SD-WAN Security Options in a Multi-Cloud Architecture

By: Dave Ginsburg

As WANs become more complex and the enterprise perimeter dissolves, establishing an effective security posture becomes more complex. Be it the branch, the data center, remote workers or the cloud, each new on-ramp increases the attack surface. And, with the increasing use of software as a service (SaaS) applications, expected to reach $200 billion by 2024, backhauling all traffic to a single point is just not feasible.

Unfortunately, enterprise planners are not quite ready to migrate many of their mission-critical applications to the cloud, primarily due to gaps in integration, configuration and a general understanding of a given SaaS vendor's security capabilities. An effective multi-cloud security architecture in the context of a managed software-defined wide area network (SD-WAN) service must therefore include this evolved connectivity and the various business processes, yet at the same time be consumable. A single breach, whether resulting from ignorance or malicious intent, is enough to bring down an organization.

Understand Connectivity Requirements

With enterprises undergoing WAN transformation and adopting SD-WAN, the best architecture is one that is manageable, well understood and universally adopted within the enterprise. The adage is that the enterprise always needs to be at the top of its game, while the hacker only needs to succeed once. In the context of WAN transformation, the enterprise needs to take stock of its connectivity requirements—what traffic stays within the branch, what is destined for HQ, and what terminates in the cloud, either within the organization's virtual firewall, or at a SaaS application.

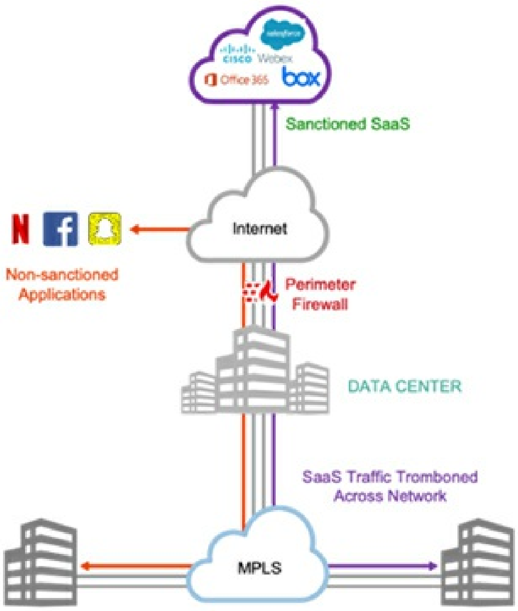

Figure 1: Legacy Architecture: Internet and SaaS application traffic backhauled ('tromboned') through HQ or data center to a perimeter firewall.

Branch sites are a major consideration because legacy architectures (Figure 1, above)—where all traffic flows through a small number of larger HQ sites before heading to the Internet—don’t offer the demanded cloud agility. With SD-WAN and an Internet-first connectivity paradigm, this is even more the case. For the branch, the question becomes about what firewalling must be local (to the branch), and what can be handled within the cloud. If we consider remote workers to be no different from extended branches, the same considerations apply, with some traffic destined to the corporate intranet, while other data is carried via tunnels to SaaS applications. To repurpose the old networking phrase ‘switch when you can, route when you must,’ a modern-day equivalent could be ‘firewall in the cloud when you can, firewall at the branch when you must.’

Security ‘Of’ the Service

Once an enterprise’s connectivity requirements are understood, it’s important to consider how to go about securing the HQ, branches and cloud-based applications. For example, imagine an enterprise with an HQ, branches and cloud connectivity [infrastructure as a service (IaaS) and SaaS] that has signed up to a managed SD-WAN service.

The first consideration must be the security of the service itself, including any underlying transport, as well as the different SaaS applications consumed. Service infrastructure security includes distributed denial of service (DDoS) protection, encryption of user data as well as control traffic, any required certifications such as SOC 2 or ISO 27002, as well as network operations center (NOC) training, security protocols, monitoring and incident response. Where data residency is a requirement, such as GDPR in the EU, the service must follow suit. So, include in any vendor or provider RFI how the solution(s) under evaluation ensures data integrity and reliability.

Other business process considerations include who will handle key management: the enterprise, the provider, or both, and what this means for how traffic is handled across the WAN. Planners must also have a firm grasp of identity and access management (IAM) requirements/single sign-on (SSO). And, it’s important to consider the ramifications of Shadow IT, where employees access unsanctioned SaaS applications. This is potentially mitigated by monitoring.

HQ and Branch Security Options

HQs have traditionally deployed physical firewalls for connectivity outside of the enterprise, as well as for connectivity—SD-WAN included—to one or more cloud providers. Traffic internal to the enterprise— including cloud workloads such as AWS VPCs—remain within the firewall perimeter. Conversely, traffic to trusted SaaS applications such as Office 365 or Salesforce will traverse a simpler L4 FW and NAT. Ideally, these IaaS/PaaS/SaaS handoffs are regionally based, optimizing application performance via cross-connects from the SD-WAN provider’s PoPs to the corresponding public cloud or SaaS application. For example, an engineer in Romania would connect via the SD-WAN service to a handoff to AWS or Box in Central Europe, rather than having to backhaul to the US or even to the UK (Figure 2, below).

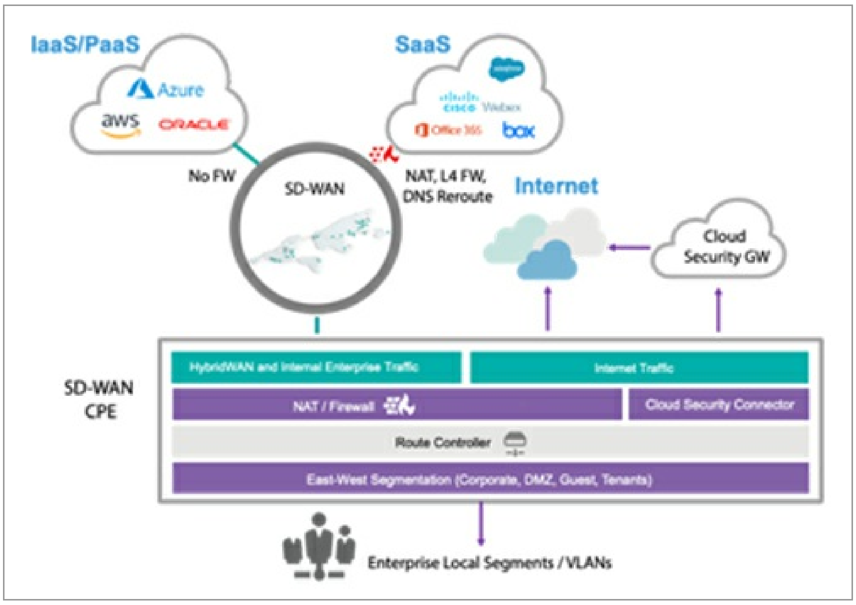

Figure 2: Evolved connectivity, with SD-WAN connection to IaaS/PaaS/SaaS and local or cloud-based firewall for internet traffic

Alternatively, the HQ may dispense with the traditional firewall and rely instead on a cloud-based service, an option quickly gaining in popularity. Considerations here include cloud firewall scalability and geographical distribution, how this impacts provisioned bandwidth, and costs. In any case, the heavyweight security stack is under siege at the branch, now delivered as part of a cloud-based service. Gartner has described this trend in their “Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge” report.

An intermediate stage is where the SD-WAN vendor, as part of a converged edge offering, includes a full security suite on their managed customer-premises equipment (CPE). This may be native to their SD-WAN stack or, alternatively, running as a network functions virtualization (NFV). This second option is one method by which an enterprise, after selecting an SD-WAN vendor, may maintain its existing security vendor relationship at the branch.

In the recent Aryaka ‘State of the WAN’ survey, the majority of respondents stated that they would prefer a multi-vendor security solution from their SD-WAN supplier, though as expected, the percentage opting for a single-vendor solution was higher in North America than in EMEA or APAC. One challenge is integrating any NFV-based security solution with the enterprise’s installed workflows and third-party instrumentation. Ultimately, the success of deploying one vendor’s virtual firewall on the SD-WAN CPE of another is not driven by the VM hosting but instead by the operational aspects.

As noted earlier, branches in the past would connect via the existing WAN, MPLS included, to the HQ site, leveraging the central firewall for Internet and cloud connectivity. Now, branches connecting to SD-WAN have the same options as above as part of the vendors SD-WAN CPE, though with quicker uptake of cloud-based security as older standalone appliances, where deployed, are retired.

Anticipate the Need to Accommodate Multiple Security Vendors

If deploying security solutions from multiple vendors—for example, some security delivered by the SD-WAN provider, NFV or otherwise, and some delivered by an incumbent security vendor—the workflows and visibility need to integrate the two. Any security within the SD-WAN solution must adapt to the existing security architecture of the enterprise, and not the other way around. The actual division of security responsibilities between the edge and the cloud is not as important as maintaining control and visibility.

With more than half of all enterprise WAN traffic moving to and from the cloud, global businesses are moving away from legacy architectures such as MPLS to SD-WAN technologies. As this changeover happens, it’s paramount that security doesn’t become an afterthought. Every enterprise SD-WAN strategy must include a roadmap for how security will fit into the new network architecture.