Evaluating AlgoSASE vs Traditional VPN

Topic	AlgoSASE	Traditional VPN
Network type	Dynamic Network Overlay Control (DYNOC): does not requires changes to the existing architecture, based on agile cryptographic algorithms (e.g. Wireguard, Nebula) that address resource constraint	Traditional VPNs rely on protocols like IPsec, L2TP/IPsec, or OpenVPN which require extensive manual configuration and can impact the existing network architecture. These are resource-intensive and can be challenging to implement on devices with limited hardware capabilities such as IoT devices.
Topology model	No constraints (hub/multi-hub and spoke, full mesh, policy based mesh, multi enclaves, etc.). For example, AlgoSASE can replace any VPN by overcoming its limitations.	Typically operates on a hub-and-spoke model which restricts configuration to scenarios like remote-to-local traffic. Some advanced providers may offer more flexible configurations but are generally less adaptable than mesh solutions.
Network segmentation	Software Defined Network/micro Perimeter (SDN/SD(m)P) autonomously controlled by policy, from the whole network down to the micro-segmentation level.	Utilizes static segmentation which necessitates manual reconfiguration for any changes, lacking support for dynamic software-defined segmentation.
Dynamic Device Isolation	Active Isolation Topology (AIT) based on ML/AI e.g. blocking device Internet access, segregating devices into separate enclaves, etc.	Generally lacks active isolation capabilities or dynamic reconfiguration, limiting effectiveness in environments requiring high security or frequent configuration changes.
Layers separation	Separated Control Layer (DYNOC Algorime) and Data Layer (Nebula by Defined Networking). This also allows data traffic and control traffic to be separated.	In most VPN setups, control traffic and data travel together, increasing the risk of security exposures.

Evaluating AlgoSASE vs Traditional VPN

Topic	AlgoSASE	Traditional VPN
Supported Operating System	Node components written in Go language; the compilers can target Android, DragonFly BSD, FreeBSD, Illumos, Linux (e.g. OpenWrt), macOS/iOS (Darwin), NetBSD, OpenBSD, Plan 9 and Windows.	Requires client installation; supports major operating systems such as Windows, macOS, iOS, Android, and Linux. Limited by the compatibility of client software.
Supported hardware architecture	Natively Running on 32-bit Intel 386, 64-bit Intel 386 (a.k.a. amd64), ARM, ARM64, PPC64, IBM z/Architecture, a.k.a. s390x, MIPS, MIPS64.	Dependent on client device capabilities; generally supports common architectures like x86, x64, and ARM, but can be limited by the specific VPN client and OS compatibility.
Support natively Android and iOS	Supported integrated Android and iOS VPNs.	Requires installation of VPN client apps which may vary in features and performance across devices.
Technology release mode	Software only. The central components are in a Linux container format and integrate natively with frameworks like Istio for Kubernetes, enabling them to be structured as a SaaS (Software as a Service) platform. The distributed components come in different versions, depending on the operating environment and hardware they support.	Primarily software-based; some providers offer hardware appliances for larger enterprise environments.

Evaluating AlgoSASE vs Traditional VPN

Topic	AlgoSASE	Traditional VPN
Infrastructure dependencies	AlgoSASE is infrastructure agnostic: no modifications are needed to implement the current network infrastructure or hardware. AlgoSASE software components are installable in supported operating/hardware environments. Where this is not possible, Proxy functions must be used to access the mesh (Edge Nodes, Gateway Nodes). Firewall configuration is only necessary in certain situations (UDP hole punching used by the Data Layer).	Often requires extensive configuration of network firewalls and routers, potentially needing additional hardware depending on the scale and security requirements.
Cloaking	Secures communications with the most advanced cryptographic frameworks. SPA (Single Packet Authorization) and Fails Closed (designed to close in case of failure) for enhanced security.	Utilizes standard encryption methods like AES-256; may include features like stealth modes to bypass network restrictions but generally less advanced than AlgoSASE.
Data Layer cryptographic framework	Confidentiality and integrity for each communication. Crypto agility features e.g. AES256/SHA256, ChaCha20/Poly1305.	Commonly uses strong encryption standards like AES-256 for IPsec; may also employ older or less secure protocols depending on configuration.
Quantum resistance	Post-Quantum Cryptography (PQC) ready e.g. adopting PQ hybrid certificates.	Not typically designed for quantum resistance; depends on future updates or specific cryptographic enhancements.
Integrated firewall	Built-in policy-based distributed firewall with the capability of granular access control (CIDR, protocol, and port). Two levels of firewall: Data Layer integrated and kernel (Netfilter based).	Usually requires an external firewall; does not typically include an integrated distributed firewall capability.

Evaluating AlgoSASE vs Traditional VPN

Topic	AlgoSASE	Traditional VPN
Zero Trust Network Access	Native ZTNA (Zero Trust Network Access) mutual authentication based on node/user identity.	Limited implementations; mostly relies on traditional perimeter-based security models.
Verified identity	Verified devices (device identity) (mutual authentication) and accounts	Relies heavily on traditional user credentials; some systems may incorporate device checking. Virtual appliance identity can be spoofed.
Authentication	Each node/user object can be authenticated by an existing federated AD/LDAP Identity Provider (IdP-SSO via SAML2, OAuth2 or OpenID Connect) or a fully isolated system using 2FA (OTP) and associated to one (or more) Security Group.	Supports standard VPN authentication methods like password, token-based, and certificate-based authentication.
Authorization	Based on Security Groups: each Security Group is associated with policies that govern the visibility of services in the mesh through templates e.g. data layer firewall, authorized routes, kernel firewall, etc. An adaptive merge function is invoked when an object belongs to more Security Groups.	Typically employs group-based access control; lacks the dynamic and granular control offered by more modern network solutions.
Certified Addresses	The IP addresses of the AlgoSASE nodes and subnets that the Edge Nodes and Gateway Nodes manage are authorized via dynamically assigned certificates and, therefore, cannot be falsified	Generally uses a static address assignment; lacks the dynamic certificate-based address management found in AlgoSASE.

Evaluating AlgoSASE vs Traditional VPN

Topic	AlgoSASE	Traditional VPN
Performance	Increases speed over traditional stacks e.g. the Noise framework can be faster than traditional IPsec. Hardware accelerators can dramatically increase performance. Proxy functions for environments that do not support AlgoSASE relieve them of encryption costs.	Can be impacted by the VPN server's location and load, resulting in potential latency and reduced throughput.
Overhead	Autonomously the mesh network uses preferably direct connections without intermediate hops, resulting in better performance and confidentiality. Where direct connection is not possible due to restrictions in network firewalls, it is possible to use Brokers limited to the sole function of traffic relay.	Typically introduces additional latency due to encryption processing and routing through VPN servers.
Ethernet connection	Wired and Wireless Ethernet is supported. This also includes mobile devices such as cell phones, tablets, and general devices.	Supports both wired and wireless connections, dependent on the client device's capabilities.
End node configuration	ZTNC (Zero Touch Network Configuration). No configuration work must be performed on the edge nodes.	Requires manual configuration of VPN clients on each device.
Easy deployment for large systems	Up to many thousands: the limit on the number of AlgoSASE nodes supported depends on the number and performance of the central controllers.	Scaling can be labor-intensive, requiring manual configuration and management of multiple VPN servers.

Evaluating AlgoSASE vs Traditional VPN

Topic	AlgoSASE	Traditional VPN
Single Visibility Point	The central components of AlgoSASE technology are Brain, Broker, Portal and Repository. Their number and topological distribution must satisfy the needs and requirements of security and resilience.	Management typically centralized through a VPN server or management software, which may not offer the granularity of AlgoSASE.
AlgoSASE User/Management Portals	The User and Management Portal supports the configuration, registration, and other control functions. They centralize and simplify security management.	Often provides a basic management interface; advanced configurations require direct access to the VPN server or specialized management software.
APIs	Microservices exposed by the central controller to enable functional extension.	Limited or no API access for extending functionality or integrating with other systems.
Support for Hybrid environments (cloud, on prem, dedicated)	AlgoSASE distributed technology: Consumer nodes (physical/virtual) support applications (.e.g. Linux server/desktop), Edge nodes (physical/virtual) support Consumer Instances (e.g. IoT devices), Gateway nodes (physical/virtual) support Data Center Instances (e.g. mainframe).	Compatible with various environments but may require significant configuration and management effort.

Evaluating AlgoSASE vs Traditional VPN

Topic	AlgoSASE	Traditional VPN
Auditing and Monitoring	AlgoSASE provides the facility for logging to be centralized in an enterprise solution such as ELK/EFK (Elasticsearch Logstash/Fluentd Kibana). This means that security auditing and troubleshooting can be achieved through a single point and is hence far more efficient. The Repository also integrates with ML/AI tools for autonomous reaction to security events.	Basic logging features; more comprehensive monitoring may require additional network management tools.
Continuous traffic monitoring and auditing	Each AlgoSASE node centralizes traffic and security logs for auditing and troubleshooting at the individual user and node level.	Continuous traffic monitoring and auditing: Typically limited to connection logs; lacks detailed traffic analysis and real-time monitoring capabilities.