INFOBRIEF

How State and Local Government Can Strengthen Edge Access Security and Improve Application Performance in a 'Work from Anywhere' Environment

Overview

As cyberattacks increasingly target remote staff through vulnerabilities in Virtual Private Networks (VPNs), state and local governments need to consider an alternative remote-access strategy that enhances security without degrading digital application performance. Implementing a Secure Access Service Edge (SASE) strengthens remote access security while ensuring application performance.

Challenges with traditional VPNs

A hybrid workforce in state and local government appears to be here to stay. According to a recent survey by the National Association of State Chief Information Officers (NASCIO), 85 percent of respondents expect to retain 'work from home' policies.[1] Government IT teams are also subscribing to more Software-as-a-Service (SaaS) applications to enable employees to access digital government applications and services regardless of where they are physically located. Unfortunately, many SaaS applications are so-called 'shadow IT,' which means they are not managed by the CIO organization and thus there is no visibility into these apps.

At the beginning of the pandemic, CIO teams deployed tens of thousands of VPNs to enable employees to remotely access the applications and services needed to continue serving citizens and constituents. But government IT organizations are now discovering that traditional VPN technologies are lacking in two significant areas:

1. Traditional VPN architectures can create network traffic bottlenecks, which cannot meet the performance requirements of today's multicloud environment, where critical and sensitive services are spread across traditional data centers, on-premises clouds, and commercial clouds.
2. Cyber adversaries are increasingly targeting VPN vulnerabilities to break into networks, more than most other attack avenues.[2]

In addition to the rising frequency of cyberattacks, the average cost of a successful data breach increased from 2020 to 2021. According to a recent Ponemon Institute survey:[3]

- The average cost of a public-sector data breach increased from $1.08 million in 2020 to $1.93 million in 2021.
- The average cost is about 24 percent higher in breaches where remote work was a factor in causing the breach.
- Organizations that had more than 50 percent of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50 percent or less working remotely.

According to the survey, data breach costs were significantly lower for organizations that deployed a more mature security posture that included zero-trust network access, cloud security, artificial intelligence, and automation.

Security continues to be a priority

Given these factors, state and local government CIOs continue to focus on strengthening cybersecurity. For the last several years, 'Cybersecurity and Risk Management' has taken the top spot in the annual State CIO Top 10 Priorities list compiled by NASCIO:[4]

State CIO Top 10 Priorities
2022 Strategies, Policy Issues and Management Processes

1. **Cybersecurity and Risk Management:** governance; budget and resource requirements; security frameworks; data protection; training and awareness; insider threats; third party risk

1 NASCIO, "Driving Digital Acceleration: The 2021 State CIO Survey," October 2021, https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf
2 Jai Vijayan, "Attackers Heavily Targeting VPN Vulnerabilities," Dark Reading, April 21, 2021, https://www.darkreading.com/perimeter/attackers-heavily-targeting-vpn-vulnerabilities-/d/d-id/1340770
3 Study sponsored by IBM Security and research conducted by Ponemon Institute, "Cost of a Data Breach Report 2021," July 2021 https://www.ibm.com/downloads/cas/OJDVQGRY
4 NASCIO, "State CIO Top 10 Priorities," December 8, 2021, https://www.nascio.org/wp-content/uploads/2022/02/NASCIO_StateCIOTopTenPriorities_2022_a.pdf

2. **Digital Government / Digital Services:** framework for digital services; portal; improving and digitizing citizen experience; accessibility; identity management; digital assistants; privacy
3. **Broadband / Wireless Connectivity:** strengthening statewide connectivity; implementing rural broadband expansion; 5G deployment
4. **Cloud Services: cloud strategy;** selection of service and deployment models; scalable and elastic services; governance; service management; security; privacy; procurement
5. **Legacy Modernization:** enhancing, renovating, replacing, legacy platforms and applications; business process improvement
6. **Identity and Access Management:** supporting citizen digital services; workforce access; access control; authentication; credentialing; digital standards
7. **Workforce:** preparing for the future workforce and reimagining the government workforce; transformation of knowledge, skills and experience; more defined roles for IT asset management, business relationship management skills, service integration
8. **Enterprise Architecture:** governance; formulating, refining or implementing an EA strategy; business architecture; business process modeling; statewide EA program management; federal reference models; whole-government enterprise architecture
9. **Data and Information Management:** data governance; data architecture; master data management; open data; sustained access to government data; data portals; enhancing the role of data; information & intelligence, knowledge management; data integration; data management strategy; roles and responsibilities; dataops
10. **Consolidation/Optimization:** centralizing; consolidating services; operations; resources; infrastructure; data centers; communications and marketing "enterprise" thinking

Many CIOs indicated that they have had to accelerate their cyber strategies and investments to quickly pivot to mitigate risk and meet the needs of their workforce and citizens. CIOs point to ransomware and Identity and Access Management (IAM) as top cybersecurity risks and are seeking solutions that go beyond traditional VPN services. But network architecture is becoming more and more complex, and government network defenders must deal with a threat environment that is constantly changing, with sophisticated attackers out to discover and exploit new vulnerabilities.

SASE framework

SASE is a framework that combines networking and security to create a secure bridge between user access and the service edge (that is, the cloud, data center, corporate network, and internet). SASE predicates access on the identity of an individual, device, application, or service. Simply put, the goal of SASE is to provide secure work from anywhere (WFA) user access to all applications and data, no matter where the user is located.

SASE combines Software-Defined Wide Area Network (SD-WAN) and network security functionality via the cloud so that state and local government IT teams can manage security at the edge more effectively. Deploying SASE solutions helps government CIO organizations:

- Deliver optimal user experience
- Mitigate network vulnerabilities
- Increase security
- Reduce IT complexity and costs through a single service

SASE is comprised of six main technologies:

Key security functions and terms that are part of SASE
All operate in the cloud

ZTNA Zero Trust Network Access	Enables users to securely connect (without a VPN) to corporate network or data center resources via access control policies
SWG Secure Web Gateway	Provides user threat prevention via web content/reputation filtering, SSL/TLS decryption, web proxy, and anomaly-based protection
FWaaS Firewall as a Service	NGFW functions (threat prevention, anti-malware, security policy enforcement, DNS security, web content filtering, etc.
CASB Cloud Access Security Broker	Provides proxy between users and SaaS apps, allows/block SaaS apps based on security policies or user behavior
DLP Data Loss Prevention	Scans and blocks sensitive data from being transmitted (emailed, uploaded, etc.) to destinations that do not meet corporate security policies
RBI Remote Brower Isolation	Runs web pages in cloud to check for threats, removes or blocks threats, then renders web page on user's browser

Above terms have overlapping functions based on a vendor's implementation and marketing

SASE capabilities

SASE shifts away from a network traffic flow model in which traffic is forced toward a specific policy enforcement point. Instead, it is structured around an architecture where capabilities are ubiquitous and security controls are applied based on user identity and context. These capabilities are ubiquitous in the sense that they are provisioned in software at points supporting efficient access, either as SaaS in the cloud or in more traditional on-premises capabilities.

SASE benefits

- Zero-Trust Network Access (ZTNA): SASE assumes zero trust whenever a client (user, device, or service) requests access to private assets. SASE requires all clients to be authenticated, authorized, and continuously validated before granting access to private applications and data.
- Multicloud and mobile initiatives: SASE eliminates forced traffic flows around policy enforcement points, which are typically not optimized for the wide range of cloud environments. This allows for cloud migrations to be unconstrained by typical traffic flow bottlenecks. Mobile and remote employee access is streamlined with controls applied at the optimal point of access, with policy tailored to the identity, context, and sensitivity of the application access request.
- Cost and complexity: By eliminating duplicative hardware or software 'stacks' and backhaul communication flows, SASE reduces the cost of introducing next-generation cyber defense capabilities and streamlines the operation of communication networks.
- Network performance: The single-pass parallel processing architecture mitigates the security vulnerabilities that are usually introduced when running multiple software stacks, service chains, or appliances. This reduces latency, improving network and application performance.

Requirements for a successful SASE introduction

Following are important attributes of a successful SASE solution:

- **Genuine multi-tenancy** within the SASE security stack and the control system allows role-based user access to the critical policy-setting control functions.
- **Interoperability** allows integration of capabilities from the primary SASE vendor with third-party solutions. This enables use of SASE as an extension of legacy solutions as well as to support third-party solutions that address any gaps in the primary SASE vendor's capabilities.
- **Single software stack** is key if SD-WAN is deployed. The SASE solution's cloud security services should be combined with their SD-WAN capabilities in a single software stack to minimize operational complexity and avoid potential software incompatibilities as well as maintenance or upgrade problems.

Additional considerations for a successful launch include:

- Setting clear objectives when piloting SASE—identifying specific goals for the SASE pilot with respect to security capabilities, integration, and performance.
- Evaluating how the SASE implementation plan will support ZTNA. One of the biggest potential benefits of SASE is it offers a clear path to introducing ZTNA into the network. It is important that the SASE solution supports specific ZTNA objectives and plans.
- Looking at SASE beyond the cloud: As important as SASE will be to supporting cloud migration objectives, the SASE implementation should also address on-premises capabilities to maximize the return on the SASE investment.

SASE components

1. **Self-management portal**
   Visibility, policies, and access control for users and apps
2. **SASE cloud gateways**
   Securely connect to enterprise network and SaaS apps
   Provides SASE security functions to protect users and apps
3. **Secure access client for end-user devices**
   Smartphones, tablets, laptops, and desktops