SOLUTION BRIEF

VERSA NETWORKS

Why user-to-app performance is a requirement for your Security Service Edge (SSE) deployment

As applications move to the cloud and the workforce becomes increasingly hybrid, enterprises are quickly transitioning to cloud-delivered Secure Access Service Edge (SASE) and Security Service Edge (SSE). In this blog, we will identify the challenges seen when deploying SSE without taking user-to-app performance into account. We will then highlight the benefits that SASE with SD-WAN brings to the table, especially from a network performance standpoint.

SSE is a model for delivering cloud-based security services, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Zero Trust Network Access (ZTNA). SASE additively incorporates SD-WAN in conjunction with SSE services.

Let's examine an analogy to better understand the differences. The route to an SSE service is akin to navigating to a destination using a map. All the paths to reach the destination can be seen, but there is no real-time information like traffic updates to advise the user on which route to take for the shortest travel time. The SSE solution provider's responsibility starts when the traffic reaches the cloud gateway; the path it takes to reach the cloud gateway is typically not their responsibility.

A SASE solution with SD-WAN is akin to navigating with a satellite-powered GPS device that provides traffic updates and automatically selects the route based on real-time road conditions. It ensures that the user's connection to the gateway is through the best possible path. For branch office users, the solution provider takes responsibility right at the customer's branch office to ensure that the best path to the gateway is chosen when multiple WAN paths are available. For users connecting from anywhere, the client devices automatically selects a better performing cloud gateway when multiple of them are available.

For many enterprises, one of the main drivers for implementing SD-WAN is the fact that when using bundled internet links, the end-user application experience was similar, if not better, compared to traditional private MPLS circuits. Apart from cost savings, if users had a poor application experience, then SD-WAN adaptation would not have been as successful as it has been today. The same applies to a cloud-delivered SSE solution, it is important for the success of the solution to take the user application experience into account, and this is only possible with a network optimized path using SD-WAN technology.

In an SSE solution, there is a cloud hosted gateway to which the user connects. The user can be connecting remotely or from behind a branch office. For remote users, the access is typically through a client installed on the user's device or by using a PAC file. For users behind a branch office, the connection to the gateway is using a statically created IPsec tunnel or a GRE tunnel from each of the WAN edge routers in the enterprise branch office.

For branch office users, some of the challenges with statically defined tunnels include the following.

- To allow for redundancy, the **WAN edge router sets up redundant tunnels to the SSE providers cloud gateway**. There is additional complexity in managing these redundant tunnels especially since branch offices typically have redundant WAN edge routers, each with multiple internet WAN links for access.
- With redundant tunnels, **brown-out scenarios on the primary tunnel** can cause the redundancy to fail. Typical monitoring options only rely on keepalive packets that don't measure the network performance over the tunnel.
- **There is no traffic load-balancing over the tunnels** even when multiple internet WAN links are available. This is because each tunnel is mapped to the IP address of the WAN link. Using multiple IPsec/GRE tunnels for load-balancing is not a common approach. Even if they are used, the WAN routers would do an equal cost load-balancing which does not factor in the available bandwidth on the WAN links causing one link to be congested even when there is capacity on the other.
- IPsec tunnels have limitations to how much **throughput it can handle per tunnel**. This is because on a software-based system like a typical WAN edge router, a single CPU core is assigned to handle all traffic for one IPsec tunnel negating the benefits of having a multi-core system.

- In the case of traffic loss on the WAN path, **there is no mechanism to recover lost packets** using traffic conditioning techniques like FEC or Packet Replication.
- **No Quality of Service (QoS)**. When there is congestion on all the WAN links, business critical traffic gets treated the same way as all other traffic.

A unified SASE solution which incorporates the use of SD-WAN to connect to the cloud hosted gateway, offers the following advantages.

- **Ability to bundle multiple internet WAN links** on the branch SD-WAN router.
- **Policy-based traffic steering capabilities** based on real-time WAN path performance metrics like packet loss, latency, jitter, utilization etc. This is possible to do on a per user or application basis.
- **Traffic load balancing across multiple WAN links** based on real-time WAN link utilization, allowing the WAN links with different bandwidths to be fully utilized.
- **Traffic conditioning capabilities** like FEC and packet replication to recover lost packets.
- **Dynamic path bandwidth measurement to the cloud gateway** for Quality of Service (QoS). QoS ensures that the business-critical traffic is prioritized over other traffic when there is congestion.
- **Higher per-session IPsec throughput** when compared to static IPsec tunnels since SD-WAN routers are session aware and have the capability to spray the sessions within the IPsec tunnel across multiple CPU cores.

Agnostic to where the user is and where the application resides, a unified SASE solution with SD-WAN ensures the best convergence of security and networking services over the WAN network. IT administrators can easily transition from their on-premises firewall to cloud-based security solutions without the fear of compromising the end user experience.

Versa Unified SASE

Versa's unified SASE solution is a comprehensive offering that combines a feature-rich SSE and SD-WAN solution that is all managed through a single portal. In Versa SASE, the cloud hosted gateway and the SD-WAN router on the enterprise branch site runs the same VOS software thereby offering a consistent policy engine for all its SSE and SD-WAN services. Versa's SASE service includes the Versa Secure Private Access (VSPA) service for ZTNA, Versa Secure Internet Access (VSIA) service for internet security and Secure SD-WAN service for branch network access.

With many applications moving to the cloud or becoming SaaS-based, and the location from where the user connects changing, the Versa SASE solution ensures that enterprise IT administrators can transition to a cloud-based security service without duly impacting the user's application experience. To learn more about Versa's unified SASE solution and how it can benefit your enterprise, visit https://versa-networks.com/sase/.

References to Gartner's definition of SASE and SSE:

- SASE
- SSE