

Aryaka HybridWAN

Technical Overview

Overview

Aryaka's HybridWAN capability allows customers to deliver optimal business-critical application performance while reducing overall connectivity costs by leveraging public internet connectivity for non-critical applications. HybridWAN delivers on this optimal balance in an easy-to-deploy manner as a built-in capability using Aryaka's ANAP (Aryaka Network Access Point).

Furthermore, Aryaka's HybridWAN offers built-in MPLS support in the ANAP in order to smoothly bridge between traditional MPLS-based WAN deployments and Aryaka's innovative SD-WAN approach – or allow both to easily co-exist in order to allow for a no-risk migration strategy.

HybridWAN leverages single or redundant internet links to provide simultaneous connectivity to the high-performance global Aryaka private backbone, the public internet as well as existing MPLS connections. This allows customers to get MPLS-like deterministic performance over the Aryaka core, while also benefiting from using internet connectivity directly for non-business-critical applications. Furthermore, existing MPLS connectivity can be leveraged wherever it best serves an enterprise's network strategy.

The Aryaka Private Core, MPLS, and the internet are referred to as VPN Path-Aryaka, MPLS Path and VPN Path-Internet respectively in this document, as well as in the MyAryaka customer portal, now part of SmartInsights.

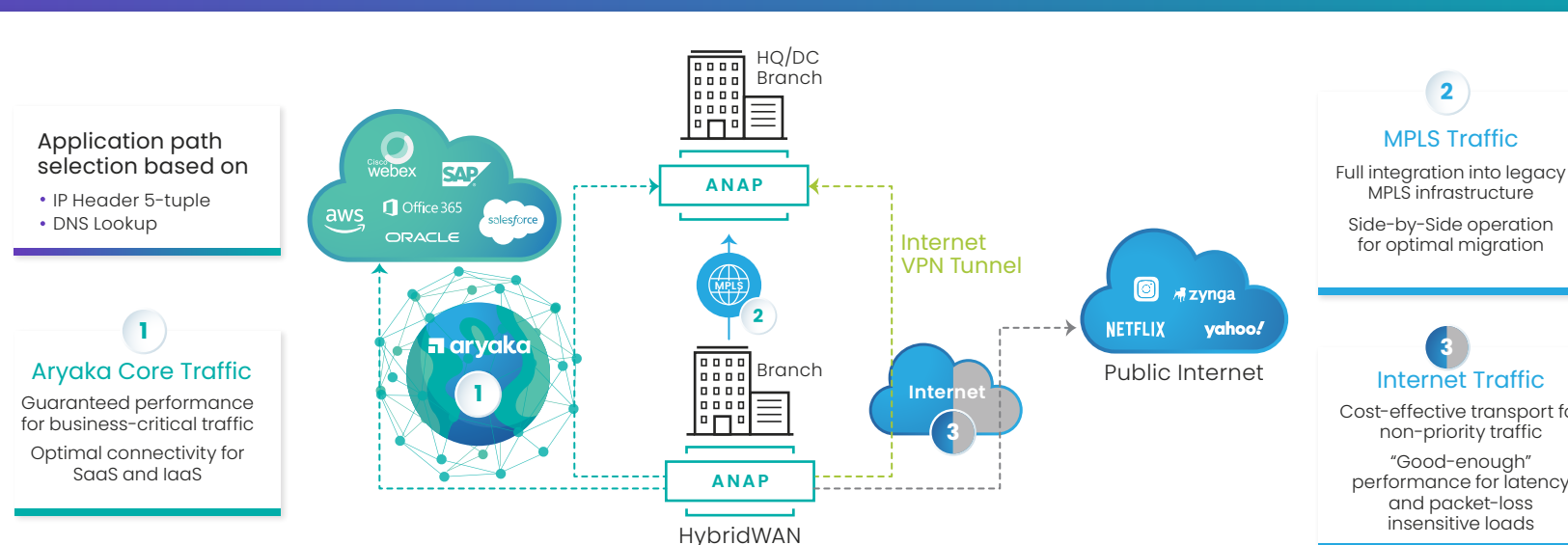
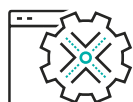


Figure 1: Aryaka HybridWAN Overview: Built-in support for transport paths over the Aryaka Private Core, MPLS, and the internet

1. Use Cases



Application-Aware Traffic Routing

In general, most enterprises will choose to route business-critical traffic over the VPN Path-Aryaka, while non-critical traffic is sent over the VPN Path-Internet between customer sites. Enterprises can also pick which applications should use the MPLS Path. Network architects can take advantage of different paths to suit their applications' needs in any manner they prefer.



Simplify and consolidate WAN connectivity for regional VPN solutions

Aryaka's HybridWAN can also be used by customers to simplify and consolidate an existing regional MPLS and/or IPsec VPN solution. This can apply wherever the branches and DCs are near each other, and internet performance can meet application performance needs.



MPLS Migration

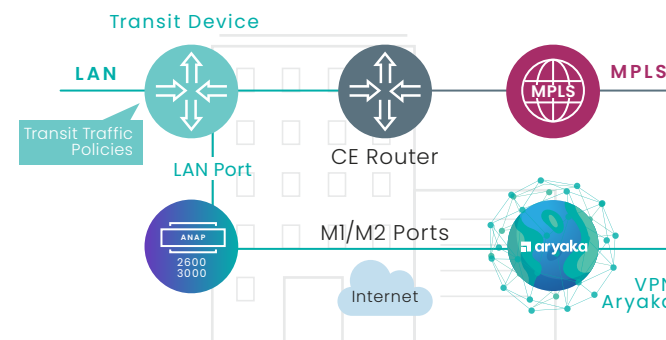
Aryaka's ability to support simultaneous connectivity to the high-performance Aryaka Private Core, MPLS, and the internet allows enterprise to evaluate the performance of these connectivity options as well as establish an optimal migration plan based on their very own enterprise architecture needs.

Unlike other SD-WAN vendors, Aryaka does not perpetuate the dependency on MPLS to provide always-on, 100% deterministic performance and five 9s SLA availability. The VPN-Aryaka Path offers a real alternative that provides MPLS-like performance and reliability levels. That means that enterprises do not have to incur any risk as they plan their migration strategy from MPLS. A key benefit of the Aryaka HybridWAN solution is that it always guarantees adoption success when it comes to WAN transformation.

2. Branch Deployment Models

ANAP Connects to Transit Device

In this model, a branch router acting as transit device decides which path traffic headed from the Branch LAN to the WAN should take. This means the transit device decides which traffic is routed to the CE Router or to the Aryaka ANAP CPE. The ANAP peers with the transit device via eBGP over the LAN port. This deployment model allows for easy addition of the Aryaka solution to the existing branch architecture.

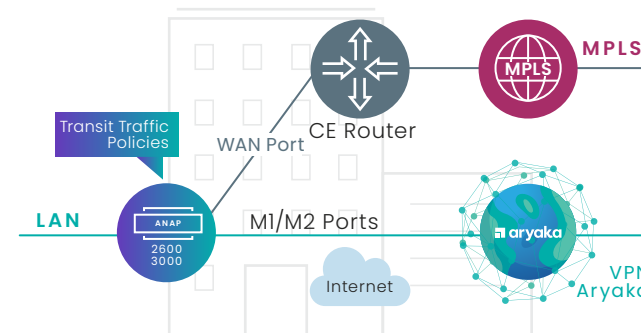


MPLS Co-Existence Model

ANAP connects to Transit Device: Traffic routing policies on Transit Device

ANAP Acts as Transit Device

In this model, the ANAP acts as a transit device and implements all the routing policies. It connects to the Branch LAN via the ANAP LAN port. Based on routing policies, the ANAP directs traffic to the MPLS CE Router or to the different paths supported over the M1/M2 ports on the ANAP. Note that the ANAP peers with the MPLS CE Router via eBGP over the WAN port to exchange routing prefixes for the MPLS domain. This deployment model simplifies the branch architecture by eliminating the need for a legacy router.

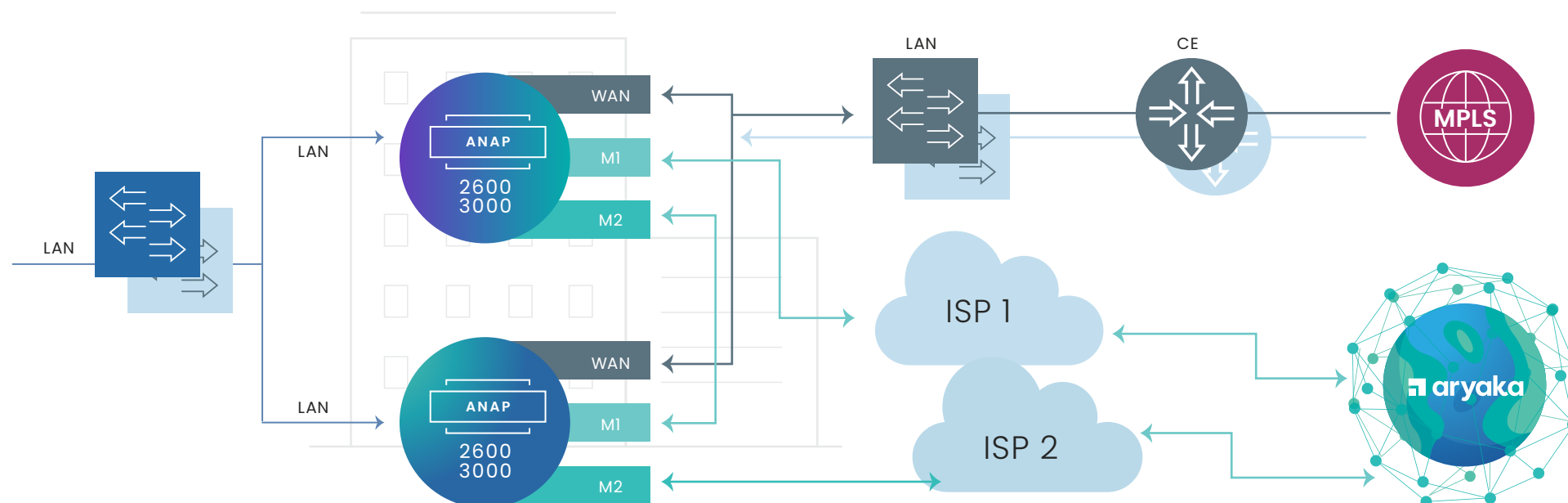


ANAP with Direct MPLS

ANAP acts as Transit Device: Traffic routing policies on ANAP

Redundancy Options

The Aryaka solution supports several redundancy options that best suit any particular site's needs, ranging from simple redundancy to high availability options, as the diagram shows at a high level. ANAP redundancy options are further explained in the ANAP Data Sheet.



3. Aryaka HybridWAN Path Overview

Aryaka's HybridWAN solution supports 4 types of paths out of the branch to which traffic may be assigned based on Traffic Match Rules that are defined in the MyAryaka configuration portal:



VPN Path-Aryaka

This is the fully optimized path and leverages all Aryaka features to deliver business critical applications globally. The VPN Path-Aryaka is always configured to support at least a minimal amount of control. The VPN Path-Aryaka includes all of Aryaka WAN optimization features including TCP optimization, data de-duplication application proxies, private core network connectivity with guaranteed SLAs, Hierarchical QoS, high availability capabilities for packet error recovery, dynamic path selection and others. The VPN Path-Aryaka is supported as an encrypted VPN connection over the M1/M2 ports on the ANAP CPE that connects to the nearest Aryaka Services PoP.



VPN Path-Internet

This is an optional path between two ANAPs deployed at customer locations directly connected over the internet using redundant IPsec tunnels. This path also benefits from Aryaka's traffic optimization features, although some of the optimization features available on the VPN Path-Aryaka are not effective without the direct handshake with an Aryaka Services PoP. The VPN Path-Internet is a separate encrypted VPN connection over the ANAP's M1/M2 ports that connect to a remote ANAP site over typically redundant internet paths.



MPLS Path

Aryaka's ANAP supports direct connectivity to the MPLS CE (Customer Edge) router via the WAN port. Typically, the ANAP device and MPLS CE router will establish BGP peering to exchange routes. Traffic Match rules can be configured for MPLS path selection.



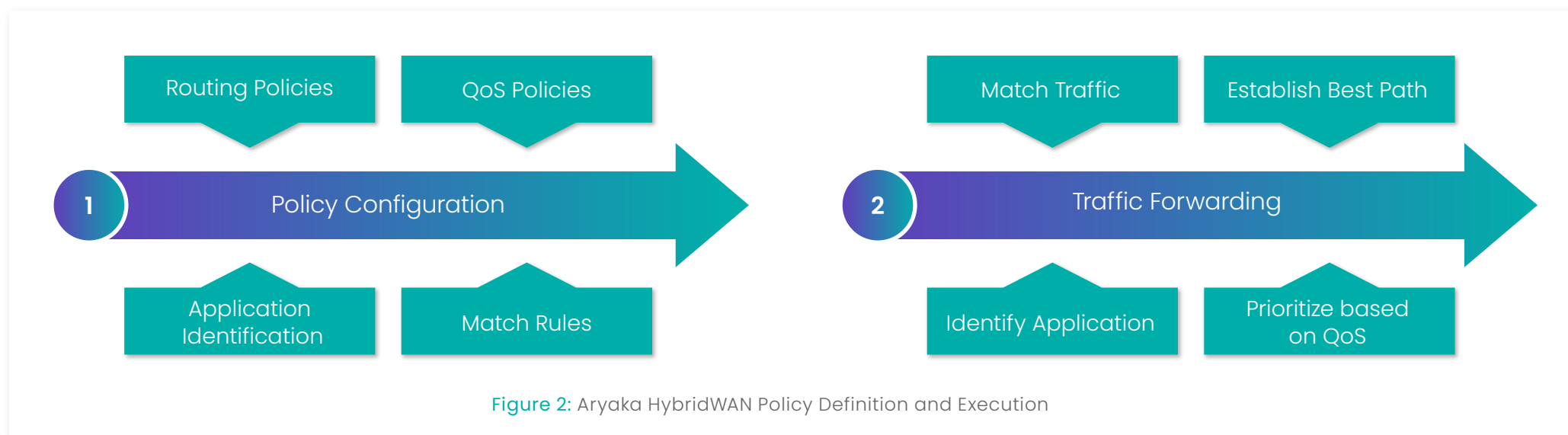
Public Internet

Enterprises can also route certain traffic (typically consumer grade applications like YouTube, Facebook, etc.) directly to the public internet. Some SaaS vendors recommend this path to be used to access their services, even though this may not always be an optimal solution in all geographies and for all end users and the Aryaka SmartConnect and SmartCloud services may deliver superior performance. This path is also supported via the M1/M2 ports and should be protected by a state of art security solution and advanced security postures.

4. Aryaka HybridWAN Policy Definition and Execution

In this section, we will explore the intuitive and intent-based approach to the configuration of forwarding rules that govern application-based routing and path selection in the Aryaka Cloud-First WAN solution.

Unlike other SD-WAN solutions that claim simplicity, and then require users to define extremely complex sets of multi-tiered, syntactically complex policies, the Aryaka architectural model is intent-based and streamlines it in two simple tiers of policies that can be global or local.



Aryaka HybridWAN Policy Definition and Execution

In general, business-critical traffic gets routed over Aryaka or MPLS, while non-critical traffic can be routed over the internet directly in an active-active manner using typically redundant ISP connectivity. Moreover, real time collaboration applications will also typically benefit from the high performance Aryaka core, or -in the case of on-premise UC (Unified Communications) deployment - may also be routed over the established MPLS path. The rules that govern these fundamental application identification, routing and QoS decisions are defined as abstracted global and local policy rules in the MyAryaka configuration portal and can be tailored to fit any enterprises' design choices.

Match Rules

Match rules are defined with the 5-tuple match, DNS match (typically identifying XaaS applications) or other ways to identify specific traffic policies governing flows. Match rules can be applied globally or locally.

Once a match rule identifies a relevant traffic type, additional policy sets are applied to handle traffic, specifically **Application Identification**, **Routing policies** and **QoS policies**.

These policies will establish the optimal transport path (out of the 4 previously discussed possible traffic paths) as well as the QoS priority within the path traffic flows. In the abstracted Aryaka system to overcome network complexity, that means internet policies and QoS policies.

NAME	CONFIG STATUS	SRC IP	SRC PORT	DEST IP	DEST PORT	PROTOCOL	TOS
ICMP TEST	CONFIGURED	172.17.6.30/32	Any	61.12.65.22/32	Any	Any	Any
SHHS_Test_Rule	CONFIGURED	Any	Any	1.0.0.1/32	Any	Any	Any
VPN1_Traffic_Pilot	CONFIGURED	(1)	Any	(2)	Any	Any	Any
VDIP-ANAP-SEC-ISP-ROUTING	CONFIGURED	172.17.21.9	Any	59.145.150.131	Any	Any	Any
Aryaka VDI	CONFIGURED	172.17.21.9	Any	59.145.150.131	Any	Any	Any
Switching to Reliance	CONFIGURED	172.17.21.9/32	Any	59.145.150.131/32	Any	Any	Any
SMB Server	CONFIGURED	Any	Any	172.16.56.37	Any	Any	Any
svcd-BL1-metragic	CONFIGURED	(2)	Any	(2)	Any	Any	Any
SMB test	CONFIGURED	172.16.56.37	Any	Any	Any	Any	Any
svcd-metragic-BL1	CONFIGURED	(2)	Any	(2)	Any	Any	Any
lat	CONFIGURED	Any	Any	199.50.224.4/32	Any	Any	Any
ILAT_test_machines	CONFIGURED	172.16.54.2	Any	172.16.15.205	Any	Any	Any
MBFL-Traffic-Redirection-for-Pilot	CONFIGURED	(2)	Any	172.16.1.36	Any	Any	Any
Forwarding Rule: To AWS	CONFIGURED	Any	Any	18.216.159.95/32	Any	Any	Any

Application Identification

Every enterprise may have different needs when it comes to handling the traffic for specific applications, which is why identifying applications via a variety of technologies is important. As seen to the right in the MyAryaka configuration screen for Monitored Applications, the Aryaka solution can accurately identify many enterprise- and consumer-grade applications, allowing routing and QoS policies to be applied with granularity.

APPLICATION NAME	PROTOCOL	TYPE	PORT	IP
HubSpot	TCP	Port	10019	
IBM	TCP	Port	10032	
IMAP	TCP	Port	143	
IMAPS	TCP	Port	993	
Jelastic	TCP	Port	10048	
Kamatera	TCP	Port	10051	
Konnect	TCP	Port	10056	
Logzio	TCP	Port	10071	
Marketo	TCP	Port	10013	
MATLAB	TCP	Port	10023	
MicroStrategy	TCP	Port	10055	
MIS Remote Desktop	TCP	Port	3389	
MSSQL	TCP	Port	1433	
MuleSoft Anypoint Platform	TCP	Port	10067	
NetScout	TCP	Port	10065	

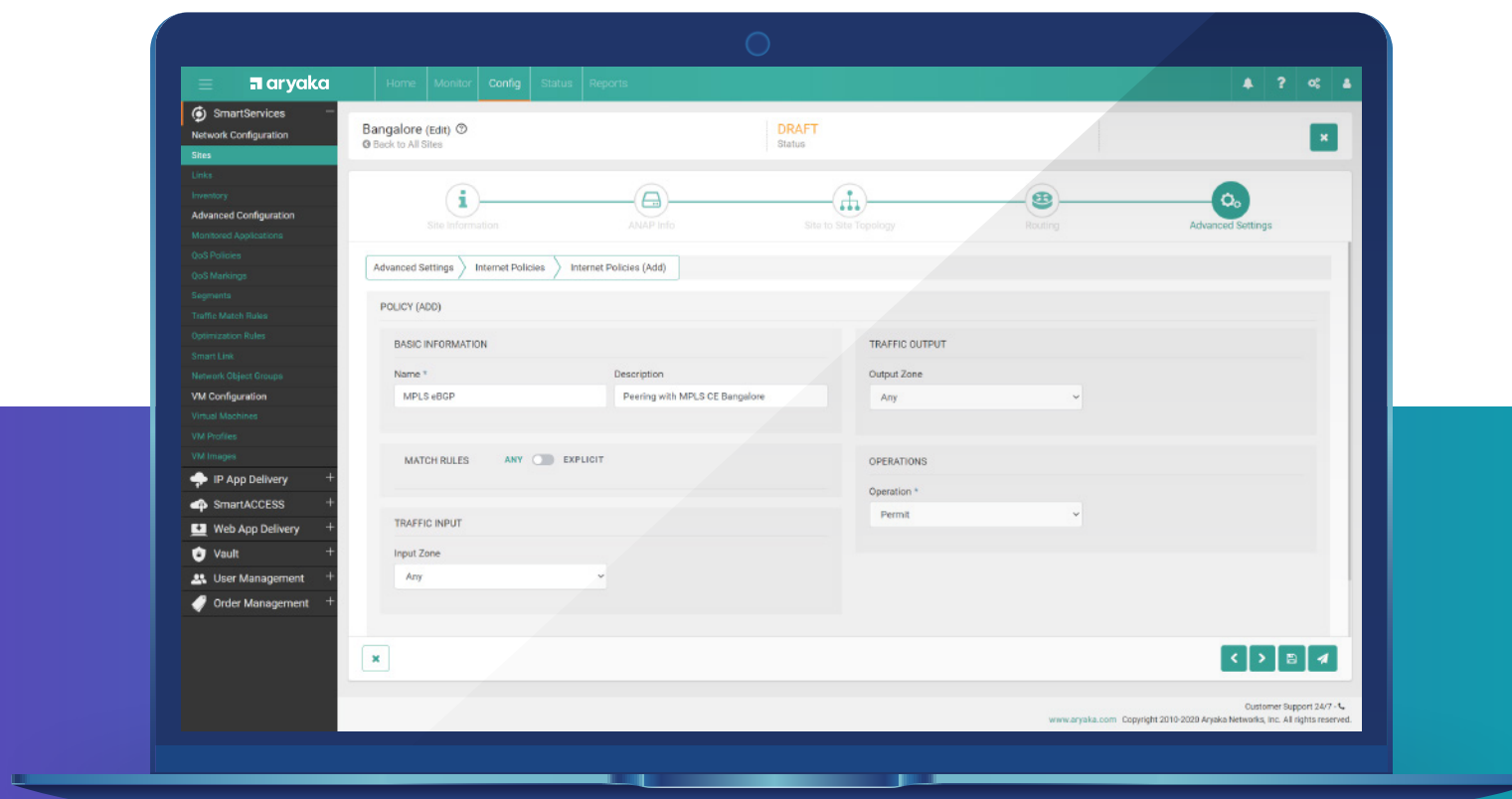
Routing Policies and Path Selection

Internet policies map the routing match rule to the optimal path, which is picked based on dynamic SLA measurements from available routing options.

Aryaka supports both dynamic and static routing.

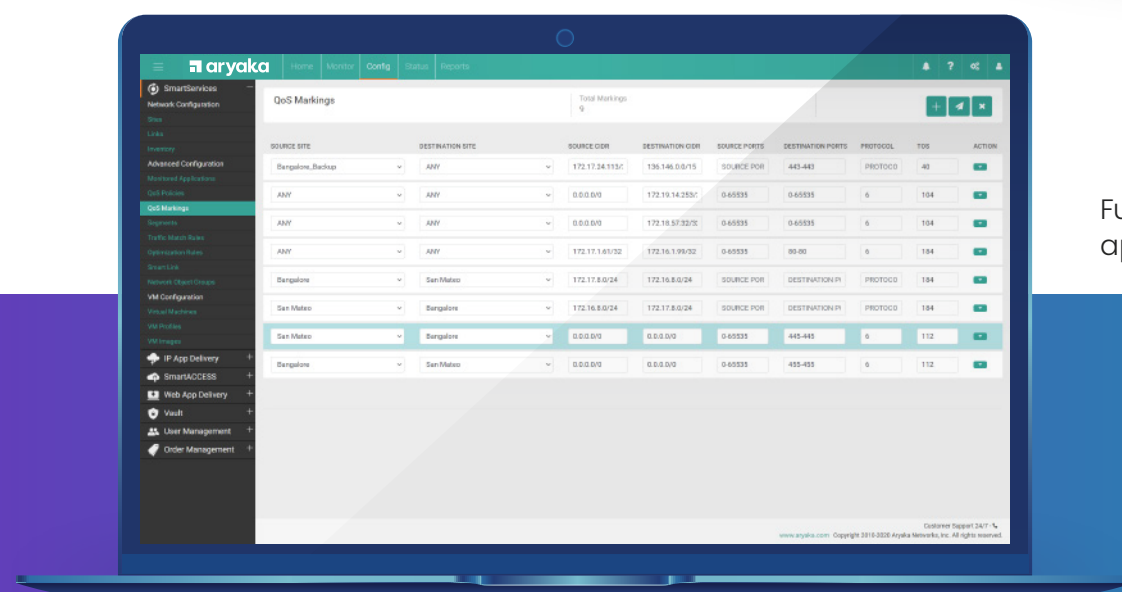
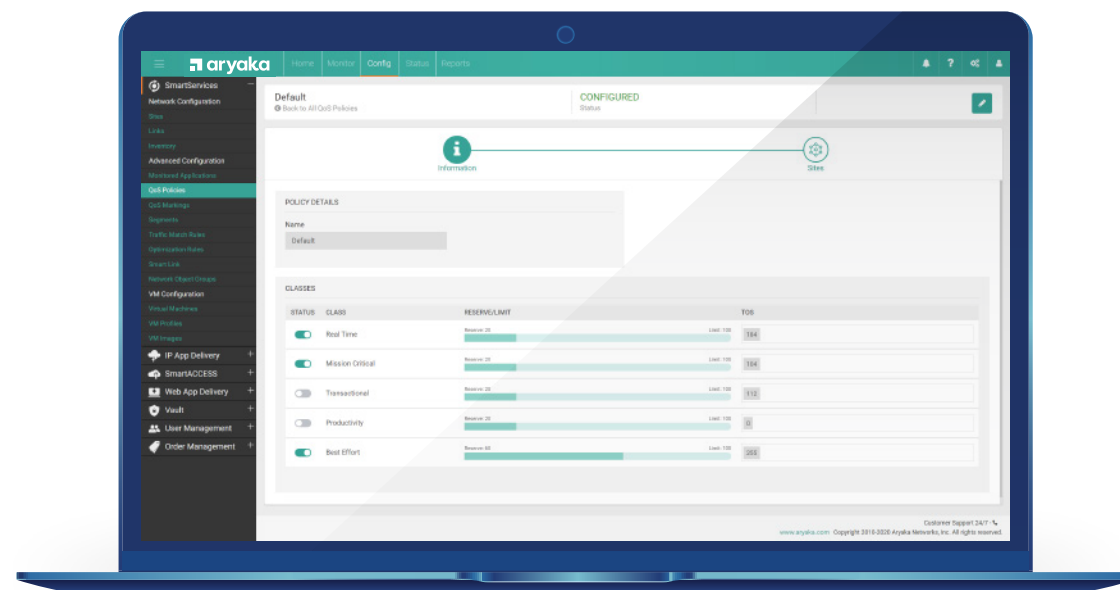
Dynamic routing paths are established via route exchanges with routing protocols between peering Aryaka devices or third-party devices, including MPLS CE (customer edge) routers.

Static Routes are entered manually to customize routing paths. Whenever there are dual route matches, the static route will be prioritized.



QoS Policies

QoS policies govern traffic priorities within the optimal path that match rules are linked to. Based on the ToS (Type of Service)/DSCP (Differentiated Services Code Point) assigned to a flow, QoS will dynamically schedule traffic over the assigned path with the appropriate behavior to deliver on latency, jitter and packet loss guarantees assigned to the different traffic classes.

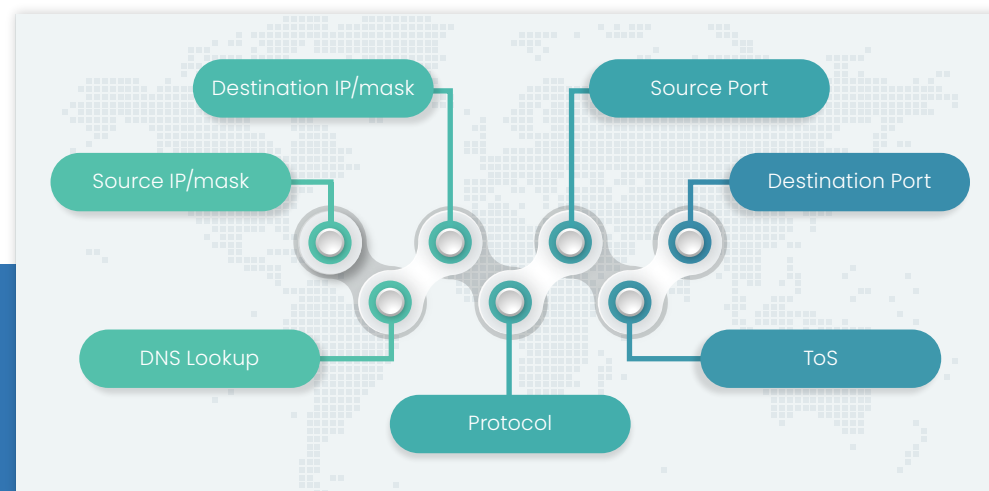


Furthermore, QoS marking policies establish which QoS class applications and traffic matches are assigned to.

5. Traffic Forwarding

Application-Aware Traffic Forwarding

Application traffic is routed over available paths based on the configured policies discussed previously. Path selection is based on the following selectors:



The default policy is that all traffic uses the VPN Path-Aryaka, while the VPN Path-Internet acts as a backup. However, customers can easily customize their path selection policies.




Some common configuration examples for custom application routing policies include:

- Send all data replication traffic between a pair of servers over VPN Path-Internet.
- Optimize a regional IPsec VPN solution by applying routing policies between sites such that VPN Path-Internet always has higher preference than VPN Path-Aryaka.
- Route all latency/jitter critical voice/video traffic over VPN Path-Aryaka, while sending all other traffic to VPN Path-Internet.
- Send legacy client-server application traffic over the MPLS path.

Note that the policies are of course completely configurable to match any enterprise's existing architectural needs.

SLA-based Path Monitoring

Aryaka also monitors the health of the VPN Paths as described below.

 VPN Path-Aryaka	 VPN Path-Internet	 MPLS Path
<p>This path supports redundant IPSec tunnels setup over dual internet links to connect to the closest Aryaka Service PoP. These tunnels are monitored using pings for loss and latency. Configured thresholds on loss and latency control the availability of the path based on the quality of the path. This is over and above the regular Dead Peer Detection control that establishes the availability of the path.</p> <p>Furthermore, redundancy features dynamic path selection based on application specific policies.</p>	<p>Aryaka supports redundant IPSec tunnels set up over dual internet links directly over the internet. These tunnels are monitored using custom pings to constantly measure loss and latency.</p>	<p>The ANAP and the MPLS CE Router establish MPLS path availability as well as route exchange via eBGP peering.</p>

Adaptive QoS

Adaptive QoS helps customers assign available internet WAN bandwidth when the ANAP is deployed as a branch edge device. This ANAP deployment mode is referred to as Edge Routed Mode (ERM), as is the case when the ANAP controls WAN routing and forwarding policies. This feature prioritizes traffic sent VPN Path-Aryaka over VPN. While it is the default operational mode when the Aryaka ANAP acts as the transit device, behavior can be easily tailored to individual enterprises' operational needs, and QoS policies can be tailored for the different forwarding paths.

At a high level, the different paths are prioritized as follows:

- VPN Path-Aryaka: This traffic is always prioritized but shaped to the subscribed bandwidth. It can also support bursting. This is given the highest priority over the M1/M2 ports and is guaranteed to be always available.
- VPN Path-Internet: Traffic sent to this path is prioritized after VPN Path-Aryaka, but ahead of Internet Access traffic over the M1/M2 ports.
- Internet Access: Recreational internet traffic like YouTube, Facebook etc. This traffic is assigned the lowest priority over the M1/M2 ports.
- MPLS path: Aryaka's ANAP immediately forwards MPLS Path traffic to the MPLS CE router, which in turn implements forwarding priority rules over MPLS based on FEC (Forwarding Equivalence Class) considerations. This traffic is not subject to the Adaptive QoS rules explained below.

Adaptive QoS Over ANAP M1/M2 WAN Ports

The following figure shows the conceptual approach of Aryaka's Adaptive QoS over the M1 and M2 ports as it prioritizes bandwidth allocation and the traffic mix changes during a series of timeframes that range from T1 to T4:

T1

Adaptive QoS guarantees that VPN Path-Aryaka bound traffic always gets its assigned subscribed and burst bandwidth, thereby always delivering on the needs of business-critical traffic. This is a key core architectural principle of the Aryaka solution: business critical traffic always takes the VPN Path-Aryaka and is always guaranteed an industry-leading SLA.

T2

At this point in time, the prioritized traffic over VPN Path-Aryaka starts to ramp down. VPN Path-Internet and Internet Access are now allowed to grow elastically as VPN Path-Aryaka is not claiming its guaranteed traffic allocation. Note that VPN Path-Aryaka could claim back its subscribed and burst bandwidth anytime.

T3

At this point in time, VPN Path-Internet and Internet Access traffic start to compete for resources. Whenever that happens, VPN Path-Internet traffic always gets higher priority over Internet Access traffic: if VPN Path-Aryaka is not utilizing its assigned bandwidth, VPN Path-Internet gets preference as it grows, and Internet Access traffic is only allowed to scavenge the rest of the bandwidth not claimed by VPN Path-Aryaka (first priority) and VPN Path-Internet (second priority).

T3

Finally, T4 illustrates how some bandwidth -called the "Guard Band"- is always reserved for VPN Path-Aryaka bound traffic to guarantee fast ramp-up and optimally support the initial burst of VPN Path-Aryaka flows. This allows VPN Path-Aryaka to always immediately ramp up to its guaranteed allocation. VPN Path-Aryaka never competes for resources against lower priority traffic - the resources are always guaranteed. The Guard Band delivers superior user experience independent of traffic loads. It should also be noted that AdaptiveQoS also reserves a portion of the internet bandwidth. This configurable internet bandwidth is required for Aryaka service management as well as to access other internet-based services.

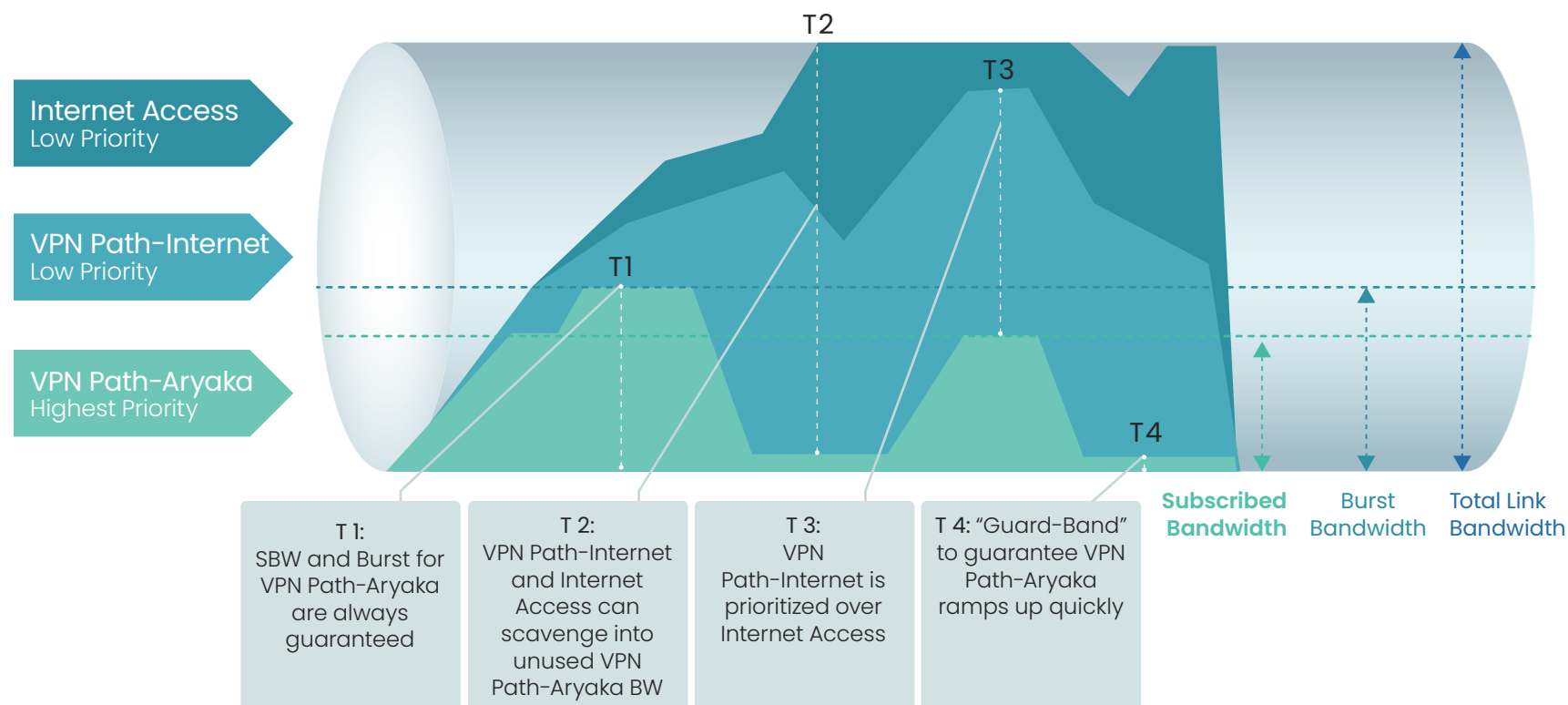


Figure 3: Conceptual traffic prioritization model on internet link

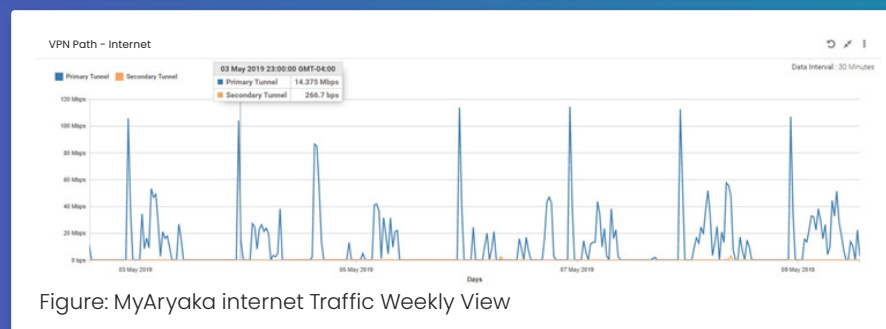
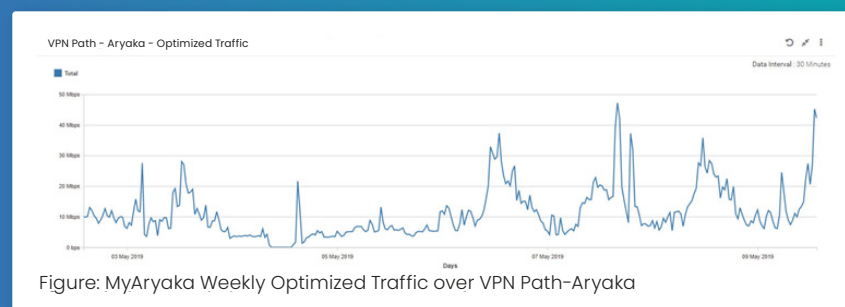
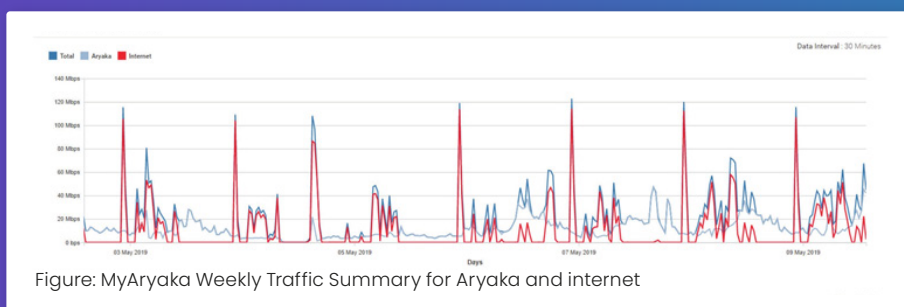
6. SmartInsights: MyAryaka Visibility

The MyAryaka customer web portal offers end-to-end, real-time network visibility and application performance metrics and is an integral part of Aryaka's fully-managed service. Network managers can get a real-time view of network health through the dashboard, and can address performance issues proactively before user experience is impacted.

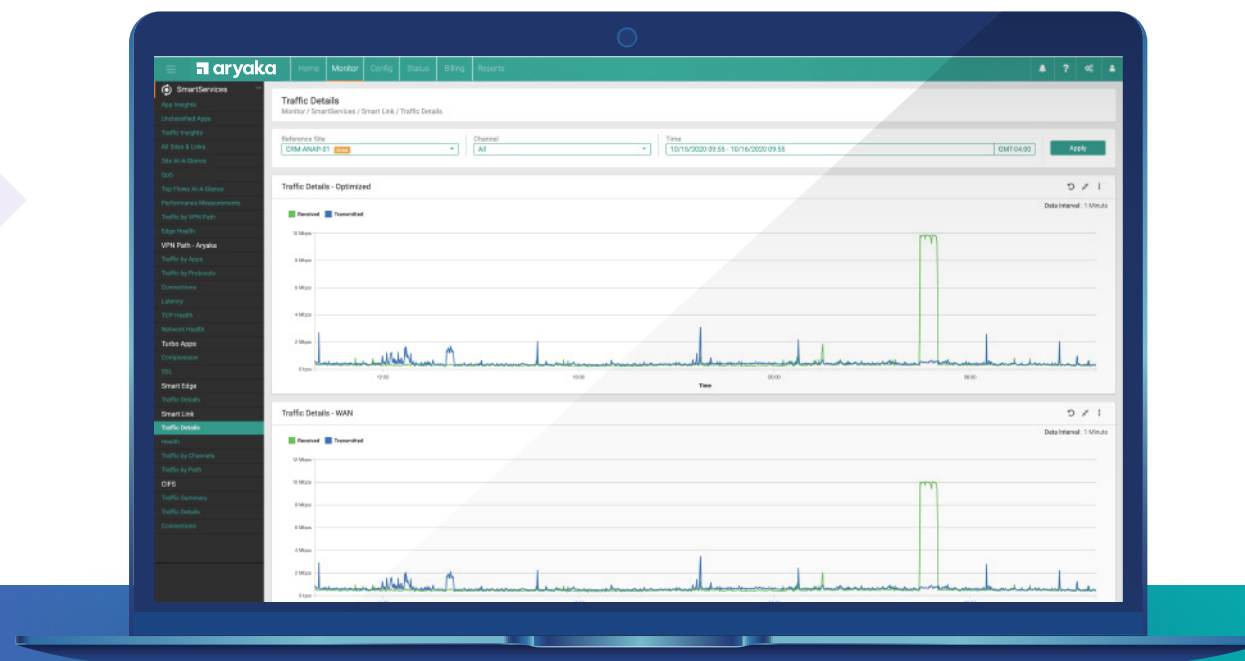
MyAryaka provides complete visibility into HybridWAN operation. It presents HybridWAN operational views allowing customers to check the status of links, check the amount of traffic being traversed via the respective paths and easily establish path integrity.

Traffic via VPN Paths

Traffic across the VPN paths will show throughput usage on VPN Path-Aryaka and VPN Path-Internet. The VPN Path-Aryaka views do not include IPSec overhead or traffic that could have been dropped by QoS. On the other hand, VPN Path-Internet stats include IPSec overhead as well as traffic dropped by the path.



MPLS Path traffic levels are also shown:



Traffic via VPN Paths

Traffic across the VPN paths will show throughput usage on VPN Path-Aryaka and VPN Path-Internet. The VPN Path-Aryaka views do not include IPsec overhead or traffic that could have been dropped by QoS. On the other hand, VPN Path-Internet stats include IPsec overhead as well as traffic dropped by the path.

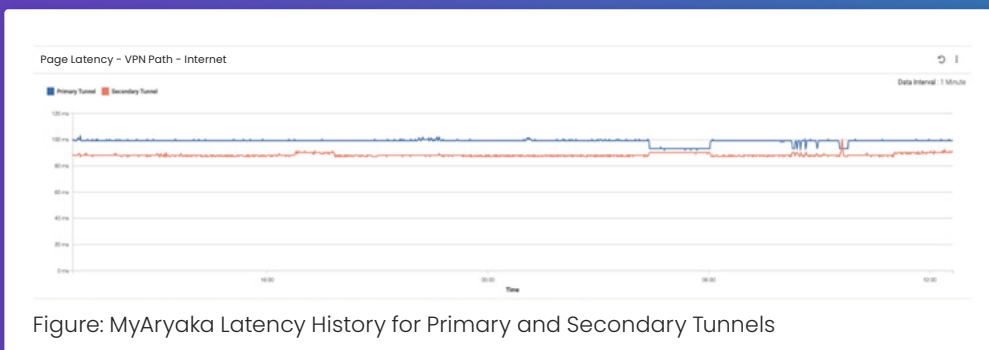
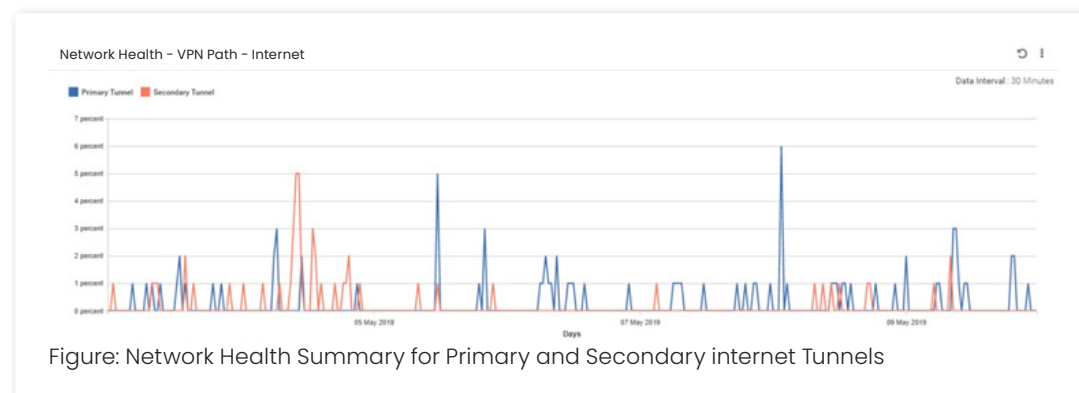


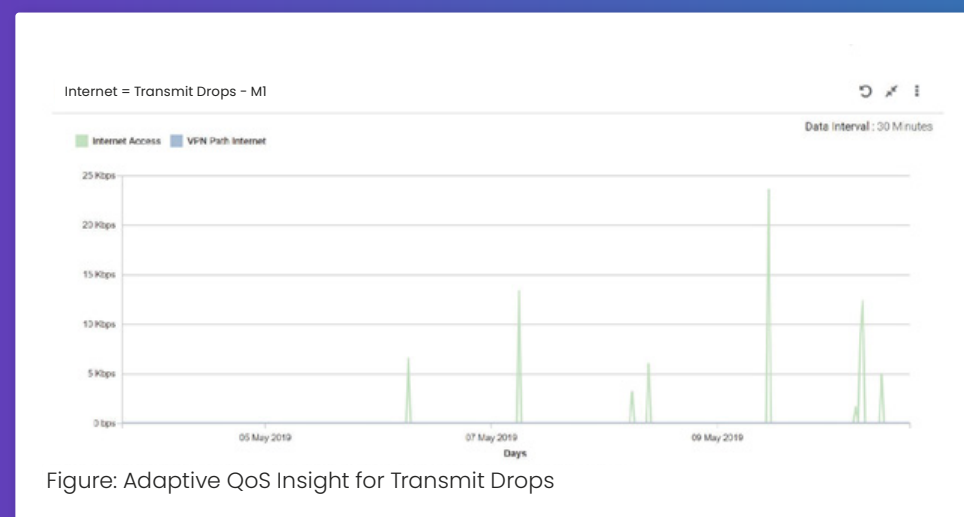
Figure: MyAryaka Latency History for Primary and Secondary Tunnels

Adaptive QoS

Customers can quickly gain insights into overall network health for all traffic paths.



The Adaptive QoS MyAryaka views also provide customers with insights into internet transmit and receive drops via available interfaces (MI shown in next figure) over any timeframe chosen by a customer.



Link Status

MyAryaka immediately detects and advertises changes in link status, both for the VPN Path-Aryaka as well as VPN Path-Internet.

Customers logging into the MyAryaka Portal > Status > Links will immediately see if the VPN Path-Aryaka and VPN Path-Internet paths or MPLS Paths are up or down or N/A. N/A indicates that the VPN Path-Internet is not applicable for the site .

Link Status			Search	Show 10	Entries
Remote Site	Aryaka	Internet			
AWS Ashburn	Up	N/A			
AWS_ASH1_Oracle	Up	N/A			
AWS_ASH1_Oracle(Backup)	Up	N/A			
AWS_ASH1_Oracle_Public	Up	N/A			
AWS_ASH1_Oracle(Public)_Backup	Up	N/A			
Azure WAN West Coast	Up	N/A			
Bangalore	Up	N/A			
Bangalore_Backup	Up	N/A			
Beijing Office	Up	N/A			

About Aryaka

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com



Schedule a Free Network
Consultation with an Aryaka Expert

[See How It Works Live →](#)



Experience Aryaka's
Unified SASE as a Service

[View Interactive Tour →](#)



3945 Freedom Circle, Suite 1100 Santa Clara, CA 95054

Follow us on :

