SSE or SASE: vendors need to consider the implications of a failed strategy

June 2022

Tom Rebbeck

Security vendors are either packaging SD-WAN with cloud security products (this approach is known as secure-access service edge (SASE)) or are focusing on cloud security services only (this approach is known as security service edge (SSE)). If one of these approaches becomes the dominant supply model, as is possible, vendors with the failed strategy, and the service providers that have adopted it, will need to reconsider.

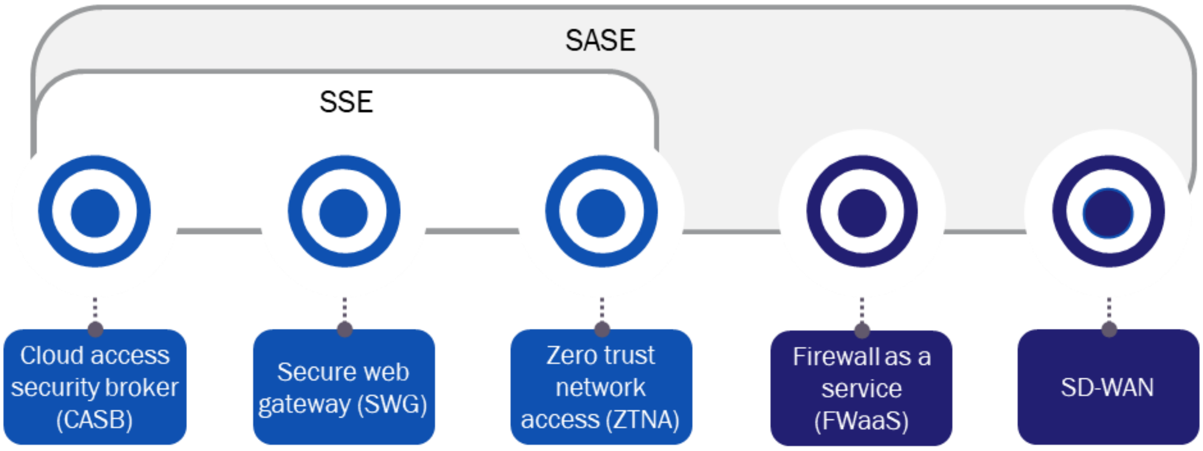
This article is based on our recent report, *Approaches to SASE: 11 vendor profiles*.

SASE or SSE: vendors are adopting one of two approaches to networking

The term SASE was first used in 2019 to describe an offering that combines a range of security and networking products. The products covered by SASE vary, but most definitions include the five elements in Figure 1. Some vendors and service providers also include additional services, such as remote browser isolation (RBI).

Gartner invented the phrase 'SASE' but has moved away from using it. It now talks of security service edge (SSE), which includes just the three cloud security components. Gartner's change has added to the confusion surrounding SASE, and may have given licence to operators and vendors to be more flexible in how they use the SASE term.

Figure 1: Elements of SASE and SSE


SASE
SSE
Cloud access security broker (CASB)
Secure web gateway (SWG)
Zero trust network access (ZTNA)
Firewall as a service (FWaaS)
SD-WAN

Source: Analysys Mason

SASE has more components to it than SSE and is therefore obviously a more complex product. Crucially, the inclusion of SD-WAN means that it requires on-premises equipment. This makes set up and support more complicated and means that the pricing model has to cover the cost of hardware.

Vendors that are pursuing a SASE model include Cato Networks, Fortinet, Palo Alto Networks, Versa, VMware and others. Most of these vendors have a background in hardware, either for on-premises firewalls or SD-WAN (or both). The cloud components (for example, SWG, CASB) are later developments. In some cases, the quality of these cloud components is not as good as the quality of those from vendors that previously specialised in them.

SSE is purely a cloud product with no on-premises hardware element. This makes it simple to switch on, and also means it can be sold as a service, just like any other software product. Vendors that take the SSE approach include Netskope, Perimeter 81, Zscaler and others. These vendors typically started with one of the SSE elements, and then developed the other components. Typically, they do not have, and do not intend to develop, on-premises solutions, preferring instead to position themselves to investors (and customers) as pure software companies.

Approaches to SD-WAN differ

Vendors that are developing SASE solutions believe that SD-WAN combined with security components from the same vendor is what most businesses will want. The underlying assumption is that the advantages of a single solution will more than outweigh any benefits of buying best-of-breed solutions from separate vendors. They argue that the benefits of multi-vendor solutions are likely to decline because most single-vendor solutions will provide similar features and capabilities in the next 2–3 years.

The SSE vendors' approach to SD-WAN is more nuanced. Broadly speaking, there are two alternative positions.

- **SD-WAN can be bought from a separate vendor**. Some SSE vendors contend that SD-WAN is essentially a separate market. Many SSE vendors already have integrations with SD-WAN solutions (for example, Zscaler has integrations with 17 SD-WAN solutions) and they consider this sufficient.

- **SD-WAN is unnecessary.** Some vendors argue that a business premises with multiple high-capacity (1Gbit/s or 10Gbit/s) internet circuits does not need SD-WAN. With plenty of spare bandwidth, these businesses will not need to prioritise traffic or load balance between connections.

The two positions can be compatible – a firm could buy SD-WAN separately before giving it up when it can buy two independent 10Gbit/s connections.

The rise of remote working also means that highly reliable connections to central locations, such as offices, are less important than in the past. Techniques for securing remote users (such as ZTNA and SWG) become more important.

The idea that SD-WAN could be replaced entirely is extremely challenging for vendors and service providers (like telecoms operators) that have used on-premises equipment as a starting point from which to sell other services.

One vision is likely to prevail, but it is unclear which one

It seems likely that both visions – SSE and SASE – will find a market. Larger enterprises are always likely to need some sort of WAN networking technology such as SD-WAN, and will find a single vendor SASE solution attractive. Many small firms are unlikely to need SD-WAN but will need some cloud security services. However, it is possible that one of these models will dominate, forcing the other to be a niche solution. Vendors and service providers need to think through the implications of this.

If SSE dominates, SASE vendors will need to ensure that their cloud security products match the SSE vendors for features and quality. They will also need to look for other ways to differentiate their products, such as integration with other security products. Acquisition is likely to be part of this strategy. Traditional strengths, such as partners to distribute hardware, will weaken or disappear.

If SASE dominates, SSE vendors will need to find a way to offer SD-WAN. Adding SD-WAN through integrations with other vendors is likely to be a short-term fix only because all SD-WAN vendors are developing (or have developed) SSE components. Vendors will probably need to make acquisitions. These SSE vendors will also need to consider how to change their pricing model to cover hardware costs and their distribution model to manage hardware. They will also need to be careful how to communicate this change to the stock market. As of June 2022, Zscaler's market capitalisation is around 22 times its 2021 revenue compared to the 12 times multiple for Palo Alto Networks.

The competing visions also have implications for telecoms operators. Almost all operators in our report *Approaches to SASE: 12 operator case studies* are pursuing a strategy built around SD-WAN and hardware. The exception is T-Mobile USA, which is promoting a hardware-light, SSE-type solution. Operators may need to re-think their approaches, not just to SASE but also to their ability to increase revenue related to security services if the link between SD-WAN and cloud security is broken.

For more on operator approaches to SASE, see our article, *SASE: telecoms operators' approaches could be weakened by the lack of a long-term vision*.