Solving Hybrid and Multi-cloud Networking Challenges

3 Steps to a Secure, Resilient, and High-performance Infrastructure

Table of Contents

Executive Overview

With digital transformation in full swing and customer behaviors and preferences changing rapidly, enterprises almost unanimously now operate services in hybrid and multiple clouds. At the same time, more users than ever are logging in remotely. This puts tremendous strain on a traditional wide-area network (WAN), which is designed to route all traffic through the data center for security screening, and relies on hardwire connections with branch locations. Security for this increased network traffic is also a challenge, with every cloud deployment representing an expansion of the attack surface and an additional resource located outside the corporate perimeter.

These problems are best addressed together, and solutions must be designed correctly to deliver the level of network performance and security necessary for today's enterprise. This eBook will describe how businesses can build a secure, resilient, and high-performing network while bringing networking and security together around common priorities. We will outline three critical capabilities of such an architecture—the flexibility and scalability of software-defined WAN (SD-WAN), centralized visibility and control, and an integrated networking and security architecture.

92%

of enterprises have a multi-cloud strategy; 80% have a hybrid cloud strategy.[1]

The Multi-cloud Enterprise: Networking Challenges and an Expanded Attack Surface

The cloud has become a universal element in the contemporary enterprise, and an astounding 92% of firms have now embraced a multi-cloud strategy.[2] More and more of a company's business-critical functions and data lie outside the corporate data center. What's more, users of those services are more distributed than ever—something that was exacerbated by COVID-19, when millions of people suddenly found themselves working from home.[3] Every indication points toward more employees working remotely after the pandemic than did before it began.

The result of these two trends is that networking is more widely distributed than ever, and the attack surface available to cyber criminals is continually growing. It was not that long ago when organizations simply needed to secure the perimeter of their headquarters network and create secure, hardwire connections with branch locations.

But with a growing share of network traffic from endpoints to distant cloud services moving away from headquarters, routing everything over a fixed wire through the corporate data center—where security screening is housed—is no longer a viable strategy for either performance or security. The data center becomes a bottleneck for network traffic, and this results in latency, performance issues, and user frustration.

Securing a multi-cloud architecture is complex because every public and hybrid cloud solution has a unique architecture that is incompatible with other clouds. Built-in security tools offered by each cloud provider work differently and have somewhat different functionalities. As a result, visibility of the entire infrastructure from a single console is difficult to achieve—as is enforcement of security policies consistently across every cloud.

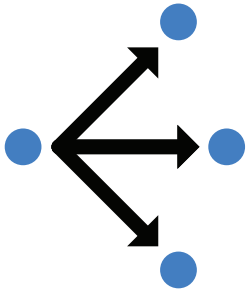
"One of the key factors CISOs are taking into account is the difference between each of the cloud platforms ... [E]ach of them has different built-in security tools, and functions with different command structures, different capabilities, different syntax and logic."[4]

Elements of Secure, Resilient, and High-performance Networking

So, organizations operating in multiple clouds face twin challenges that are interrelated, but are historically addressed by two siloed groups in the traditional organization. Networking teams have been tasked with providing adequate network bandwidth to accommodate an organization's online business traffic, preserving application performance and ensuring business continuity. Security teams have had the responsibility of keeping that network traffic free of ransomware, malware, and other cyberattacks.

But today's quickly evolving marketplace requires that both challenges be solved in tandem. As digital transformation continues to accelerate, networks must have the resilience to accommodate rapidly increasing traffic to and from different clouds from widely distributed endpoints and Internet-of-Things (IoT) devices at the network edge. This includes coverage for significant spikes in traffic at specific times. And that resilience must extend to security, ensuring that the networks over which traffic moves do not expose an organization to increasingly sophisticated attacks.

This eBook explores three essential elements of resilient networking in a distributed, multi-cloud network—**secure SD-WAN** as a resilient way for traffic to move, **centralized management** to tie together a sprawling cloud infrastructure, and an **integrated approach to networking and security** that eliminates both silos and security gaps. Such a comprehensive approach creates a "multi-cloud freeway" that enables swift, secure movement across the infrastructure.



“Multi-cloud deployments often suffer from lack of visibility, disjointed management tools, and security issues. An effective SD-WAN solution can provide an application-aware network infrastructure that spans multiple cloud environments.”[5]

1 Secure SD-WAN: Flexible and Scalable Networking

As organizations embrace a hybrid and multi-cloud strategy, they are quickly faced with the fact that traditional networking lacks the flexibility required for modern digital transformation initiatives. It is also expensive: Dedicated multiprotocol label switching (MPLS) lines are costly, complicated to expand, and take months to deploy. And the dedicated circuits to branch locations serve less purpose for organizations that have a significant percentage of workers logging in remotely and working primarily with cloud-based services.

These deficiencies have resulted in the rapid growth of a key technology—software-defined wide-area networking (SD-WAN). SD-WAN provides high-performance access to cloud applications for users located away from headquarters, enabling a more agile network. It does this by allowing network traffic to travel on the public internet when doing so would result in the most efficient transmission. SD-WAN brings several benefits:

- **Direct cloud access.** SD-WAN eliminates the need for backhauling—routing branch office and remote traffic through the data center before accessing the internet—enabling direct access to critical cloud services.
- **Better application performance.** SD-WAN can prioritize business-critical traffic and real-time services like Voice over Internet Protocol (VoIP), steering it over the most efficient route and incorporating advanced WAN remediation. Having several options for moving traffic helps reduce packet loss and latency from heavy traffic.
- **Increased business agility.** Organizations can easily scale to whatever traffic levels they experience, eliminating the need to plan network upgrades months or years in advance.
- **Cost savings.** SD-WAN allows traffic to be routed efficiently over multiple channels—including existing MPLS circuits and the public internet via LTE, broadband, and now 5G. This maximizes the usage of available WAN capacity and eliminates the need for new MPLS bandwidth.

To build out an information freeway using SD-WAN technology, the first requirement is an SD-WAN solution that combines security and efficient networking—rather than tacking on security as an afterthought. Ideally, the SD-WAN technology is integrated with next-generation firewall (NGFW) protection to enforce security policies and inspect encrypted and non-encrypted traffic, and available in physical and virtual form factors. The solution should have application awareness and support advanced routing like multicast, IPv6, and Border Gateway Protocol (BGP) to allow for dynamic routing to meet specific network requirements.

"[T]he need for SD-WAN to enable a self-healing network—one that automatically fixes issues before they are widely realized—from the WAN edge to the cloud edge has now become a key requirement for organizations."[6]

2 Centralized Management: Visibility for Efficiency and Security

When networking and security are managed by different tools, the networking and security teams often work with less information than they need. Network administrators may have limited visibility into security, and vice versa. Even if cross-functional visibility is available, it may require opening and monitoring multiple dashboards, and correlating the data in an automated fashion may be impossible. A lack of visibility can also result in security gaps that security team members are not even aware of and increases the odds of human error.

A secure SD-WAN architecture should include centralized management of both networking and security from the same console. Look for solutions that include these features:

- **Visibility.** Achieving transparent, centralized visibility of the entire network security infrastructure is one of the most important things an organization can do to reduce its overall risk exposure. A secure SD-WAN solution should provide a single view into connections between and within clouds, and between clouds and branches and remote users.
- **Control.** An organization's SD-WAN solution should provide a single tool that enables administrators to provision SD-WAN capabilities, set up IPsec virtual private networks and static routes, and set and monitor security policies from a single console.

- **Management.** One-touch management from a single console is the most efficient and secure architecture. It enables organizations to prioritize the most important network traffic, and facilitates real-time sharing of threat intelligence across the entire network.
- **Policy.** A fully integrated networking and security solution should enable consistent policies to be set across every cloud and for on-premises resources.
- **Compliance.** Centralized visibility and control, automated processes, orchestrated and consistent policies across the entire network, and robust reporting should make compliance a proactive, automated process rather than a reactive, manual one.

These elements are critical to transform an SD-WAN deployment into a multi-cloud freeway.

"There are many ways you can manage activity across cloud services, but centralized visibility and management is the most effective approach to ensure protection and compliance across multiple environments simultaneously."[7]

3 Integrated Security: An Automated, Holistic Approach

A disaggregated networking and security infrastructure creates many problems. When networking and security are managed by disconnected tools, they often work at cross purposes. Networking tools apply IP address and subnet-based policies to prioritize network traffic and to take an optimal path to reach the destination. Security tools, on the other hand, use a different set of criteria to make decisions to allow, deny, or inspect traffic. In most cases the decisions are not consistent and can adversely impact application performance and end-user experience.

When an organization has multiple, unintegrated tools for security and networking, the problems are compounded. Security team members are forced to spend valuable time manually correlating log data and inputting information into disconnected tools. This reduces security by increasing the lag time between when a problem is discovered by one security tool and when that information has been shared across the network.

The ideal solution collates and analyzes logs and events from all security tools for the most comprehensive threat intelligence and response across the infrastructure, including the multi-cloud architecture.

And it is not enough to have an integrated security tool that happens to include SD-WAN. Consideration must be given to all aspects of integration:

- **Connectors.** One key problem for integration is making sure that workloads in the different environments in a cloud use consistent application tags and rules when they communicate with each other. In a multi-cloud environment, the user should ensure that tags and rules are implemented consistently across the different cloud environments and the underlay network. It is also key to integrate the tags/rules with the SD-WAN policies for the overlay network across these clouds.

- **Bookended solution.** SD-WAN is all about performance and simplification. In on-premises environments, physical appliances use hardware acceleration to deliver performance. In the cloud, high-performance networking capabilities are offered by the different cloud platforms and can be leveraged to improve performance. It is important that security tools do not slow down that performance. A security solution with native integration can ensure protection without sacrificing performance. Organizations can deploy a simpler but high-performance cloud infrastructure by having the same consistent network and security operating system run on both on-premises and cloud endpoints.
- **Automation scripts.** In a multi-cloud environment, third-party automation scripting solutions that simplify deployment and provisioning, and enable quick reaction to system failures or major security events across clouds, are critical. An alternate approach could be to utilize the native scripting capabilities of each cloud system, and utilize those capabilities to automate processes consistently across all clouds.
- **Service integration.** Native integration must enable the network and security infrastructures to integrate with appropriate network and security services on each individual cloud platform. Examples include threat intelligence tools, cloud virtual network monitoring tools, managed network services, and serverless functions.

Integration of every aspect of networking and security is the best way to facilitate freeway-level performance in a multi-cloud network—rather than sending network traffic into a cul-de-sac.

“If networking and security are separated, multi-cloud deployments won’t be able to reach their full performance potential because each layer tends to use different technologies from different vendors that can’t see or talk to each other.”[8]

Conclusion: The Convergence of Networking and Security

Secure SD-WAN represents a convergence between the traditionally siloed networking and security functions at an organization—a trend that has accelerated in recent years.[9] Designed properly, it can mitigate both the networking problem of increased traffic between branch offices, remote users, and cloud-based resources, and the increased security risks caused by a burgeoning attack surface.

While SD-WAN was originally designed to create a flexible and scalable connection between headquarters and branch offices, public cloud providers have provided tools like Amazon Web Services' (AWS) Transit Gateway Connect and Google Cloud Network Connectivity Center, which make it easier to support SD-WAN gateways that can be accessed from corporate locations and by remote users. These tools also enable organizations to build SD-WAN connections between multiple clouds, providing organizations with unlimited opportunities for different applications to work together and for data to be shared across solutions.

To maintain network performance and protect against cyberattacks, it is important that the entire networking and security architecture be integrated for centralized visibility and control, real-time sharing of threat intelligence across the network, and efficient routing of network traffic. When these priorities are managed by the same tool, none of them falls through the cracks. Secure SD-WAN makes such a comprehensive solution possible.

[1] "2021 State of the Cloud Report," Flexera, accessed September 5, 2021.

[2] Ibid.

[3] Susan Lund, et al., "The future of work after COVID-19," McKinsey, February 18, 2021.

[4] Alain Sanchez, et al., "Hybrid and Multi-Cloud in the Era of Work from Anywhere," Fortinet, June 21, 2021.

[5] Vince Hwang, "Multi-cloud Security: 3 Pressing Challenges You Must Address," Fortinet, March 25, 2021.

[6] Nirav Shah, "Enabling Self-Healing SD-WAN from the WAN Edge to the Cloud Edge," Fortinet, June 22, 2021.

[7] Aaron Walker, "5 keys to securing multi-cloud environments," TechBeacon, accessed September 8, 2021.

[8] Vince Hwang, "A New Approach to Multi-cloud Security," CSO, March 24, 2021.

[9] Zeus Kerravala, "How Pandemic Accelerated Convergence of Network, Security," eWeek, February 8, 2021.

FORTINET

www.fortinet.com

October 14, 2021 6:50 PM

[illegible]