HPE aruba networking

Solution overview

Making the shift to a business-first networking model

HPE

HPE Aruba Networking's EdgeConnect SD-WAN platform powers a self-driving wide area network for cloud-first enterprises

A sea change is upon us

A sea change is upon us, and that sea change is the migration of applications to the cloud. While every enterprise's digital transformation journey is unique, Gartner predicts that by 2026, 75% of organizations will adopt a digital transformation model predicated on cloud as the fundamental underlying platform.[1] While many enterprises continue their cloud migration, some have already moved 100 percent of their application instances to SaaS and IaaS and have ceased operating their own data centers.

In fact, many enterprises have a multi-cloud strategy and are already running applications in three or more different clouds. Not only are applications distributed across multiple locations and multiple clouds, but users must also be able to access them from any device and from anywhere. However, traditional router-based networking approaches weren't designed for the agile cloud era, complicating the task of connecting users to applications.

The router-centric WAN model has hit the wall

While the majority of enterprises have moved applications and IT infrastructure to the cloud, many have yet to realize the full promise of the cloud. The underlying reason is that the cloud has caused the fundamental nature of applications and network traffic patterns to change.

The traditional router-centric wide area network (WAN) architecture was designed when all applications were hosted in enterprise data centers; there was no cloud. In a router-centric model, all traffic is routed from branch offices to the data center. With the emergence of the cloud, applications are no longer centralized.

But traditional routers require enterprises to inefficiently route all applications from branch offices back to the data center instead of directly to SaaS and IaaS from branch sites, and this impairs application performance. The requirement to backhaul is due either to an inflexible architecture and/or security requirements that dictate advanced inspections that conventional routers lack the functionality to perform.

[1] Gartner, April 2023

In the new multi-cloud era, enterprises are faced with an entirely new set of challenges. They are struggling to determine how to:

— Use the internet to connect users directly to cloud applications for the best performance

— Continuously deliver a high quality of experience for every business-critical app

— Keep up with changes to their WAN without configuring and administering device-by-device

— Deliver new applications to 100s or 1000s of sites, across multiple clouds, in 10 percent of the time

— Continuously monitor all applications and WAN services to know which issues to focus on across 1000s of sites

— Deliver significantly more bandwidth at the WAN edge, for the same budget

— Ensure their WAN is never a roadblock and always keeps pace with the business

— Protect their business when the cloud is open, accessible and everything is connected

— Provide secure access to a growing hybrid workforce

Unfortunately, today's choices weren't designed for the cloud era, and as a result force compromise. Enterprises struggle trying to stretch the old router-centric WAN—it's too cumbersome and complicated. Even basic SD-WAN solutions which emerged as an alternative, are a step in the right direction, but they too fall well short of the goal of the fully automated business-driven networks that enterprises require in today's cloud-era. There is a better way forward.

The imperative: Shift to a business-first networking model

A business-first networking model is a top-down approach. It is one in which the network conforms to the business in contrast to the legacy router-centric approach where applications—and the business—must conform to the constraints imposed by the network. The device-centric model starts from the bottom up with the deployment of routers (and usually discrete firewalls) at every branch location. This generally requires on-site IT expertise and always requires manual, device-by-device configuration and management. Any changes that arise when adding a new application or changing a QoS or security policy, once again requires manually reconfiguring every router at every branch in the network.

Table 1. A comparison between a router-centric model and a business-first model

Option 1 Router-centric model	→	**Better way** ✓ Business-first model
Business conforms to constraints of the network		Network enables the business
Bottoms-up, device centric		Top-down: start with business intent
Network creates a bottleneck		Network is a business accelerant
Manual, elongated delivery		Fully automated, continuous delivery
One size fits all		Give every application what it needs
Unsustainable economics		10x bandwidth, same budget
Surprises, always behind		Delivers highest quality of experience

Re-programming is time consuming and requires utilizing a complex, cumbersome command line interface (CLI).

With a business-first networking model, IT centrally orchestrates QoS and security policies for groups of applications based on business intent. The configuration is programmed automatically to 100s or 1000s of locations across the network. From that point onwards, the network automatically and continuously connects users directly and securely to applications delivering optimum performance. Through real-time monitoring of applications and WAN services, a business-driven network automatically "learns" of any changes in network conditions that might impact application performance—packet loss, latency, jitter. It then automatically "adapts" to give every application the network and security resources it needs to deliver the highest quality of experience to users.

Table 2. A comparison between a basic SD-WAN model and a business-first model

Option 2 A basic SD-WAN model gives you:	Better way ✓ A business-first model delivers what you need:
Zero-touch provisioning	Full orchestration and lifecycle automation
Automated templates	Continuous, self-learning, outcome oriented
Path selection	Consistent WOW experience, even voice & video over broadband
Encrypted VPN overlay	Continuously enforce end-to-end segmentation
Fixed app definitions, ACLs	Identify millions of applications on the fly, updated daily
Service-chained VNFs	Seamless, holistic implementation of multiple functions

Business-first networking model vs. basic SD-WAN

In the past few years, the industry has seen more than 60 companies market SD-WAN as part of their offerings. Most include basic SD-WAN features such as the ability to use multiple forms of transport, dynamic path selection, centralized management, zero-touch provisioning, and encrypted connections. However, they do not deliver on the vision of a business-first networking model. A business-driven SD-WAN follows the tenets of the top down, business-first networking model described earlier. There are some key differences:

Lifecycle orchestration and automation—Most basic SD-WAN offerings provide some level of zero-touch provisioning. However, most do not provide full end-to-end orchestration of all WAN edge functions such as routing, security services including firewall, integration with security service edge (SSE) solutions and WAN optimization. A business-first networking model provides automated orchestration and lifecycle management of all WAN functions. When the enterprise deploys a new application or when a QoS or security policy change is required, a business-first networking model centrally configures and implements the required changes to the WAN in a few hours instead of weeks or months.

Continuous self-learning—A basic SD-WAN solution steers traffic according to pre-defined rules, usually programmed via templates. However, to deliver optimal application performance under any network condition, a business-driven SD-WAN continuously monitors and self-learns the state of the network to deliver optimal application performance, even when network changes, congestion or impairments occur. A self-learning SD-WAN not only detects a resource deterioration or an outage, for example a WAN transport service or even a third-party cloud security service, it automatically remediates to keep traffic flowing while maintaining continuous compliance with business policy.

Consistent quality of experience—A key benefit of an SD-WAN solution is the flexibility to actively use multiple forms of WAN transport. A basic solution can direct traffic on an application basis down a single path, and if that path fails, or is underperforming, it can dynamically redirect to a better performing link. However, with many basic solutions, failover times around outages measures in the tens of seconds or longer, often resulting in perceptible—and annoying—application interruption.

A business-driven SD-WAN more intelligently monitors and manages transport services. It has the ability to overcome the problems of packet loss, latency and jitter to deliver the highest levels of application performance and quality of experience to users, even when WAN transport services are impaired. A business-driven SD-WAN handles a total transport outage seamlessly and provides imperceptible, sub-second failovers that don't interrupt business-critical applications such as voice and video communications.

Next-generation firewall—A business-driven SD-WAN includes advanced security capabilities such as a next-generation firewall, enabling organizations to replace legacy firewalls in branch offices. The next-generation firewall includes capabilities such as deep packet inspection, intrusion prevention, DDoS defense, as well as micro-segmentation. It gives IT leaders the ability to block malware from entering the network based on application, identity and context, while providing an increased visibility into network activity and potential risks. Since the next-generation firewall is centrally managed, it significantly reduces configuration errors and does not require local expertise.

End-to-end segmentation—While basic SD-WANs provide the equivalent of a VPN service, a business-driven SD-WAN provides more comprehensive, end-to-end security capabilities. In addition to supporting a next-generation firewall within the platform, the SD-WAN platform should orchestrate and enforce end-to-end segmentation spanning the LAN-WAN-Data Center. Centrally configured security policies are far more consistent—due to far fewer human errors—than with a device-centric WAN model or a basic SD-WAN model that often require configuring policies device-by-device.

If a policy requires a change, it is programmed once with a business-driven SD-WAN and pushed to 100s or even 1000s of nodes across the network, providing a significant increase in operational efficiency.

End-to-end segmentation helps protect organizations against the proliferation of IoT devices that are difficult to secure and demonstrate compliance with standards and regulations such as HIPAA and PCI DSS.

Direct internet breakout to cloud applications—Many basic SD-WANs provide some application classification capabilities based on fixed definitions and manually scripted ACLs to send SaaS and IaaS traffic directly across the internet. This approach might work fine when initially deployed, but cloud applications change constantly. A business-driven SD-WAN must keep pace by continuously adapting to these changes, doing so with daily application definition and IP address updates. If they are not updated, the application breaks, users are disrupted and satisfaction and productivity deteriorates.

Holistic unification of all WAN edge functions—The WAN edge consists of a number of network services and functions including routing, WAN optimization, a multitude of security services, connectivity to DNS servers, application and network performance monitoring, load balancing and more. Many of these network services or functions are well-suited to be unified within a single SD-WAN platform. However, more sophisticated functions often require specialized technologies. To support all of the WAN edge requirements at branch offices, the SD-WAN should be able to automatically orchestrate with network functions provided by industry segment leaders. This requires not only extensive business partnerships but often times, custom developments that simplify and streamline the integration of network functions with the SD-WAN platform.

Secure access service edge (SASE)—To address the growing demand for security in the era of hybrid working and cloud computing, a business-driven SD-WAN should seamlessly integrate with security service edge (SSE) to create a robust SASE architecture. The SD-WAN solution is either integrated in a unified SASE platform from a single vendor or tightly integrated with third-party cloud delivered security services.

SASE extends the capabilities of SD-WAN to meet the security needs of remote users and hybrid workers with zero trust network access (ZTNA). ZTNA ensures that access is granted based on the principle of least privilege, strengthening the overall security posture. The SASE platform also safeguards web users against cyberattacks, including ransomware and phishing, through secure web gateway (SWG). It ensures that sensitive data hosted in SaaS applications remain protected, it helps monitor shadow IT and prevents data loss with cloud access security broker (CASB).

Why HPE Aruba Networking EdgeConnect SD-WAN

With thousands of production deployments, customers have identified four unique areas of business value as the reasons they've chosen the HPE Aruba Networking EdgeConnect SD-WAN platform. The platform enables customers to build a unified WAN edge that is business-driven, delivers the highest quality of experience, continuously adapts to changing business needs and network conditions. It is designed to enable enterprises to fully realize the transformational promise of the cloud.

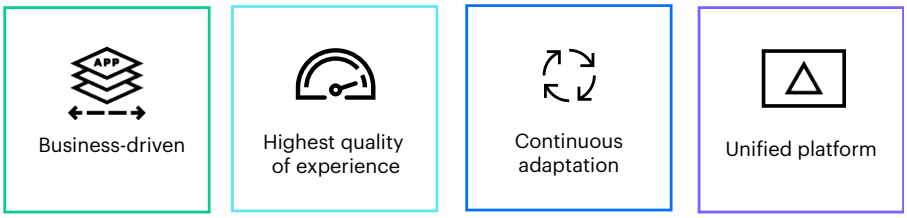

Figure 1. Forward-thinking executives choose the EdgeConnect SD-WAN platform

Business-driven SD-WAN

By deploying the HPE Aruba Networking EdgeConnect SD-WAN platform, application performance, security and routing are dictated by top-down business policies, not bottoms-up technology constraints.

Enterprises ensure that the priorities of their business are always reflected in the way the network delivers applications to users. Business intent dictates application QoS and security policies. Business intent also drives the way network resources are applied to match the business criticality of every application.

The EdgeConnect SD-WAN architectural model utilizes virtual WAN overlays based on business requirements (business intent overlays) for every class of application. Once overlays and their associated policies have been defined via WAN Orchestrator, configurations are pushed to all sites across the network. At that point, traffic handling is fully automated to optimally route—or steer—applications based on pre- configured parameters. EdgeConnect SD-WAN continuously learns about any network condition changes and automatically adapts traffic handling to maintain continuous compliance to application QoS and security application QoS and security policies.

Highest quality of experience

Leveraging technologies that continuously learn, adapt and automate how traffic is directed across the WAN, the EdgeConnect SD-WAN platform delivers the highest quality of experience for both end users and IT. End users enjoy always-consistent, always-available application performance, including the highest quality of voice and video, across any combination of transport services, including cost-effective consumer broadband services. With capabilities including adaptive local internet breakout, path conditioning and the optional WAN Boost for WAN optimization, HPE Aruba Networking enables IT to keep users satisfied and productive.

Centralized orchestration simplifies the implementation of changes, minimizes human errors and enables faster troubleshooting so that IT can be more responsive to the business. With high application performance and availability and automated network resiliency, even when underlying transports experience disruptions or outages, EdgeConnect SD-WAN frees IT to reclaim their nights and weekends—and to contribute to more strategic digital transformation initiatives instead of just "keeping the lights on."

Continuous adaptation

Through advancements in machine-learning, HPE Aruba Networking is going beyond automation and templates to enable customers to build a self-driving wide area network that gets smarter every day. The EdgeConnect SD-WAN platform automates real-time response, eliminating the impact of brownouts and blackouts as continuous monitoring and analytics detect changing conditions and trigger immediate adjustments.

Basic SD-WANs can break out some cloud applications by manually scripting ACLs which rely on the overhead of constant, manual updates to address application definition changes. The applications themselves change as new features are added, and the IP addresses utilized by common SaaS applications are updated frequently. However, when application definitions or IP addresses change, a basic SD-WAN will revert to backhauling traffic it cannot classify, resulting in degraded cloud application performance. HPE Aruba Networking adaptive internet breakout automates application definitions and IP address updates daily for more than 10,000 SaaS applications and 300 million web domains. With HPE Aruba Networking adaptive internet breakout, users can always connect to any application without manual intervention from IT.

Unified platform

The EdgeConnect SD-WAN platform was designed from the ground up as a single system. It unifies SD-WAN, firewall, segmentation, routing, WAN optimization and application visibility and control in one centrally managed platform. This is in contrast to competitive offerings that merely integrate key branch wide area network functions through service chaining.

EdgeConnect SD-WAN also seamlessly integrates with HPE Aruba Networking SSE to form a unified SASE platform, providing faster deployment and a simpler adoption of SASE. And HPE Aruba Networking allows enterprises to leverage existing investments, through service chaining to ecosystem partners, including industry-leading security, cloud and service providers. In fact, HPE Aruba Networking supports the broadest security and cloud partner ecosystem with leaders including Check Point, Forcepoint, McAfee®, Netskope, Palo Alto Networks, Symantec, and Zscaler; cloud providers including Azure, AWS, Google Cloud™, and Oracle® Cloud Infrastructure. In addition, more than a dozen service providers deliver fully managed or co-managed SD-WAN service offerings powered by the EdgeConnect SD-WAN platform.

Centralized orchestration

The foundation or the brains of the EdgeConnect SD-WAN platform is WAN Orchestrator. WAN Orchestrator centrally defines business intent overlays that dictate how applications are delivered across the wide area network. From a single pane of glass, IT can quickly define quality of service policies, security policies, failover prioritization and service chaining to third-party network and security services. Once policies have been defined, they are automatically pushed to 100s or 1000s of sites without the need to manually program individual devices or send IT experts out into the field. With WAN Orchestrator a new application or a policy change can be configured, provisioned, and deployed in a matter of hours instead of days, weeks, or months.

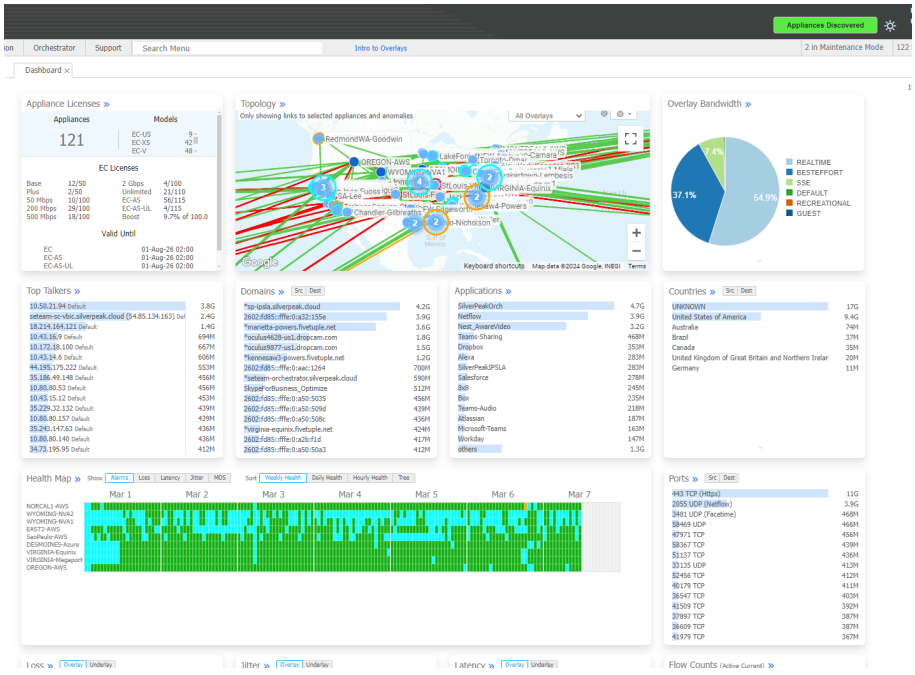

Figure 2. Real-time and historical monitoring and analytics simplify SD-WAN administration and accelerate troubleshooting

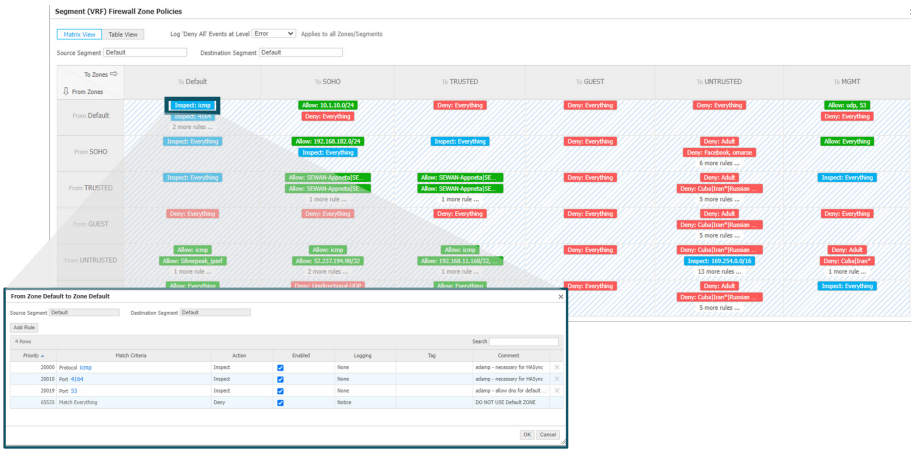

Figure 3. Centrally defined end-to-end segmentation ensures consistent security policy enforcement

WAN Orchestrator also provides historical and real-time dashboards displaying a wealth of metrics for network health, application performance, network performance, WAN transport service performance and more. It provides complete observability—or visibility—of your entire wide-area network from a single pane of glass, enabling faster troubleshooting and comprehensive reporting.

Delivering the highest quality of experience

To ensure customer networks always run at their optimal levels of performance and availability, HPE Aruba Networking provides a fully insourced, 24x7x365, "follow-the-sun" support model. A global network of spares depots provides rapid response should a hardware replacement be needed. HPE Aruba Networking provides complementary SD-WAN training and offers several industry-recognized certifications.

Visit HPE.com

Chat now

a00142255ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com