AlgoSASE by Algorime Srl

The Agile Cyber Security Solution

A

Algorime Srl

Nov 2023

Contents

Introduction to AlgoSASE

Why AlgoSASE?

AlgoSASE was developed in response to the evolving state of cyber threats in today's world. It is designed to simultaneously increase security whilst also reducing the complexity and TCO of defending against modern cyber threats.

This document will introduce AlgoSASE and describe the benefits it provides, the security threats it mitigates and discuss some example real-world use-cases.

The challenges of cyber security in the modern world

In traditional network infrastructures, the security perimeter is the boundary between secure internal private networks and insecure external public networks. Within this perimeter, security teams have traditionally implemented tools to monitor and respond to external threats and attacks, thus protecting any sensitive data and applications that are deployed in the secure network. However, due to the continuous evolution of attack vectors and the increased complexity of networks, it has become difficult to defend and monitor them using a traditional security perimeter approach.

Gartner recently stated, "Legacy DMZs and VPNs were designed for 1990s networks and have become obsolete." Other analysts such as Forrester agree, stating that "legacy perimeter-based security models are now ineffective against new types of cyber attacks."

Integrating these legacy preventive tools with investigative tools has also proven insufficient to protect organizations from today's sophisticated cyber attacks.

The gap in the development of more sophisticated defense tools for the perimeter is easy to explain; cloud applications, use of mobile devices, BYOD, virtualization, third-party access (consultants, vendors, and business partners), remote/mobile working and IoT devices have redefined the perimeter. Today the perimeter is a less clearly definable entity; it is wherever the users are and whatever the Internet-connected device they are using.

To address these challenges, the Cloud Security Alliance (CSA) has defined guidelines such as the Software Defined Perimeter (henceforth referred to as SDP) to outline new defensive strategies against network attacks and to promote reduction of the attack surface. SDP is an approach to security that enables the concept of Zero Trust Network Access (hereafter referred to as ZTNA), or a software-defined security network with access no longer defined at the networking level, but at the application-specific level, thereby providing protection regardless of whether a service is on-premises or in the cloud.

AlgoSASE: A full-featured SDP/ZTNA security platform

AlgoSASE is an SDP/ZTNA security platform developed by Algorime Srl with the goal of providing a solution fully based on SDP/ZTNA principles and innovative cybersecurity strategies.

The AlgoSASE framework is based on the idea that by default no device or user can be trusted, regardless of whether they are inside or outside the network perimeter. This means that all activity is validated against the identify of each verified device and user.

In the cloud, AlgoSASE networking aims to create secure network communications without relying on the physical or logical security of the underlying physical or virtual network. This approach to security is further necessitated by the fact that in modern technology architecture, information is commonly spread throughout the cloud and distributed across various data centers, rather than being stored in a single on-premises location.

The principles of AlgoSASE

In an SDP/ZTNA architecture, security measures are implemented wherever necessary (e.g., at the endpoint itself) in order to isolate services from unprotected networks and create secure enclaves.

AlgoSASE replaces centralized security controls with distributed software agents that operate under the control of an application manager and provide access to resources only after verification and authorization of the identity of the user and the device they are using.

These agents create encrypted connections between requesting systems and networked resources, creating a secure network connection with a 1:1 relationship between users and the data they access.

The basic principles of the framework are:

- Identity: the user is at the heart of the AlgoSASE architecture. Their identity is defined before they can access a resource in what is called a dynamic attestation, which is a binding contract between a client (and related user) and the service provider.
- Zero Trust: as suggested by Gartner, the SDP paradigm enforces the "zero-trust model," since anyone accessing a resource must first authenticate themselves and the implementation of the principle of minimum privilege is thus made possible. Since all unauthorized resources then remain invisible through micro-segmentation, the attack surface is effectively reduced and controlled.
- Dynamic Secure Network Overlay: in an AlgoSASE architecture, each client establishes trusted connections to the resources it needs to function. AlgoSASE software agents create layering in the network by generating multiple, separate, virtualized network layers on top of the physical network. These overlays are called Dynamic Secure Network Overlays (henceforth referred to as DSNOs).
- Scalability and resilience: peer-to-peer networks are scalable by leveraging cloud technologies and inherit their resilience.

AlgoSASE feature summary

In summary, AlgoSASE provides a complete Zero Trust Network Access solution with the following features:

- Secures communications with the most advanced cryptographic framework, Noise (Noise Protocol Framework, for more details www.noiseprotocol.org).
- Replaces traditional VPNs and other security measures with a superior solution in terms of security, scalability, ease of installation, management and TCO.
- Increases speed; the Noise framework is faster than traditional IPsec.
- Infrastructure-agnostic; can be installed in on-premises networks, full or hybrid clouds from any provider and across any combination of operating systems.
- Implementation does not require changes to existing infrastructure nor hardware; just the addition of AlgoSASE devices.
- Centralizes and simplifies security management
- Centralizes security logs for auditing and troubleshooting at the individual user level.
- Strong identity control: users can use an existing Identity Provider (IdP-SSO via SAML2, OAuth2 or OpenID Connect) or a fully isolated system using 2FA (OTP).
- Natively integrates with frameworks such as Istio for Kubernetes.

- IP addresses of destinations authorized by dynamically assigned certificates.
- Granular filtering for access based on security groups (integrated with AD/LDAP).
- Built-in firewall with the possibility of granular access control (CIDR, protocol and port).
- Automatic mesh network that uses direct connections without intermediate hops, resulting in better performance and confidentiality.
- Through micro-segmentation AlgoSASE removes implicit trusts and by implementing micro-perimeters (Software Defined Micro Perimeters) it prevents hacking techniques such as lateral movements that are possible with traditional VPNs.
- The mesh topology is easily adaptable and dynamic.
- It is structured as a SaaS (Software as a Service) solution usable by software client agents and/or as a version with dedicated client hardware; any device can be connected via LAN/WLAN to AlgoSASE (Windows, Linux, macOS, iOS, Android etc.).

The advantages of AlgoSASE

The following tables describe the significant benefits of AlgoSASE (drawing from the Cloud Security Alliance SDP/ZTNA Architecture Guide v2, 2019) in the areas of Business, Operations and Security.

Business benefits

Direct cost savings

There are number of direct cost savings that can be realized through the implementation of AlgoSASE for cyber security:

- Replacing traditional network security components with AlgoSASE reduces licensing and support costs.
- Implementing and enforcing security policies through AlgoSASE reduces operational complexity and dependence on traditional security tools.
- AlgoSASE can also cut costs by reducing or replacing the use of leased lines or MPLS, since organizations can minimize or eliminate the use of private backbones.
- AlgoSASE can bring efficiency and simplicity to organizations, i.e. reduce the need for manual activity.

Increased agility of IT operations

Traditional IT security can be a labor-intensive and manual process, slow to respond to business processes.

AlgoSASE implementations, on the other hand, can be automated and proactive, automatically driven by IT or IAM events, enabling IT to be more agile in meeting business and security needs

Reduction in compliance effort and costs

AlgoSASE presents reduced risk compared to traditional approaches. AlgoSASE mitigates threats and reduces attack surfaces by preventing network-based attacks and external exploitation of applications.

AlgoSASE can feed into and respond to governance, risk, and compliance (GRC) systems, such as when it integrates with SIEM, to simplify system and application compliance activities.

AlgoSASE can provide additional connectivity tracking for online businesses.

The micro segmentation provided by AlgoSASE is often used to reduce the scope of compliance, with a significant impact on reporting efforts.

Acceleration of cloud adoption

AlgoSASE can help companies adopt cloud architectures quickly, securely, and with minimal risk by reducing the cost and complexity of the security architecture required to support applications in public cloud, private cloud, data center, and hybrid environments.

New applications can be deployed faster with equivalent or better security than traditional cyber security solution.

Improved agility in business and innovation

AlgoSASE can enable companies to implement their priorities quickly and securely. Some examples include:

- Transitioning call center agents from office to home office.
- Outsourcing of non-core business functions to specialized third parties without creating security holes.
- Rapid, secure deployment of customer-facing kiosks on remote third-party networks and locations.
- Secure deployment of enterprise resources on customer sites, creating stronger integration with those same customers and generating new business.

Operational benefits

Cloud provider agnostic

Today there are diverse cloud computing offerings available to users and businesses in their daily operations such as Microsoft Azure, Amazon AWS, Google Cloud, IBM Bluemix, Alibaba Cloud and others.

With so many different options and uses for cloud computing and cloud services and the fact that some organizations use multiple cloud service providers, being "cloud neutral" is an important feature in implementing new tools and systems.

AlgoSASE is cloud-neutral by design as is a software solution rather than a hardware solution. Therefore, AlgoSASE can be implemented independently on a variety of systems and operating systems making it suitable for both cloud and hybrid cloud environments.

Reduction in the need for VPNs and firewalls

VPNs have been a major cornerstone of network security for decades, since their first implementations in the late 1990s. The technology enables the secure connection of remote users to corporate networks and the creation of secure connections between points as diverse as workstations, servers, and cloud-based resources.

Despite the advantages provided by VPNs, they carry a relatively high TCO; organizing the many policies and users, ensuring continuous and transparent VPN operation, and managing and coordinating all VPNs and firewalls deployed in the organization can be a complex and

laborious exercise. This complexity can also increase the possibility of error or oversight resulting in incorrect configurations which could be exploited for an attack.

With AlgoSASE, administration and management are greatly simplified; all network resources can be integrated by administrators into the AlgoSASE platform. Security policies can then be centrally managed, thus avoiding the need to configure and synchronize different policies across different networks and locations, as with traditional VPNs.

Because all logic and security definitions/policies run within the AlgoSASE platform, updates to the system occur in a central location and take effect immediately, without the need to configure multiple devices in different networks and locations

Improved availability

One of the risk factors affecting critical high availability services is DDoS attacks. AlgoSASE operates a security model that has been shown to significantly mitigate the risks of a DDoS attack as it will by design not trust or allow any network connections to pass. Thus, once implemented, the application itself cannot be flooded by a DDoS attack as the traffic will not reach it.

Transparent for users

Over the years additional security has been added to systems to make them continually more secure. This same attention has also been directed toward users who use systems; corralling them through security gateways & practices before they gain access to the end systems.

These multiple layers of security create more interruptions and checkpoints that slow down a user's workflow; for instance, it is not uncommon for a user to have to log in to their workstation, start and log in to a VPN, and finally log in again and authenticate to the application they are trying to access. When users are presented with many security hurdles in their work and daily operations, the risk increases that they will try to circumvent or simplify security measures; for example, the notorious post-it note on the user’s monitor with all the passwords written on it!

AlgoSASE by design is transparent to the user and should generate a simpler experience such that the user is minimally impacted by security measures and is free to focus on their job.

Security benefits

Reduction of attack surface

One of the main security advantages of AlgoSASE is its ability to significantly reduce an organization's attack surface.

As we have previously discussed, today's enterprise networks are rarely confined to a traditional trusted network within a well-defined perimeter. With AlgoSASE, the enterprise can reduce the attack surface of the network by making endpoints invisible to unauthorized external devices and users.

As noted by the Cloud Security Alliance (CSA) the AlgoSASE security model has been shown to stop or greatly mitigate all forms of network attacks including DDoS, Man-in-the-Middle, Server Query (OWASP10) and Advanced Persistent Threat.

Reduction in the risk of security configuration errors

All network resources and applications can be integrated by administrators into the AlgoSASE platform and security policies can thus be centrally managed with immediate effect, without the need to configure multiple devices (e.g., VPNs and firewalls) in different networks and locations.

This greatly reduces the risk of misconfiguration on one of many devices, and hence gives increased confidence in the security implementation.

Stronger connection-based security

Traditionally, IP-based security has been the strategy for dealing with external threats and attacks. IP addresses are identified and added to black or whitelists to control their access to network resources. This approach requires a great deal of organizational effort since multiple devices in the network must have their own updated rules. In the case of blacklists, this can be an ongoing battle, where attackers use new Ips, resulting in new rules to block them. In the case of whitelists, each change of IP address for requires reconfiguration (very common in the case of teleworkers).

AlgoSASE mandates that any endpoint communications require two-way cryptographic authentication and that all communications must be securely encrypted. This allows for the abandonment of weak, IP address-based security as access is now determined not by IP, but by where the user/device has been authenticated by the AlgoSASE controller and can complete mutual authentication to allow it to connect.

Another advantage of connection-based security is that it can be used to prevent man-in-the-middle (MITM) attacks. The main method of MITM attacks is to use expired or forged responses, which are prevented by the mutual authentication adopted in AlgoSASE.

Pre-authentication and authorization

Traditional authentication and authorization methods need a connection as the first step, so authorization implies that a user must connect to the application before it can authenticate.

With the AlgoSASE approach, all protected resources will not allow connections or authentication until the user has authenticated to the AlgoSASE controller and been granted access.

This "authenticate first, connect later" approach allows organizations and security teams to centrally control who can connect, from what devices, and to what services, infrastructure, and other resources.

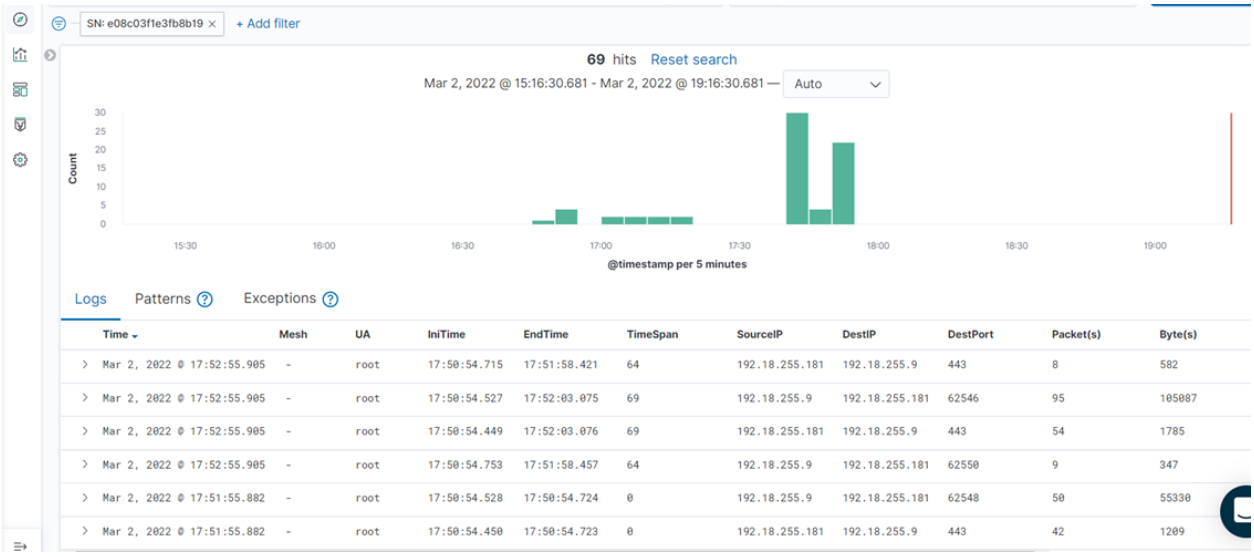
Centralization of security logging

AlgoSASE provides the facility for logging to be centralized in an enterprise solution such as ELK (Elasticsearch Logstash Kibana). This means that security auditing and troubleshooting can be achieved through a single point and is hence far more efficient.

AlgoSASE's log solution has multiple features:

- Captures and organizes IP traffic traversing AlgoSASE by recording it locally on the device and simultaneously sending it to enterprise solutions such as ELK usable in SaaS mode
- Minimizes log writing traffic by identifying traffic sessions.
- Resolves traffic from an IP source for ICMP, UDP and TCP protocols at the level of a single packet or a traffic session.
- Reports, for each packet or session, the S/N of the device and the User Account of the authenticated and authorized user who activated AlgoSASE, as well as the session times (with resolution times to the millisecond) and important fields of the IP, ICMP, TCP, and UDP headers.
- For privacy reasons, the payload of IP packets is not analyzed and recorded.
- Bandwidth statistics in terms of packets, packets/sec, Bytes, and Mbits/sec are reported for traffic sessions.

The Kibana module, which can be delivered in SaaS mode, allows customization of log views and configuration of custom dashboards as in the following example.



Time	Mesh	UA	IniTime	EndTime	TimeSpan	SourceIP	DestIP	DestPort	Packet(s)	Byte(s)
Mar 2, 2022 @ 17:52:55.905	-	root	17:50:54.715	17:51:58.421	64	192.18.255.181	192.18.255.9	443	8	582
Mar 2, 2022 @ 17:52:55.905	-	root	17:50:54.527	17:52:03.075	69	192.18.255.9	192.18.255.181	62546	95	105087
Mar 2, 2022 @ 17:52:55.905	-	root	17:50:54.449	17:52:03.076	69	192.18.255.181	192.18.255.9	443	54	1785
Mar 2, 2022 @ 17:52:55.905	-	root	17:50:54.753	17:51:58.457	64	192.18.255.9	192.18.255.181	62550	9	347
Mar 2, 2022 @ 17:51:55.882	-	root	17:50:54.528	17:50:54.724	0	192.18.255.9	192.18.255.181	62548	50	55330
Mar 2, 2022 @ 17:51:55.882	-	root	17:50:54.450	17:50:54.723	0	192.18.255.181	192.18.255.9	443	42	1209

Example use case

In this section we will describe an example use case of AlgoSASE in a real-world implementation.

Let us consider a company whose business involves placing consumer-facing kiosks at remote sites, such as booking/ticketing booths (also providing payment facilities) at trade shows, which occur regularly but in varying locations and with different and unpredictable network configurations.

This company has a network topology consisting of:

- Head office, within which are housed:
  - On-premises server
  - Desktops for all staff
  - WiFi network allowing staff mobiles to connect
- Amazon AWS cloud containing:
  - RDS database platform that must be accessed by the kiosks
  - CloudFront CDN that must be available to the kiosks
  - S3 buckets that must be available to the kiosks
  - Other AWS services that should not be available to the kiosks
- Customer-facing sites during shows, where the kiosks must be deployed

To implement the AlgoSASE security solution, the following additions to the topology would be made:

- AlgoSASE micro devices to connect the kiosks (providing either a WiFi or wired connection as desired, in a one-to-one or many-to-one configuration)
- AlgoSASE micro device to serve the WiFi access point in the head office. *Note: In a SOHO environment this would likely replace the WiFi AP, but in a large office, the client may have some high-power WiFi APs that can be leveraged*
- AlgoSASE gateway server at the head office
- EC2 instance running AlgoSASE software in the AWS Cloud
- AlgoSASE central server for managing the AlgoSASE platform hosted by any cloud provider. *Note: this could be in the existing AWS cloud, of course.*
- AlgoSASE audit system connected to an ELK stack for enterprise logging and auditing) hosted by any cloud provider. *Note: this could be in the existing AWS cloud, of course.*
- Any existing VPNs etc. could be retired.

The network topology would hence be as shown in the following diagram:

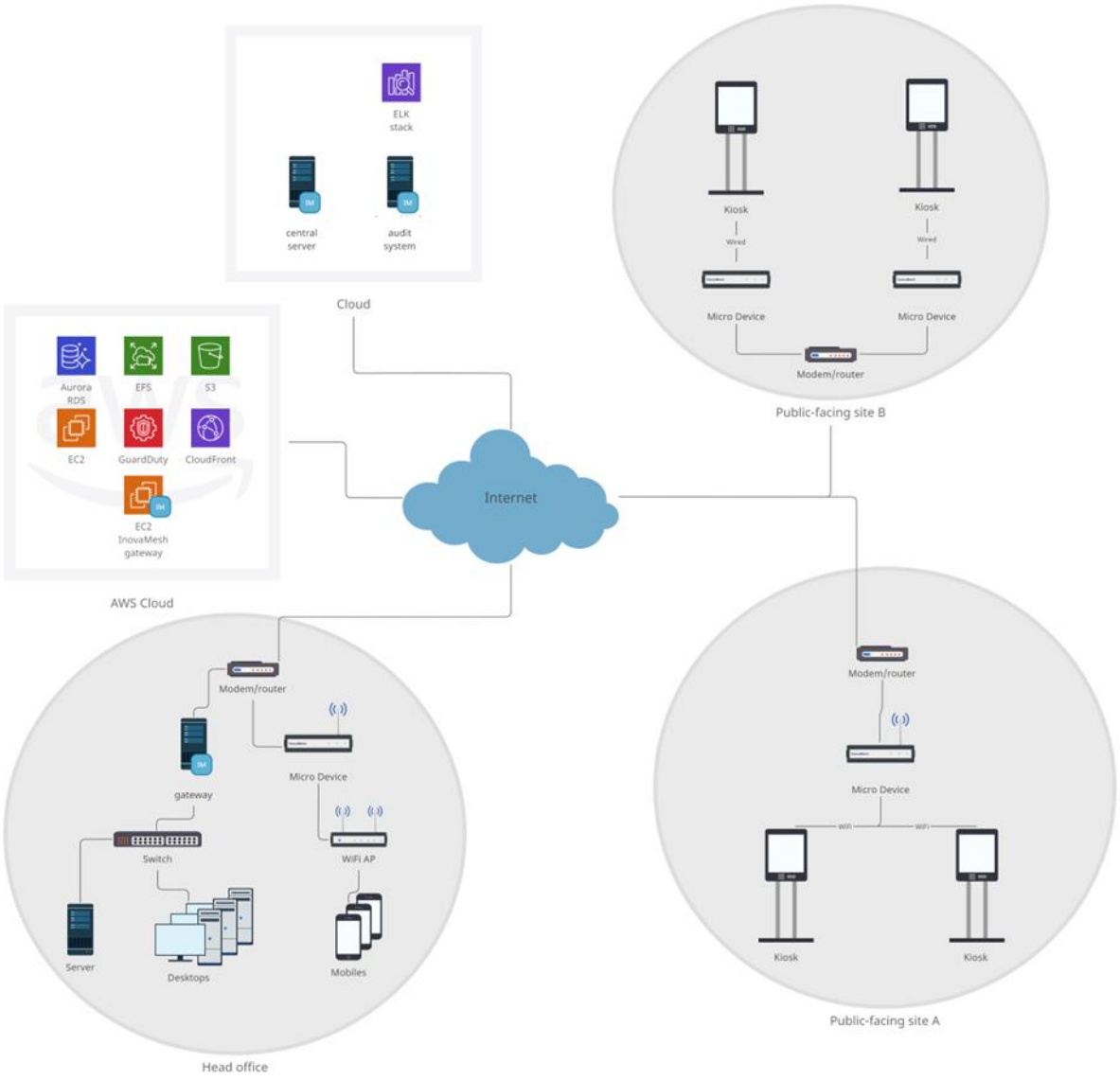


FIG 1. OVERALL NETWORK TOPOLOGY

Within this topology, AlgoSASE allows us to configure access to resources based on roles and groups, which are configured via the AlgoSASE central server. We will now show some examples of possible groups.

Network visibility and access to customer-facing kiosks

The first role we'll consider is that of the Kiosks themselves. As described above, these devices will be running in remote locations, in which we often have little control over the wider network topology, as this is dictated by the owners of the location space.

The kiosks will require access to our RDS instance, S3 buckets and CloudFront CDN. They should not have access to other resources.

The Kiosks group/role would be configured within AlgoSASE, which would grant access via the micro-devices to which the Kiosks are connected.

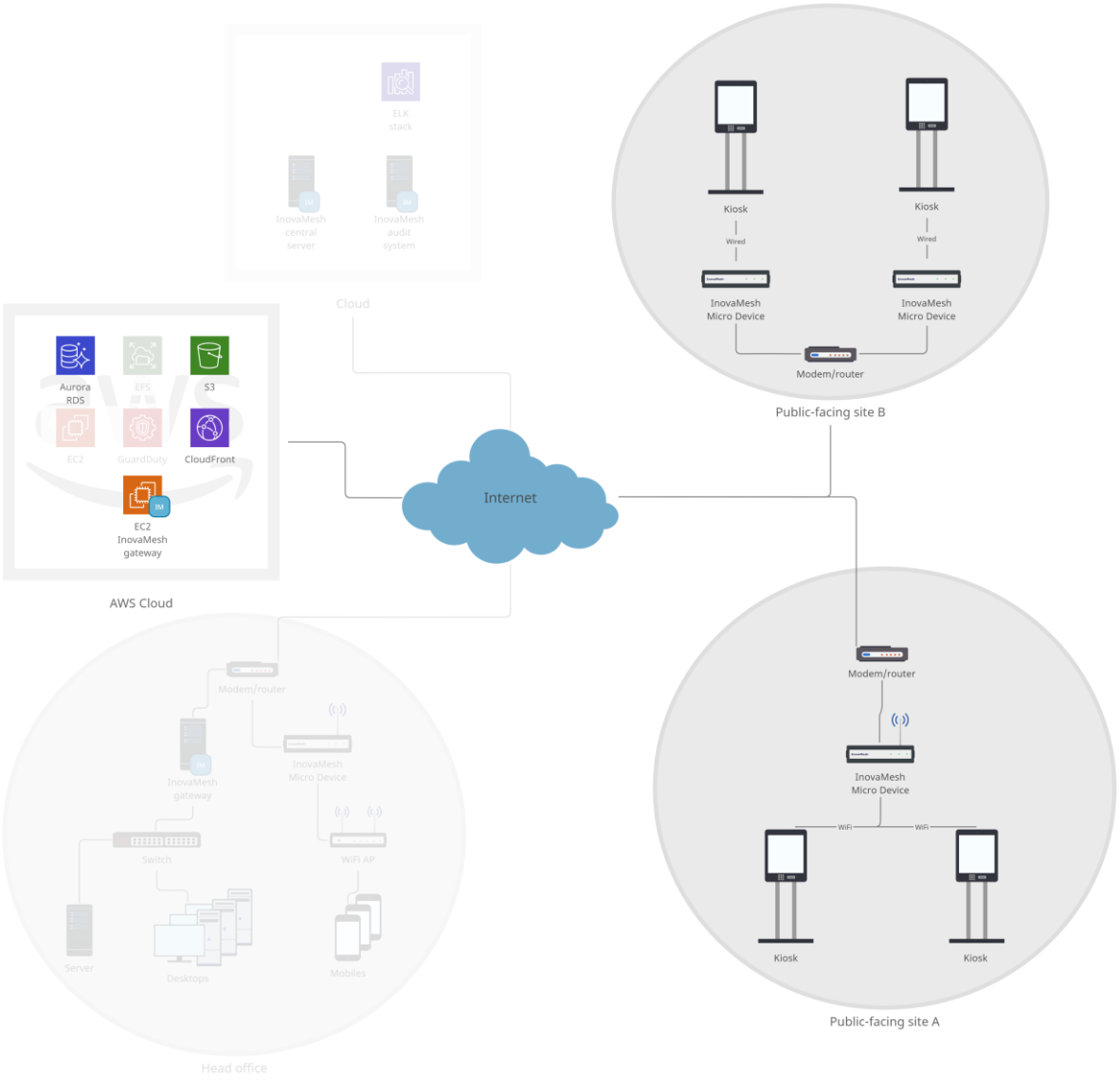


FIG 2. NETWORK ACCESS AVAILABLE TO CUSTOMER-FACING KIOSKS

Network visibility to role/group “Kiosk Manager”

Next, we consider the role that we’ll call “Kiosk Manager”. This is a staff role fulfilled by someone within the head office. They require access to the remote kiosks for configuration, troubleshooting, monitoring etc. They also need access to the same resources that the kiosks themselves can access.

The below diagram visualizes the access available to this role. Note that the Kiosk Manager does not have access to the devices on the WiFi network within the head office.

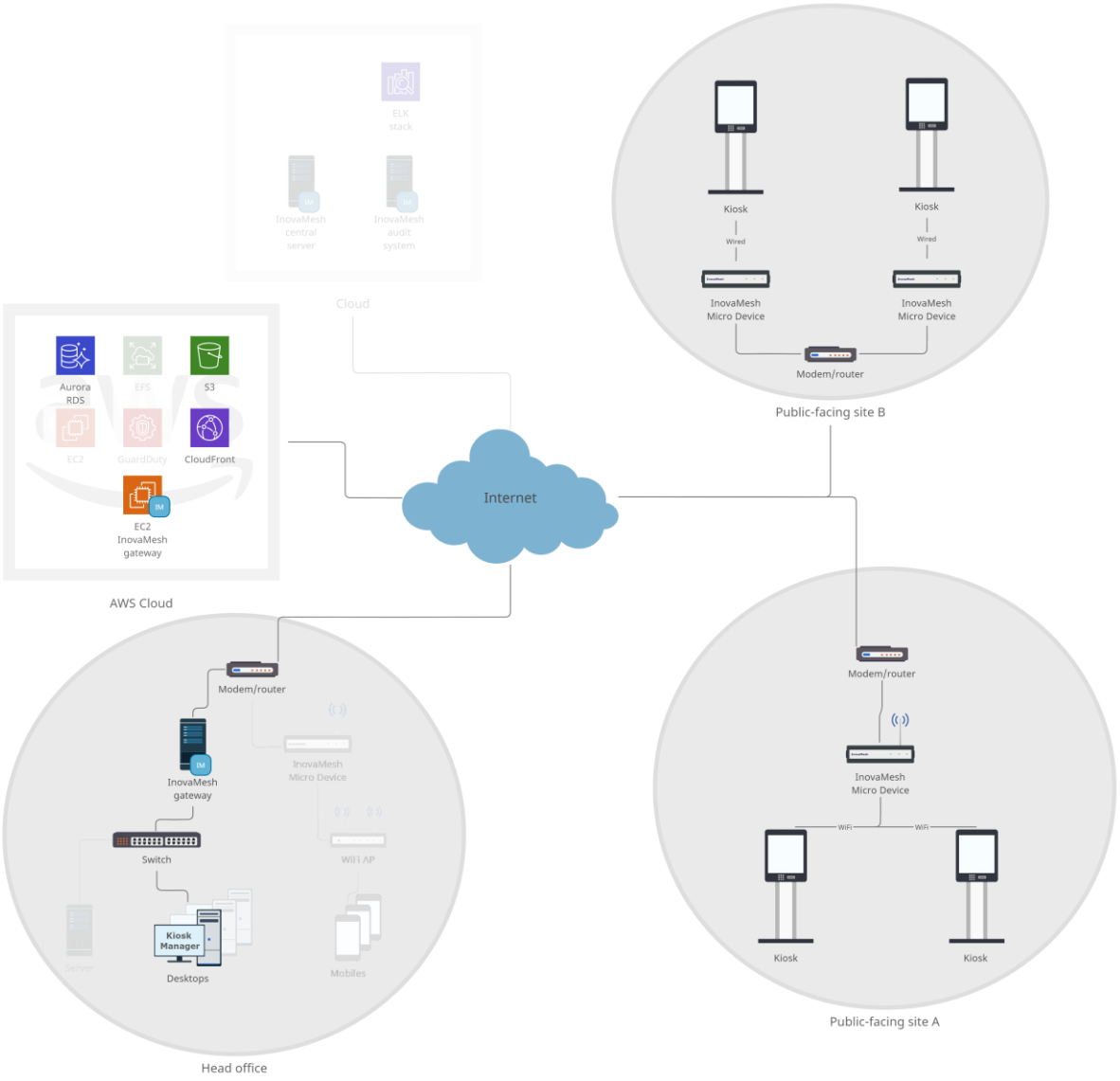


FIG 3. NETWORK ACCESS AVAILABLE TO KIOSK MANAGER ROLE

Network visibility to role/group “Office worker”

The following diagram shows network access available to a role named “Office worker”. This role provides access to resources within the on-premises network, plus our S3 buckets, but nothing else.

FIG 4. NETWORK ACCESS AVAILABLE TO GENERAL OFFICE WORKER

Network visibility to role/group “Security Manager”

Finally, we consider a role named “Security Manager”. This is the role through which the AlgoSASE platform is configured and administered. This role is granted access to the AlgoSASE platform server and audit system, all on-premises resources in the head office, plus some selected AWS resources. The do not require access to the Kiosks themselves.

FIG 5. NETWORK ACCESS AVAILABLE TO SECURITY MANAGER

Summary

We have shown how AlgoSASE can centralize and simplify network security in a scenario where the endpoints can be physically and technologically varied. In our example use case, the kiosks can simply be moved (with their associated micro-devices) to a new show/location and immediately have access to the resources they require, without re-configuration and without the risk of exposing any inappropriate resources to other devices present at the remote location.

The applications and benefits of AlgoSASE are of course applicable to any number of scenarios and we would love the opportunity to discuss how this modern approach to cyber security could help provide your business with greater security, and a competitive advantage.

Please feel free to contact us for further information.