TENEO
OPENING MINDS

SD-WAN REGIONAL DESIGN WITH SASE ARCHITECTURE

Overcoming Connectivity, Performance and Security Issues in Regions Like China

SD-WAN Regional Design with SASE Architecture

Author: Roumen Doukov, Lead Global Solutions Architect, Teneo

Overcoming Connectivity, Performance and Security Issues in Regions Like China

Many enterprises that have branches in remote and poorly connected regions, such as China, experience significant connectivity and performance issues when accessing services and data hosted outside of those locations. For example, from a bandwidth and security perspective, China's local internet heavily restricts communication outside of the country, causing severe problems with secure connectivity to applications in data centers or cloud locations in other regions.

The Great Firewall of China is the combination of legislative actions and technologies enforced by the People's Republic of China to regulate the internet domestically. Its role in internet censorship in China is to block access to selected foreign websites and to slow down cross-border internet traffic (Wikipedia). Performance issues for international traffic are not exactly related to the Great Firewall of China but to the different internet quality links.

Implementing a modern SASE (Secure Access Service Edge) architecture from these branches requires the traffic to go via Cloud Security Providers (CSPs), such as Zscaler or Palo Alto Networks Prisma. However, these services do not adequately address performance problems. That's because branch users send the traffic via the CSP node in China, resulting in the same performance and connectivity issues after the CSP puts the traffic back on the internet.

In the case of Zscaler, the other problem is that China's ZEN nodes (Zscaler Public Access Points) do not have good connections to the international internet. Therefore, even if a site uses premium or extra-premium internet to connect to the China Zscaler and then tries to connect to the international internet, this traffic will often experience high packet loss and congestion issues.

These same connectivity issues also affect SaaS. SD-WAN vendors cannot 'spin up' virtual machines (VMs) in SaaS clouds, and some SaaS solutions are only in a single cloud or a few locations. They also have other restrictive requirements, such as a maximum of 150 milliseconds Round Trip Time (RTT). Bearing in mind that RTT from China/Africa/Australia to Europe alone is well over 200 milliseconds, how could an office in China, or South Africa, for example, connect to SaaS applications based in Europe or the United States?

Although several solutions can address connectivity issues, the performance issues will remain.

These connectivity solution options include:

#	Service Provider	Pros	Cons
1	MPLS provider	• Guaranteed connectivity	• Low performance • Needed at each branch, so expensive to implement • Low bandwidth • Very slow to deploy
2	Microsoft Azure vWAN	• Guaranteed connectivity • Fast to deploy	• Low performance, similar to MPLS • Manual IPSec (Internet Protocol Security) tunnels needed from each branch • Low/moderate bandwidth • Expensive
3	Cloud-based SD-WAN (e.g. CATO, Alkira)	• Guaranteed connectivity • Fast to deploy • Some performance improvements	• Moderate bandwidth • Expensive

The above alternative solutions like Microsoft vWAN and Alkira still use legacy MPLS, internet, or private P2P (Peer to Peer) links. Therefore they cannot deliver significant performance enhancements. CATO has its own SD-WAN type 'backbone', but it does not support WAN Optimization in terms of compression. Therefore the performance enhancements are minimal.

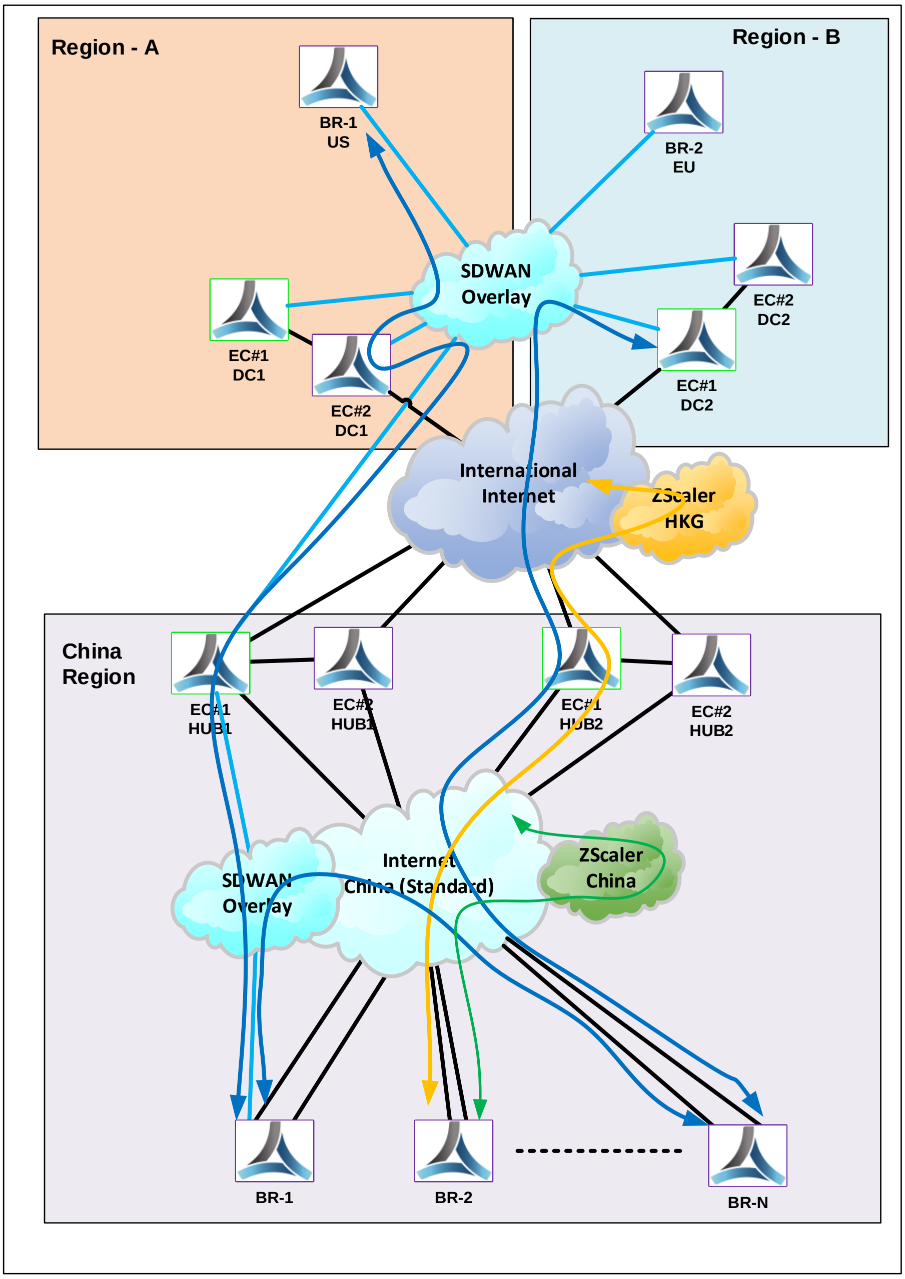
A regional design, however, takes full advantage of the different link qualities and eliminates the performance issues relating to the Great Firewall.

Solution based on Aruba/Silver Peak Regional Design with SASE architecture

At Teneo, we've created an alternative service based on an Aruba/Silver Peak Regional Design with a SASE architecture. This solution brings numerous connectivity and performance improvements, including enhancements to security, connectivity and network, SaaS and remote user connectivity optimization, and cloud cost reduction.

The complete solution is depicted in the below diagram:

Figure #1: SD-WAN Regional Design and traffic Paths



Solution Overview

1. Each region has several hubs, which can incorporate specific sites or data centers with communication between the areas implemented via the hubs

2. Each region will also provide separate treatment of business applications, which in Aruba/Silver Peak EdgeConnect terms means the Business Intent Overlays (BIOs) and the IPSec SD-WAN topology are region-specific.

3. Internet browsing can be done via the CSP:

    a. For example, with Zscaler, each branch's EdgeConnect in China builds an IPSec tunnel automatically configured via the Aruba Unity Orchestrator API to the closest ZEN node(s) (Zscaler Enforcement Nodes) in China for local internet sites only. See the green path from BR-2 on the above diagram.

    b. Each branch's EdgeConnect in China has SD-WAN connectivity via the hubs to the closest International ZEN nodes (such as Hong Kong or Singapore) for secure browsing of all international internet sites. See the yellow path from BR-2 on the above diagram.

    c. This 'split' is a design based on Aruba's BIO technology and delivers a SASE (Secure Access Service Edge) architecture to improve security, connectivity, and performance.

4. China branch connectivity to corporate data centers and applications (outside of China) are delivered via the hubs utilizing the SD-WAN Fabric and supporting all SD-WAN features. This includes FEC (Forward Error Correction) for packet loss mitigation, performance-aware routing based on link bonding policies, redundancy, and WAN Optimization (Data Duplication and Application Acceleration). The blue path in the diagram below represents China branch connectivity to the data center or another branch (in or outside the China region).

5. Connectivity and Performance improvements:

Testing based on 30 days of live traffic monitoring by Teneo on an enterprise network with 18 sites in China, connecting to services in London, UK, produced the following results:

		Before	After (using the regional design)	Notes
1	Delay (China to a data center in London)	200+ ms	100+ ms	The delay reduced by almost 50%
2	Packet loss (China to a data center in London)	Constantly between 1% - 6% and more than a few spikes per day, up to 50% packet loss	A few spikes <1% pkt loss	Path conditioning FEC technology completely mitigate packet loss
3	Jitter (China to a data center in London)	Constantly between 1 ms-6 ms and more than a few spikes per day, up to 40 ms	0 ms	Path conditioning removed Jitter completely
4	WAN Optimization	N/A	Hub to hub WAN Optimization can deliver 3X-5X performance enhancement to data transfer times	TCP Optimization together with data compression
5	SaaS Optimization		SaaS Optimization using hub to hub SD-WAN and WAN Optimization delivers 3X - 5X performance enhancement	Each hub in a global region can become a SaaS gateway, therefore the SaaS traffic will be using SD-WAN from the branch to the hub

6. Security Enhancements:
    a. The above design is fully compliant with the SASE architecture providing significant performance improvements supporting many CSP's (e.g. Zscaler, Palo Alto Networks Global Protect/Prisma, Akamai, CheckPoint).

7. Connectivity and Network Enhancements:
    a. BIOs are 'regional', supporting full mesh, partly mesh, or hub and spoke topologies
    b. The number of tunnels is reduced significantly
    c. The regions can be 'segmented' (e.g. Virtual Router Functionality (VRF's)) to provide a network and application level of separation. For example, a payment system can be 'placed' in a completely separate segment to other applications (totally isolated) and will not be accessible for any regions.

8. Performance Enhancements:
    a. Like a few other SD-WAN vendors, Aruba/Silver Peak has full support for TCP Optimization. This technique will improve file transfer time by 50-100% for sites with long delays (>100 ms).
    b. Aruba EdgeConnect is one of only a few SD-WAN vendors that support WAN Optimization (Data compression – Aruba Boost). Using WAN Optimization, most of the traffic can be compressed (some up to 95%), reducing the actual file transfer size. For example, instead of sending a file size of 20MB, 2x hubs can exchange only 1MB (95% reduction) and performance increases significantly by 5-10X. The benefits are clear:
        i. 10 x reduction in data transfer time
        ii. Significantly reduces link bandwidth utilization
        iii. If the data needs to be transferred to the public cloud (AWS, Azure), this will significantly reduce the charges

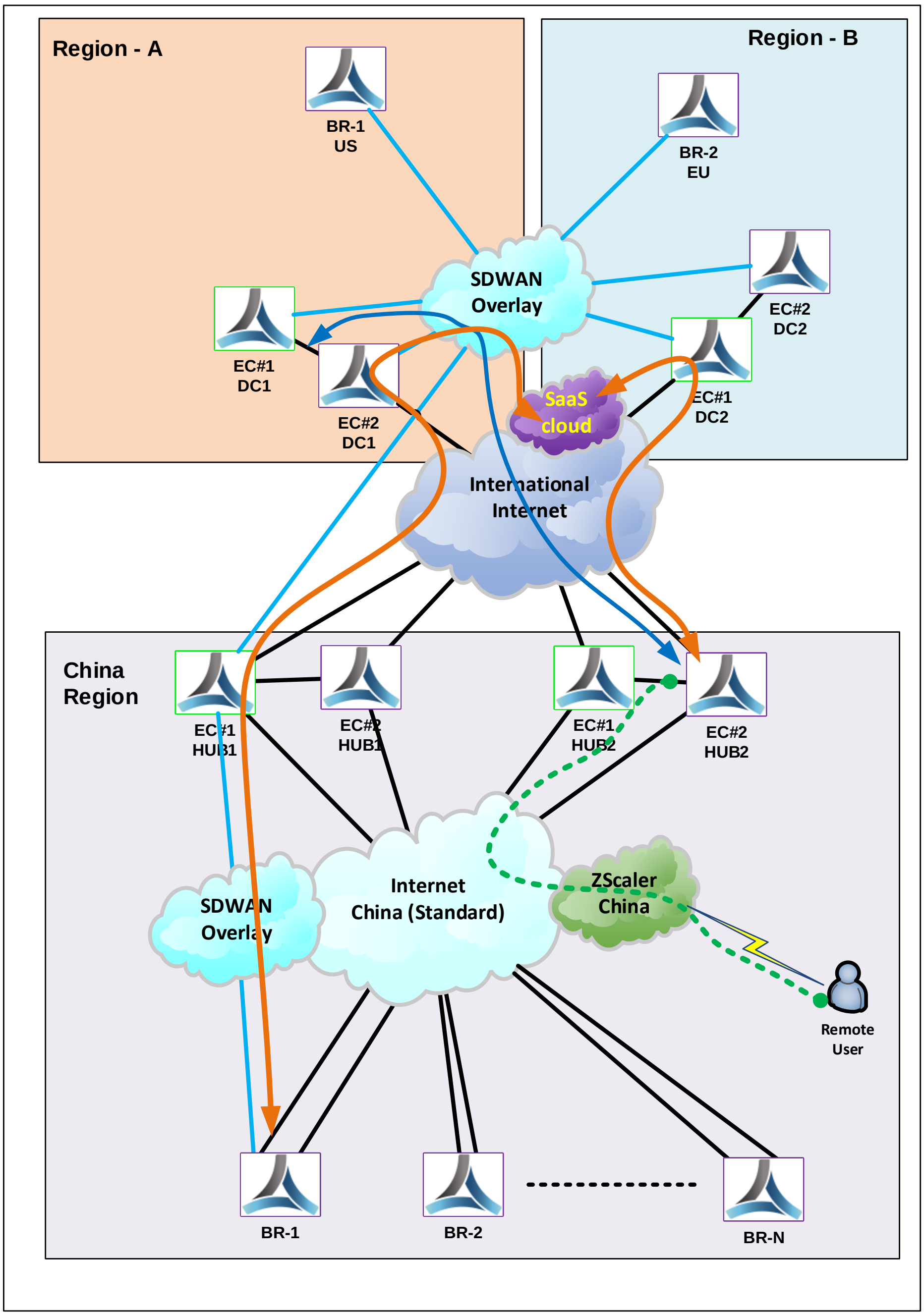
9. SaaS Optimization
    a. To improve this, most of the SD-WAN vendors can nominate some of the SD-WAN nodes to become a SaaS gateway and can then provide alternative paths to the SaaS application. This is also known as SaaS path or routing optimization. While this won't improve the performance, it will guarantee 'best case' performance most of the time. For the most part, this is where SD-WAN vendors' SaaS Optimization solutions end
    b. However, the Aruba EdgeConnect SD-WAN solution goes further. Its SaaS Optimization solution supports full WAN Optimization on the path from the branch to the SaaS gateway. This means that the Aruba EdgeConnect SaaS Optimization

solution can perform path (routing) optimization as well as WAN Optimization (TCP Optimization and compression), with both features combining to reduce the RTT and increasing performance by 2-5X. Path optimization on its own, which is what most other SD-WAN vendors offer, cannot deliver true end to end SaaS Optimization

10. Remote User Connectivity Optimization (Work From Anywhere – WFA)
    a. Remote users in China connecting to the CSP (Zscaler) via the internet establish a secure tunnel. Traffic inspection will then be securely terminated to the China hub (Zscaler Private Access – ZPA).
    b. Once in a hub, the traffic path can be fully optimized. Security is sent to the company data center or public cloud region or can benefit from full SaaS Optimization
    c. Therefore, a WFA user can achieve a 2-5 X performance increase for all the data center/ cloud and SaaS-type applications

11. Cloud cost reduction:
    a. Public cloud integration with SD-WAN covers each of the public cloud Availability Zones (AZs), just like another branch. Therefore traffic from the SD-WAN branches and WFA users can be fully optimized and, as well as benefiting from significant performance improvements, can achieve significant cost reductions – at approximately 70%

Figure #2: SaaS and WFA User Traffic Optimization



Could such a regional SD-WAN design with a SASE architecture help you to overcome connectivity, performance and security issues in regions like China, too?

For more information about Teneo's SASE and SD-WAN services, visit our services page, or use this meeting link to arrange a suitable time to talk.