FORTINET

What to Look for in a Secure SD-WAN Solution for Multi-Cloud Environments

Table of Contents

Executive Overview

Cloud adoption is becoming an increasingly large part of CIO budgets, to the point where some enterprise organizations are using many different cloud environments to build their IT infrastructure. A multi-cloud model involves the custom selection of multiple cloud services to serve specific functions. Enterprises today have almost entirely embraced multi-cloud for its flexibility—93% currently have a multi-cloud strategy in place.[1] However, connecting workloads on multiple clouds at the data-center WAN edge creates several challenges, including deployment complexity, inconsistent network performance, and expensive connectivity.

Software-defined wide-area networking (SD-WAN) can help facilitate adoption of multi-cloud deployments while simplifying WAN infrastructure and reducing connectivity costs. But in order to be successful, SD-WAN needs to be kept secure.

The global cloud Infrastructure-as-a-Service (IaaS) market is projected to grow at a compound annual growth rate (CAGR) of nearly 28% to reach $101.56 billion by 2023.[2]

Why Enterprises Are Rapidly Embracing Multi-Cloud

A multi-cloud strategy enables organizations to avoid vendor lock-in and to select the best cloud services available for a particular application or workload. Multi-cloud is not the same as hybrid cloud, in which public and private clouds are integrated to optimize performance, security, and flexibility. Multi-cloud simply means that organizations have the flexibility to select the best cloud provider for each of their various infrastructure and application needs.

Organizations can choose cost-optimized services and leverage geographically dispersed clouds for disaster recovery, to meet data sovereignty requirements, and to improve the user experience, among other needs.

The multi-cloud model also provides redundancy that reduces the risk of operational downtime. Although service provider outages are not as common and pervasive as they once were, the potential risk of outages disrupting enterprises is still great. As organizations continue to migrate more mission-critical workloads to the cloud, an outage or performance degradation can severely impact the continuity of their business operations or the overall quality of experience.

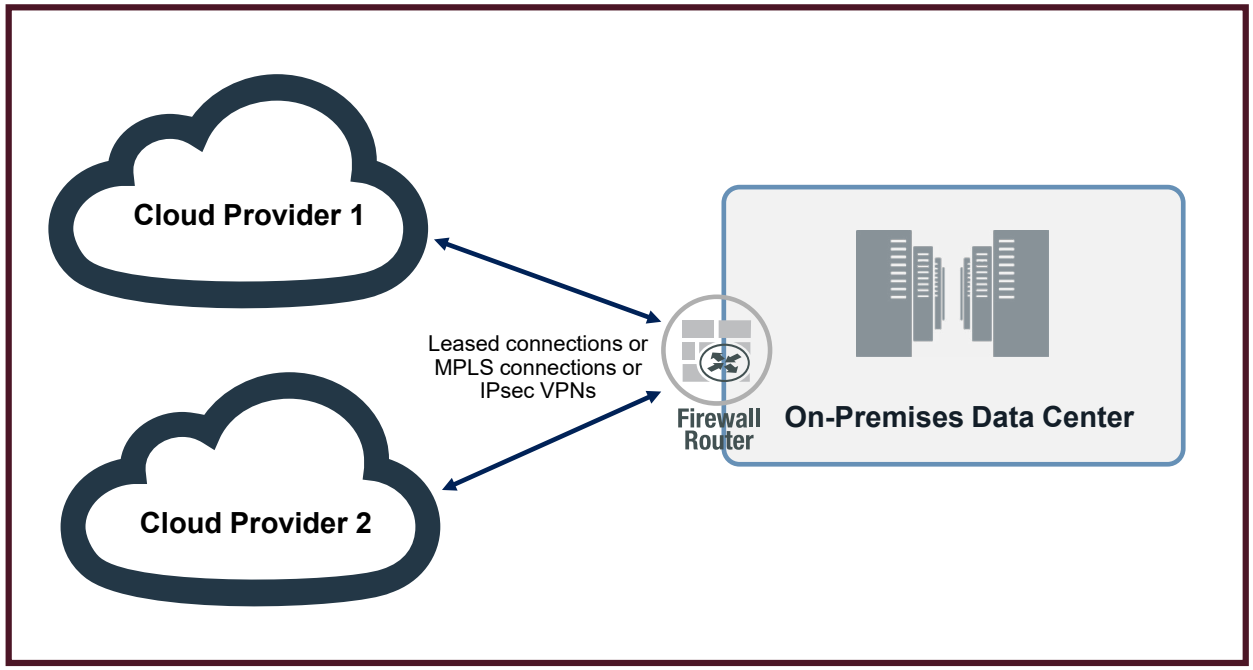
More Clouds Means More Complexity

Despite the myriad benefits, multi-cloud adoption undoubtedly adds extra layers of management complexity—especially if adding cloud services happens in an ad hoc manner rather than being planned from the ground up.[3] This complexity creates management and operational challenges, from deployment, to network performance, to operational costs. Few IT teams have the expertise to manage a mixed deployment of multiple public cloud, private cloud, and on-premises environments—especially considering the ongoing lack of skilled IT (and specifically cybersecurity) talent. Resource-constrained organizations will struggle to keep up.

To maintain centralized control and visibility with traditional "hub-and-spoke" network infrastructures, application traffic from each cloud is typically backhauled from providers to an on-premises data center over expensive multiprotocol label switching (MPLS) connections—which increases operational cost and may impact application experience due to security bottlenecks.

As organizations continue to increase their use of the cloud to host applications, direct access with high performance is critical.[4]

What's more, organizations that are not implementing centralized management and monitoring are then burdened by fragmented security policies across multiple cloud environments. They also lack end-to-end visibility of their infrastructure, which increases the risk of breaches, data loss, compliance penalties, and other damages to the enterprise. Fortunately, there is a better way to architect this.



- Deployment Complexity
- Degrades Application Performance
- High Connection Costs

Figure 1: Current multi-cloud IT deployments.

Multiple Clouds Require Unified Management and Security

Maximizing the benefits and flexibility of a multi-cloud strategy requires security and networking technologies that are capable of delivering the following benefits:

- Use optimal connections to route application traffic for reliability and performance
- Leverage high-bandwidth internet connections to lower costs
- Get visibility across your entire network infrastructure
- Balance workloads across separate public and private clouds
- Enforce consistent network and security policies across multiple clouds

Because of its automation capabilities and also where it resides strategically in the network, SD-WAN has become the solution of choice for rapidly evolving cloud network innovations (including multi-cloud).[5] SD-WAN allows enterprises to augment or replace expensive MPLS connections with an application-aware selection of more cost-effective internet connectivity options. This in turn offsets performance degradation that is becoming an increasing problem due to the amount of traffic from cloud application workloads in use across the enterprise.

Applications that are hosted in the public cloud can use advanced, cloud-based SD-WAN gateways to direct traffic between these applications.[6]

What to Look for in an SD-WAN Solution

SD-WAN solutions vary widely in terms of capabilities. Enterprises should carefully consider all associated costs—both capital expenses (CapEx) and operating expenses (OpEx)—as well as management, performance, and especially, security requirements.

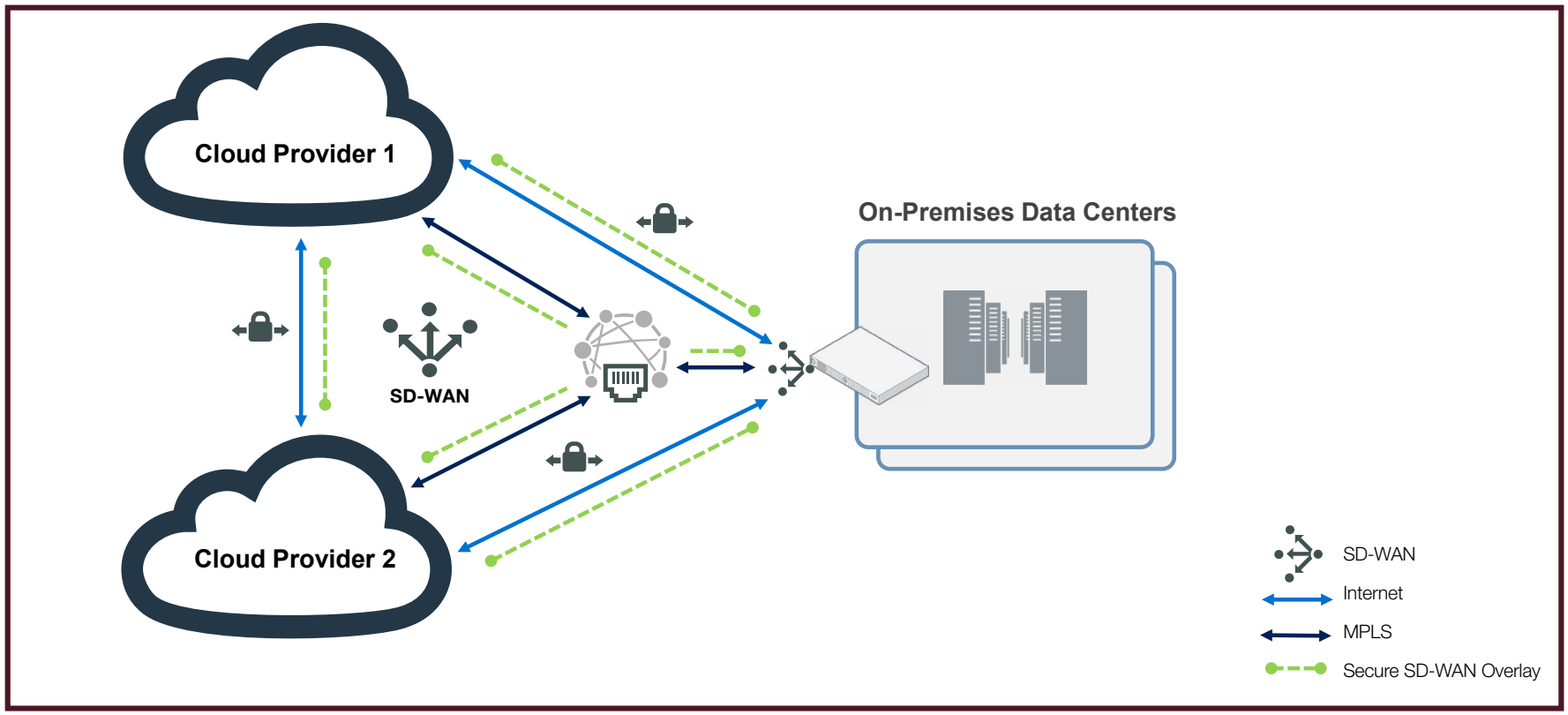


Figure 2: Connecting multiple clouds over SD-WAN.

- **Consolidated Secure SD-WAN.** A disaggregated approach to SD-WAN requires investment in multiple devices in order to provide all the necessary networking and security capabilities that go into a fully functional solution. But these piecemeal approaches have inherent gaps in security that can be exploited by cyberattacks. A single solution that integrates advanced SD-WAN networking capabilities within a next-generation firewall (NGFW), however, can eliminate these security gaps while reducing overall CapEx investment costs.
- **Simplified Deployment and Management.** Disaggregated SD-WAN also increases OpEx in terms of staff time dedicated to solution deployment, orchestration, and management. A consolidated SD-WAN solution centralizes these processes. A common **single-pane-of-glass** interface simplifies operations and eases the burden on limited staff. Look for a solution featuring **deep cloud-native integrations and broad cloud support** to help expedite initial setup and configuration.
- **Performance.** An SD-WAN solution featuring intelligent **application awareness** capabilities can address bandwidth and performance issues. The solution should reference a broad database of known applications and use custom signatures which then allows it to prioritize traffic and automatically manage connections based on the real-time needs of the enterprise.
- **Visibility and Control.** Tracking vulnerabilities across multiple distributed cloud deployments can be difficult. An SD-WAN with centralized management and support integration with cloud provider security constructs like tagging can provide end-to-end, actionable visibility across all cloud iterations for advanced prevention and detection capabilities—as well as automated enforcement of policy-based controls. This in turn can help ensure compliance with data privacy laws and industry regulations, regardless of where sensitive data is stored.

Effective SD-WAN Simplifies Multi-Cloud Challenges

An effective SD-WAN solution can provide an application-aware network infrastructure that spans multiple cloud environments. It removes inconsistency through a uniform policy-defined infrastructure while simplifying management and reducing infrastructural costs. It can also improve agility of deployments and application experience across the enterprise. Finally, integrated security features offered by a robust, consolidated SD-WAN solution can lower risks and enforce controls across enterprise infrastructures that rely on multiple cloud environments.

When evaluating an SD-WAN solution to optimize multi-cloud functionality and improve security, the following questions may be useful:

- ☐ Does the solution consolidate security and networking functionality?
- ☐ Does the solution provide end-to-end visibility and granular control across all cloud environments?
- ☐ Does it offer a centralized management console (single pane of glass) with the ability to enforce global policies?
- ☐ Is there any testing to validate the solution's performance, reliability, or value (TCO) in cloud environments?
- ☐ Does the solution support the broad range of public and private cloud environments?

[1] Kim Weins, "Cloud Computing Trends: 2020 State of the Cloud Report," Flexera, May 21, 2020.

[2] "Global Infrastructure as a Service (IaaS) Market 2019-2023," Business Wire, October 23, 2019.

[3] Charles McLellan, "Multicloud: Everything you need to know about the biggest trend in cloud computing," ZDNet, July 1, 2019.

[4] Sasha Emmerling, "The Network Edge: Stretching the Boundaries of SD-WAN," Network Computing, August 7, 2019.

[5] Ibid.

[6] Ibid.

www.fortinet.com

719125-0-0-EN

July 10, 2020 10:46 PM

eb-FA-what-to-look-for-in-a-secure-sdwan-solution-for-multicloud-environments-7112020