POINT OF VIEW

Why Digital Acceleration Needs a Hybrid Mesh Firewall Approach

Executive Summary

Organizations large and small have adopted digital transformation initiatives to enable them to deliver business growth and meet organizational objectives. The pace of this transformation has accelerated as organizations have sought to address challenges caused by the global pandemic. IT teams were forced to move many applications to the cloud faster than originally planned. These rapid changes increased cybersecurity risks and imposed a heavy burden on infrastructure teams, often due to the plethora of new, platform-specific security tools.

With moving to public clouds and modernizing data centers at the heart of this transformation, care and attention must be given to ensuring that your networks and data are secure and that security can be easily managed across clouds and data centers.

"The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams."

Jessie Hawkins
Systems Architect
University of South Carolina

Digital Acceleration: The Journey to Cloud Starts with a Hybrid Mesh Firewall

Organizations pursuing digital acceleration have various strategies and are at different stages with their cloud adoption and application journey. In many cases, organizations are lifting and shifting virtualized application workloads from their virtual data centers into the cloud, while some are refactoring applications to integrate with cloud provider services, and a few are actually architecting applications to be cloud native. Regardless of where they are in their journey, all of them have major concerns about their applications and data security.

For most organizations, securing this application journey to the cloud begins with securing the network that connects their users, branches, and data centers to the cloud. As a next step, they focus on securing the cloud network that connects to cloud provider services and workloads in the public cloud and hybrid cloud. Organizations at an advanced level of cloud maturity then move on to securing the networks that connect their application infrastructure in a multi-cloud deployment. Getting the cloud network ready for deploying applications causes plenty of challenges, including setting up a robust cloud perimeter for every network setup by various types of users, implementing advanced security for compliance, and streamlining their network and security operations without being run over by runaway cloud costs.

A hybrid mesh firewall (HMF) is a network of next-generation firewalls (NGFWs) able to run locally and in the cloud that can be centrally managed and can automate security updates and responses across the entire network. By utilizing an HMF, organizations can reduce management overhead, consolidate security analytics, and reduce the strain on staff that comes from having to manage disparate firewalls on each cloud and in each data center.

Cloud Network Security Challenges and Trends

Because cloud transformation plans and application journeys vary across organizations, network security challenges differ. There are, however, some fundamental challenges that are the same across organizations. Here are some key challenges faced by organizations deploying applications into public and private clouds:

- **Uncontrolled outbound communications**

  This type of communication from a cloud deployment happens when outbound web traffic attempts to connect to low-reputation sources (based on the domain or hostname). These connections could be established by malicious spyware or malware trying to exfiltrate sensitive data or connect to an external command-and-control server. On the other hand, the traffic could originate from developer workloads contacting developer tools like GitHub or application workloads contacting external servers for software updates.

- **Lateral movement of threats**

  In the cloud and virtualized data centers, there is typically no control or protection put in place to inspect the traffic flowing between different VNETS or between workloads in the same virtual network. This leaves room for malicious or compromised internal actors to introduce threats that can quickly propagate through the virtual data center or in the cloud. Another important threat vector to consider is the software supply chain and open-source software, which may have been compromised. Developers inadvertently use these resources, introducing external threats that can propagate laterally and launch catastrophic attacks.

- **Limited bandwidth for secure connectivity into the cloud**

  As organizations use more and more cloud services, they onboard traffic at many locations, including HQ, on-premises data centers, branches, and remote locations. In many of these cases, they may use virtual private network (VPN) technology to connect to the cloud. Organizations have an option to use cloud-provider VPN gateways. Still, most of these gateways do not offer the bandwidth performance needed to deliver the best application experiences to users across different locations.

- **Fragmented management and policy infrastructure**

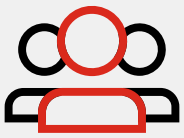
  When organizations start using more than one cloud provider, often alongside their physical, virtual data centers, their operations teams are too frequently burdened with managing multiple, often incompatible, platform-specific security tools. They must manage different consoles and set up different policies across these diverse platforms. This leads to a higher cost of training and may leave security gaps among the various environments.

An Effective Roadmap to Protect the Cloud Network

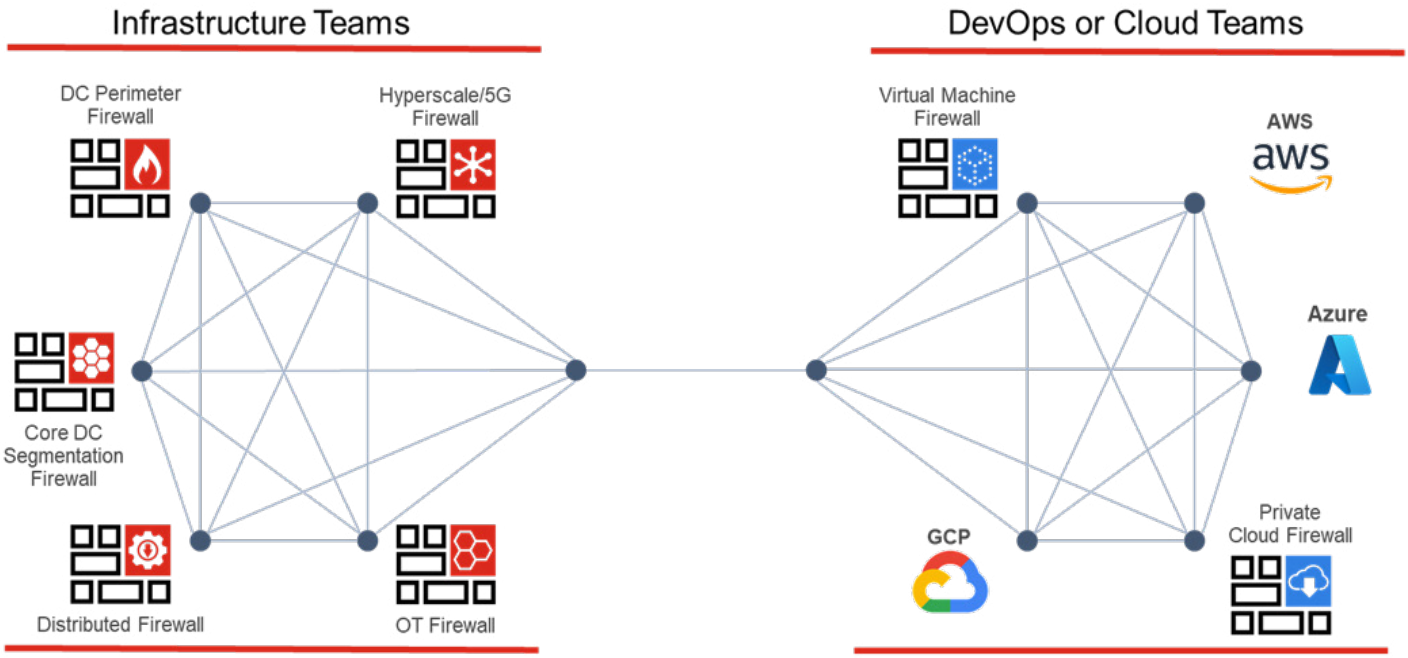
The application journey for any organization essentially lays out the evolution of their cloud transformation, which in turn drives the roadmap for rolling out their cloud network security. It starts with the application journey's lift-and-shift phase, essentially the organization's cloud migration phase. In this phase, they are focused on providing secure connectivity from various locations to the application workloads in the cloud.

Once the organization gets accustomed to cloud usage, it evolves to refactor and rearchitect a select set of applications or even create cloud-born applications. In this cloud expansion phase, it may expand its footprint to tens or hundreds of cloud networks. At this stage, organizations are primarily deploying robust, high-scale routing to interconnect the organization's virtual networks on any cloud provider. But it will also need to ensure that it can effectively manage security on-premises and in the cloud. This requires eliminating siloed security solutions for ones that work together in a security mesh. In most cases, this means weaving the network firewalls, both cloud-based and physical, into an HMF infrastructure.

Next, the organization builds and deploys cloud-native architectures or runs complex IT infrastructures spanning multiple clouds. Organizations in this cloud-native or multi-cloud phase typically implement efficient networks to get users from tens or hundreds of locations to access their workloads in multiple clouds. The organization may even connect application infrastructures across cloud providers by routing the traffic at their data centers or leveraging cloud-provider, or service-provider managed network services. In any case, the organization will need to secure the network connecting to these multiple clouds and also **secure the networks connecting across the clouds.**



Organizations need AI- and ML-powered intrusion prevention systems (IPS), aggressive patch management strategies, and the threat intelligence all coupled into a hybrid mesh firewall to secure modern, multi-site environments.



On-Premises Data Center, Campus, and Data Firewall

Cloud and Cloud-Native Firewall

Conclusion

The answer to safely moving to the cloud for digital acceleration is reducing complexity and increasing security effectiveness with an HMF approach. An HMF benefits organizations with centralized visibility, management, and automation across all solution points, allowing them to leverage intelligence sharing for faster response times. Ultimately, this reduces complexities, solves cloud cybersecurity skills and resource gaps, and increases overall security effectiveness. As such, organizations should look for solutions that integrate and support a broad, integrated, and automated cybersecurity fabric.

July 12, 2023 9:18 PM

2264006-0-0-EN