



Aryaka Security Model

As a WAN Optimization and Application Acceleration Service, delivered as a Software As A Service (SAAS) model, Aryaka enables companies to scale bandwidth on demand and mitigate the need to over subscribe for future growth and free up budget for other mission critical projects.

Security of our customers data as it passes through our network has been a key consideration in the architecture and operational management. Aryaka implements security features at many levels within the network, providing network security, data security and physical security at our global points of presence.

Network Security

The Aryaka core network is a **closed network** that consists of private high speed layer 2 links, connected in a partial mesh. This network is built, operated and managed by Aryaka Networks out of a centralized NOC with 24x7 operations.

Transport of any data through the Aryaka Network is done through **enterprise grade end-to-end encrypted tunnels**. These tunnels are using industry standards based IPsec technology and are established between each of the enterprise locations and the Aryaka network. A dedicated tunnel in the core of the network provides continued security over the global network and guarantees strict traffic segregation. The tunneling mechanisms in place provide data authenticity; privacy and non-repudiation security services that are superior to MPLS offered services.

IPsec is a standardized protocol suite for securing IP flows by encrypting and authenticating each IP packets in the flow. The suite includes a key management protocol that allows mutual authentication of devices to provide a secure management channel, over which further protocol negotiation can take place.

Traffic flowing in or out of the Aryaka points of presence (PoPs) will always be secured by an IPsec tunnel. Should any traffic arrive that is already encrypted (e.g. HTTPS, SSH, etc ...), this will pass through all levels of optimization but no inspection will be performed on its payload.

The Aryaka POPs are **fortified with industry grade, redundant firewalls**. Ingress traffic flow into the servers is highly restricted and only known endpoints that are authenticated are able to pass traffic to the server farm. All networking equipment nodes are bolstered using industry standard and current best practices.

Aryaka can also provide an **optional, direct Layer 2 link** into the nearest Aryaka POP to shield all customer traffic from any external intrusions. This link can optionally be encrypted.

The Aryaka service is bundled with a management portal, called MyAryaka, which provides insight into the network utilization and behavior. This site is made available **through HTTPS using SSL/TLS encryption**, guaranteeing data privacy and authenticity of the data being displayed.

Data Security

Beyond security for data in transit, data at rest also needs to be secured as the service provides an advanced form of caching in our POP locations.

The data redundancy removal algorithm (ARR: Advanced Redundancy Removal) utilizes a fast SSD based history at both the POP and the optionally deployed ANAP appliance at the enterprise locations. ARR operates at a **byte level** and never stores entire objects or the relations between data segments. Therefore, in the unlikely event of the data being compromised, it will still appear as a random set of bytes.

The SSD history can be **AES encrypted** for an additional level of protection. In the POPs this will be stored on a dedicated partition, eliminating the risk of any data contamination between context. At the ANAP appliance, the chosen encryption key is saved on a removable keycard, facilitating secure physical transport through mail carriers as key and data can be sent through different handlers.

This same philosophy extends to the processing context as well where data is associated to a **dedicated process** for data inspection and service application.

Physical Security

Aryaka's network of globally deployed Points of Presence (POP) are located in **Tier3+ carrier-neutral data center facilities**. All facilities that are in use are SAS-70 certified, ensuring the highest level of facility security. All Data Centres are equipped with biometric access controlled man vaults and all networking equipment and servers are mounted in individually locked cages with key-code access. All facilities have 24x7 security staff on premises.

© 2010-2011 Aryaka. Confidential and Proprietary. Do not reproduce or distribute without prior permission.