INFOBRIEF

Strengthen Cybersecurity and Improve Application Performance in the Evolving Enterprise 'Work from Anywhere' Environment

As cyberattacks increasingly target remote staff through vulnerabilities in Virtual Private Networks (VPNs), enterprise customers need to consider an alternative remote-access strategy that enhances security without degrading digital application performance. Implementing a Secure Service Edge (SSE) addresses strengthening remote access security while ensuring application performance.

Challenges with traditional VPNs

A hybrid workforce in most industries appears to be here to stay. According to a recent survey conducted by researchers at Ladders, 25 percent of all professional jobs in North America will be remote by the end of 2022, and the percentage will grow through 2023[1]. Enterprise IT teams are also subscribing to more Software-as-a-Service (SaaS) applications to enable employees to access digital 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 potential security vulnerabilities associated with these apps. At the beginning of the pandemic, CIO teams deployed thousands of VPNs to enable employees to remotely access the applications and services needed to continue serving citizens and constituents.

But 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 often than 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 data breach increased from $3.86 million in 2020 to $4.24 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, enterprises continue to focus on strengthening cybersecurity. According to a recent report by Tata Communications, 49 percent of respondents indicated that cybersecurity is the topmost priority for their organization.[4]

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

1 Ladders, "25% of all professional jobs in North America will be remote by end of next year", 7 December 2021, https://www.theladders.com/press/25-of-all-professional-jobs-in-north-america-will-be-remote-by-end-of-next-year
2 Verizon, "2021 Data Breach Investigations Report", 2021, https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
3 2021 Cost of a Data Breach Report, Sponsored by IBM Security, Conducted by the Ponemon Institute https://www.ibm.com/account/reg/us-en/signup?formid=urx-50915
4 Help Net Security, "Cybersecurity is top priority for enterprises as they shift to digital-first operating models", 18 August 2021, https://www.helpnetsecurity.com/2021/08/18/cybersecurity-top-priority-enterprises

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.

SSE framework

SSE is a collection of security functions that create a secure bridge between user access and the service edge—that is, the cloud, data center, corporate network, and internet. SSE predicates access on the identity of an individual, device, application, or service. Simply put, the goal of SSE is to provide secure Work-From-Anywhere (WFA) user access to all applications and data, no matter where the user is located. SSE provides cybersecurity functionality via the cloud so enterprise IT teams can manage security more effectively.

Deploying SSE solutions helps enterprise CIO organizations:

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

SSE is comprised of six main technologies—key security functions and terms that are part of SSE:

- Zero-Trust Network Access (ZTNA) – Enables users to securely connect (without a VPN) to corporate network or data center resources via access control policies
- Secure Web Gateway (SWG) ¬– Provides user threat prevention via web content/reputation filtering, Secure Sockets Layer (SSL)/Transport Layer Security(TLS) decryption, web proxy, and anomaly-based protection
- Firewall as a Service (FWaaS) – Next-Generation Firewall (NGFW) functions such as threat prevention, antimalware, security policy enforcement, Domain Name System (DNS) security, web-content filtering, etc.
- Cloud Access Security Broker (CASB) – Provides proxy between users and SaaS apps, allows/block SaaS apps based on security policies or user behavior
- Data Loss Prevention (DLP) – Scans and blocks sensitive data from being transmitted (emailed, uploaded, etc.) to destinations that do not meet corporate security policies

Requirements for a successful SSE introduction

Following are important attributes of a successful SSE solution:

- **Genuine multi-tenancy** within the SSE 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 SSE vendor with third-party solutions. This enables use of SSE as an extension of legacy solutions as well as to support third-party solutions that address any gaps in the primary SSE vendor's capabilities.

Additional considerations for a successful launch include:

- Setting clear objectives when piloting SSE and identifying specific goals for the SSE pilot with respect to security capabilities, integration, and performance.
- Evaluating how the SSE implementation plan will support ZTNA. One of the biggest potential benefits of SSE is it offers a clear path to introducing ZTNA into the network. It is important that the SSE solution supports specific ZTNA objectives and plans.

SSE components

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