Today's Networking Security Challenges

Tailoring a managed SASE architecture for your enterprise's requirements

Authors : Paul Liesenberg | Hugo Vliegen

Whitepaper | 2021

aryaka

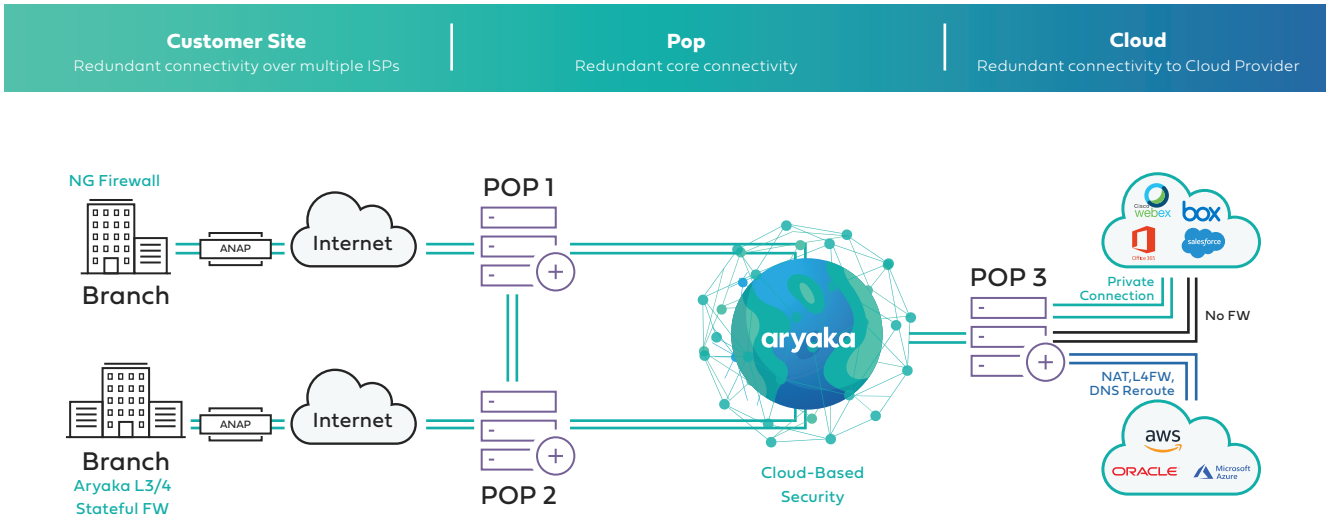
Network Security Update

There is universal consensus around the fact that network security is undergoing dramatic transformation. New security concepts such as SASE (Secure Access Service Edge) and ZTA (Zero Trust Access) promise to deliver on the architectural changes required to address the security requirements of the digital enterprise.

But the simple truth is that no single vendor in the market -despite their own claims to the contrary- addresses all capabilities required to deliver on those desired security target architectures. Nor will any single vendor be able to provide class-leading solutions in every required functional area in security.

Enterprise security has never been and will never be a technology area where any monolithic, universal solution can cover every enterprise's need. Different enterprises will always have specific security needs that need to be tailored to regulatory, compliance and overall enterprise architecture needs.

In this paper, we'll examine the emerging challenges in network security and how Aryaka's open, partner-led, and best-of-breed approach allows enterprises to optimally tailor their security architecture to their needs.



Network Security History and Trends

The history of network security has largely seen network security vendors introducing new, function-specific and increasingly complex security solution elements to implement a largely passive security posture: network security moved from first-generation stateless firewalls to stateful firewalls, then to next-generation firewalls that added increasing levels of application- and web-awareness. We shall explore all these existing as well as emerging security elements in the following chapter.

The key in understanding network security lies in also understanding the evolution of enterprise architecture over the last 20 years. Initially, as the internet started to transform enterprises world-wide, a medieval castle approach to security was enough. The traditional enterprise network simply had to protect centralized enterprise assets that all were on-premise, such as servers, on-premise apps and data as well as users and their endpoints. And even as cloud-adoption started to take off, for a long time the enterprise network security posture held on to the centralized model: traffic from remote offices and remote users was backhauled in its entirety to HQ or the main DC (see Figure 1), to then be broken out into the Internet if necessary. While this provided a convenient centralized model to security decisions, this model was not enough to combat ever more elaborate threats and furthermore started to incur severe performance problems as cloud resource usage (SaaS, IaaS, PaaS, UCaaS etc.) invariably grew, especially for remote offices and users. The resulting penalty in latency, jitter, and packet loss especially impacted remote offices and users. In addition, the model often resulted in the need for ever increasing and costly MPLS bandwidth, particularly for real-time collaboration applications. Enterprises started to look at a more effective model to optimize application performance.

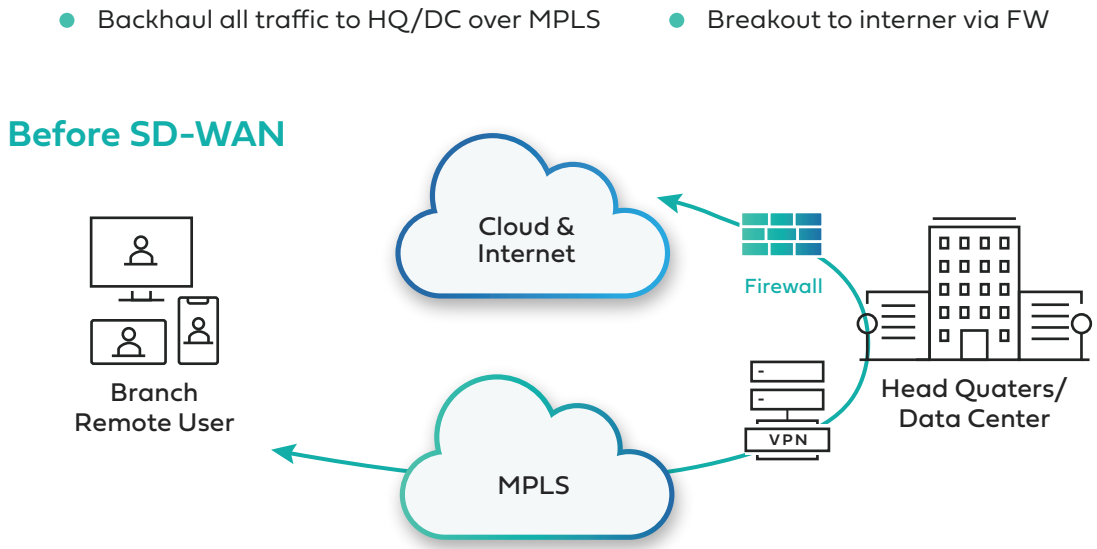


Figure 1: Traditional Network Architecture

SD-WAN Security

The answer to the "back-haul" problem discussed in the previous section is seemingly simple. Enterprises can implement DIA (direct internet access) wherever it proves beneficial, be it to optimize performance when accessing cloud resources or to achieve MPLS bandwidth savings. With this connectivity model, which is one of the driving forces behind the rapid emergence of SD-WAN, branches or remote users can break out traffic to the internet locally based on configured policies. It could be that Guest WiFi or UCaaS traffic only are broken out directly, but there is no end to the path routing possibilities that can be configured. Naturally, security considerations can also be used to determine a path, like, for example, that no PCI or HIPPA traffic types ever take the internet. But these are all examples to illustrate the flexibility of the model shown in Figure 2. This flexibility explains why DIA adoption in enterprise networks has become wide-spread, from less than 50% in 2017 to 80% in 2019, thus becoming the de-facto enterprise network standard: one premium path ensures SLA (service level agreements) for business-critical applications, while the other path routes best-effort traffic to the Internet.

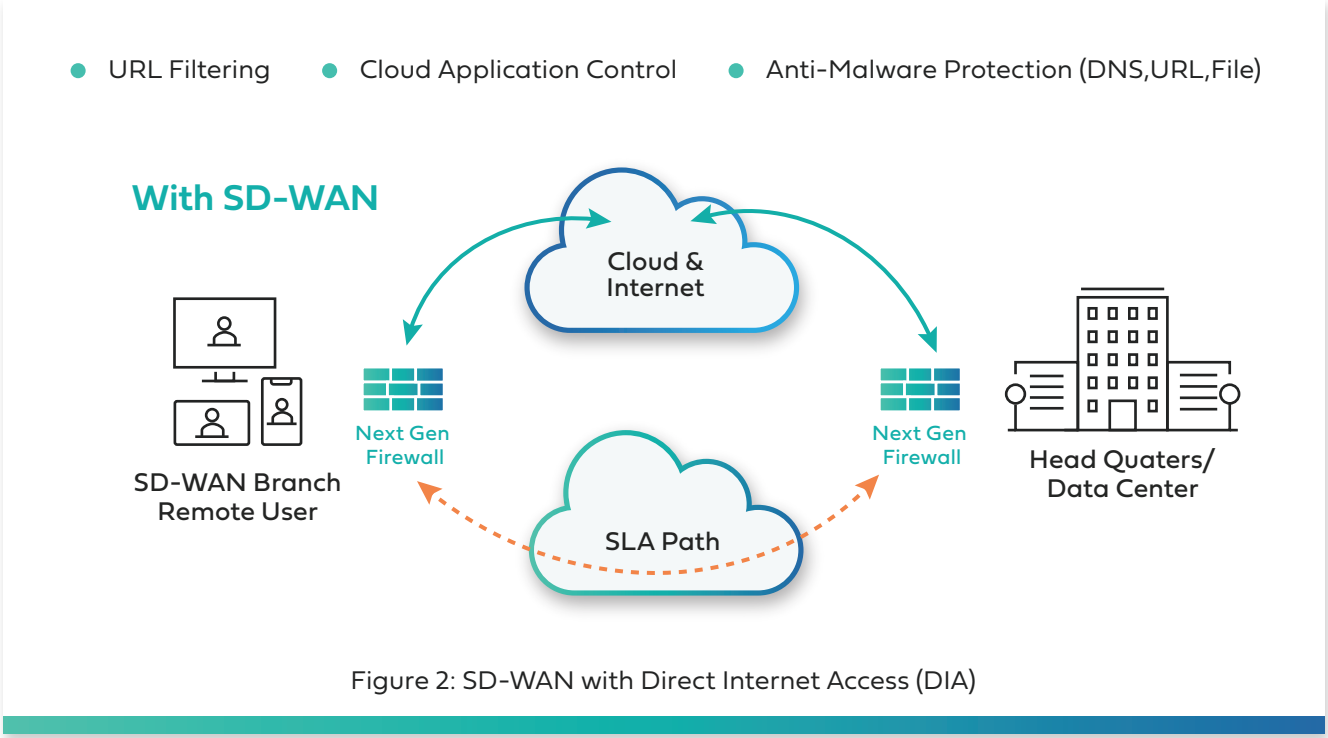


Figure 2: SD-WAN with Direct Internet Access (DIA)

However, the adoption of DIA does pose obvious new security challenges. By opening a distributed internet gate across the entire enterprise network architecture, the attack surface to increasingly sophisticated threats becomes much larger. And a bigger attack surface and the constantly increasing number of attacks and threats is most certainly a very worrisome combination. So, what to do about it?

The Heavy Branch

With the need for DIA, the model for the so called "heavy-branch" became increasingly omni-present. As happens so often in the history of networking, slowly but surely additional features keep being added to the networking stack. Networking functions like policy-based routing or application recognition and many others were added to branch routers. Simultaneously, security functions also became broader in scope. We'll explain these functions (which are listed in Figure 3) in subsequent sections. But let's take note that these separate network and security functions were delivered as several separate appliances, greatly adding to the administrative burden, complexity and operational cost of any enterprise location. The heavy branch model is prevalent with current SD-WAN DIY (Do-It-Yourself) solutions, which emphasize branch device capabilities despite the fact they often need to be complemented with additional devices providing functionality not covered by the DIY vendor's branch CPE.

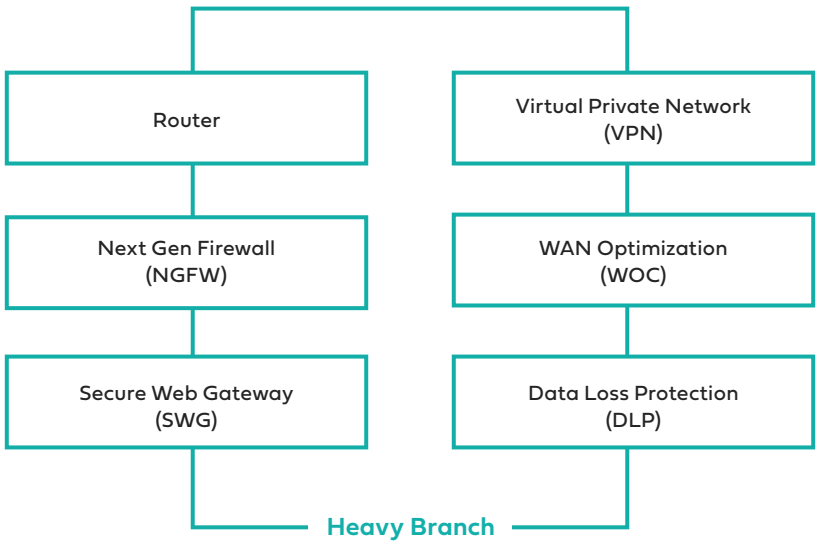


Figure 3: Heavy Branch Functionality

The heavy branch model represents the logical evolution of the branch based on established network design practices. While it delivers on all the required network and security functionality to respond to current design challenges, the fact of the matter is that it results in functional complexity, high operational cost and thereby curtails the agility to respond to new business needs.

Cloud-Based Security

An alternate approach that can help simplify the architecture in the branch is cloud-based security. As a response to the enterprise journey to the cloud, more cloud-centric models to security started to emerge. Instead of performing advanced traffic classification and security checks in every location, why not simply route some or all traffic into the cloud, especially since an ever-increasing amount of traffic is headed there anyhow? Why not simply perform advanced security functions there? Branches and other enterprise locations then are left to provide networking functions and merely require a basic security function like a stateful firewall and policy based L2 and L3 segmentation. That way, any unknown traffic that doesn't pass the firewall rules is routed to be handled by cloud-based security functions as shown in Figure 4.

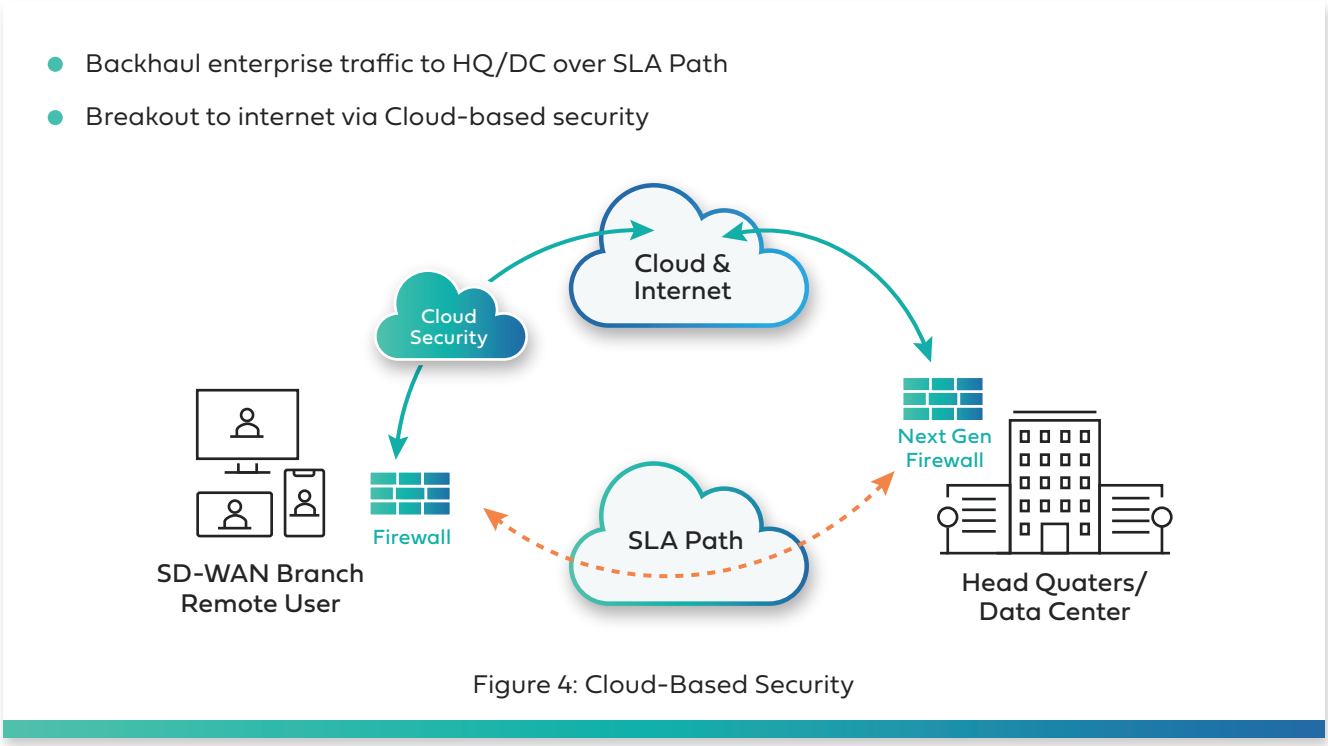


Figure 4: Cloud-Based Security

While the cloud-based security model offers the advantage of simplifying the security needs in the branch, it isn't without potential drawbacks. The cloud security hop may impact SLA performance for some time-sensitive traffic to and from branches. The branch devices still implement a complex and functionally heavy networking stack that impacts business agility as well as operating cost. Finally, it may result in inconsistent security postures being implemented across the enterprise, since some locations with very high traffic loads are likely to stay operating with the "heavier" architectural model.

SASE Overview (Thin Branch and Heavy Cloud)

When discussing SASE – the Secure Access Service Edge- it's best to avoid paraphrasing its definition, which several vendors do in order to conveniently position their proprietary -but as yet incomplete- offerings in the context of SASE.

The definition of SASE by Gartner, who invented the concept of SASE in the article "The Future of Network Security Is in the Cloud [ID G00441737]", is as follows: "The secure access service edge is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure access needs of digital enterprises. SASE capabilities are delivered predominantly as a cloud-based service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions."

SASE is predominantly delivered as a "heavy cloud" solution, meaning that the majority of functions can be provided in the cloud. However, the Gartner SASE model does not eliminate the need to provide a certain set of network and security functions in the branch CPE (the "thin branch"), as shown in Figure 5.

To sum it up, SASE represents the convergence of network and security as a service. As previously mentioned, SASE is not about any new networking or security technologies. As with many emerging trends in IT, SASE's goal is to make existing functions easier to consume and manage. Figure 5 highlights the multitude of network and security functions that exist in a SASE solution. Optimally configuring and managing all these complex functions is very work-intensive for IT network staff, a burden that SASE will lighten in the future.

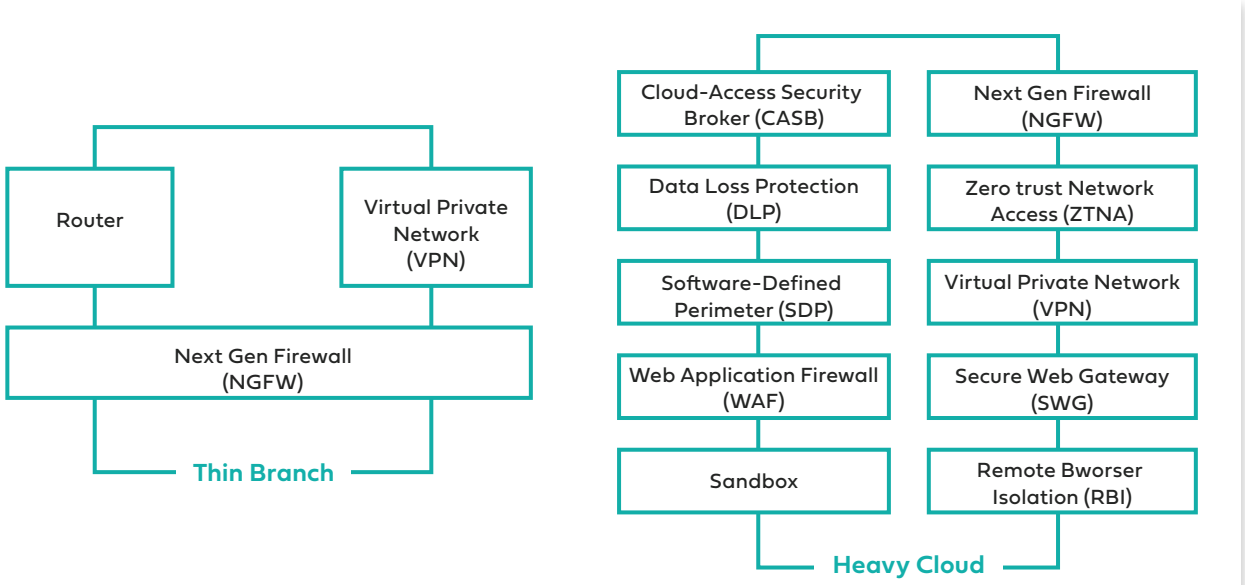


Figure 5: SASE Functional Stack

SASE Functional Stack

In the following sections, we will provide an overview of the many functions that are consolidated in a SASE solution.

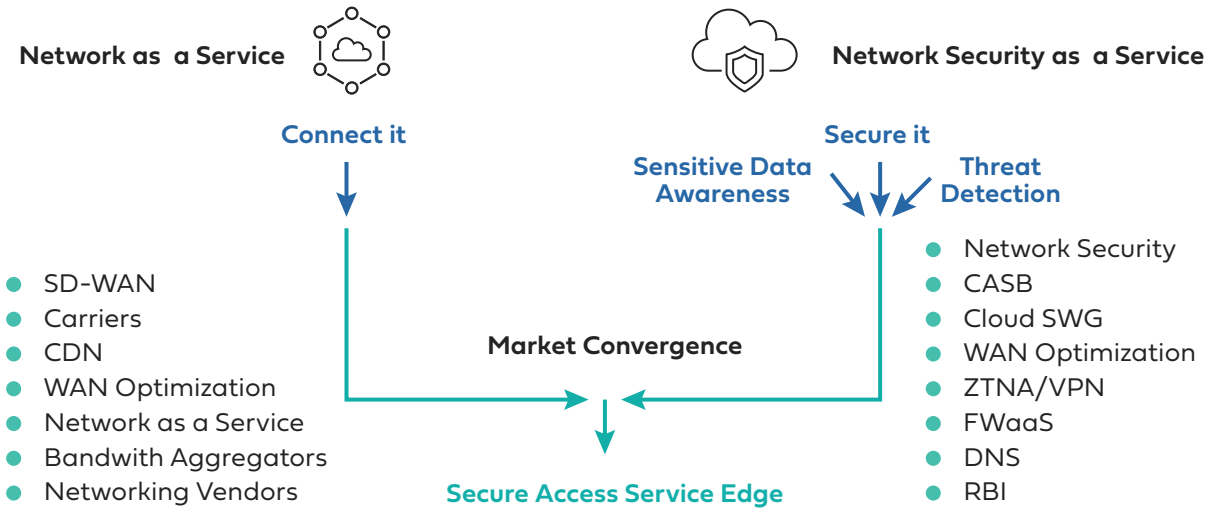


Figure 6. SASE Convergence

Network as a Service Functions

Software-Defined Wide-Area Network (SD-WAN)

SD-WAN represents the evolution of the traditional enterprise wide-area network. Its goal is to greatly simplify the management and operation of an enterprise's WAN, which has grown increasingly complex over time and lacks the agility to keep up with emerging digital enterprise business needs. SD-WAN can be delivered as a DIY (Do-It-Yourself) solution that requires re-training and re-skilling network IT staff, or as a managed service that empowers network IT staff to adopt DevOps patterns and focus on business outcomes rather than basic network operations.

WAN Optimization

WAN optimization includes a wide array of technologies that increases wide-area network traffic efficiency as well as performance. TCP/IP optimization focuses on maximizing throughput by optimizing latency, providing congestion control and minimizing packet loss. UDP traffic can also be optimized in order to enhance the user experience for real time collaboration applications that require optimal voice and video performance. Among others, technologies for WAN Optimization include deduplication, wide area file services (WAFS), SMB proxy, TCP and HTTPS proxies, media multicasting, web caching and overall bandwidth management.

Network-Based Application Recognition (NBAR)

The WAN can handle traffic far more efficiently if it gains awareness of the application that is using a certain session. Application recognition technology allows the network to gain such awareness. At its simplest, this consists of identifying ports at Layer 4, however DPI (Deep Packet Inspection) as well as DNS lookup information can be leveraged to gain application awareness and apply adequate traffic policies.

Policy-Based Routing (PBR)

PBR finds the optimal path for WAN traffic based on granular policies defined by the network operator. With SD-WAN in particular, it is important to define which traffic types should be routed over the Internet, and which traffic should be kept on a transport infrastructure that delivers on strict SLAs, such as traditionally MPLS but also increasingly more cost-effective global or regional transport options such as Aryaka's SmartConnect Global Layer 2 Core Network.

Security as a Service Functions

Cloud-Access Security Broker (CASB)

A cloud access security broker (CASB) sits between cloud service users and cloud applications and monitors all activity and enforces security policies. A CASB monitors user activity, warns administrators about potentially hazardous actions, enforces compliance with security policies and prevents malware.

Next Generation Firewall (NGFW)

Next-generation firewalls (NGFW) represent the third generation of firewall technology. NGFWs combine traditional firewall functionality with new capabilities such as device filtering functions, application firewall with in-line deep packet inspection (DPI), intrusion prevention system (IPS), encrypted traffic inspection, website filtering, antivirus protection and even more functions.

The goal of next-generation firewalls is to offer protection to the upper layers of the OSI model, improving filtering of network traffic based on the packet contents by checking packet payloads and matching signatures.

Data Loss Protection (DLP)

The data loss prevention function is tasked with detecting potential data breaches. DLP detects data that is transmitted in violation of information security policies.

Zero Trust Network Access (ZTNA)

While security technologies have grown to protect the enterprise with a growing number of functions that offer defense mechanism against an ever-increasing number of threats, the traditional enterprise security posture is a passively defensive one. Zero Trust It is a security posture that doesn't allow anything or anyone into the enterprise unless their identity is confirmed, and when granted access they are mapped via policy to a few chosen micro-segments in the network.

Zero Trust represents the countermovement to the universal connectivity premise that IP networks enabled. IP's universal connectivity stack enabled an industry revolution, but we know that universal connectivity opens the enterprise to attacks. The history of network security is one of limiting that inherent universal connectivity in IP networks. Firewalls came first. Intrusion detection followed. Unified threat management was the next stop. But those are all passive defensive postures. Zero Trust represents a disruptive, offensive move in enterprise security architecture.

Software-Defined Perimeter (SDP)

The software-defined perimeter (SDP) is a security approach developed by the Cloud Security Alliance (CSA) and controls resource access by leveraging identity. User identity and device posture and identity are established before granting access. This approach is useful in fending off a variety of common attacks that can be initiated by unauthorized users: server scanning, denial of service, SQL injection, operating system and application vulnerability exploits, man-in-the-middle, etc.

Virtual Private Network (VPN)

VPN technology securely connects remote users and branch offices to enterprises resources. The tunnel connecting the user to the VPN server is encrypted. VPN users also need to authenticate with passwords and/or certificates.

Web Application Firewall (WAF)

A web application firewall inspects bi-directional web-based (HTTP) traffic and blocks any malicious activity. It represents a security policy enforcement point positioned between a web application and the client endpoint. WAFs leverage rule-based logic, parsing, and signatures to detect and prevent attacks such as cross-site scripting and SQL injection. The OWASP (Open Web Application Security Project) keeps a list of the top ten web application security risks.

Secure Web Gateway (SWG)

A Secure Web gateway protects Web-surfing PCs from infection and enforces company policies, filtering unwanted software/malware from user-initiated Web/Internet traffic. SWGs provide URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype.

Sandbox

A Sandbox provides a safe environment and separates running programs in order to mitigate system failures or software vulnerabilities from spreading. It is used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the extended enterprise. A Sandbox represents a tightly controlled set of resources for guest programs to run in, such as storage and memory scratch space. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.

Remote Browser Isolation (RBI)

As the name implies, RBI isolates a user's browsing activity in order to protect the local network and infrastructure. RBI is delivered as a cloud-based service, allowing enterprises to deploy browser isolation solution to their users without having to build a local infrastructure.

User Entity Behavior Analytics (UEBA)

UEBA solutions establish behavioral patterns and then apply algorithms and statistical analysis to detect meaningful deviations from established, “normal” patterns. Such anomalies are further investigated to establish if they represent threats, or merely establish a new pattern that is then incorporated into the list of accepted patterns. UEBA is increasingly adopting AI (Artificial Intelligence) to reduce the incidence of false positives and make the platform trainable, rapidly merging with SIEM (Security Information and Event Management).

The Need for Architectural Choice

In the previous sections, we established that -according to Gartner- the future of network and security is to unequivocally be in the cloud. Or is it? In May 2019, ONUG (Open Networking Users Group) polled hundreds of enterprise networking professionals about their preference between on-premise and cloud-based delivery models for network security. The result is shown in Figure 7. It shows that Gartner's SASE vision will take some time to materialize, since in the current environment 67% of network professionals expressed a preference for an on-premises security model, whereas 33% chose a cloud-based model. Clearly that means that there is still room for both approaches for enterprise security.

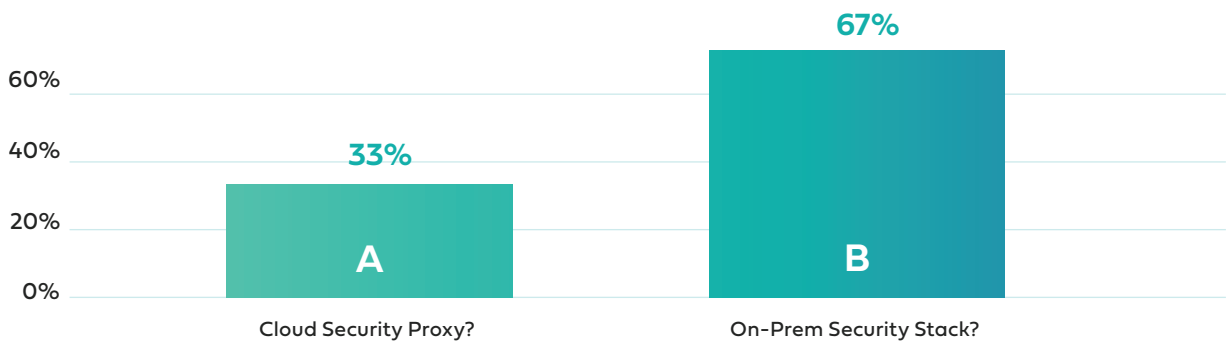


Figure 7 : https://www.onug.net/onug-spring-2019-poll-day-2/

As so often, probably trying to answer architectural questions with a one-size-fits-all answer fails to consider the many different scenarios enterprise architects needs to address. The fact is there are too many variables that need to be taken into consideration, starting with the fact that legacy architectures can't be changed overnight. Then there is also the fact that different enterprises in different industries often face a variety of regulatory as well as other very particular requirements that can only be optimally addressed with custom-tailored network and security solutions. The old cliché that "customers need choice" most certainly applies to an area with as many variables as network and security architecture.

The Aryaka security architecture takes this into account. As Figure 8 shows, Aryaka's security approach offers its enterprise customers complete and total flexibility by supporting on-premise, cloud-based as well as any desired hybrid architectural approach to network security. This allows enterprise architects to truly tailor their security architecture to their very own needs, instead of limiting them to limited, prescriptive approaches. Like any other requirement, security needs can and do change over time, thus making flexibility a key consideration to keep the solution future-proof.

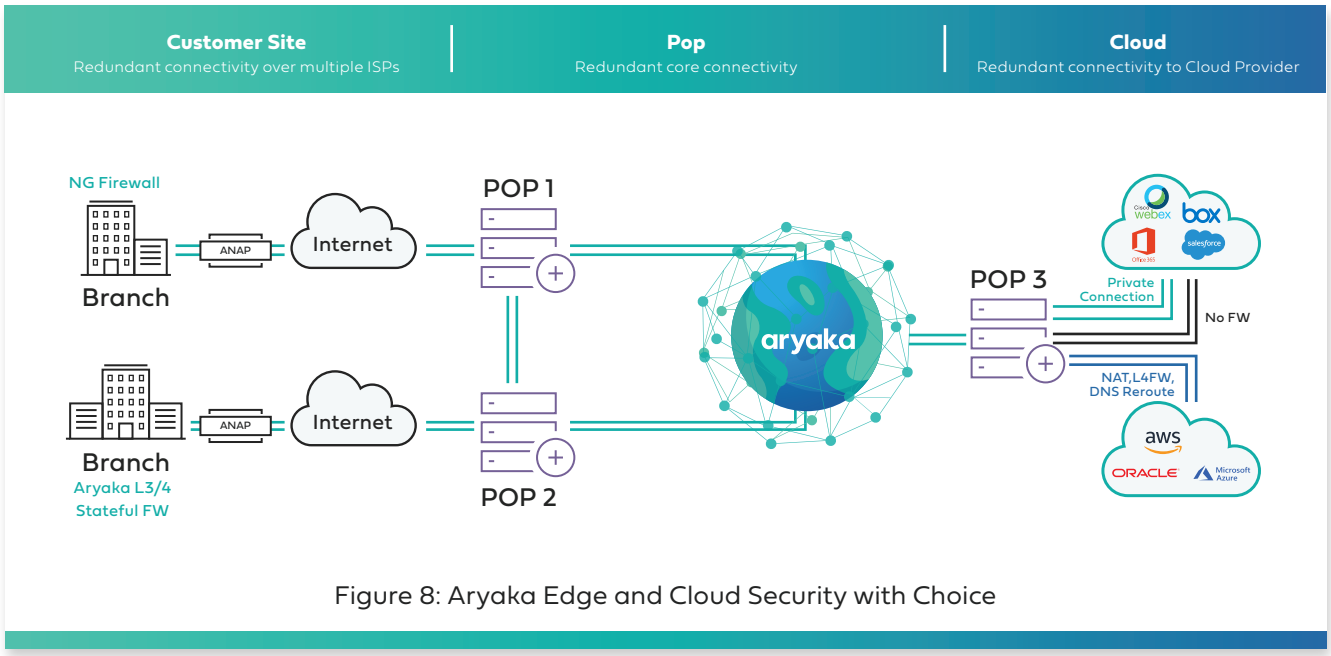


Figure 8: Aryaka Edge and Cloud Security with Choice

Single-Vendor or Best-of-Breed?

Just like the cloud-based vs on-premises consideration in the previous section, different enterprises will also have different preferences when it comes to deciding between an integrated, single-vendor solution or whether to pick best-of-breed solution elements. Aryaka's 2020 State of The WAN Report questioned over 1,000 network professionals and confirmed that -as established in the previous section- the key is to provide enterprises with the power of choice. Interestingly, those enterprises that prefer an on-premise security model seem to also prefer best-of-breed solution components. This could be because those who need to tailor a solution to their very particular needs have more stringent security requirements. On the other hand, those architects that favor the cloud for its ease of consumption furthermore have a preference for a single vendor solution in order to further simplify deployment.

However, the key takeaway, just as in the previous section, is that customers demand the power of choice. Yet again, Aryaka's approach to security delivers on enterprises' preference for choice by supporting several architectural security models so that enterprises can build out their optimal security solution:

- Aryaka's stateful firewall (Zones) is a complementary software feature on the ANAP CPE and furthermore supports robust L2/L3 segmentation capabilities to provide the foundation for a ZTNA architecture.
- Aryaka partners with leading cloud security vendors to provide cloud-based security.
- Aryaka's ANAP CPE supports 3rd party VNFs (Virtual Network Functions) and thus also offers best-of-breed on-premises capabilities, as evidenced by technology partnerships with leading security vendors to provide NGFW and other security functions.

Aryaka will continue to add best-of-breed security solutions to its catalog by continuing to closely partner with leading security vendors.

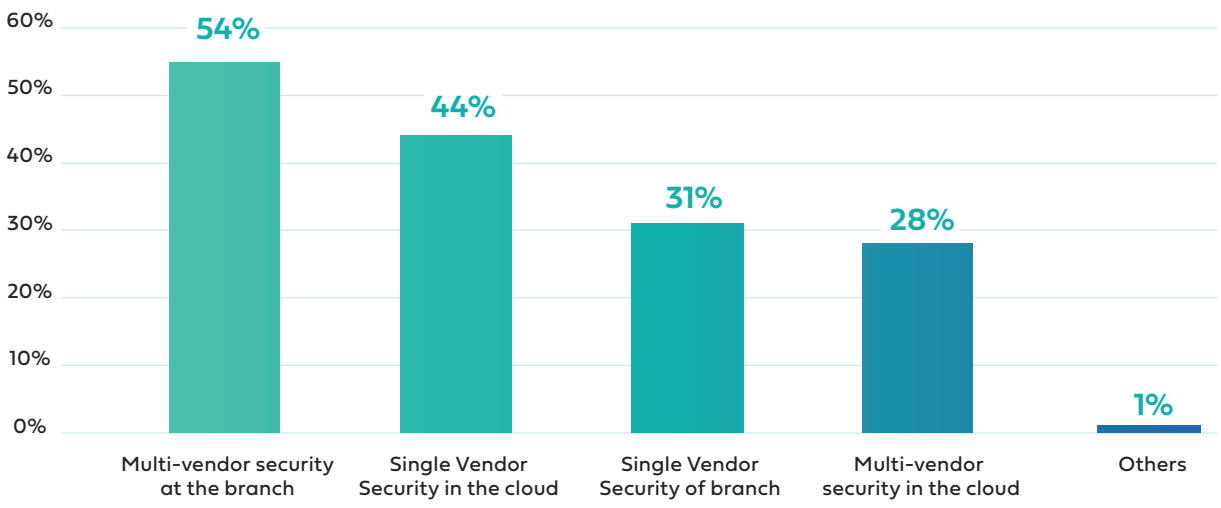


Figure 9: Enterprises Prefer Best-of-Breed Solutions

SASE as a Managed Service

In previous sections, we have established that security has evolved -just like networking- into yet another IT area where many complex capabilities are needed. Security is a vital area in IT that ensures business operations and continuity. But it is also very complex and challenging for IT departments to constantly stay on top of every aspect needed to configure, operate and update all the elements that comprise a state-of-art security solution.

In SD-WAN, a rapidly growing number of enterprises have cast their vote in favor of adopting SD-WAN as a managed service in order to increase business agility and lower the operation burden of hands-on management of their network infrastructure, which enables the IT team to increasingly focus on new business-relevant initiatives.

As enterprises migrate to their future network and security architectures, it stands to reason that -given the complexity of the consolidated network and security functional stack- enterprises will seek to increasingly consume it as a managed service.

Aryaka is pioneering the delivery of network and security as a service. While customers with a preference for do-it-yourself can of course deploy the security solutions that Aryaka offers in that way, Aryaka also offers a fully-managed option for both networking and security services.

Conclusion

Security is top of mind with enterprise architects. Security is shown to be one of the top considerations when establishing SD-WAN vendor preference. Furthermore emerging consolidated network and security concepts such as SASE provide enterprises with the opportunity to complete their security architecture with all the functions required to protect the digital enterprise, while at the same time challenge IT teams with the complexity of managing such a comprehensive functional stack of network and security capabilities.

Figure 10 : Aryaka Security Strategy Summary

Aryaka's strategy offers its customers a full portfolio of options to successfully navigate the changing landscape of networking and security that concepts such as SASE advance. Enterprises can rest assured that Aryaka will not limit their architectural choices by only offering a home-grown solution that is unlikely to combine best-of-breed capabilities for every required function.

Aryaka's ability so support both on-premises and cloud-based security approaches, its commitment to offer third-party, best-of-breed solutions from leading security vendors and -finally- its ability to support both do-it-yourself as well as fully managed consumption options are unique in the industry. While many vendors try to reduce the SASE discussion to a one-size-fits-all, lowest-common-denominator discussion, Aryaka provides enterprises with all the building blocks and consumption options to ensure success as enterprises embark on the journey to implement their next generation network and security infrastructures.

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 and SASE service and sets the gold standard for application performance. Aryaka's SmartServices platform offers 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.

LEARN MORE | info@aryaka.com | +1.877.727.9252