aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

Enable federal government to modernize network infrastructure and improve cybersecurity

BUILD A PREDICTABLE AND SECURE NETWORK INFRASTRUCTURE WITH ARUBA EDGECONNECT SD-WAN

When the pandemic hit, governmental agencies had to deliver essential services to citizens, accelerating digitization initiatives and cloud migration. The transformation of public services also involves improving the "citizen experience" (CX) by developing enhanced digital services to meet the same expectations as the private sector. To ensure trust to these services, and to respond to growing data privacy concerns caused by past cyberattacks, the Joe Biden administration created in 2021 an Executive Order on Improving the Nation's Cybersecurity. The SolarWinds attack in December 2020 was indeed a wake-up call as it penetrated multiple parts of the United States federal government resulting in a series of data breaches. The executive order calls to improve the government efforts to identify, deter, protect against, detect, and respond to increased cybersecurity threats. Among other measures, the order plans to adopt security capabilities available in the cloud and develop a zero-trust architecture assuming that users and device cannot be trusted by default and are inherently insecure.

The federal government is also moving to a hybrid work model for employees so that they can work from anywhere. As the security perimeter is dissolving, governments have to tackle security concerns around authentication.

Edge computing and IoT are other key components of this transformation. They have many applications such as climate change monitoring, military operations, emergency management, transportation and much more. But they also expose the government to increased vulnerabilities caused by a larger attack surface.

The acceleration to digitization and the need for more security require enhanced networking capabilities that traditional MPLS lines can no longer provide. Private lines are often complex and expensive compared to agile internet broadband and 5G connections.

Aruba EdgeConnect can help!

ARUBA SOLUTIONS FOR DIGITALLY CONNECTED SECURE EXPERIENCES

Based on these above challenges, let's look at how adopting an advanced SD-WAN platform can help the public sector tackle these challenges.

Improved network experience and cost reduction

Aruba EdgeConnect tunnel bonding feature combines multiple WAN transport services including MPLS, internet broadband and 5G to create a single, higher bandwidth logical link. It enables the federal government to use internet instead of expensive and complex MPLS and get a similar performance as private lines. Internet and wireless links indeed often suffer from packet loss and jitter and are more prone to outages. With Aruba's EdgeConnect Forward Error Correction (FEC) feature, lost packets are automatically reconstructed. In addition, when load-balancing traffic between multiple WAN transport services using tunnel bonding, Packet Order Correction (POC) re-orders any packets that arrive out of sequence at their destination. Aruba Boost WAN Optimization also significantly accelerates the transmission of data by applying TCP protocol acceleration as well as data deduplication and compression.

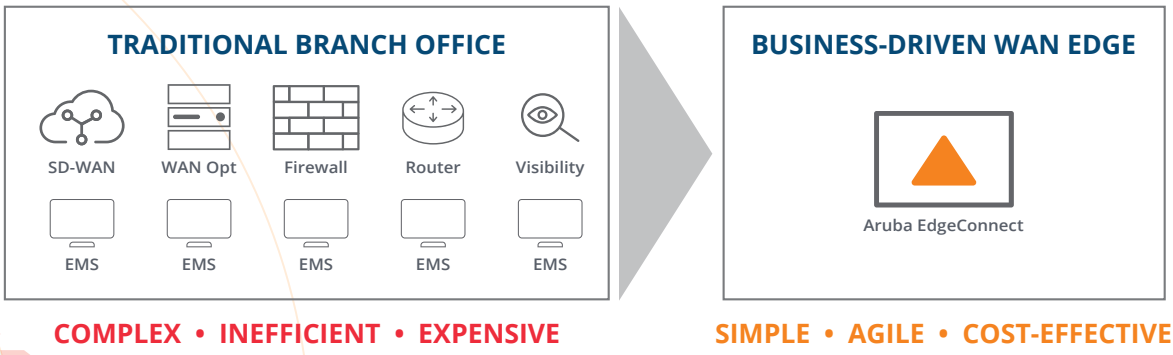

Figure 1: Aruba EdgeConnect enables federal organizations to move from a complex architecture to a simple cost-effective network infrastructure.

Simple deployments

Aruba EdgeConnect SD-WAN helps reduce equipment sprawl as it integrates a certain number of features that are generally scattered in multiple devices such as wan optimization, routers and firewall devices. Additionally, Aruba SD-WAN is centrally orchestrated. With its zero-touch provisioning feature, settings, as well as security parameters, are automatically sent to remote locations so that it doesn't require any experienced IT staff to configure Aruba EdgeConnect at a local facility.

Advanced security

Aruba EdgeConnect embeds a zone-based firewall, providing advanced segmentation capabilities, with logical separation to isolate parts of the network and limit the spread of cyberattacks and malware. It ensures that users and devices can only connect with destinations on the network that are consistent with their role in the organization.

Additionally, with secure internet breakout, the EdgeConnect First-packet iQ™ feature identifies and classifies applications based on the first packet, enabling automatic traffic steering to the internet or to the data center according to security requirements. With this feature, governmental organizations can build security policies that:

- send trusted cloud application traffic, such as Office 365 or UCaaS traffic, directly to the internet,
- send internet-bound traffic, including SAP, Salesforce, and web browsing traffic to a third-party cloud security provider
- backhaul untrusted applications to the data center for advanced security inspection

Aruba EdgeConnect is the foundation for a robust SASE architecture. Through a tight integration to third-party cloud security providers, governmental organizations can implement best-of-breed security capabilities such as ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway) and CASB (Cloud Access Security Broker) and ensure maximum security.

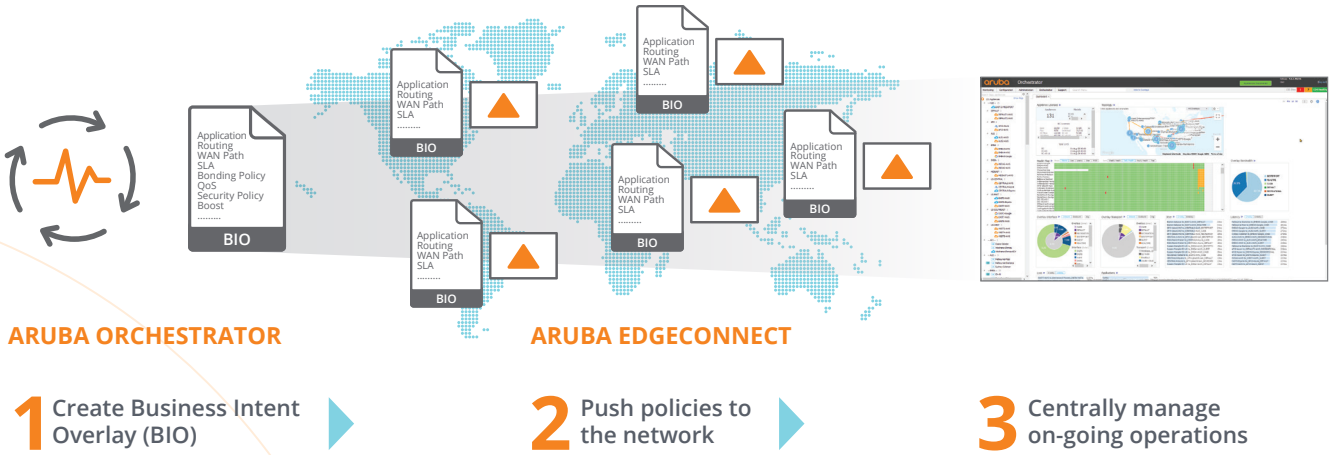

Figure 2: Simplify and accelerate deployments and improve with a top-down model and business-driven policies

Working from Home

As remote working is becoming the new normal, government agents should experience the same level of digital services in their home. Aruba Microbranch connects home offices to the headquarters in an easy and flexible way. It protects remote agents by providing SD-WAN capabilities in an easy-to-use Wi-Fi access point device, including orchestration and secure internet breakout.

SUMMARY

The COVID-19 crisis has accelerated digitization but exposed the government to more cybersecurity risks. Aruba EdgeConnect is the foundation of a robust SASE architecture by providing advanced SD-WAN capabilities and tightly integrating with third-party cloud security vendors to implement best-of-breed security capabilities. It helps governmental organizations strengthen security with a zero-trust architecture and micro-segmentation capabilities. The solution also offers enhanced connectivity and flexibility by virtualizing network links and providing private line-like performance over the internet and wireless connections. In addition, with centralized orchestration and zero-touch provisioning, the solution is easy to deploy and manage.

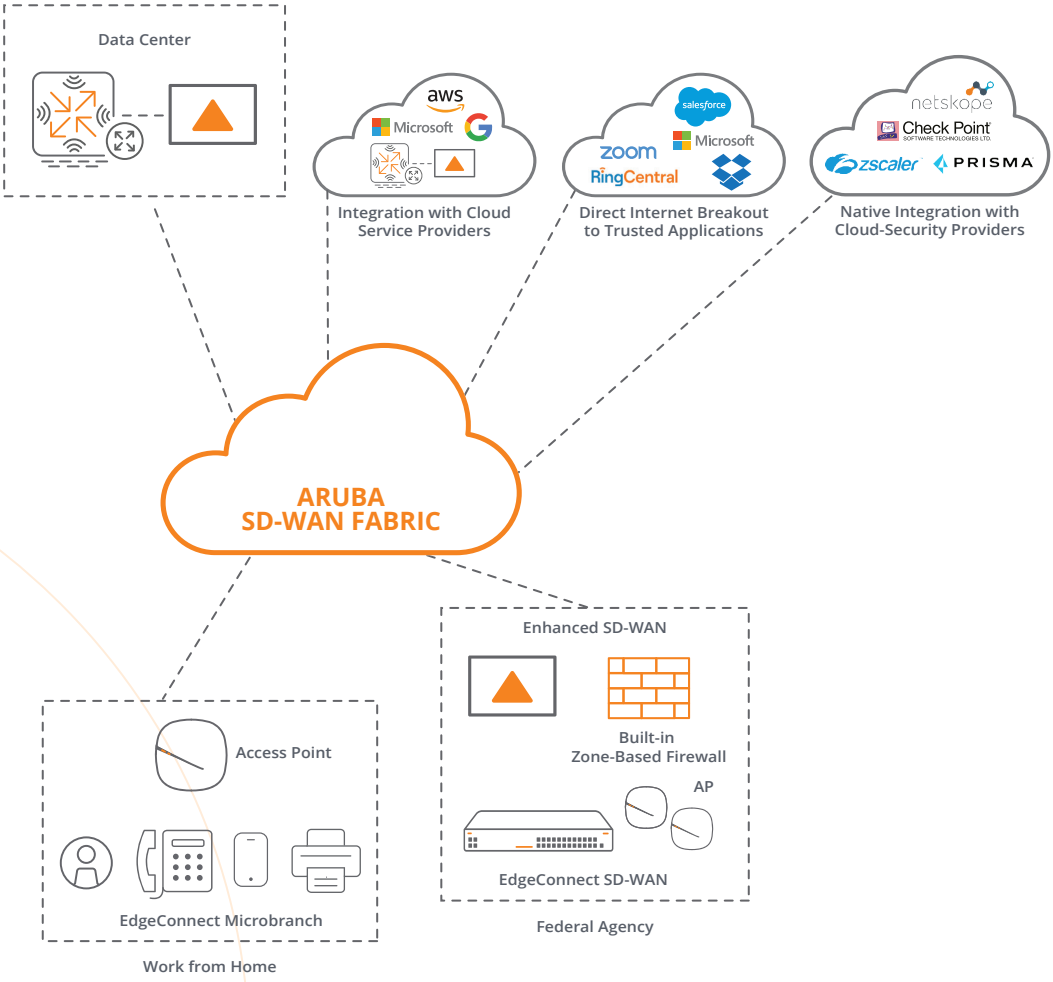

Figure 3: Automate security orchestration based on application type and threat with Aruba EdgeConnect

KEY FEATURES & BENEFITS	
Provide an advanced network experience while reducing costs	
Higher performance and cost reduction	Aruba EdgeConnect SD-WAN combines multiple line protocols including MPLS, internet, 4/5G in a virtual link. It enables the use of efficient and flexible internet and 4/5G lines, instead of rigid and expensive MPLS lines at a lower cost and higher flexibility.
Use in limited bandwidth store locations	With its WAN optimization feature, data is compressed and deduplicated reducing the amount of data to be transferred.
Unified wireless and wired network experience	Completely integrated with Aruba Central that monitors Aruba access points and the wired network, Aruba Unified Infrastructure simplifies and improves IT operations with a cloud-native, uniform console for WLAN, LAN, and SD-WAN across remote locations and corporate data center.
Easily deploy new locations and monitor network activity	
Quick deployments	With zero-touch provisioning, Aruba EdgeConnect is easy to install and doesn't require an experienced IT staff in local agencies. It is centrally orchestrated so that configurations and security policies are easily deployed in minutes to remote locations.
Full visibility	Aruba EdgeConnect provides specific details into SD-WAN health and performance. A health map gives an aggregated view of EdgeConnect appliance status and network health based on configured thresholds for packet loss, latency and jitter. Network operations are centrally monitored bringing a quick response to potential issues.
Cloud ready	Aruba EdgeConnect provides end-to-end connectivity to any of the public cloud providers by extending the SD-WAN fabric and deploying a virtual instance of EdgeConnect in any or all of the four public cloud providers. It avoids backhauling the internet traffic to a headquartered data center providing predictability and application performance.
Improve cybersecurity	
SASE at your own pace	Aruba EdgeConnect provides native integrations and automated orchestration with multiple cloud security vendors. It enables agencies to choose the best-of-breed SASE capabilities including CASB, SWG and ZTNA to build the best SASE architecture with Aruba EdgeConnect as the foundational component.
Micro-segmentation	Aruba EdgeConnect includes a zone-based firewall that segment the traffic into zones. Segmentation improves security and protects data by splitting the network into subnetworks, limiting the spread of cyberattacks and malwares.
Working from home	Aruba EdgeConnect Microbranch seamlessly extends on-campus Zero Trust and Secure Access Services Edge (SASE) security frameworks to the home office. It comprises access points and a suite of SD-WAN services including policy-based routing, tunnel and route orchestration.

ADDITIONAL RESOURCES:

- U.S. Federal Government Networking Solutions
- Six Ways SASE Can Help Federal IT Improve the Nation's Cybersecurity
- Implementing Zero Trust Architecture and Comply-to-Connect Best Practices
- Designing Hyper-aware Civilian Government Facilities

aruba
a Hewlett Packard Enterprise company

SO_FedGovttomodernize-nw-infra_SK_031622 a00121120enw

Contact us at www.arubanetworks.com/contact