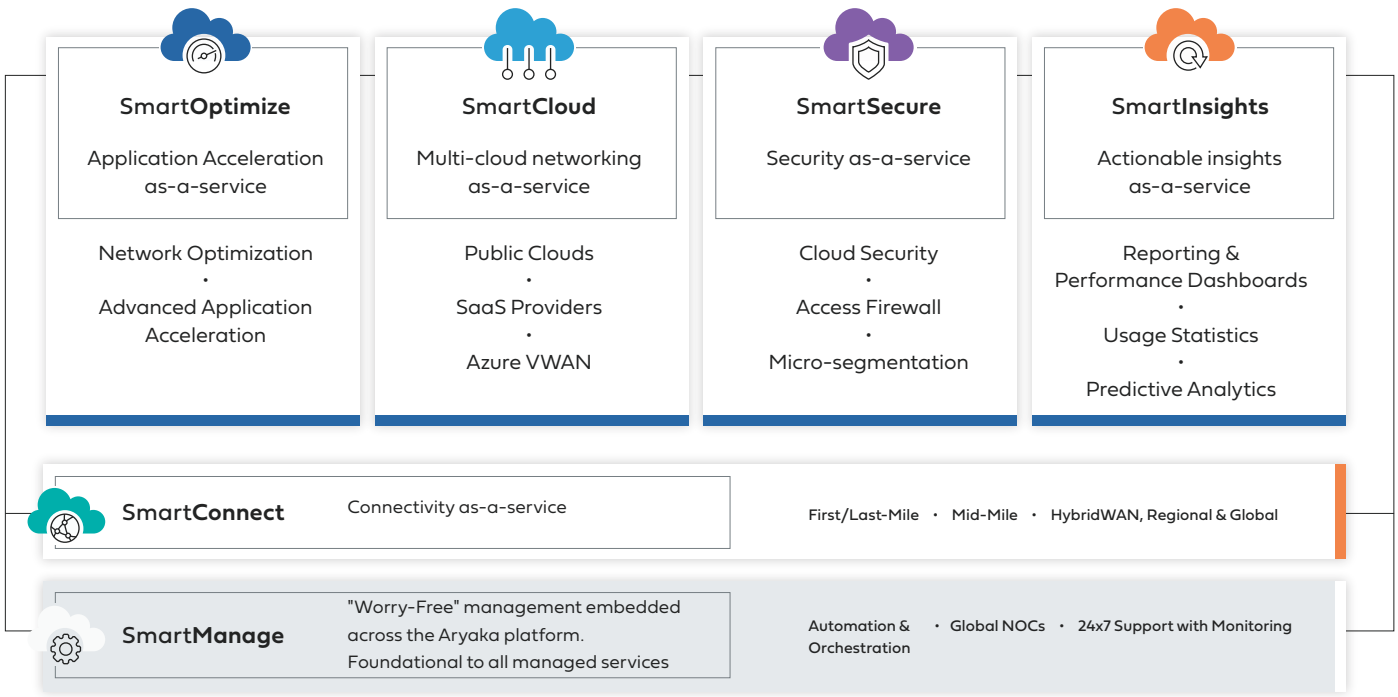
Aryaka Network Access Point (ANAP) Datasheet

ANAP Datasheet

Aryaka's ANAP (Aryaka Network Access Point) is an appliance that delivers on a virtualized, software-defined branch (SD-Branch) solution and is included and is part of Aryaka's SmartServices. It aggregates multiple WAN connections and provides converged network services including routing, encryption, security and traffic management. ANAP also supports redundancy with high-availability configuration options.

Aryaka Solution Overview



Aryaka's ANAP appliance helps enterprises simplify their branch by consolidating networking and security into a single software-defined and cloud-managed device, eliminating the need for a multitude of separate, function-specific appliances. Aryaka's ANAP is the on-ramp to the Aryaka managed global SD-WAN enterprise networking solution and integrates advanced networking, application optimization and acceleration as well as security functions.

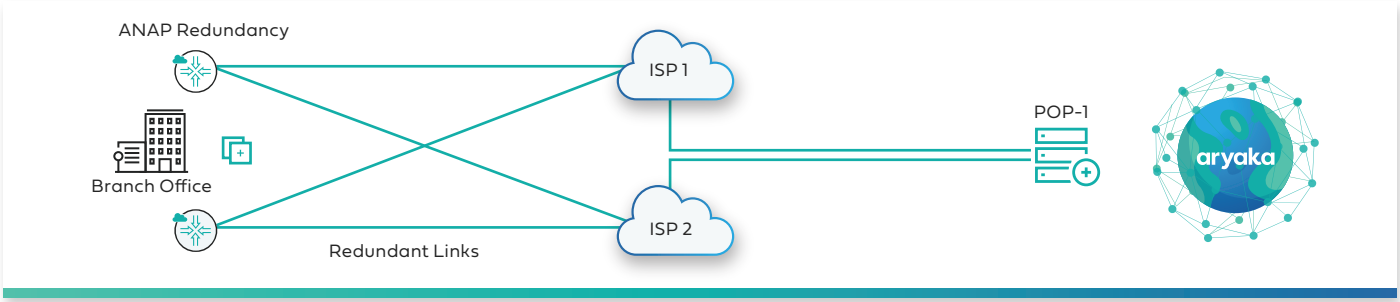
The ANAP product family consists of appliances based on an extremely adaptable white box architecture running the industry-standard Linux operating system, which provides built-in virtualization (KVM) and containerization technology to support Virtual Network Functions (VNFs).

Aryaka's ANAP, enterprises can deliver enterprise-class connectivity to remote locations (which often lack qualified IT personnel) within less than 48 hours by leveraging the ANAP's ZTD (Zero Touch Deployment) model. Zero Touch Deployment means that appliances are simply sent to any location without the need to configure them beforehand. The Aryaka Managed SD-WAN solution helps enterprises reduce the CAPEX and OPEX of their WAN and branch infrastructure while delivering on superior application performance as well as optimal cloud connectivity.

Benefits

- **Deployment simplicity and integrated design:** Aryaka's ANAP comes pre-configured and is easily implemented with a zero-touch deployment model.
- **Software-defined solution:** Built on top of a hardened Linux operating system, Aryaka's ANAP implements networking, application optimization and security services as software functions, avoiding the built-in obsolescence of custom architectures.
- **Built-in SD-WAN:** Aryaka's ANAP is an integral component of Aryaka's SmartServices. It helps enterprises leverage any last-mile transport (MPLS, hardened internet) and can leverage the high-quality Aryaka core network to attain MPLS quality-of-service levels.
- **HybridWAN** support providing Aryaka L2 Core, MPLS, site-to-site internet and public internet path options.
- **Built-in** Azure Virtual WAN support.
- **Built-in security:** The ANAP implements a stateful, L3/4 firewall to thwart attacks to the branch. It also implements branch traffic segmentation: corporate traffic is kept strictly separate from other types of traffic such as DMZ or Guest WiFi traffic. The ANAP also supports NFV-based virtual firewalls from Tier-1 security vendors.
- **Redundancy:** Support for link (dual ISP links) and device (VRRP) redundancy delivers on very high availability requirements (see illustration). Fail-to-wire is supported for inline mode.
- **Better user experience:** Deterministic, predictable performance for applications residing in the data center or in the cloud.
- **Multi-Tenant Solution:** Aryaka's ANAP supports up to 32 tenants via micro-segmentation.
- **Flexible branch deployment** options including inline, simple routed, hybrid and edge routed mode.
- **Greater agility:** Faster, easier deployment and operation of of your managed SD-WAN, with greater performance using less bandwidth. Add new revenue generating services in minutes not months.

ANAP Redundancy



Hardware Specifications

	ANAP 1500	ANAP 2500/2600	ANAP 3000	ANAP 10000
Bandwidth	Up to 150Mbps	Up to 650Mbps	Up to 1 Gbps	Up to 3Gbps
Interface type	Copper	Copper	Copper/Fiber	Copper/Fiber
NFV Capable	No	No/Yes	Yes	Yes
QoS / WAN	Yes	Yes	Yes	Yes
Optimization	Yes	Yes	Yes	Yes
Routing	Yes	Yes	Yes	Yes
Edge Security	Yes	Yes	Yes	Yes
Cloud Security	Yes	Yes	Yes	Yes
Connectors	Yes	Yes	Yes	Yes
Monitoring	Yes	Yes	Yes	Yes
Recommended for	Small Sites	Medium Sites	Large Sites	Large Sites

ANAP Architecture Highlights

- QoS

Classification and Marking	IP 5-tuple-based marking DSCP/ToS-based classification DNS lookup SNI lookup DPI (Deep Packet Inspection)
Class of Service Shaping	5 classes of service with bandwidth reservation/limits Hierarchical token-bucketbased queuing and shaping
TCP/IP Shaping	TCP-IP flow-level advanced shaper with two classes
Adaptive QoS	Sharing unused ASN link capacity with low priority internet traffic Supported on ERM only and enabled by default

- WAN Optimization

TCP Boost	Minimize latency and congestion avoidance over the last-mile with WAN rate control
ARR	Patented compression and data deduplication algorithms

- Routing

eBGP	eBGP support with Preferred Path selection using AS PATH Prepend and MED (Multi-Exit Discriminator) attributes MP-BGP and BGP Communities support
Thin RIP (T-RIP)	RIPv2.0-compliant routing advertisements to simplify routing configuration
Static Routing	Static route configuration for local subnets, default gateway and IPSec tunnel gateway Forwarding decision based on 6-tuple match criteria and/or DNS
Policy-based Routing	• Forward to LAN • Forward to Internet • Forward to Aryaka • Drop
Policy-based Routing based on Source Address	Forward packets based on IP source address
Route Filters	Granular 6-tuple policy control to forward/drop Aryaka- and internet-bound traffic

- Redundancy

Edge Redundancy	Dual IPSec tunnels to different ISPs for link redundancy
VARP (Virtual ANAP Redundancy Protocol)	VRRP-like model for ANAP redundancy in active-standby model
ANAP-to-ANAP backup tunnels	Direct IPSEc tunnels between ANAPs across the internet in the unlikely case the primary Aryaka tunnel fails
ISP link redundancy	SMARTlink allows the use of 2 ISP links in an active-active configuration • Path Selection: Selective routing across the links • Load Balancing: Distribute traffic across the links on a per-packet basis • FEC: Replicate or duplicate traffic across the links to recover lost packets • Timed Replay: flows can be replayed within a link after a delay, to recover lost packets • Path Loss Recovery (PLR): Introduces a feedback mechanism between the POP and ANAP to determine the exact packets lost during transmission, and recover these packets
MPLS link redundancy	Dual MPLS tunnels with redundant ANAP deployment

- Security

NAT Support	Stateful flow tracking based on NAT policies • Source NAT support – 1-to-1 NAT, dynamic IP and port • Destination NAT support – port forwarding and port translation

Firewall and Branch Segmentation	L3/ L4 Stateful Firewall for perimeter firewalling and East-West Branch Segmentation
Multi-Tenancy	Multi-Tenancy support through VRF-based Microsegmentation
Check Point	Hosted VM Next Generation Firwewall as VNF (Virtual Network Function)
Palo Alto Networks	Hosted VM Next Generation Firwewall as VNF (Virtual Network Function)
Zscaler	IPSec IKev1 support (in addition to GRE tunnels)
Private VLANs ANAP Hardening SEC-2	Ability to group a set of VLANs and restrict access only to internet Secure ANAP bootstrap process with secure ANAP image

- Cloud Security Connectors

Check Point	IPsec IKEv1, IKEv2 or GRE tunnels Policy-based routing between internet, Aryaka and Check Point CloudGuard Connect bound traffic
CloudGuard Connect	MyAryaka for Tunnel Connectivity monitoring to Cloudguard Connect
Zscaler	Support for Redundant GRE tunnels Policy based routing between internet, Aryaka and Zscaler bound traffic MyAryaka support for visibility and configurability
Palo Alto Prisma	IKEv1 based IPsec tunnel Policy based routing between internet, Aryaka and Palo Alto Prisma bound traffic MyAryaka support for visibility and configurability
Symantec	IKEv1 based IPsec tunnel Policy based routing between internet, Aryaka and Symantec bound traffic MyAryaka support for visibility and configurability

- Monitoring

Syslog	Flow logs for packets routed between LAN, internet and Aryaka sites Flow Logs for packets dropped due to policies or firewall rules System logs RFC 5424 support Key, value pair-based attribute logging for easier parsing Support for UDP and TCP based connectivity to collector
Netflow	Support for NDE version 1,5 and 9. Default of 9. Ability to monitor LAN, Internet, cloud security connectors, and Aryaka traffic. 1:1 sampling rate Flow information is uploaded to ANAP to MyAryaka every 300 seconds

- Virtual Network Function Support

Hosted Virtual Machine (VM)	Support of 3rd party VMs via Linux KVM

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 offer 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.