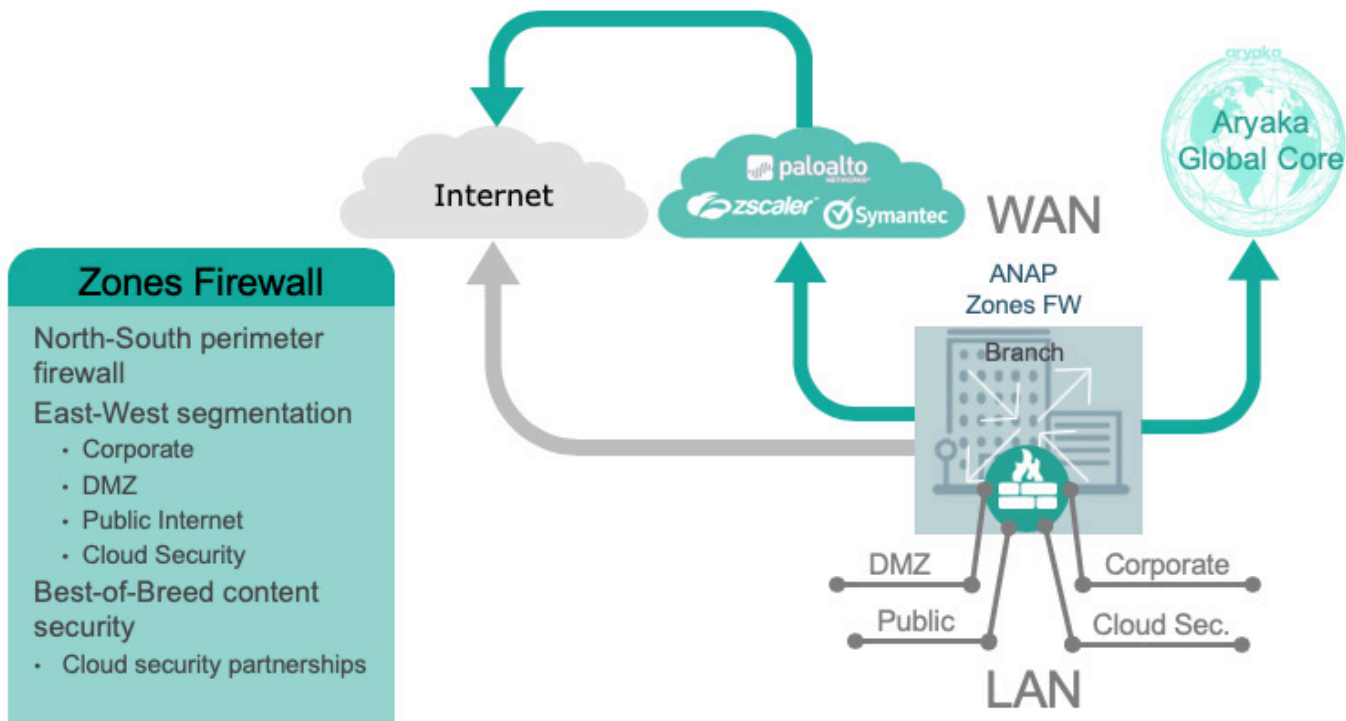


## Aryaka Zones Access Security and Multi-Tenancy Solution Brief

The foundation for business growth is secure connectivity that can scale to protect your enterprise. Aryaka Zones is a stateful firewall capability that runs on Aryaka's ANAP (Aryaka Network Access Point), which is an integral part of Aryaka's global, 100%-managed SD-WAN service.

Aryaka's ANAP delivers on access security in the branch as it connects to the Aryaka Core network, the public internet and cloud-hosted security solutions. ANAP keeps your network scalable, secure, easy to manage, and lets your business meet its goals: rolling out new services and applications, connecting to the cloud, meeting compliance requirements, or improving operational efficiency. By integrating a L3/4 stateful firewall function into ANAP -in addition to Layer 7 application-based DNS classification - enterprises can reduce the number of devices in the branch. In addition, Zones provides the foundation to support multi-tenancy via Layer 3 micro-segmentation (aka virtual routing and forwarding - VRFs).

The Zones Firewall function delivers on essential north-south as well as east-west security functionality, as illustrated below:



The North-South firewall effectively blocks external unauthorized traffic from the network while ensuring the unimpeded flow of data packets vital to the operations of the enterprise. The North-South access security solution intercepts external incursion but does not necessarily prevent security issues inside the branch network itself.

# Aryaka Zones Access Security and Multi-Tenancy Solution Brief

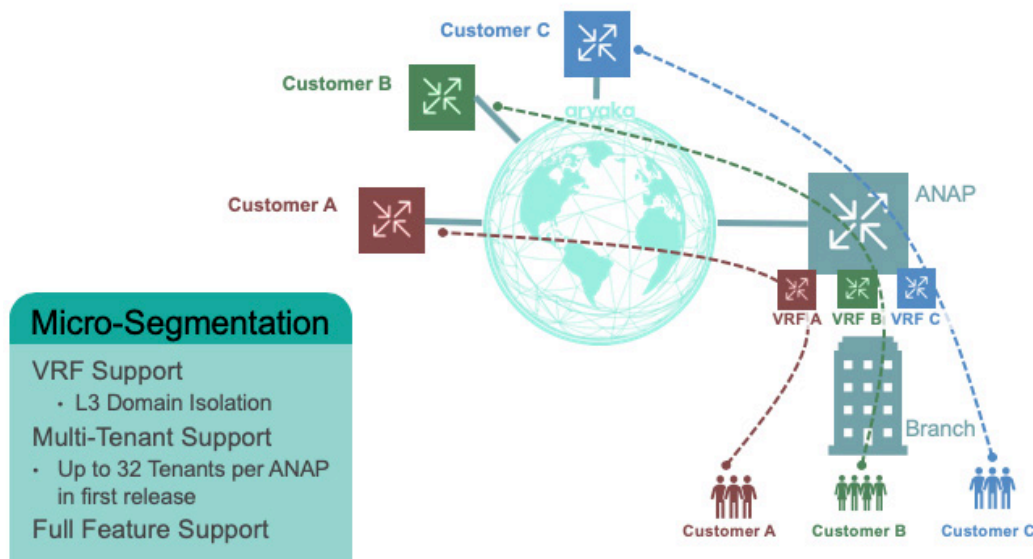
The East-West firewall provides secure segmentation inside the branch into 4 distinct zones:

- A corporate zone (also called the VPN Zone) for all corporate traffic, which will reach remote enterprise sites via encrypted VPN tunnels.
- A DMZ zone which hosts internet-facing services, which can include application servers (web, email, etc) as well as Guest WiFi access.
- The cloud zone to connect to cloud-based security solutions.
- A public zone for direct internet access.

The Aryaka Zones Firewall is a critical component of any enterprise's layered defense. It provides a flexible security foundation as enterprises embark on their WAN transformation journey. As enterprises rearchitect their network with SD-WAN, they need security across branches, cloud, users and applications.

The Zones firewall functionality provides essential capabilities that connect, secure, and manage branches sized from a handful to hundreds of users. By consolidating fast, highly available switching, routing and security in a single device, enterprises can protect their resources as well as economically deliver new services, safe connectivity, and a satisfying end-user experience.

Multi-tenancy is enabled via Layer 3 micro-segmentation, also known as VRFs. This capability permits the ANAP to support a multi-tenant branch or site, extending this logical separation across the SD-WAN.



Enterprises also require the power of choice as they build their layered security architecture. Aryaka augments the Zones branch security solution with best-of-breed cloud security by partnering with other industry leaders, allowing enterprises to build a security solution optimally tailored to their specific needs.

The Aryaka Managed SD-WAN solution helps enterprises build a highly secure SD-WAN fabric with the most flexibility, from the branch to the cloud edge.

V.092019

[LEARN MORE](#) | [info@aryaka.com](mailto:info@aryaka.com) | +1.877.727.9252

## About Aryaka Networks

Aryaka delivers the #1 fully-managed, end-to-end global SD-WAN service for the cloud-first era. Our unique technology integrates multi-cloud connectivity, application optimization, security, last-mile management and visibility into an SLA-driven OPEX-only solution that provides unmatched agility and improved TCO for the global enterprise.