TATA COMMUNICATIONS

TATA

DELIVERING RESILIENT NETWORK SECURITY AT THE EDGE THROUGH SPAED

TRANSFORMATIVE MOMENTUM: SCALING UP IN INDIA'S DYNAMIC FINANCIAL LANDSCAPE

The Indian financial landscape is undergoing a systemic and rapid transformation. The widespread adoption of digital technologies and elevated consumer expectations is propelling this transformation. In response, financial institutions are engaging in strategic expansions, broadening their service portfolios and extending their geographic footprints, establishing branches and ATMs to serve customers even in remote areas.

Traditional banks have embraced a digital renaissance, racing to offer a comprehensive suite of digital services to an increasingly digital-first customer base. At the same time, the FinTech ecosystem is riding the crest of a disruptive wave, with startups introducing innovative solutions that challenge and reshape conventional norms, fuelling the momentum of this financial evolution.

This wave of digital transformation has also been boosted by the government's proactive efforts towards financial inclusion, identity and technology in banking. Notably, the rise of zero-balance accounts has taken formal banking to every corner of the country, transcending the traditional urban centres.

As a result, this transformative wave focuses on a holistic approach that prioritises technological advancements, the fortification of data security measures, and the creation of tailored financial products to address specific demands in a diversifying market.

At the heart of this evolutionary journey of innovation and resilience, financial institutions require robust network solutions and secure frameworks to navigate the intricacies of a digitised, interconnected financial ecosystem.

NETWORK CHALLENGES CONFRONTING FINANCIAL INSTITUTIONS

While digital and network transformation are driven by the need for speed, flexibility, security, and affordability, the critical intersection of security and agility is a business imperative.

In the digital transformation era, traditional network architectures are no longer fit for purpose. The dispersion of critical financial services across multiple clouds and service providers amplifies these limitations. This dispersion poses a risk of bottlenecks in network performance, particularly at branch locations, which are crucial for banking and NBFC operations, necessitating a robust security infrastructure

The challenges faced by financial institutions are below:

Unreliable performance: The challenge of unreliable network connectivity is particularly pronounced in branches, especially in remote areas where the absence of a reliable underlay poses substantial operational hurdles. In these locations, the need for a dependable network infrastructure is underscored by the critical use of financial transactions – like direct benefit transfers, pensions, financial support for farmers and other lower-income demographic groups. Furthermore, additional complexity arises when accessing security applications, requiring the establishment of multiple VPN connections to the cloud or data centre. This amplifies the network's vulnerability and introduces potential points of failure, impacting the overall reliability and efficiency of financial operations..

Slow and complicated deployments: Deploying private connectivity solutions, such as MPLS or SDWAN-based options, becomes a bottleneck, even for smaller branches and ATMs. The extended lead times for rollout pose a significant threat to the rapid scalability that financial institutions aim to achieve in a dynamic market. Beyond time considerations, the intricacy involved in the configuration and installation processes adds layers of complexity, contributing to significant overheads. This not only hampers the agility of financial institutions but also impedes their ability to keep pace with customer needs and technological advancements.

Insecure connectivity: Ensuring secure connectivity is paramount for all branches as it is a bulwark against unauthorised access from untrusted networks and aligns the institutions with regulatory norms set by governing bodies and agencies. The confidential nature of financial data requires institutions to safeguard against cyber threats and potential data breaches, emphasising the need for comprehensive and effective security measures across all network connections.

High total cost of ownership: For small and medium-sized financial enterprises, creating and maintaining private networks present a formidable financial challenge. Relying on solutions such as private WANs using MPLS or comprehensive SDWAN solutions proves to be financially burdensome for such institutions. The high total cost of ownership encompasses not only the initial infrastructure investment but also ongoing operational expenses, including maintenance, upgrades, and potential security enhancements. This financial burden restricts the capabilities of these institutions, limiting their capacity to adopt and sustain cutting-edge networking solutions that are essential for staying competitive in a rapidly evolving market landscape.

INTRODUCING SPAED AS AN AFFORDABLE, RESILIENT AND SECURE SOLUTION

Figure 1 illustrates an overview of the SPAED (Secure Private Access Edge Device) solution. This plug-and-play 'branch-in-a-box' solution involves deploying compact CPE devices at branches and site locations, ensuring secure application and web access with dependable network connectivity. As a fully managed solution, it can be remotely monitored for efficient management and oversight.

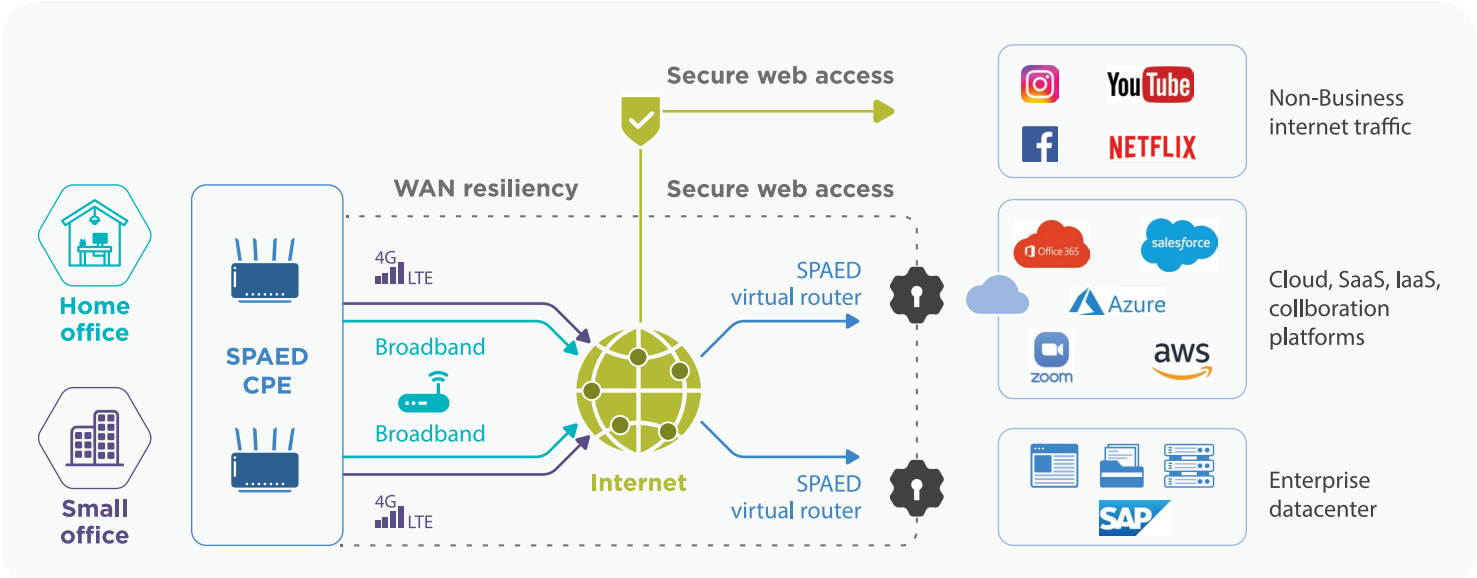

Figure 1: Overview of the SPAED solution

KEY FEATURES OF THE SPAED SOLUTION

Plug-and-Play solution

SPAED devices boast **rapid deployment cycles** and feature **zero-touch provisioning**, ensuring that bulk configurations can be efficiently executed remotely, streamlining the setup process for enhanced convenience and operational efficiency.

Multiple WAN support

The SPAED solution offers versatile support for various underlay WAN connectivity options such as **broadband, ILL,** etc. SPAED CPE devices feature **dual LTE modules** with failover in regions lacking reliable underlay. SIM cards can be inserted into these modules, ensuring dependable network connectivity even in **remote areas.**

Resilient network connectivity

The SPAED solution is equipped with a sophisticated **sub-second auto-failover** feature, offering a seamless transition in case of a primary link failure. This ensures uninterrupted connectivity as the device swiftly switches to the backup link, mitigating potential packet loss. This level of reliability is particularly crucial in maintaining consistent network performance and availability.

Moreover, the SPAED device provides the flexibility of operating in **load-balancing** mode. This configuration optimises traffic across multiple WAN links based on a predefined ratio. This load-balancing capability enhances network efficiency by strategically distributing data traffic, preventing congestion on any single link and optimising overall network performance. Whether safeguarding against link failures or optimising traffic distribution, the SPAED solution offers a robust and adaptable approach to meet diverse connectivity needs.

Secure connectivity

The SPAED CPE devices are equipped with **Layer 3 firewall capabilities**, offering comprehensive security features such as URL filtering, DDoS attack prevention, and SYN flood attack prevention. These capabilities enhance the overall cybersecurity posture of the network, ensuring robust protection against a range of potential threats.

Furthermore, the solution introduces **split tunnel capabilities,** establishing Wireguard/IPSEC tunnels between the SPAED device and the destination IP. This feature ensures that traffic is encrypted between the source and destination, adding an extra layer of security.

There is also an option to connect to the Tata Communications-hosted Global Secure Gateway Cloud. This connection enables access to **Unified Threat Management** capabilities, requiring a SWG license. These capabilities encompass Next-Gen firewall functionalities, Quality of Service (QoS), deep packet inspection, and malware intrusion detection. Integrating these features provides a holistic and proactive approach to network security, safeguarding against evolving cyber threats and ensuring the integrity and confidentiality of data transmissions within the network.

End-to-end managed solution

SPAED solution features a **sophisticated real-time dashboard,** presenting device and link status and detailed data consumption metrics. This dashboard provides customers with immediate, comprehensive insights, enabling efficient monitoring of device performance and network efficiency. Users can make informed decisions and optimise network management based on up-to-the-minute information.

Various Day 0 and Day 1 processes like hardware deployment and configuration, platform management and maintenance, change management and incident management would be provided as managed services as per the Service Level Agreements, ensuring quick deployments and reliable internet connectivity.

Optimal TCO

The SPAED solution removes the need for expensive on-premise equipment, offering cost savings between **2x-3.5x** times compared to current connectivity solutions. SPAED allows customers to choose between a capital expenditure (CapEx) or operational expenditure (OpEx) pricing model based on their specific requirements.

SPAED AS AN INTEGRATED SOLUTION FOR FINANCIAL INSTITUTIONS

The secure connectivity solution offered by our 'branch-in-a-box' system is highly effective in establishing reliable connections and seamlessly integrating a variety of applications used by financial institutions. The illustrative depiction in Figure 2 outlines a standard topology tailored for the financial sector. This comprehensive solution facilitates the smooth integration of diverse endpoint devices at branch sites, encompassing end-user laptops, printers, ATMs, and CCTV cameras.

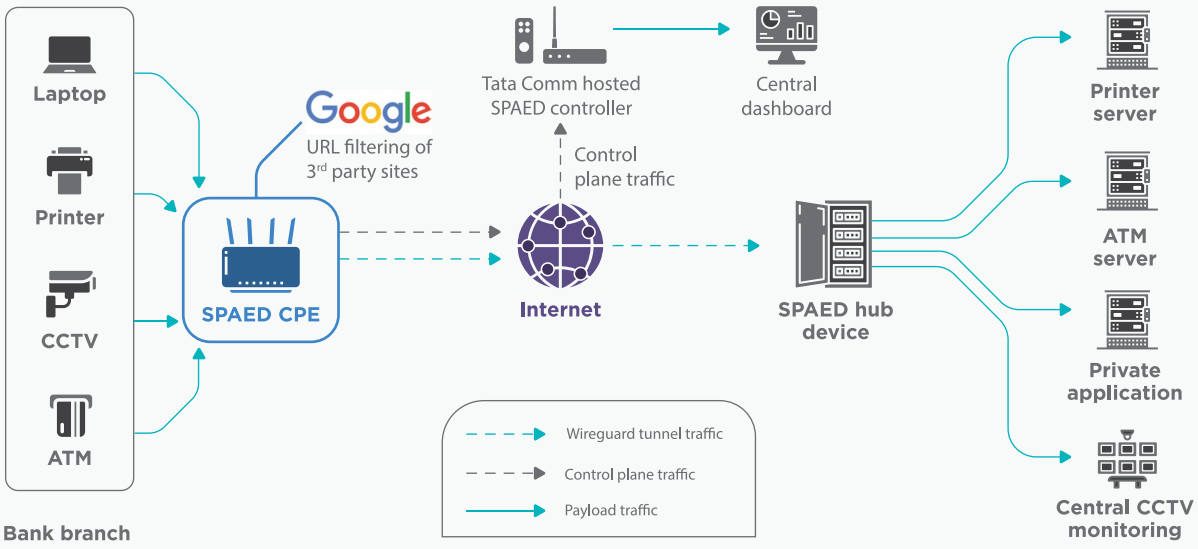

Figure 2: Branch-in-a-box solution for the BFSI sector

The traffic originating from printers and ATMs is securely and efficiently channelled through dedicated tunnels to servers located at central hub locations. Simultaneously, the CCTV camera feeds are reliably transmitted to a central location, allowing for centralised monitoring as needed. This approach ensures that CCTV feeds are accessible and viewable centrally, contributing to enhanced security and surveillance capabilities.

Furthermore, the solution empowers users at branch sites to securely access private applications hosted at the central data centre. The SPAED solution utilises URL filtering to maintain a controlled and secure environment. This restricts users from accessing third-party applications. This feature enhances the overall security posture of the network.

For efficient management and oversight, the SPAED solution has a real-time monitoring feature that allows users to view the status of devices and links centrally through an intuitive dashboard. This centralised dashboard offers a comprehensive view of the network's health, enabling prompt responses to any issues and ensuring a robust and secure connectivity infrastructure for financial institutions.

IN CONCLUSION

Tata Communications SPAED solution is a pivotal asset in providing financial institutions with a comprehensive, fully managed, and resilient connectivity solution. This in-house solution ensures robust connectivity and is cost-effective while meeting the stringent standards for security and network resilience. With its capability for rapid deployment cycles, the SPAED solution empowers financial institutions to exhibit agility in scaling up operations. This strategic advantage enhances operational efficiency and allows institutions to quickly adapt to evolving market dynamics. In essence, Tata Communications SPAED solution emerges as a cornerstone in fortifying the connectivity infrastructure of financial institutions, providing them with the necessary tools to navigate a dynamic and demanding landscape.

TATA COMMUNICATIONS

TATA

ABOUT TATA COMMUNICATIONS

Tata Communications is a leading global digital ecosystem enabler that powers today's fast-growing digital economy. The company's customers represent 300 of the Fortune 500 whose digital transformation journeys are enabled by its portfolio of integrated, globally managed service that deliver local customer experiences. Though its network, cloud, mobility, Internet of Things (IoT), collaboration and security services, Tata Communications carries around 30 per cent of the world's internet routes. It connects businesses to 60 percent of the world's cloud giants and four out of four-five mobile subscribers.

Its global reach underpins the company's capabilities. It owns the world's largest wholly-owned subsea fiber backbone and operates a Tier-1 IP network connecting to more than 240 countries and territories. Tata Communications globally delivers a superior, always-on experience. We maintain a Leader position in the Gartner Magic Quadrant. Plus, reassuringly, we are a Cisco' Gold Standard UC Experience' partner globally. We have your business covered.

For more information, visit us at www.tatacommunications.com

CONTACT US

©2023 Tata Communications. All Rights Reserved. TATA COMMUNICATIONS and TATA are registered trademarks of Tata Sons Limited in certain countries.