VMware SD-WAN and VMware NSX Data Center

velocloud™
Now part of VMware

A software-defined approach

The demand to rapidly decentralize the hosting and operation of business functions, in order to enhance the success of a business, is increasing. The challenge faced by organizations in pursuit of this goal is the complete lack of visibility, control, and consistency in a network fabric that spans the data centers and wide area networks where the applications that drive these business functions exist and transit.

In order to successfully decentralize to achieve scale, higher levels of availability, and business agility, an organization must embrace a software-defined approach to developing a unique network fabric that allows an application stack to untether itself from the traditional data center dependencies, such as a storage area network (SAN), physical core network, core-edge, and compute machines. In a software-defined world, an application stack can be wrapped in just-in-time networking for a path to be paved directly from sources to destinations.

To fully realize a software-defined application platform, we must look to overlay technologies to provide this capability. Combining overlay technologies with automation and a decoupling of the management, control, and data planes, helps us achieve an optimal software-defined state.

The VMware Virtual Cloud Network (VCN) has a broad set of capabilities for various forms of applications. The VCN is a cloud networking fabric, with intrinsic security, powered by a network completely delivered in software.

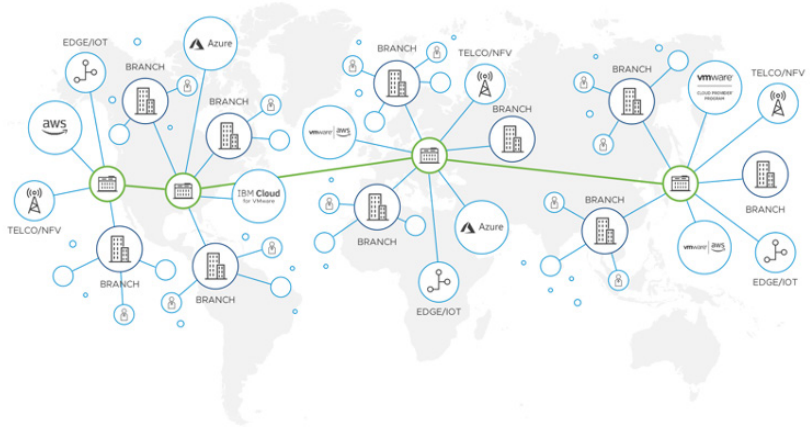

FIGURE 1: Virtual Cloud Network

The VCN has allowed us to commoditize both the physical network and the physical wide area network (WAN) using two key technologies: VMware NSX® Data Center for the data center and VMware SD-WAN™ by VeloCloud® for the WAN.

vmware®

Providing seamless connectivity and integration

How do we go about providing seamless connectivity and integration into each respective domain?

To start, if your deployment has already leveraged software-defined wide area network (SD-WAN) and you have an island of resources serviced and protected by VMware NSX Data Center, you have achieved an initial state connectivity. This initial state allows you to leave intact your existing NSX footprint by utilizing an SD-WAN enabled branch to create a non-VMware SD-WAN site (NVS) connection to this island. An NVS is simply a mechanism for connecting a non-SD-WAN site. This may be due to an acquisition of a company or simple consolidation of various resource islands. With an NVS, an IPsec tunnel with appropriate parameters is established from an edge/hub to a VMware SD-WAN Gateway, and from the Gateway to the VMware NSX Data Center Edge for IPsec termination.

Once you are ready to extend further SD-WAN capabilities, you can then deploy a physical or virtual VMware SD-WAN Edge appliance in the same data center where VMware NSX Data Center lives. This setup is advantageous because you are truly leveraging the software-defined fabric to support the needs of your applications, regardless of where they reside.

VMware NSX Data Center key concepts

VMware NSX Data Center decouples networking and security functions from physical hardware components and delivers an abstraction completely in software. Traditionally, networking functions are performed by physical appliances that contain integrated data planes (packet forwarding), control planes (networking protocols) and management planes (the CLI). At the same time, the control plane is, by necessity, distributed and relies on collaboration and synchronization between the physical devices in order to establish a forwarding fabric.

The Software-Defined Data Center (SDDC) takes the approach of separating the data, control, and management planes and uses a centralized control plane in the form of controllers and a centralized management plane for configuration, troubleshooting, and more. These reside as three highly available and federated virtual appliances in virtual machine (VM) format. Each appliance contains both the management plane function, as well as the controller function. The VMware NSX Data Center data plane is where all NSX application traffic is routed, forwarded and firewalled efficiently.

The NSX Data Center data plane consists of familiar networking functions such as:

- **Overlay switching**
- **High-performance distributed routing**
  - Logical routing done in hypervisor kernel
  - Optimizes routing for east-west communication
  - Routing done closest to source
- **Distributed L2-L7 firewalling**
  - High-performance east-west firewall
  - Delivery of context-aware microsegmentation
  - Kernel-based, distributed amongst all hosts

With further data plane extensions made possible by the platform to achieve the extensive ecosystem. Figure 2 highlights key VMware NSX Data Center capabilities. Overlay switching by VMware NSX allows for Layer 2 to span Layer 3 using overlay techniques, such as Virtual Extensible LAN (VXLAN) or Generic Network Virtualization Encapsulation (GENEVE). This capability allows IP subnets to stretch across Layer 3 boundaries, across geographical locations. This addresses significant use cases around disaster recovery and workload mobility.

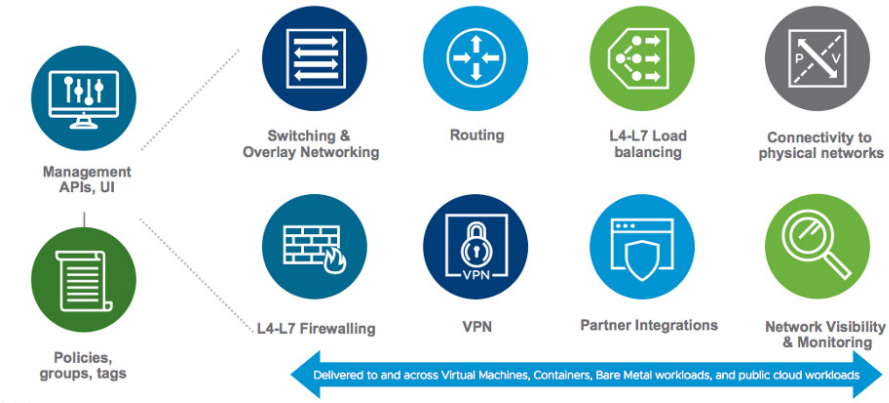

FIGURE 2: VMware NSX Data Center networking and security capabilities

VMware NSX Data Center is hypervisor and cloud-agnostic and is meant to provide a unified security and networking framework, delivered in software, to any kind of workload. NSX Data Center is meant for true workload decentralization and hybridity.

NSX Data Center natively provides tenancy using the concept of tiered gateways. Currently, NSX-T Data Center supports multiple Tier-0 (T0) gateways, with numerous Tier-1 (T1) gateways. T1 gateways act as points of tenancy where multiple T1 gateways are deployed and are backed to T0 gateways. This provides great scale for multiple operating environments and allows for overlapping subnets within a given environment. In short, the T1 acts as a distributed routing entity to enhance east-west communications, while the T0 acts as a centralized routing entity to provide stateful services and connectivity to the physical network. The T0 provides much more functionality, specifically, north-south communication, Border Gateway Protocol (BGP), and virtual private network (VPN) capabilities. This will align to VMware SD-WAN segments. T1 gateways can also provide IPsec VPN capabilities.

NSX Data Center has native capabilities for security. More specifically, it has micro-segmentation capabilities in which two or more entities, regardless of which networks they are a part of (same or different), can be segmented at a micro level. Effectively, this is the concept of bringing security, or more specifically, distributed firewalling, closest to the workload. In short, two or more end-point objects will have respective L2-L7 firewalls, which police traffic both on the ingress and egress. The concept of security adheres to the model where security follows the workload.

VMware SD-WAN key concepts

VMware SD-WAN is a cloud delivered software-defined WAN solution that provides assured application performance, delivers east on-ramp to the cloud, and provides simplified management. VMware SD-WAN aims to simplify connectivity, while providing security from branches to data centers and cloud locations.

The VMware SD-WAN solution is comprised of a decoupled management, control, and data plane. The management plane is the VMware SD-WAN Orchestrator. It is the single pane of glass for all management, operations, and visibility. All activities start at the VMware SD-WAN Orchestrator from configuring, operating, and monitoring to troubleshooting.

The control plane is a function of the VMware SD-WAN Gateways, in which the VMware SD-WAN Gateways deployed in the cloud act as learning agents for the entire SD-WAN. They act as mid-mile constructs which get us to the last mile. The VMware SD-WAN Gateways learn routes and prefixes and maintain this information with the VMware SD-WAN Orchestrator. The VMware SD-WAN Gateways, being stateless, obtain configuration from the Orchestrator, giving us immense scalability. VMware SD-WAN Gateways can be deployed non-impactfully, while providing increased horizontal scale. The VMware SD-WAN Gateways can be leveraged as a data plane if there is a requirement to connect to an NVS or any software as a service (SaaS)-based offering.

The VMware SD-WAN Edge is the final piece of the puzzle, which acts as the primary data plane of the solution. While maintaining a database of all clients connected, the VMware SD-WAN Edge is used to make intelligent steering decisions of application traffic using an umbrella of technologies. We refer to this umbrella as VMware SD-WAN Dynamic Multipath Optimization™ (DMPO). The VMware SD-WAN Edge uses DMPO to make intelligent decisions about whether to send and steer traffic on a particular link, or all links. DMPO also enables sub-second failover to secondary, tertiary or even quaternary links to ensure a particular stream of traffic isn't dropped mid-flow.

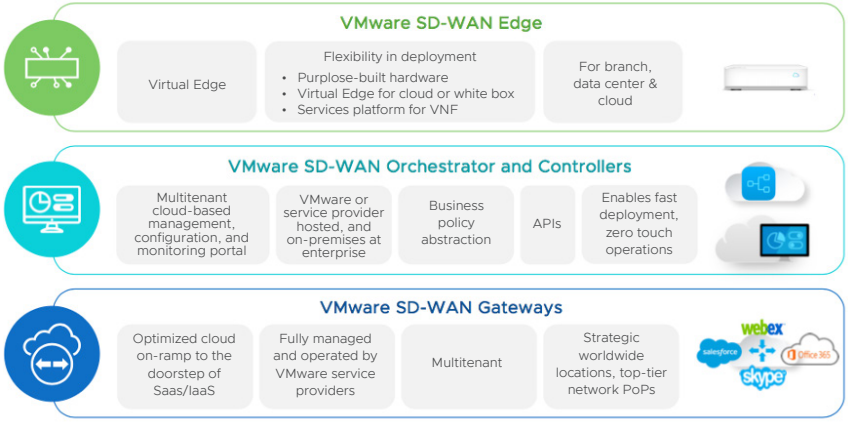

FIGURE 3: VMware SD-WAN components

As defined by Gartner, key capabilities of an SD-WAN solution must include the following:

- Transport independence
- Secure overlay
- Dynamic path selection
- Simple interface

VMware SD-WAN strongly adheres to these key capabilities and more, while also adhering to key business values, including, cloud on-ramp, assured application performance and simplified WAN management. Let's have a look at key features of the solution that help address unique use cases.

Zero touch deployment

The ability to minimally touch a VMware SD-WAN Edge, while the deployment of this Edge is done through the VMware SD-WAN Orchestrator.

Redundancy and scale

Being able to achieve redundancy using high-availabilities principles on both the VMware SD-WAN Edge and VMware SD-WAN Orchestrator side. The VMware SD-WAN Edge can be deployed in a high availability (HA) pair for active/standby traffic operations, or active/active in a clustered configuration. The VMware SD-WAN Orchestrator is backed onto cloud technologies and is built on cloud HA principles. The VMware SD-WAN Gateway, as a stateless entity, can be spun up on-demand, and torn down when required. This provides horizontal scale.

Assured application performance

DMPO provides the following key capabilities which contribute to the overall VMware SD-WAN solution.

- **Deep application recognition engine (DAR)** – A deep packet inspection (DPI) engine containing 3000+ applications for correct recognition and classification of traffic.
- **Overlay protocol** – VeloCloud Management Protocol (VCMP) is the tunneling mechanism that allows for multitenancy and segmentation, while, at the same time allowing for utilization for multiple links. Re-assembly of packets is done using the VMware SD-WAN Edge.
- **Link qualification** – Measurements of bandwidth, latency, jitter, and packet loss to be populated and calculated in the VMware SD-WAN Orchestrator for the best steering of traffic.
- **Application-based steering** – Leveraging business policy to steer traffic according to traffic type and provide on-demand remediation.
- **On-demand link remediation** – Leveraging forward error correction (FEC), negative-acknowledgement (NACK), and de-jitter buffer to condition the link and provide sub-second steering.
- **Business policy framework** – A policy-link framework that resembles a firewall rule table but simply dictates how traffic should flow out of a VMware SD-WAN Edge.
- **Cloud VPN** – The simplification of construction of VPN tunnels from site-to-site, site-to-hub, or site-to-NVS, using a few checkboxes. This feature will automatically construct IPsec VPN tunnels to respective locations based on traffic needs.
- **Routing capabilities** – With routing configurations around BGP, Open Shortest Path First (OSPF) and static routes with IP service-level agreement (SLA), you can click your way to a simple routed design or something a touch more complex.
- **Segmentation** – This main security and tenancy feature of the VMware SD-WAN solution, is what is used to separate different types of traffic from product to test to

payment card industry/cardholder data environment (PCI/CDE).

- **Security service chaining** – While the VMware SD-WAN Edge provides a local firewall, sometimes it might be necessary to service chain to an industry-standard unified threat management (UTM) appliance. Using automation and the principles of virtualization, the ability to run a virtual network function (VNF)-firewall alongside the SD-WAN software in a singular box, is entirely achievable.
- **API and automation capabilities** – The API is made available for those wishing to integrate into a third-party system, or to leverage programmatic languages to capture information from the VMware SD-WAN Orchestrator.

SD-WAN connecting to a non-VMware SD-WAN site

Typically, if an SD-WAN solution is already deployed, it is highly likely that it has been deployed in a phased approach. Certain sites may not be SD-WAN enabled, meaning they may not have an SD-WAN edge deployed at the branch. How do these sites connect back? The current two options are by specifying a particular site as a Non-VMware SD-WAN site (NVS) and connecting via IPsec or, by going direct through the private underlay via Multiprotocol Label Switching (MPLS) or equivalent circuit.

When reaching an NVS site direct through the underlay, the Overlay Flow Control (OFC) table is leveraged. In the OFC, we can observe a route that specifies a branch prefix being reachable only through this direct underlay.

When not going through the underlay, this site can be specified as an NVS and through the Cloud VPN, an IPsec VPN can be deployed. In this scenario, we are calling on the VMware SD-WAN Gateways (or designated Hubs) to construct the last mile VPN. In certain situations, the site in question might be a potential future hub. As a result, the VMware SD-WAN Gateways must be used to establish IPsec tunnels to this location. Through the VMware SD-WAN Orchestrator the NVS is deployed and an IPSec configuration for the NVS site's branch device is created for simplification and ease of configuration. Once the configuration is applied, we can verify the connection state as being up in the VMware SD-WAN Orchestrator. We can additionally see the events within the VMware SD-WAN Orchestrator to see a tunnel established.

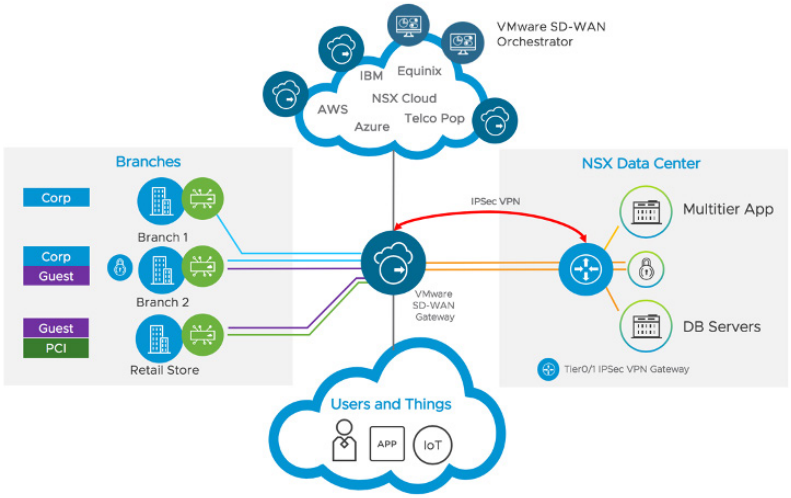

FIGURE 4: VMware SD-WAN to NVS

Once we've established an IPsec VPN to an NVS using the VMware SD-WAN Gateways, we now have connectivity between SD-WAN enabled branches and NVS sites. Branch locations enabled for SD-WAN can reach applications or functions within the data center, which is now an NVS. The NVS site is the data center containing NSX Data Center. The point of VPN termination can either be the T0 gateway or T1 gateway in NSX-T Data Center.

VMware SD-WAN segment extension into NSX Data Center

With VMware SD-WAN, the concept of isolation and security is provided using segmentation. Segmentation allows for a VCMP tunnel to carry a specific segment header for a given Enterprise ID. For example, an Enterprise ID might contain multiple different segments that cannot communicate with each other such as, voice/video, PCI, guest, corporate, or customer-facing segments. These can be analogous to virtual routing and forwarding (VRF) in the routing world. Each segment can be configured on a profile level; edges assigned to a profile will inherit the segments and capabilities configured within each segment.

In NSX-T Data Center, the concept of isolation, tenancy, and security is achieved using the tiered routing constructs, the T0 or T1 gateways. The T0 gateway can be comprised of both service router and distributed router constructs. With the T0 SR, we can establish BGP connectivity north-bound. With the ability to establish connectivity, we can now effectively peer, on a per-segment basis, from multiple T0s to multiple segments. More specifically, each T0 deployed will house a tenant or segment, and that specific T0 will map to a VMware SD-WAN segment. By doing so, only the necessary prefixes originating from each individual T0 will be shared into each respective segment. Prefixes will not be learned on all segments, only the ones mapped to their T0 segment association. Once achieved, VRF-like isolation is present, and all segments and tenants communicate within their respective segments, while still maintaining isolation.

Take, for example, a CDE that must be PCI compliant. This requirement of CDE is that it must maintain isolation from the current production network. In NSX-T Data Center you will leverage the T0 and its connected logical networks, and it will be isolated from other networks backed onto other T0 gateways. Those same T0 gateways will map and connect to their respective segments in VMware SD-WAN. The PCI segment configured on the VMware SD-WAN Edge will map to the PCI specific T0 gateway. Isolation is present all throughout both software-defined environments, providing secure end-to-end segmentation and connecting NSX-T Data Center together with VMware SD-WAN.

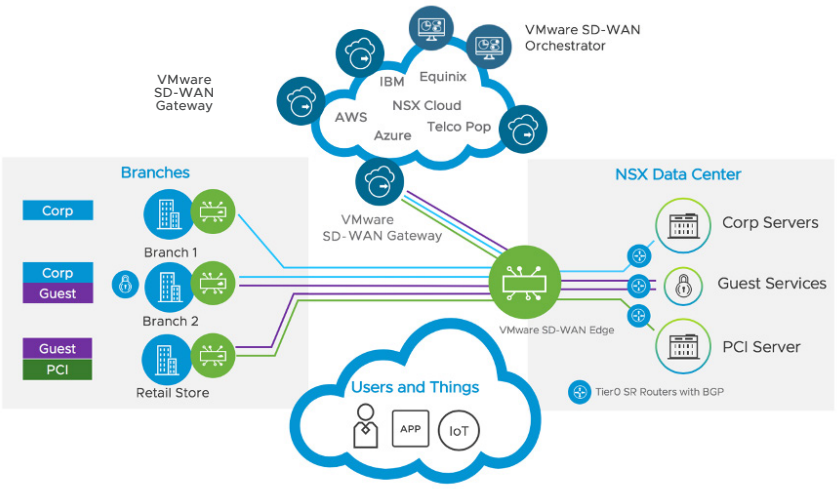

FIGURE 5: VMware SD-WAN segments extended into NSX Data Center

End-to-end visibility with vRealize Network Insight and VMware SD-WAN

vRealize Network Insight (vRNI) is an end-to-end network visibility solution which allows administrators to visualize how traffic moves from one endpoint to another within a data center and from branches to data centers to clouds. vRNI uses telemetry and metadata typically from compute managers, like vCenter, as well as cloud environments, such as Amazon Web Services (AWS), and Microsoft Azure. Using the APIs of vCenter, AWS, Azure and others, data about objects are shared with vRNI. Additionally, IP Flow Information Export (IPFIX) and NetFlow information of various network devices is captured to understand and correlate flow data to metadata. With enhancements to VMware SD-WAN's visibility and capabilities around IPFIX and NetFlow, flow records from client endpoints originating from VMware SD-WAN Edges can be populated within vRNI. The overlay and underlay health of VMware SD-WAN branches, in addition to traffic metrics, packet metrics, and which applications are being accessed, are all shared with vRNI using the VMware SD-WAN Orchestrator's API.

With vRNI having full visibility into VMware SD-WAN and NSX Data Center, we now have full end-to-end visibility from a branch user flowing through a VMware SD-WAN Edge to an application protected by NSX Data Center, allowing for a very powerful Day-2 operations tool.

Looking ahead

While integrations are already in-place to support VMware SD-WAN and NSX connectivity and visibility, further integrations will be made available. Looking ahead, policy management and automation between SD-WAN and NSX will be the next major development.

While both VMware SD-WAN and NSX Data Center offer software-defined solutions in their respective spaces, both technologies can collaborate together to provide a unified, secure connective fabric. This fabric is delivered in software to allow complete agility and consistent performance of applications. As both technologies continue to grow, there will be additional integrations to ensure the best possible and consistent experience for any device, any application, and any cloud.

For more information see, *www.velocloud.com*.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: sdwan-879-vmware-nsx-data-center-so-0420 5/19