Palo Alto Networks and Aryaka
Global SD-WAN with Next Generation Security

Solution Brief

The Challenge

With more than half of all enterprise WAN traffic moving to and from the cloud, global businesses are moving away from legacy architectures like MPLS to SD-WAN technologies. Typically, Internet traffic was backhauled across the WAN to centralized firewalls to maintain security. However, in to-day's cloud-centric context, ensuring application performance over such a backhauled setup becomes a challenge. In addition, security is not scalable when the organization has globally distributed users and locations.

Enterprises require a cloud-native SD-WAN platform that integrates private connectivity, application acceleration and security without adding network complexity and costs.

Aryaka Global SD-WAN

Aryaka's Global SD-WAN enables enterprises with fast global connectivity along with accelerated access to mission and business critical applications. Aryaka uses a global private network with built-in optimization and security capabilities that include a multi-layer security approach with a global private core network, fortified security on the POPs, end-to-end encrypted tunnels, and stateful firewalls.

Unlike legacy connectivity solutions that take months to deploy, Aryaka's Global SD-WAN can be deployed within days. It is delivered as a service, so IT organizations can consume global networking services the way they would consume SaaS applications like Salesforce and Infrastructure-as-a-Service solutions like Amazon Web Services and Microsoft Azure.

Key Benefits:

Accelerated Application Access:

Enable fast high-perfor-mance access to mission & business-critical appli-cations hosted locally or in the cloud.

Advanced Security:

Secure all enterprise and web traffic using compre-hensive security, threat intelligence, visibility, and control.

Network Visibility

Deliver complete visibility into application usage and performance over both the Aryaka and Palo Alto services

Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats and securing our digital way of life. The platform, comprised of next-gen-eration firewalls, threat intelligence cloud, and advanced endpoint protection, uses an innovative traffic classification engine that provides full context by identifying all traffic by application, user, and content. By combining network, cloud, and endpoint security with advanced threat intelligence in a natively integrated security platform, Palo Alto Networks safely enables all applications and deliver highly automated, preventive protection against cyber threats at all stages in the attack lifecycle without compromising performance.

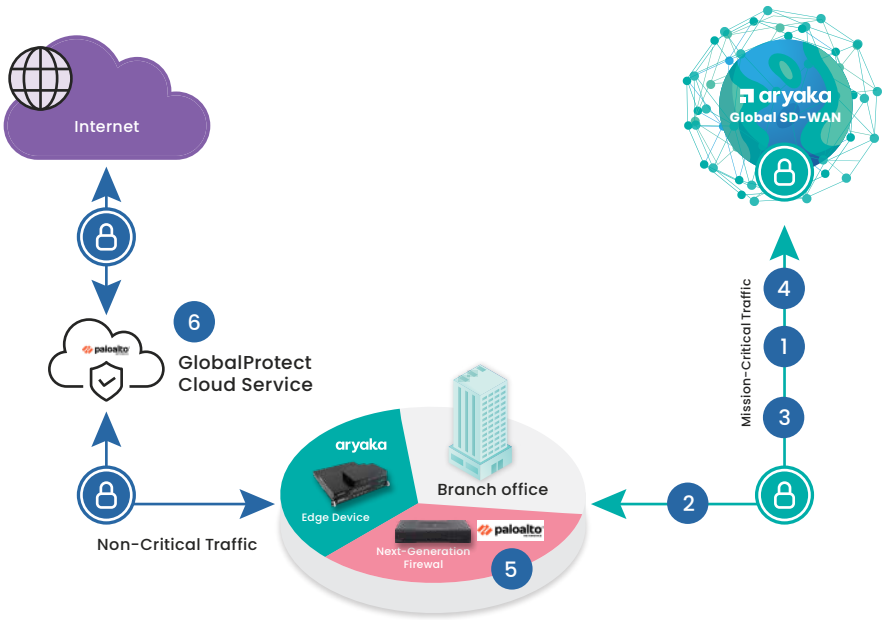
Palo Alto Networks + Aryaka

Palo Alto Networks and Aryaka seamlessly integrate to deliver a joint solution of enterprise-grade security with a cloud-native Global SD-WAN that has private connectivity, WAN Optimization, and application acceleration capabilities.

Aryaka's SmartCONNECT delivers SLA-based reliable global connectivity and significantly faster application perfor-mance for enterprises, and Palo Alto adds a layer of advanced security controls needed for web and cloud-bound traffic.

The Aryaka Edge device (ANAP) can seamlessly forward all Internet- and cloud-bound traffic directly to the Palo Alto GlobalProtect™ cloud service or the Palo-Alto next-generation on-premises firewall.

Together, Aryaka and Palo Alto, deliver a best-of-breed SD-WAN and security platform for enterprises accessing mis-sion-critical internally hosted applications as well as those going directly to the Internet for accessing cloud applications.



Aryaka and Palo Alto Networks provide a multi-layer security solution for your global enterprise WAN.

Aryaka and Palo Alto Networks Seven Layers of Global Enterprise Security

1. Global Private Network
2. Multi-Path Encryption
3. Advanced DDoS Mitigation
4. Aryaka Virtual Firewall
5. Palo Alto Networks Next-Generation Firewall
6. Palo Alto GlobalProtect Cloud Services
7. Palo Alto Virtualized Firewall for the cloud

Use case #1

Secure branch office: Aryaka Global SD-WAN and Palo Alto next-generation firewall

Challenge: Enable direct and secure hand-off of Internet traffic from the branch.

Solution: Using advanced routing policies, the Aryaka Edge Device (ANAP) automatically forwards all public Internet traffic to a co-located Palo Alto Networks Next-Generation Firewall appliance.

Benefits: By eliminating the backhaul of public Internet traffic, direct hand-off conserves WAN bandwidth and expense, and improves application performance and SLAs to deliver a superior edge-to-edge user experience. The Aryaka Edge Device includes built-in capabilities of a router, dynamic path control and WAN optimization in a single integrated solution. Co-location of the physical firewall at the branch enables secure hosting of services from the branch firewall.

Use case #2

Security for the distributed enterprise: Aryaka Global SD-WAN and Palo Alto GlobalProtect™ cloud service

Challenge: Enterprises are increasingly leveraging direct Internet breakouts at remote locations to provide optimal and scalable connectivity for the purposes of guest Wi-Fi or SaaS applications. This approach provides the best overall user experience, but it also creates challenges when securing an increased number of Internet access points and maintaining compliance with the organization's security policies.

Solution: The Aryaka Edge device seamlessly forwards all Internet and cloud bound traffic directly to the Palo Alto GlobalProtect™ cloud service.

Aryaka uses a Global Private Network with built-in optimization and security capabilities that include a multi-layer security approach with a global private core network, fortified security on the POPs, end-to-end encrypted tunnels, and stateful firewalls.

Palo Alto's security platform has highly differentiated cyberthreat prevention capabilities.

Together, this ensures that all enterprise, web and cloud traffic obtain enterprise-grade security, irrespective of whether they are going to the Aryaka global SD-WAN or to the public Internet.

Benefits: The combined solution does not require additional on-premises hardware, appliances or software and is easy and cost-effective to deploy and manage.

Use case #3

Accelerated access to IaaS solutions: Aryaka Global SD-WAN and Palo Alto VM-Series

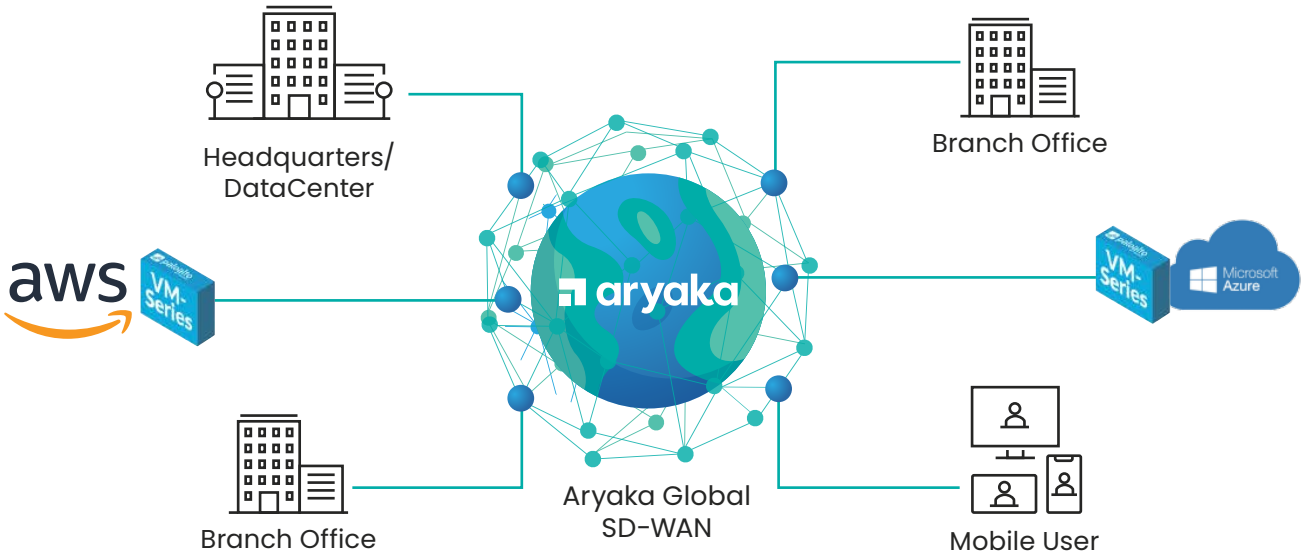
Challenge: Organizations are moving data center workloads to IaaS providers like Amazon Web Services and Micro-soft Azure. To access these IaaS instances from branch offices, customers need to configure as many tunnels as IaaS instances for every branch office, which is operationally complex. Such a topology also leads to challenges of security and performance.

Solution: With Aryaka SmartCONNECT, branch offices obtain secure and accelerated connectivity to any IaaS. Aryaka SmartCONNECT provides direct connectivity to AWS or Azure instances, via either a private connection or IPsec tunnel. This configuration ensures that only one tunnel needs to be created for one branch to the Aryaka SmartCONNECT service unlike the earlier case of one tunnel for every IaaS instance.

Palo-Alto VM-Series is a virtualized form factor of a next-generation firewall that can be deployed in an IaaS environ-ment such as AWS or Azure.

Connecting to an IaaS through Aryaka SmartCONNECT guarantees high performance access. Once the connec-tivity to the IaaS instance is established, Palo Alto Networks VM-Series can be deployed on-demand for inserting firewall services.

Benefits: Enterprises connecting to IaaS thus obtain accelerated and optimized connectivity along with the same level of security and performance as workloads in the customer data center, without the use of any additional equipment or resources.



Aryaka's Global SD-WAN accelerates access to IaaS solutions hosting Palo Alto Networks VM-Series firewall anywhere in the world.

About Aryaka Networks

Aryaka offers the only viable SD-WAN solution for global enterprises. Aryaka's global SD-WAN delivers significantly better performance for cloud and on-premises applications — voice, video and data — for enterprise data centers, branch offices and remote/mobile employees anywhere in the world.

Unlike legacy connectivity solutions that take months to deploy, Aryaka's Global SD-WAN can be deployed within days. It is delivered as a service, so IT organizations can consume global networking services the way they would consume SaaS applications like Salesforce and Infrastructure-as-a-Service solutions like Amazon Web Services and Azure. With more than 800 global enterprise customers, Aryaka is also the largest independent global SD-WAN provider by market share.

To learn more, visit www.aryaka.com.

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling ap-plications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets.

Find out more at www.paloaltonetworks.com.

aryaka | paloalto NETWORKS

+1.888.692.7925

info@aryaka.com

Aryaka, the Cloud-First WAN and SASE company, and a Gartner "Voice of the Customer" leader, makes it easy for enterprises to consume network and network security solutions delivered as-a-service for a variety of modern deployments. Aryaka uniquely combines innovative SD-WAN and security technology with a global network and a managed service approach to offer the industry's best customer and application experience. The company's customers include hundreds of global enterprises including several in the Fortune 100.

About Aryaka