wHITE PAPER

SASE & The Future of Network Access Control

sales@portnox.com | www.portnox.com

The current enterprise network security practices focus on verifying the identity of the user and the device in a perimeter-less environment, where cloud-hosted technologies prevail in the enterprise and where remote sites include branch offices and employees working from home.

In Gartner's paper "The Future of Network Security is in the Cloud", one of the key findings is that "network security architectures that place the enterprise data center at the center of connectivity requirements are an inhibitor to the dynamic access requirements of digital business." And there is a recommendation for enterprises to move their security into the cloud, based on a networking and security model called Secure SASE, a term coined by Gartner's leading security analysts.

What is SASE?

SASE, pronounced "sassy", stands for Secure Access Service Edge. It is a cloud-based network security model and category, proposed by Gartner in 2019, to support agile secure access to enterprise assets. This model includes the network security solutions in a global and cloud-native service that allows IT teams to easily connect and secure all of their organization's networks and users in an agile, cost-effective, and scalable way. This is especially useful in the currently globally dispersed digital enterprise.

According to Gartner's analysis, SASE can be characterized as an identity-driven, cloud-native, globally distributed technology that supports and impacts all enterprise edges and IT domains. For example, this would include a branch office in LA along with the main HQ in London, while traveling/mobile team members can connect on the go.

> *SASE capabilities are delivered as a service-based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions. Identities of entities can be associated with people, groups of people (branch offices), devices, applications, services, IoT systems, or edge computing locations. (Gartner)*

SASE addresses the numerous problems with traditional network security methods, many of which are rooted in the idea that network security architectures should be placed at the center of connectivity in the HQ or data center, where typically branch locations are more vulnerable to attack.

Why Should I Care? What's the Problem?

Network security legacy applications cannot efficiently support newer networking use cases that have moved to “the edge”, such as cloud applications, dynamic services, and distributed data in remote branch offices. Traditional on-premises architectures introduce challenges such as latency, large management overhead, networking blind spots, and continuous reconfiguration work by the IT team as vendors, services, and equipment change. Even though the SASE model is not without its own challenges, it can eliminate these issues by removing cumbersome technologies and networking complexities, while moving the entire security process to the network edge (The point where the enterprise-owned network connects to a third-party, particularly cloud technologies. Oftentimes, network administrators refer to their “WAN edge” or “internet edge”).

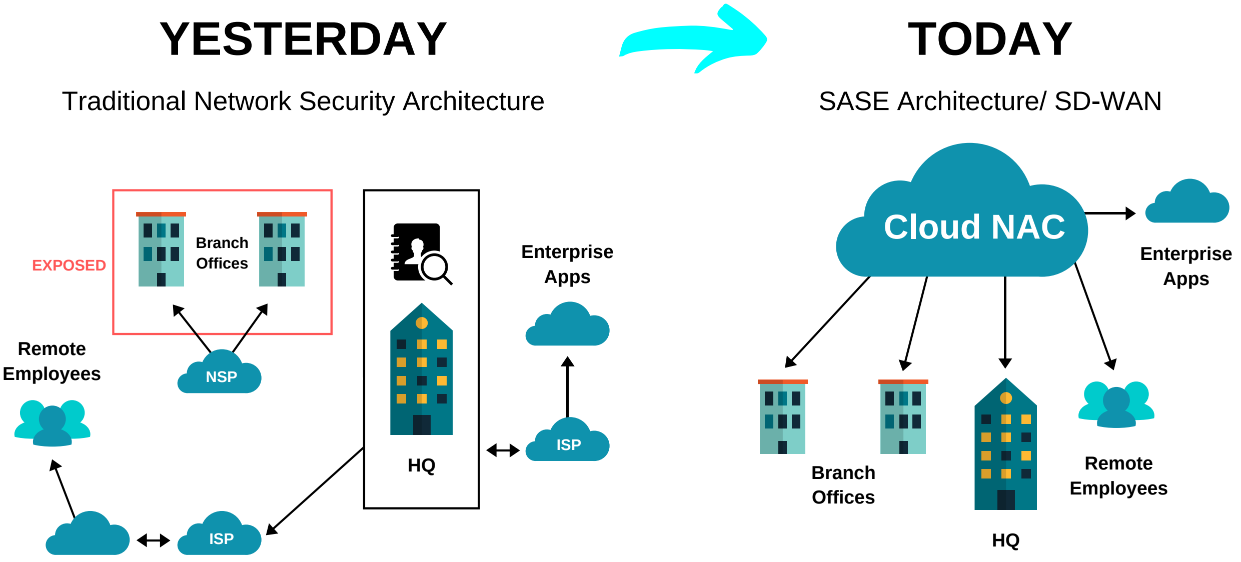
If enterprises try to solve IT challenges as they emerge, with ad-hoc/point solutions, they will be leading themselves into technical compounds that are complex and costly to manage, and that will not necessarily work well with each other in terms of efficiency and speed. Complex and cumbersome communications between IT components slow down IT and its response rate to different business requirements.

SASE can change this paradigm because as mentioned, it is identity-driven, cloud-native, globally distributed, and securely connects all edges (WAN, cloud, mobile, and IoT). With SASE, enterprises can reduce the time it takes to develop new products, deliver them to the market, and respond efficiently and appropriately to the increasing changes in business conditions.

Shift Happens

In the last few years, as more organizations around the world became more decentralized, each office location is considered to be a remote site/ a branch office location, by organizational security controls. Companies either consume access security services in a costly method through data centers, implementing redundant controls in each location, or worse, neglecting the security for that part of the enterprise network altogether. In simple terms, we are talking about delivering an all-access security suite from the cloud and not from the data center. This is in line with the trend of identity brokers moving to the cloud (such as Azure, G Suite, Okta, and others) as well as the continued migration to the cloud of many other cyber-security architectures and IT services.

In a scenario where you are implementing an on-premises NAC solution that goes with your on-premises network equipment, you can easily identify and authenticate the end-users. However, if your organization is distributed and like many others, has transitioned to using a cloud-delivered ID broker, then continuing to consume authentication and access services from the cloud make much more sense.



In the diagram, on above, we can see the price of not leaving any remote site exposed – either you pay a very high price for each location, or you need to duplicate your security mechanisms in each location which is costly. The second option is to authenticate and obtain your access rights and compliance needs via the closest, geo-redundant cloud service available.

OK, So What Happens Now?

The sensible course of action is to plan a security strategy to be scalable and efficient in the present, while at the same time future-proofing the organization’s security. With the organizational data migrating to the network edge, it makes sense to authenticate and authorize users and devices in a cloud format, thereby assuring that regardless of the equipment and geolocation, employees can securely connect in a cost-efficient and secure method to the needed resources.

ABOUT PORTNOX

Portnox provides simple to deploy, operate and maintain network security, visibility and access control solutions. Portnox software can be deployed on-premises, as a SaaS/cloud-delivered service, or in hybrid mode. It is agentless and is vendor agnostic, allowing organizations to maximize their existing network and cybersecurity investments. Hundreds of enterprises around the world rely on Portnox for network visibility, cybersecurity policy enforcement and regulatory compliance. The company has been recognized for its innovations by Info Security Products Guide, Cyber Security Excellence Awards, IoT Innovator Awards, Computing Security Awards, Best of Interop ITX, Cyber Defense Magazine and more. Portnox has offices in the U.S., Europe and Asia.

portnox™

sales@portnox.com | www.portnox.com