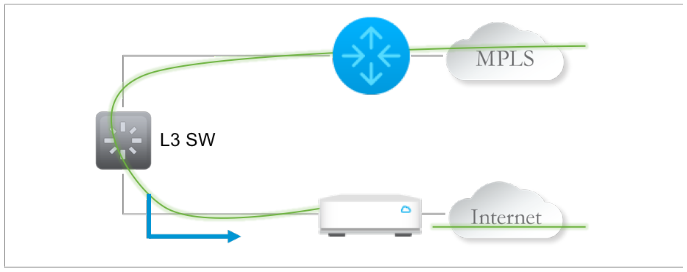
A site with hybrid connectivity can be similarly configured as in-path or off-path. All in-path deployments should consider a high availability (HA) solution.



Edge is in path & the default gateway for all traffic

Pro: Simple. Recommend & common when branch has only L2/L3 switch

- Overlay tunnels built across both MPLS and Internet
- Traffic will stop if the VCE fails. Propose HA or VRRP if availability is a concern
- Internet traffic should be backhauled or filtered through Cloud Web Security (CWS). Split-tunnel Internet traffic should only be allowed with local firewall presence



Edge is off path & is default gateway for L3 switch

Pro: Automatic fallback to MPLS when VCE fails. HA not required for survivability

- L3 switch redirects traffic to SD-WAN Edge (OSPF, BGP, or IP SLA with static route).
- Traffic to other SD-WAN sites may tunnel through the L3 SW
- Redirection stops if VCE fails and traffic follows through original MPLS path
- Split-tunnel Internet traffic should only be allowed with local firewall presence

WAN Optimization (WANop) may no longer be required due to several industry trends:

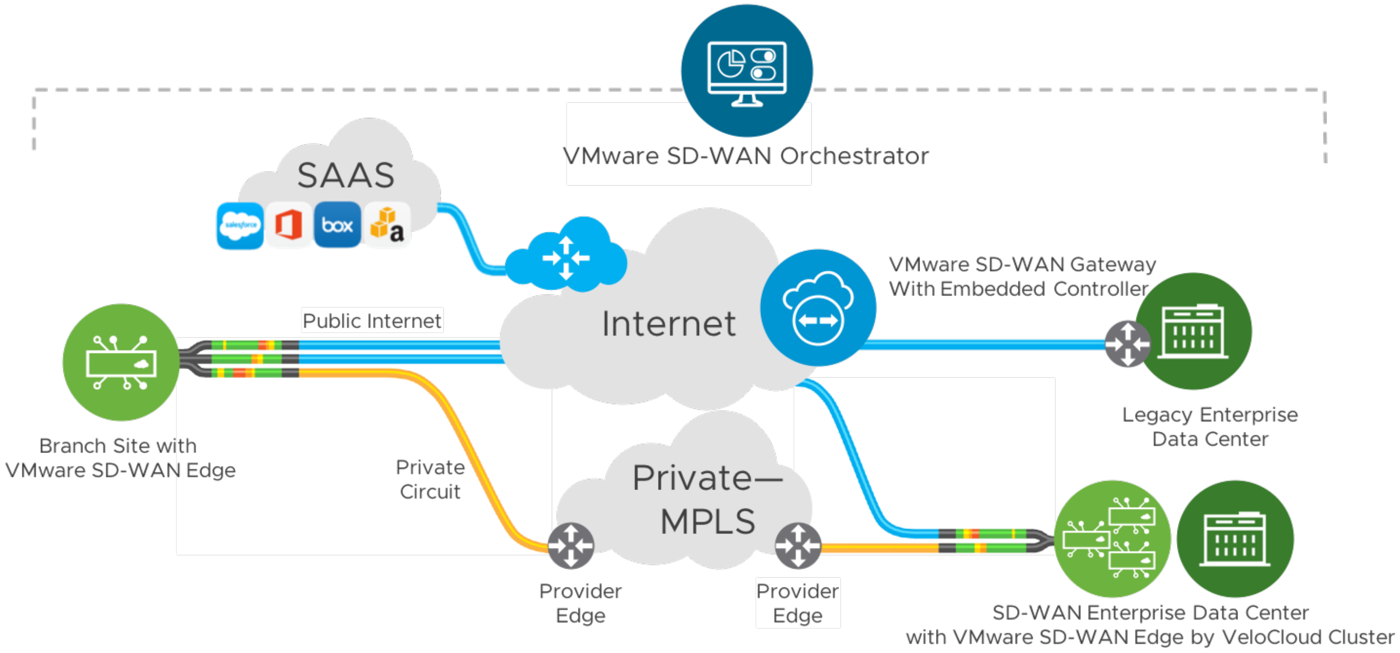
- Last mile bandwidth is less constrained than in the past
- Applications are increasingly moving to the cloud
- Recent-vintage applications tend to be less chatty than earlier and therefore perform better over WANs
- Many applications now incorporate native encryption

If WANop is still needed in your network, perhaps due to expensive long distance MPLS links, it may be better located at a regional hub site and not at each branch.

Data Center Design

The primary WAN concern at a data center is scalability. The large number of connections (likely VPN tunnels) that aggregate at the data center site requires a highly available solution that also scales readily. A clustering solution may be a good fit.

If you haven't yet migrated the data center to an SD-WAN, you can connect that site to your SD-WAN network by building a secure tunnel from an SD-WAN Gateway: this is referred to as a non-VMware site (NVS) tunnel. Alternatively, you can install a virtual or hardware edge device running an SD-WAN virtual instance, configured as a hub device.



Security Architecture and Firewalling

Most enterprises still use a data center with a centralized firewall, even for branch-originated Internet-bound traffic. But there are several firewall deployment approaches to consider: use an on-premises firewall integrated in the SD-WAN device (hardware or VNF), backhaul all Internet traffic through the centralized data center firewall, or use a Cloud Access Security Broker (CASB).

Built-in Firewall

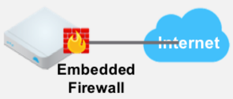
Application Aware

Embedded

Can be disable in favor of external physical firewall

Integrated rule set

Default to block inbound



CASB Integration

Best of breed integration

Direct or via Gateway

Zscaler, Forcepoint

Use Business Policy to redirect select traffic to CASB providers

Internet
CASB

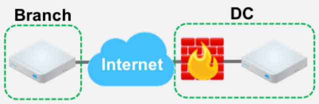
Centralized Firewall

Backhaul to the DC

Use existing DC security infrastructure

Backhaul via a hub or a Non-VC-Site

Use business policy to redirect select traffic to the DC based firewall



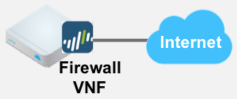
Firewall VNF

Best if breed integration local at the Edge

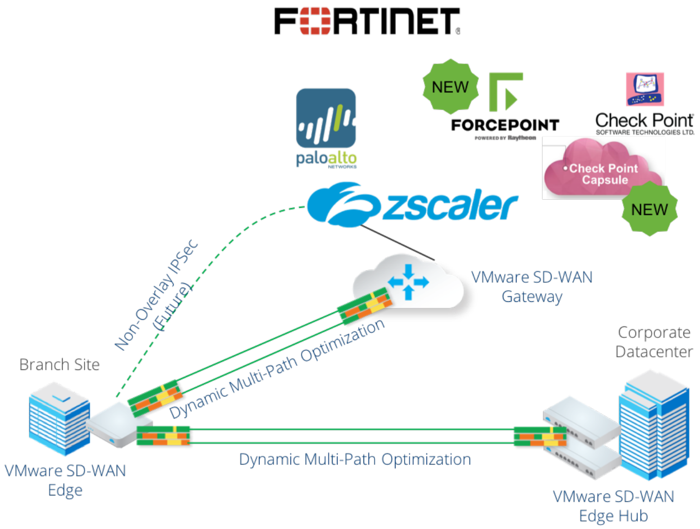
Use Edge based hypervisor

Fixed service chaining

Palo Alto Networks



You can design your network to use a direct IPSec tunnel to cloud-based security services for all Internet traffic from a branch. A VMware SD-WAN architecture integrates with best-of-breed security partners such as Zscaler or Check Point. Benefits of this approach include avoiding backhauling traffic to your data center, leveraging VMware SD-WAN Dynamic Multi-Path Optimization (DMPO) to deliver cloud-application performance and reliability, enabling single-click application-aware policies for granular service insertion, and automated tunneling that eliminates onerous per-site configurations.



Routing

There are several routing strategies to choose from.

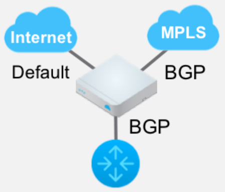
BGP

For CE replacement

Support for LAN side peering

Advanced filtering capabilities

Uplink feature to prevent transit

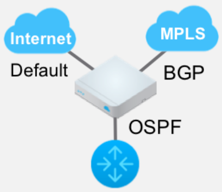


OSPF

LAN side neighbor

Can redistribute into BGP

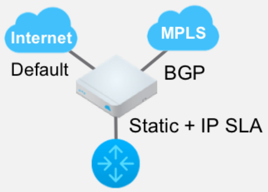
Supporting existing LAN side deployments



Static + IP SLA

Legacy support: Routers that do not support OSPF or BGP

SLA to detect unavailability of a subnet



VMware SD-WAN automatically redistributes routes within the overlay network, and can also be set up to automatically redistribute routes between the overlay network the non-overlay legacy network. This decision hinges on whether legacy branch sites are reached from the SD-WAN via the data center, or directly via the underlay network. Internet-only branch sites can only be reached via the data center. Hybrid sites with both Internet and MPLS connections can use the underlay network. Wherever possible, use the data center as the transit site as the data center knows all the routes, as well as how to reach non-SD-WAN legacy sites. The VMware SD-WAN solution supports both BGP and OSPF static clouds. For a site unable to run these protocols, you can use static routing and IP SLA.

Business Policy Considerations

It is key to make a list of business-critical applications in your network and to understand from your users which applications are critical to their jobs. Business-critical applications should be given network priority, while non-critical or non-business applications are rate-limited or blocked.

Once you set the applications and their priorities, the VMware SD-WAN solution implements your business policies with DMPO, automatic link sharing and on-demand remediation.

Ongoing Monitoring

Monitoring should be automated. The ReST API features of the SD-WAN can be leveraged if you are using a third-party monitoring tool.

Summary

SD-WAN migration need not be a difficult task. Migrating can simplify many of the network design choices, configurations, traffic flows and management tasks required by a traditional WAN. Yet an SD-WAN provides significant flexibility with many different deployment options to optimize your cost, the use of your staff, application performance, best-of-breed security solutions, traffic routing, as well as removing complexity from your network.

An SD-WAN migration does not require you to replace or disrupt your existing network; the SD-WAN is introduced as an overlay network and you can migrate a site at a time, and have both your legacy WAN and the SD-WAN run in parallel. This paper discusses some key considerations to keep in mind as you prepare for the migration, including concerns such as branch link connectivity, routing access between the SD-WAN and legacy networks, application priorities, where best to locate firewalling, and whether or not hardware or VNF edges make more sense in your network.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com