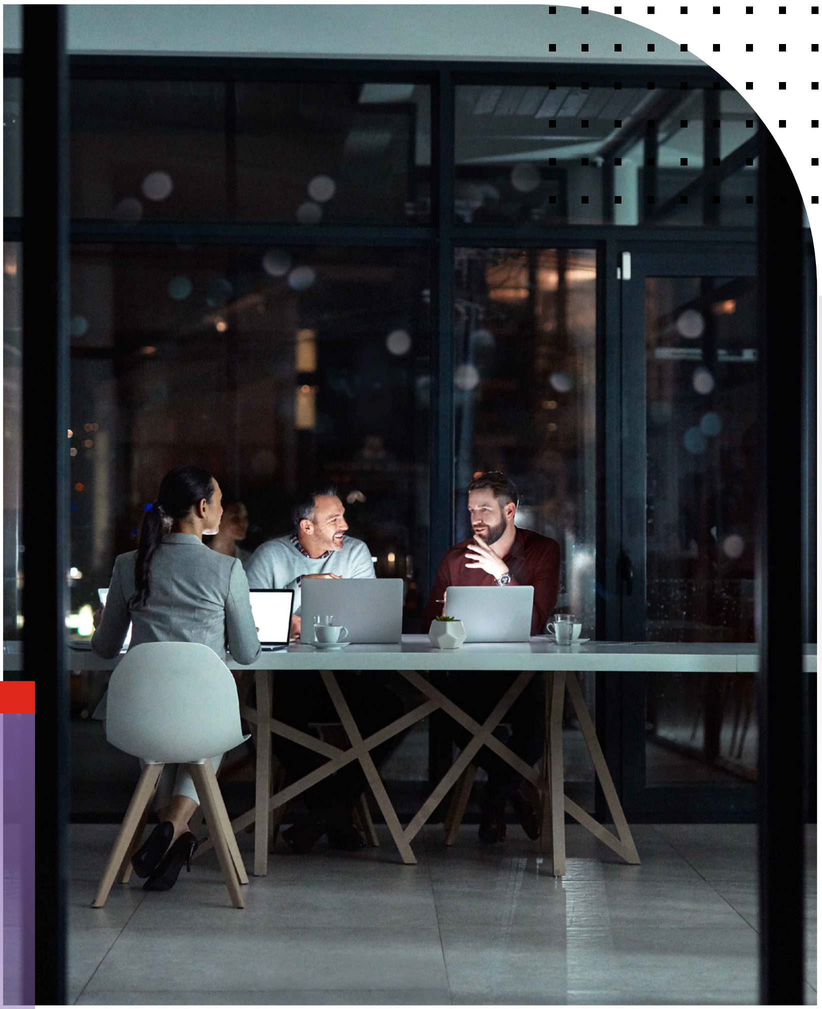
WHITE PAPER

SD-WAN Enables a Multi-cloud Freeway



Executive Summary

The COVID-19 pandemic only accelerated the already rapid pace of digital innovation at organizations in every industry.[1] This velocity of change is enabled by cloud-based services and solutions, which facilitate quick rollouts, scalable infrastructure, and minimal capital expenditure. The result is that the vast majority of enterprises—and an increasing number of small and midsize businesses—now operate hybrid clouds and even across multiple clouds.

A multi-cloud architecture enables organizations to deploy a reliable and technically appropriate infrastructure for each service, but it brings complications as well. It expands the attack surface and makes security management more challenging. It also complicates the task of connecting users to all the services they need to access, and of integrating applications and workflows that need to interact with each other.

In the words of one observer, "Clouds were born to be complex because applications were able to break away from the confines of the racked physical servers, storage, and networking devices. Once unleashed, new ways to manage, ensure, and secure applications would be required."[2] And yet the complexity of multi-cloud architectures makes finding these new ways difficult.

"Multi-cloud computing lowers the risk of cloud provider lock-in, and can provide service resiliency and migration opportunities, in addition to the core cloud benefits of agility, scalability, and elasticity."[3]

Complexity Brings Inefficiency

For example, each of the three largest public clouds in North America—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—has its own networking constructs, management consoles, and security and networking tools. They are essentially incompatible with each other, and this complicates the task of administering a multi-cloud architecture.

For network architects, connecting each public cloud with headquarters, branch offices, and the corporate data center is challenging. Configuring the correct routes and setting up and maintaining virtual private networks (VPNs) can be a waste of time if one works within each provider's console. This is because it's a largely manual process—and even automation across the various clouds is different. These increase operational complexity and security risks.

SD-WAN Addresses Complexity

Software-defined wide-area networking (SD-WAN) technology was originally developed to provide highly available WAN connections to branch locations, delivering superior performance and cost effectiveness compared with traditional WAN. But it can also play a key role with cloud connectivity. SD-WAN gateways can steer applications over policy-defined links and automatically set up Internet Protocol security (IPsec) tunnels to and across cloud service providers—all from a centralized console.

The big three cloud providers have taken steps to make it easier to support SD-WAN gateways. AWS has introduced Transit Gateway Connect designed to connect AWS VPCs in each region to a transit VPC with an SD-WAN gateway that aggregates connections from on-premises locations. GCP has launched its Network Connectivity Center with more robust options for connecting Google Cloud VPC virtual private clouds with branches and data center networks. And Microsoft has built features into its virtual WAN to integrate with SD-WAN gateways and extend connectivity to Azure virtual networks from branch offices and remote sites.

This means that SD-WAN technology can be used as a cloud overlay network to connect branch offices to cloud services, virtual networks within a single public cloud, and even across multiple clouds with one another. Its ability to prioritize traffic by application enables the most critical traffic to receive priority, and its ability to steer traffic over multiple routes for the best performance makes it ideal as a multi-cloud overlay. Access and security policies are centralized, and administrators have full visibility into application traffic, performance, and security.

Public Cloud as Transitway

While most public cloud use cases focus on applications and workloads, cloud providers have built out high-speed network backbones, and customers can take advantage of this infrastructure to simplify cloud connectivity, boost performance, ensure security, and improve agility. SD-WAN technology makes the cloud provider network backbone more efficient for organizations to deliver the best application experience.

For instance, if a company had a business requirement for a high-performance, low-latency connection between two branches in different parts of the country, the network team could leverage a cloud provider's backbone as the transport. In this use case, secure SD-WAN in each branch and in the public cloud can be used to set up IPsec tunnels that will traverse the cloud provider's backbone.

SD-WAN as Information Freeway

The idea of deploying SD-WAN in branch locations to enable public cloud access is well understood. As organizations embrace a fuller multi-cloud strategy—deliberately or by default—they can extend their SD-WAN investment to support hybrid cloud and multi-cloud deployments, enabling highly secure and efficient network traffic across an enterprise.

"Multi-cloud is not the same as hybrid cloud, in which public and private clouds are integrated. Multi-cloud simply means that organizations have the flexibility to select the best cloud provider for each of their various infrastructure and application needs."[4]

These flexible and rapid "freeways" route traffic efficiently and securely between users and different clouds, between different services in a single cloud, and between multiple public and private clouds. Ideally this would all be centrally managed and monitored. Unlike physical freeways, constructing and maintaining them does not cause major disruption. Once the IPsec tunnels are set up, secure SD-WAN technology automatically prioritizes traffic and ensures that each packet is sent over the most efficient route.

SD-WAN as Part of a Security Fabric

All of these connections of course must be monitored and secured. SD-WAN can integrate into a security fabric, which delivers security capabilities across a variety of domains, including wired and wireless networks, endpoints, web applications, the cloud, and more. A security fabric can analyze logs and events from all these security products to correlate alarms and alerts and provide greater context into incidents. A fabric can also orchestrate a response to threats across domains.

Networking for the Future

SD-WAN technology provides an extensive menu of options to network architects for connecting an organization's people with all its digital resources. In a multi-cloud world, it can provide the necessary links across the infrastructure to enable secure network traffic with high performance for users.

[1] "How COVID-19 has pushed companies over the technology tipping point—and transformed business forever," McKinsey, October 5, 2020.

[2] Emil Sayegh, "Is Further Abstraction The Answer To Cloud Complexities?" Forbes, May 3, 2021.

[3] Rani Osnat, "Mitigating the Risks of Multi-Cloud Environments," Network Computing, July 27, 2021.

[4] "What to Look for in a Secure SD-WAN Solution for Multi-Cloud Environments," Fortinet, July 10, 2020.

August 28, 2021 12:57 PM
1238653-0-0-EN