Aryaka SmartSecure Private Access Data Sheet

SmartSecure
Security-as-a-Service

SmartSecure Datasheet

VPN Solutions Overview

Even before the 2020 pandemic, it was clear that the era of the static, traditional network was coming to an end. Complexity is the enemy of agility, and hence SD-WAN technology is rapidly replacing traditional router-based enterprise networks. Now, with the dawn of the SASE (Secure Access Service Edge), SD-WAN and advanced security functions are being combined to optimally deliver on new enterprise and end user needs.

The same limitations in agility also afflict traditional VPN (Virtual Private Network) solutions. VPNs' traditional design pattern is still primarily based on the outdated assumption that a remote users' main need is to be securely connected to internal enterprise resources by connecting to a VPN server that acts as a gatekeeper to those resources. But as most user traffic now goes to the cloud (SaaS, IaaS, UcaaS, etc), back-hauling traffic into the internal enterprise network, inspecting it for compliance and finally routing it to the XaaS destination is a user experience killer. The recent pandemic exposed the lack of adaptability of enterprise-centric VPN solutions: in many cases, their close architectural coupling with traditional network architectures led to performance and user experience issues for a remote workforce.

Cloud-centric, VPN-like solutions provide an alternative to traditional VPN architectures. But a cloud-only approach also can impose severe performance limitations on the user experience: the additional security hop in the public cloud can easily turn into a bottleneck, which is particularly problematic for real-time collaboration applications.

It is also important to point out that both VPNs solutions rely exclusively on the best-effort public internet as an on-ramp to either the internal enterprise network or cloud applications.

Both VPNs and SWG solutions are challenged by deploying remote access functionality as a stand-alone environment without consolidated visibility into network or application performance, reporting or logging with the over-arching enterprise network and security infrastructure. This leads to increased complexity over time as organizations are forced to manage a multitude of complex point products that make their operations less effective and increase operational cost. Moreover, productivity suffers when user experience is not guaranteed.

Aryaka SmartSecure Private Access Overview

Aryaka's SmartSecure Private Access solution leverages the performance of Aryaka's Global Layer 2 Core Network with its architectural Cloud-First approach to provide the optimal solution for enterprises seeking a "Best of Both Worlds" approach to remote worker connectivity: a solution that combines flexible utilization of deterministic, dedicated network resources to both branch as well as remote workers over a high performance network. This architecture always delivers on maximum performance -irrespective of traffic shifts between branch and remote worker traffic- with consolidated visibility into network and application performance across enterprise core connectivity as well as VPN domains.

SmartSecure Private Access

Delivering on Superior Network Performance for Remote Workers

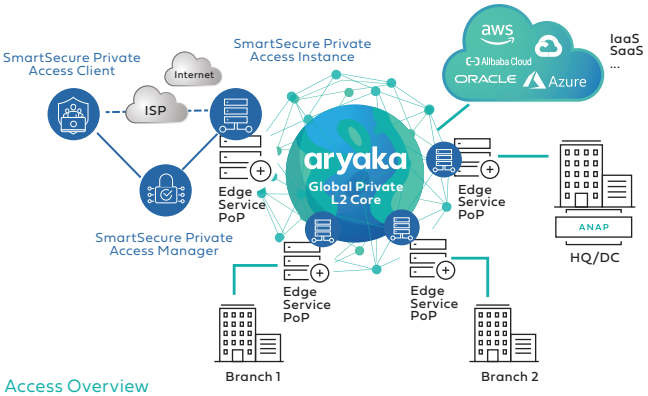


Figure 1: SmartSecure Private Access Overview

Edge Services POP

Enable a Global Private Services Core with chaining of WAN, multi-cloud & Security

ANAP Edge Services CPE

Connects enterprise offices to the Aryaka WAN Services Fabric – hosts VNFs (i.e. NGFW)

SmartSecure Private Access Instance

Connects remote users to the Aryaka Private Access VPN as-a-Service and global private core for superior performance

SmartSecure Private Access is based on the Enterprise VPN solution by NCP Engineering, a leading VPN provider.

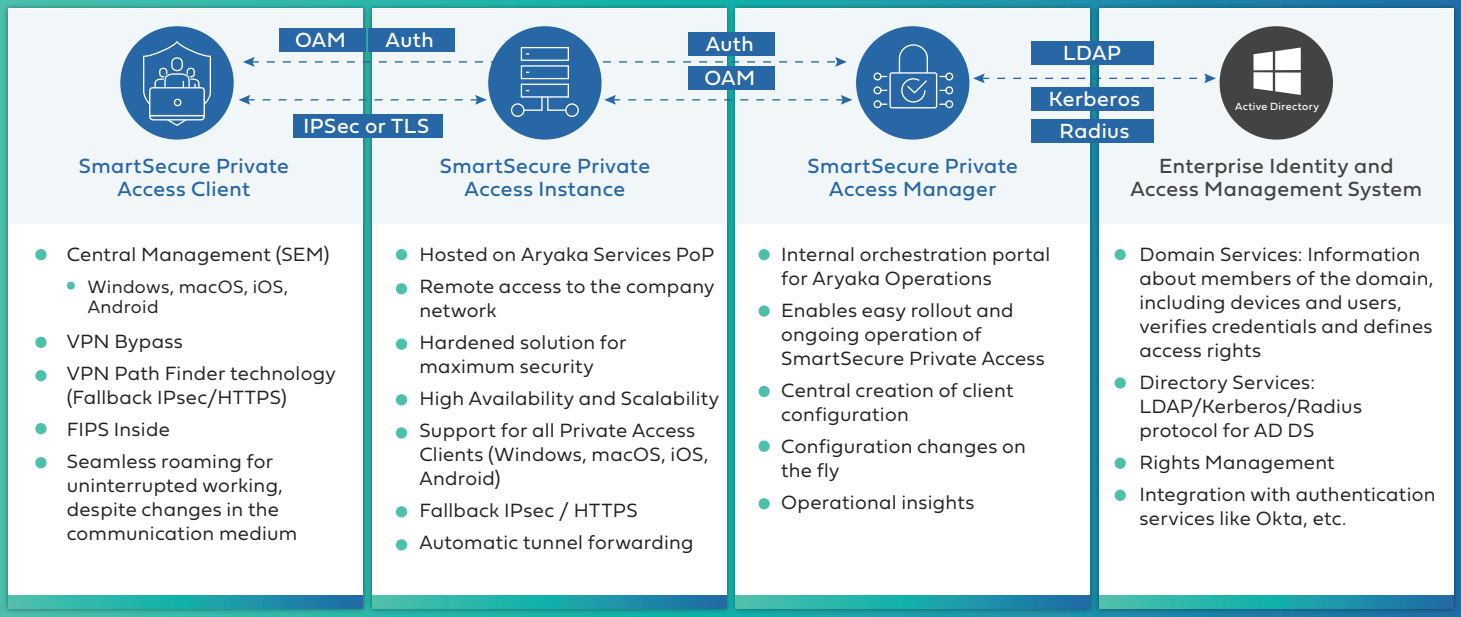


Figure 2: SmartSecure Private Access Solution Elements

SmartSecure Private Access consists of the following architectural elements:

SmartSecure Private Access Client

SmartSecure Private Access Instance

SmartSecure Private Access Manager

SmartSecure Private Access Clients

The SmartSecure Private Access solution provides a centrally managed client suite for all major desktop or mobile operating system, including:

Windows | macOS | ios | Android

Aryaka's SmartSecure Private Access Clients allow end user devices to select the closest Aryaka PoP for optimal, high-performance network access and reach it with the most effective tunneling protocol.

The SmartSecure Private Access Client ensures robust, unified endpoint compliance. It protects the integrity of the enterprise network by strict VPN access control, which first terminates on the nearest Aryaka SmartSecure Private Access Instance and then proceeds to the appropriate private or public DC destination. Traffic travels by the Aryaka Global Layer 2 Core Network, delivering the performance benefits of the Aryaka core.

The SmartSecure Private Access Client is a communication software product for universal implementation in any remote access VPN environment. It allows remote workers to access applications and data transparently and securely, on-premise or in the cloud, from any location – just as if they were in the corporate office. Seamless roaming provides an optional secure, always-on connection to the corporate network, automatically selecting the fastest medium for access to the internet. When the access point or the IP address changes, Wi-Fi roaming, or IPsec roaming maintains the VPN connection. Even behind firewalls whose settings always block IPsec data connections, the Private Access Client ensures remote access is available by finding an unlocked path. The client supports domain logon using a credential service provider after establishing a VPN connection to the company network.

A bypass function in the Private Access Client allows the IT administrator to configure the client so that certain applications are exempted from the VPN and the data is sent over the internet even when split tunneling is disabled. This prevents applications such as video streaming from unnecessarily taxing the enterprise infrastructure.

All client configurations can be locked by the administrator, meaning that the user cannot change the locked configurations.

The Private Access Client is simple to install and simple to operate. A graphical, intuitive user interface provides information on all connection and security states. Moreover, detailed log information supports effective assistance from the help desk.

SmartSecure Private Access Instance

Aryaka's Private Access Clients connect to the Aryaka Private Access Instance closest to them. Aryaka's Private Access Instance are a virtual service hosted on Aryaka's global Service PoPs, which provide a sub-30ms onramp to the Aryaka Core Network to 95% of knowledge workers around the planet. Aryaka's Service PoPs host services that go beyond basic network connectivity: network and application acceleration, strict separation of customer-dedicated resources and secure traffic encryption, among others.

After secure connections are established, the Secure Private Access Instance function receives traffic from all the clients accessing it, and routes it across the high performance Global Aryaka L2 Core network to either the enterprise HQ/DC or to a SmartCloud service location that peers optimally given the user's location.

SmartSecure Private Access Instance are based on a multi-tenant architecture and a hardened Linux operating system which is optimized for maximum security. Furthermore, the Aryaka Service PoP architecture guarantees deterministic performance and high availability.

SmartSecure Private Access Instance can handle a highly scalable number of connections to the company network via an IPsec VPN. The Private Access Clients users can be assigned the same private IP address from a pool assigned by the company each time they connect to the network. This makes remote administration much easier as each user can be identified by their IP address. If the IP address is assigned dynamically from a pool, it will be reserved for the user for a defined period (lease time). Dynamic DNS (DynDNS) ensures that the VPN Gateway is still reachable if the device is assigned a dynamic IP address.

SmartSecure Private Access Manager

The SmartSecure Private Access Manager provides the configuration and management function for all components in the Aryaka Private Access solution. Together with the Private Access Instance, it is also tasked with user authentication via communication with enterprises' existing IAM (Identity & Access Management) systems.

The SmartSecure's Private Access Manager allows Aryaka to provision and manage Private Access Clients and Private Access Instance in the PoPs. It also establishes the connectivity with enterprises' over-arching IAM systems for the authentication of Private Access Clients. With this mechanism, the security status of mobile and stationary end devices is verified prior to the device gaining access to the corporate network. All parameters are defined centrally by Aryaka on behalf of the enterprise, and remote workers are granted access rights based on their compliance to them.

SmartSecure Private Access Manager is a key component in providing a VPN solution that is easy to establish and operate.

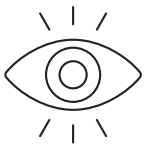
The Private Access Manager integrates with an enterprise's existing identity management (e.g. Microsoft Active Directory) and requests regular updates. As soon as a new employee is listed in this database, the Private Access Manager creates an individual configuration for this user, according to defined templates. If a former employee has been removed from the database, the Private Access Manager immediately blocks this VPN access. This eliminates the need to manually configure the computers of all mobile employees. The Private Access Manager also enables fast rollout of many users and software certificates.

Private Access Manager provides the following functions:

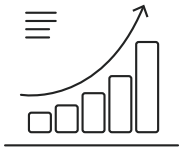
 Client Configuration	Private Access Manager provides the configuration and management of all components for the Aryaka Private Access solution. This includes the Private Access Clients for Windows, macOS, iOS and Android. All relevant parameters are predefined and stored in templates.
 Automatic Update Process	The fully automatic update process allows the administrator to centrally provide all remote Private Access Clients with configuration and certificate updates. As soon as the client logs in to the corporate network, the system automatically updates the client. If malfunctions occur during the transmission, then the previously existing configuration remains unaffected.
 License Management (Used only by Aryaka Operators)	The licenses of all connected components are centrally stored in the PAM and managed by Aryaka for enterprise customers. The system transfers them into a license pool and automatically manages them according to specified guidelines. This license transfer might be used for: transfer into a configuration per remote client or gateway, returning the license to the license pool when an employee leaves a company, or triggering a prompt when no more licenses are available.
 System Monitor (Used by Aryaka Operators)	Aryaka can offer enterprises immediate insight into all important events within the SmartSecure Private Access solution. The administrator can use the system monitor as needed to call up status information in real-time, or to access previously saved data respositories for the remote access environment.

SmartSecure Private Access Benefits

Improve end user experience and productivity with deterministic network behavior



Dramatically improve global VPN performance by leveraging the Global Aryaka Layer 2 Core



Immediate visibility into network, application performance and user experience

Technical Specifications

SmartSecure Private Access Client

Universal, centrally administrable VPN Client Suite for Windows, macOS, iOS, Android

Operating Systems	Microsoft Windows, macOS, iOS, Android
Security Features	The Enterprise Client supports all major IPsec standards in accordance with the RFCs
VPN Bypass	The VPN Bypass function allows the administrator to define applications which can communicate over the internet directly despite disabling split tunneling on the VPN connection. It is also possible to define which domains or target addresses can bypass the VPN tunnel.
Virtual Private Networking	IPsec (Layer 3 Tunneling), IPsec proposals can be determined through the IPsec gateway (IKEv1/IKEv2, IPsec Phase 2); Event log; Communication only in the tunnel; MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T); IPsec tunnel mode
Encryption	Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits; Dynamic processes for key exchange: RSA to 2048 bits; seamless rekeying (PFS); Hash algorithms: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH group 1,2,5,14-21, 25-30
Authentication Processes	IKE (Aggressive Mode and Main Mode, Quick Mode); XAUTH for extended user authentication; IKE configuration mode for dynamic assignment of a virtual address from the internal address pool (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2); Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready.
Networking Features	LAN Emulation: Ethernet adapter with NDIS interface, full WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network) support

Seamless roaming	If a communications medium error occurs, automatic switchover of VPN tunnel to another Internet communication medium (LAN/WWAN/3G/4G) without altering the IP address ensures that applications communicating over VPN tunnel are not disturbed and the session to the Private Access Instance is not disconnected.
VPN Path Finder	Fallback IPsec/ HTTPS (port 443) if port 500 (UDP encapsulation) is not possible
IP Address Allocation	DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via a DNS server
Communication Media	Internet, LAN, Wi-Fi, GSM (incl. HSCSD), GPRS, 3G, LTE, HSDPA, PSTN.
Line Management	DPD with configurable time interval; Short Hold Mode; Wi-Fi roaming (handover); Timeout (controlled by time and charges); Budget Manager; Connection Modes: automatic, manual, variable
APN from SIM Card	APN (Access Point Name) defines the access point of a mobile data connection at a provider. If user changes provider, the system automatically uses APN data from SIM card to configure Secure Client
Data Compression	IPCOMP (lzs), deflate
Quality of Service	Prioritization of configured outgoing bandwidth in VPN tunnel (may vary with client OS)
Additional Features	UDP encapsulation, WISPr-support, IPsec-roaming , Wi-Fi roaming, Split Tunneling
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over Ethernet;LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP security architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT- T), UDP encapsulation, IPCOMP; RFC 7427: IKEv2-Authentication (Padding-method)
Client Monitor Intuitive, Graphical User Interface	Multilingual (English, Spanish, French, German); intuitive operation; Configuration, connection management and monitoring, connection statistics, log-files, internet availability test, trace tool for error diagnosis; Display of connection status; Integrated support of Mobile Connect Cards, embedded; Client Monitor can be tailored to include company name or support information; Password protected configuration management and profile management, configuration parameter lock

SmartSecure Private Access Instance

Remote access to the enterprise network leveraging the Global Aryaka Layer 2 Network

General	
Aryaka Service PoP locations	Aryaka has Service PoPs in over 40 worldwide locations, within <30ms of 95% of all knowledge workers world-wide.
Management	Aryaka Private Access Manager provides the provisioning and operations portal – enterprise administrators can gain immediate insights into their VPN deployment.
High Availability	Aryaka Service PoPs are built on a highly redundancy architecture and topology to ensure High Availability.

Dynamic DNS (DynDNS)	Connection set up via Internet with dynamic IP addresses. Registration of each current IP address with an external Dynamic DNS provider. In this case the VPN tunnel is established via name assignment.
DDNS	Connected VPN clients are registered with the domain name server via Dynamic DNS (DDNS), meaning that VPN clients with dynamic IPs can be reached via a (permanent) name.
User Administration	Local user administration; OTP server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages
FIPS Inside	The IPsec client integrates cryptographic algorithms based on the FIPS standard. The embedded cryptographic module, containing the corresponding algorithms has been validated as compliant to FIPS 140-2 (Certificate #1747). FIPS compliance will always be maintained when the following algorithms are used for set up and the encryption of a VPN connection: • Diffie Hellman-Group: Group 2 or higher (DH starting from a length of 1024 bits) • Hash algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits • Encryption algorithms: AES 128, 192 and 256 bits or Triple DES
Client/User Authentication Processes	OTP token, user name and password (XAUTH)

Connection Management	
Line Management	Dead Peer Detection (DPD) with configurable time interval; Timeout (controlled by duration and charges)
Point-to-Point Protocols	LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Pool Address Management	Reservation of an IP address from a pool for a defined period of time (lease time)

IPsec VPN	
Virtual Private Networking	IPsec (Layer 3 tunneling), RFC-compliant; Automatic adjustment of MTU size, fragmentation and reassembly; DPD; NAT Traversal (NAT-T); IPsec modes: Tunnel Mode, Transport Mode Seamless Rekeying; PFS
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, IKEv2 (incl. MOBIKE), IKEv2 Signature Authentication, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, IKEv2 authentication compliant to RFC 7427 (padding process)
Encryption	Symmetric processes: AES (CBC/CTR/GCM) 128, 192, 256 bits; Blowfish 128, 448 bits; Triple-DES 112, 168 bits; Dynamic processes for key exchange: RSA to 4096 bits; Diffie-Hellman Groups 1, 2, 5, 14-21, 25-30; Hash algorithms: SHA-1, SHA 256, SHA 384 or SHA 512
VPN Path Finder	Fallback to HTTPS from IPsec (port 443) if neither port 500 nor UDP encapsulation are available
Seamless roaming	The system can automatically transfer the VPN tunnel to a different communication medium (LAN / Wi-Fi / 3G / 4G) without changing the IP address to avoid interrupting communication via the VPN tunnel or disconnecting application sessions.

Authentication Processes	IKEv1 (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication; IKEv2, EAP-PAP / MD5 / MS-CHAP v2 / TLS One-time passwords and challenge response systems
IP Address Allocation	DHCP (Dynamic Host Control Protocol) over IPsec; DNS: Selection of the central gateway with dynamic public IP addresses by querying the IP address via a DNS server; IKE config mode for dynamic assignment of a virtual address to clients from the internal address range (private IP) Different pools can be assigned depending on the connection medium (Client VPN IP)
Data Compression	IPCOMP (lzs), Deflate

SmartSecure Private Access Manager

Centrally Managed VPN as a Service with Fully Automatic Operation of a Remote Access VPN

Supported Functions	Automatic Update, Client Firewall Configuration, System Monitor
User Administration	LDAP, Novell NDS, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages
Client/User Authentication Processes	OTP token, user name and password (XAUTH)
Supported RFCs and Drafts	RFC 2138 Remote Authentication Dial In User Service (RADIUS); RFC 2139 RADIUS Accounting; RFC 2433 Microso CHAP; RFC 2759 Microso CHAP V2; RFC 2548 Microso Vendor-specific RADIUS Attributes; RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP); RFC 2716 PPP EAP TLS Authentication Protocol; RFC 2246 TLS Protocol; RFC 2284 PPP Extensible Authentication Protocol (EAP); RFC 2716 Certificate Management Protocol; RFC 2511 Certificate Request Message Format

About Aryaka Networks

Aryaka, the Cloud-First WAN company, brings agility, simplicity and a great experience to consuming the WAN-as-a-service. An optimized global network and innovative technology stack delivers the industry's #1 managed SD-WAN service and sets the gold standard for application performance. Aryaka's SmartServices platform offers connectivity, application acceleration, security, cloud networking and insights leveraging global orchestration and provisioning. The company's customers include hundreds of global enterprises including several in the Fortune 100.