HPE aruba networking

Unified SASE in state and local government

Securing and modernizing networks in state and local government with SASE

HPE GreenLake

As we examine the future of state and local government, the COVID-19 pandemic has acted as a catalyst, accelerating the pace of digitalization. Communities are now more determined than ever to uphold efficiency and provide seamless experiences for constituents. Even with limited funds and the urgent demand to enhance cybersecurity, prioritizing the organization's efficiency remains vital.

In this landscape, IT departments face the crucial task of consistently delivering enhanced and secure experiences for citizens, businesses, and fellow government entities. Accelerating digital transformation becomes imperative, necessitating the provision of digital touchpoints, online payment gateways, and the utilization of mobile applications for tasks such as license renewal and traffic updates. Additionally, embracing IoT-enabled infrastructure offers avenues to optimize facility costs, managing systems like HVAC, lighting, security, and energy consumption efficiently across distributed locations.

The state & local government sector is migrating their business applications to the cloud, including back office and management systems, so that the data center is no longer the hub of all the network connections that originate from hundreds of government locations, geographically dispersed. The need for more performance and security is increasing with the growing number of cloud-based applications. Additionally, cyberattacks and possible security breaches have raised concerns over confidentiality and privacy issues, so the modernization of the network has become a key priority in this sector.

With the digital transformation of the state and local government sector, and the need for more security, adopting an advanced SASE (Secure Access Service Edge) solution emerges as a strategic approach to address and overcome these challenges.

HPE Aruba Networking Unified SASE for state and local government

SASE is a transformative framework that combines network security functions with WAN capabilities to support the dynamic, cloud-driven needs of the state and local government sector. The two key components of HPE Aruba Networking unified SASE are EdgeConnect SD-WAN and HPE Aruba Networking SSE (Security Service Edge). Together, these components create a holistic approach to security and networking, aligning with the decentralized nature of today's state and local government organizations. Additionally, a unified approach allows simpler adoption and faster deployment, decreasing payback time.

HPE Aruba Networking EdgeConnect SD-WAN is engineered to deliver secure, high-availability access over virtually any combination of links, including MPLS, internet, 4G/5G and satcom, improving application performance and providing flexibility to accommodate these distributed environments and easily onboard new locations. EdgeConnect SD-WAN also supports multi-cloud networking by intelligently steering traffic to the cloud, eliminating the need to backhaul traffic to the data center and optimizing cloud-based traffic. It integrates a next-generation firewall to provide advanced security capabilities in state and local government sites such as IDS/IPS, DDoS defense and role-based segmentation, ensuring IoT security.

HPE Aruba Networking SSE provides key cloud-delivered security capabilities including ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway) and CASB (Cloud Access Security Broker). ZTNA enables users and authorized third parties to access resources, such as remote agents and contractors. Employees are protected against web-based threats with SWG, and sensitive data hosted in SaaS applications is securely monitored to prevent data loss with CASB.

The adoption of unified SASE from HPE Aruba Networking offers tangible benefits such as a Zero Trust, unified security, threat defense, data protection, improved application performance, centralized management, and ease of deployment.

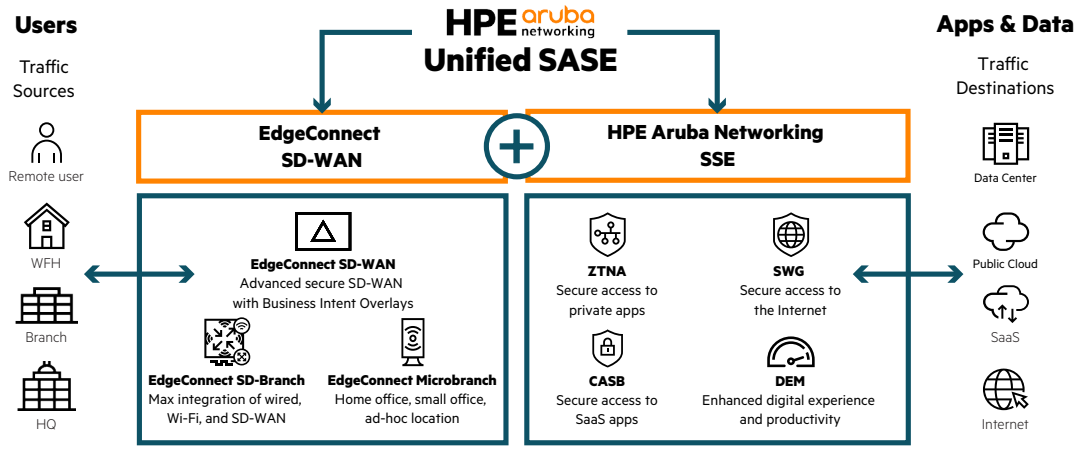

Figure 1. Implement unified SASE in state and local government with HPE Aruba Networking

Advanced security

As state and local government entities are moving to a cloud-centric architecture, security must evolve in parallel to prevent disruptions in customer services. HPE Aruba Networking SSE integrates multiple security functionalities such as ZTNA, SWG and CASB to ensure a consistent security posture.

- **ZTNA (Zero Trust Network Access)** is based on the principle to "never trust, always verify", so that a device connecting to the network is not trusted by default. It enables state and local government entities to replace legacy VPN solutions that are prone to known vulnerabilities. In addition to that, VPNs often do not deliver the experience required for remote agents to perform time-sensitive operations. With ZTNA, user access is limited to only specific applications or microsegments that have been approved for the user, enforcing least-privilege access. With ZTNA, remote agents can connect from anywhere. Third-party contractors can also be easily onboarded in the network with agentless ZTNA.
- **SWG (Secure Web Gateway)** sits between a user and a website to secure and protect state and local government organizations against malicious threats. It performs several security inspections including URL filtering, malicious code detection and web access control, and provides policies that can limit access to adult sites, gambling, dangerous sites, among others. The state and local government sector has been severely affected by ransomware in the past few years and SWG plays a key role in mitigating this risk.
- **CASB (Cloud Access Security Broker)** ensures sensitive data hosted in SaaS applications remains protected. The solution identifies and detects sensitive data in cloud applications and uncovers shadow IT. It monitors user activities in cloud services, identifies potential security risks and policy violations to prevent data loss, while controlling uploads and downloads of SaaS applications.

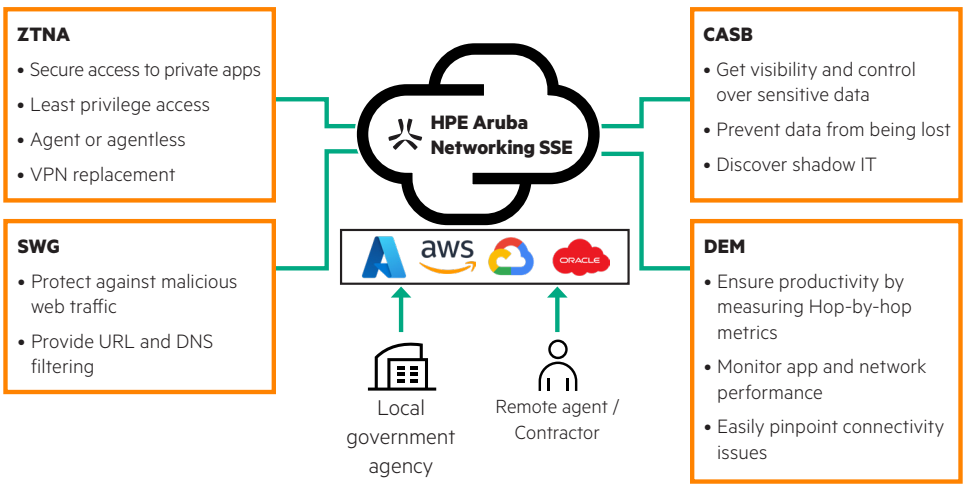

Figure 2. Secure access in state and local government with HPE Aruba Networking SSE

To improve security in state and local government sites, EdgeConnect SD-WAN's embedded, next-generation firewall extends Zero Trust segmentation from edge to cloud, protecting IoT devices, applications, and users. Segmentation is the number one control to orchestrate IoT traffic in a very heterogeneous environment with assets from various vintages, including legacy proprietary protocols. By segmenting the network based on role and identity, users and devices can only connect to their target destinations and applications consistent with policy settings.

When traffic is sent over the Internet, EdgeConnect First-packet iQ™ identifies and classifies applications on the first packet transmitted. This secure Internet breakout feature automates traffic steering to the correct destination based on defined security policies. For example, trusted cloud application traffic such as UCaaS (video conferencing) can be sent directly to the Internet. Other Internet-bound traffic - ERP, CRM, and Data Warehousing - might be redirected to HPE Aruba Networking SSE, or other third-party SSE solution. Untrusted applications can be backhauled to the enterprise data center for further security inspection.

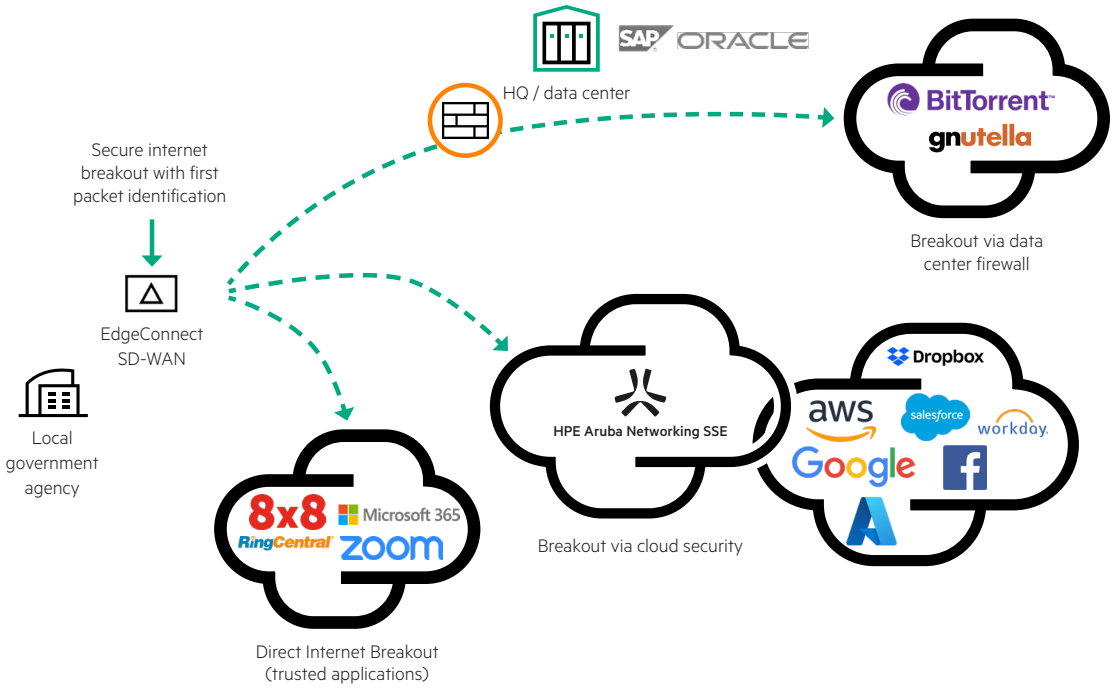

Figure 3. Securely breakout internet traffic based on first packet identification with EdgeConnect SD-WAN

Enhanced network experience

EdgeConnect SD-WAN tunnel bonding combines multiple WAN transport services - including MPLS, Internet broadband, satcom, and 5G - to create a single, higher-bandwidth logical link. Tunnel bonding enables low-cost Internet broadband to deliver equal or better performance as expensive and complex MPLS. The challenge with Internet and cellular links is that they are more prone to packet loss, jitter, and outages which in a normal scenario could impact services that require a more deterministic performance in the state and local government technology stack, such as video transmission or real-time process monitoring.

EdgeConnect SD-WAN Forward Error Correction (FEC) feature automatically reconstructs lost packets, while Packet Order Correction (POC) re-orders any packets that arrive out of sequence at their destination when load-balancing traffic across multiple WAN transport services. Slow links are addressed by the WAN Optimization option which applies TCP protocol acceleration, data deduplication, and compression to speed traffic flow. AppExpress optimizes user experience over multi-cloud networking for business-critical applications by exploiting SD-WAN path diversity and automatically selecting the best path for each application. Digital Experience Monitoring (DEM), part of HPE Aruba Networking SSE, ensures user productivity by measuring metrics, and monitoring app, device, and network performance over the internet.

Simple deployments

The unified SASE solution from HPE Aruba Networking is easy to deploy and accelerates SASE adoption. The platform offers centralized management to monitor and control the entire network infrastructure. This simplifies policy enforcement, monitoring, and troubleshooting. Centralized management includes remote set-up and diagnostics, eliminating the need for local specialized IT staff. This is particularly relevant in the current scenario of skill shortage in the state and local government sector where many sites don't have a dedicated (or just a limited) IT staff.

HPE Aruba Networking SSE is a unified platform where ZTNA, SWG and CASB share a single codebase. All policies are managed from a single user interface, making access control incredibly simple for IT admins. EdgeConnect SD-WAN integrates in one gateway WAN optimization, a router, and a firewall, eliminating the need for three separate appliances.

Summary

A Unified Secure Access Service Edge (SASE) solution is highly beneficial for the state and local government sector as it ensures protection against cyber threats and implements a zero-trust model, safeguarding sensitive data. The scalable architecture allows seamless adaptation to changing network demands, optimizing traffic routing for enhanced performance. Centralized policy management simplifies IT administration, promoting cost-efficiency through the consolidation of security services. In essence, SASE not only strengthens security but also enhances adaptability, network efficiency, and cost-effectiveness in the dynamic landscape of the state and local government sector.

EdgeConnect SD-WAN is the foundation of this approach by virtualizing network links and providing private-line-like performance over the internet and wireless connections, while intelligently steering traffic to the cloud. It improves application performance and enables state and local government organizations to easily integrate new locations without compromising security or performance. Paired with HPE Aruba Networking SSE, the solution forms a unified SASE platform, that is easy to deploy and streamlines operations.

The solution operates on a Zero Trust security model, where every user and device attempting to access the network is thoroughly verified before being granted access. This approach enables secure remote access and prevents unauthorized access. The solution also protects public facilities against malicious threats, helps them regain control over sensitive data hosted in SaaS applications and meet compliance requirements. Centralized management facilitates operations, increases visibility, and enables IT administrators to centrally orchestrate network and security policies. With unified SASE, state and local government organizations can confidently pursue their digital transformation to offer a secure and modern experience to their constituents.

Table 1. Key features and benefits

Enforce Zero Trust, improve security and compliance	
Security Service Edge (SSE)	HPE Aruba Networking SSE provides key security components including ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway) and CASB (Cloud Access Security Broker).
Support for remote work	Enable secure access to applications and data from remote locations. Replace slow and unsecure legacy VPN with ZTNA.
Micro-segment IT and IoT devices	Segment traffic based on role and identity into subnetworks, limiting the spread of cyberattacks and malware in state and local government sites and reducing the attack surface.
Advanced firewall	EdgeConnect SD-WAN next-generation firewall features deep packet inspection, intrusion detection and prevention (IDS/IPS) and DDoS defense to control incoming traffic, and monitor, flag and drop threatening traffic, enabling state and local government organizations to replace legacy firewalls.

Table 1. Key features and benefits

Provide an advanced network experience	
Higher performance and cost reduction	EdgeConnect SD-WAN simultaneously bonds MPLS, Internet, satcom or cellular links for higher performance and lower operating costs. Additionally, by consolidating network and security functions, SASE potentially reduces infrastructure costs.
Network optimization	Overcome the latency effects of WAN by compressing and deduplicating data with WAN optimization. Mitigate the effects of Internet and wireless links that often suffer from packet loss and jitter with Forward Error Correction (FEC).
AppExpress	Optimize user experience by exploiting SD-WAN path diversity and automatically selecting the best path for each application across the web.
Multi-cloud networking	Provide end-to-end connectivity with public clouds and private clouds without the need to backhauling traffic to a data center
Digital Experience Monitoring (DEM)	Give enhanced, in-line visibility and analysis into the interactions, experience, and performance of devices, applications, and networks.
Provide an advanced network experience	
Faster deployments	Centralized management and remote diagnostics speed deployments without specialized IT personnel. Seamlessly integrate new locations and remote sites without compromising security or performance.
Full visibility	Advanced dashboards provide an aggregated view of network health and security based on configured thresholds and alerts
Policy enforcement	HPE Aruba Networking SSE provides a single policy engine to configure ZTNA, SWG and CASB policies in a single interface. EdgeConnect SD-WAN centrally orchestrates security and networking policies facilitating the deployment and management of the solution.

Additional resources

- Unified SASE webpage
- State and Local Government Networking Solutions
- Why State and Local Government Choose HPE Aruba Networking
- Designing Hyper-aware Civilian Government Facilities

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise

SO_UnifiedSASE-StateandLocalGovt_RVK_030824 a00120125enw