Rethinking the Wide Area Network for the Cloud Era

Public sector IT departments are challenged with the complexity of managing the performance of an increasing number of dynamic workloads and cloud-based applications in the most secure manner possible. To make changes in the wide area network (WAN) on the fly to address increased usage or improve performance, you need a software-defined WAN (SD-WAN) solution that is built on automation and that simplifies management.

Over the years, public sector IT departments have settled into a common hub-and-spoke and WAN architecture based on supporting users in the branches with applications hosted in a centralized data center. In this model, all traffic moved between the branches and the data center, and even internet-destined traffic, came back to the central location.

That model is being challenged today. Most customers are experiencing a large growth in use of digital innovations, such as cloud-based applications and the Internet of Things (IoT), that are overwhelming WANs. Almost all public sector entities are already adopting one or more public cloud software-as-a-service (SaaS) offerings, and are either developing or have executed on a strategy to increase their use of the public cloud, both infrastructure as a service (IaaS) and SaaS. The number of software applications is also continually increasing, which adds demand to the network and the bandwidth it must provide. Conversely, as public cloud adoption and the number of applications continue to grow, so do the number of security threats.

Agencies using multiple cloud providers with multiple remote sites need to make sure these services’ performance and security are acceptable. Private multiprotocol label switching (MPLS) or metro ethernet circuits are a common method for providing reliable WAN connectivity, but they can cost up to 90% more than broadband Internet connectivity.
In the past, changing a remote location’s connectivity method to broadband Internet was difficult due to security requirements and the lack of end-to-end quality of service (QoS) to ensure performance for end-user applications. Growing the WAN link capacity to support cloud applications increases the strain on the core network and introduces suboptimal performance, as cloud-destined traffic must twice traverse the entire hub-and-spoke architecture.

In the public sector market, challenges around the WAN architecture can also vary based on what vertical you’re in. For example:

**K-12 (Cost savings)**

Most K-12 networks are configured in a hub-and-spoke fashion where schools in a district aggregate into a larger, regional hub. All schools are trying to provide broadband access that meets the recommendations of 1Gbps per 1000 students, and all the infrastructure that goes along with it. As cloud adoption continues to grow, further financial strain is added to the full suite of IT, and driving simplicity for automation and lower circuit costs is a primary concern.

**Higher education (cost savings and simplicity)**

Higher education institutions are establishing satellite campuses as part of their growth strategy as their populations gain increased mobility. Cloud adoption is continuing to grow, as part of an effort to reduce capital and operating expenses. With all that going on, for universities to remain competitive they need to provide a great user experience while lowering IT operating costs.

**State, local, and federal government (security and simplicity of management)**

Most government agencies are slower to adopt SaaS and IaaS cloud offerings than commercial customers. Given their focus on security and data privacy, it makes sense to see slower adoption in the cloud. For the same reasons, we also see a much slower adoption of direct internet access in the government space. Of course, private WAN links are expensive and difficult to grow. Government entities strive to lower operation costs while maintaining their security posture.
The value of SD-WAN

As we highlighted in the challenges above, WAN architectures are being impacted in multiple ways, and next generation WAN designs need to shift toward meeting those application-aware transport requirements, reduction in circuit costs, and overall simplification of how the WAN infrastructure is designed.

SD-WAN is clearly a term that can mean a lot of things to different people. However, there are several challenges that exist in traditional WAN designs that SD-WAN addresses. Key areas SD-WAN is targeting for next generation WAN design include:

• Major cost reduction relating to WAN, including circuit cost, operational expenditure, and the ability to leverage lower-cost bandwidth services, through transport optimization.

• Simplified deployment and installation capabilities through optimized zero-touch provisioning for remote locations, centralized deployment of policy and management, with the ability to leverage the most basic transport such as Internet/broadband or even 4G/LTE.

• Intelligent traffic steering based on application awareness of the application’s locations (on-premise, public cloud like Amazon Web Services (AWS) and Azure, or SaaS) and SLA requirements needed over a specific WAN link, including application brownout mitigation.

• Provide secure, zero-trust, authenticated transport, topology-driven network-wide segmentation (L3 VPN segmentation), and the ability to offer insertion of security services into the traffic flow, including firewalls, IDS, as well as third-party solutions.

• Provide the ability to extend the SD-WAN encrypted fabric into public cloud providers (such as AWS and Azure) by automatically instantiating virtual SD-WAN endpoints in the enterprise customer’s cloud region.

• Advanced analytics for both real-time insight to the WAN fabric’s behavior, as well as future-looking “what-if” analysis for billing, capacity planning, all cloud managed.

The advantages for SD-WAN are compelling for any commercial or public sector customer. The following section will dig deeper into these capabilities, specifically Cisco SD-WAN, and provide use cases and short-term areas that SD-WAN’s capabilities can be applied to US Public Sector WAN networks.

Cisco SD-WAN: US public sector use cases and applications

One can quickly recognize from the advantages above, why SD-WAN has so much interest among WAN designers and architects. The sheer cost savings alone of being able to leverage inexpensive WAN transport, and the zero-touch provisioning capabilities, can prove compelling enough to make the shift. However, there are other considerations as well, specifically the ability to increase an organization’s cybersecurity posture with automated software upgrades and policies across all routers, and the ability to assist agencies in the migration to cloud, which is fundamentally changing WAN designs.

With the increasing use of public cloud and SaaS application offerings, customer applications are more distributed now than ever, across multiple geographic locations, putting even more challenges on WAN networks for delivering applications within the service levels needed.
An inherent “application aware routing” capability is at the crux of what Cisco SD-WAN delivers, that is, an inherent “application aware routing” capability, that understands the service level agreements (SLA) needed for the applications. This is done by using the most optimal transport, which is not just based on routing metrics, but application SLA awareness when forwarding across the WAN fabric. Through the path liveliness and detection mechanisms embedded in the Cisco SD-WAN framework, policies, per application, can be created that align with the SLAs of the applications and validity of the paths to support those applications.

An example is shown in the diagram above, where a branch location has three WAN transport options (MPLS, Internet, and 4G/LTE) to the regional data center. Leveraging the real-time liveliness detection in the SD-WAN branch, the proper path can be chosen at the branch router location, per policy, to steer the application over the path that will meet the applications service levels.

In addition to application-aware routing, the SD-WAN offering provides the capability to inject intelligence in the path selection based on applications per their location, using “cloud on-ramp” intelligence, for both SaaS and IaaS applications. Cloud on-ramp offers the ability to optimize connectivity to hosted cloud applications in various locations, including intra-agency data centers, SaaS applications requiring Internet transport for access, or private peering connections to public cloud providers, all of which will be discussed more in the next sections.
Leveraging SD-WAN with federally mandated trusted internet connection

As discussed above, the SD-WAN solution offers the capability to inject intelligence in the path selection based on applications per their location—but more important, on how well the application is performing over a given path in the WAN.

As the location of customer application hosting continues to shift toward the public cloud and SaaS, US federal customers face an added level of complexity regarding the trusted internet connection (TIC). And the Office of Management and Budget (OMB) mandates standardization and optimization to secure individual network connections, specifically connections to or through the internet. This has a direct impact on traffic patterns and WAN designs, since the federal agencies that use SaaS applications must redirect traffic destined to SaaS providers through a TIC location, before it leaves the boundary of the federal agency.

How can Cisco SD-WAN optimize both SaaS hosted application location and performance?

Referring to the diagram above, a federal agency can leverage multiple benefits of SD-WAN as agency applications continue to shift to SaaS, and assuring the requirement is met for TIC transit for those SaaS applications hosted in the public cloud. Leveraging SD-WAN brings several key benefits, including:
- **Multiple WAN transport paths**, including cost-effective internet, to the regional data center.

- With SaaS application intelligence using Cisco SD-WAN “CloudExpress” at the agency branch, the SD-WAN edge router can make **intelligent forwarding decisions**, over those WAN paths that meet the applications’ Quality of Experience (QoE) requirements, (Office 365, Amazon Web Services, Google G Suite, etc.) improving overall end-user experience.

- **Application aware probing**, to the cloud application, to measure loss/latency and application reachability from the various exit points. In this example, application probes can be leveraged at the Government Agency Branch Location, TIC provider location, as well as the regional data center (on federal agency facility or co-location such as Equinix).

The application awareness that the SD-WAN solution offers completely transforms the WAN from forwarding IP packets based on destination IP address/domain names, to forwarding based on application performance in the private data center, public cloud (AWS, Azure, Google), and SaaS providers (Google, Cisco Webex, Microsoft Office 365, etc.)
Leveraging direct internet access for optimized SaaS access

The Cisco SD-WAN solution transforms the WAN routing to an application-aware fabric based on quality of experience (QoE). Public sector customers, like K-12 and higher education institutions not restricted to security mandates as those described for the TIC, can leverage alternative forwarding solutions, specifically direct internet access (DIA). DIA offers the branch router the ability to route traffic directly via the Internet as a transport, targeting those cases where access to applications hosted in the Internet (like SaaS) can be accessed directly, bypassing the need to traverse the corporate MPLS WAN and regional data center, which in some cases is the longer, more latency-induced path.

In the example above, application probes can be leveraged to emulate and sense the behavior of the applications being accessed at the branch office. In those cases where the measured QoE (aggregating packet loss and latency) is smaller via the Internet path (Path #1) than through the MPLS/Internet transport (Path #2 and #3) via the regional data center, traffic can be diverted directly through the Internet to the destined SaaS application. Best practice local firewall and security rules can be applied to the edge router when the DIA path is used. In addition, diverting DIA traffic through Cisco Umbrella provides assurance for securing DNS queries as they leave the DIA interface. The DIA solution is yet another advantage to optimizing traffic forwarding based on the performance of the application, rather than just shortest cost IP routing.

In the cases where non-federal customers do require some level of forced traffic inspection, those customers can leverage the methods similar to the federal TIC design.
How SD-WAN keeps costs down

K-12 SD-WAN use case
A school district was looking for a solution to support the growth of connectivity requirements to on-premise and cloud-based applications in a secure and cost-effective manner. The district consisted of 28 sites, each connecting back to a centralized data center using a single 10Mbps MPLS circuit.

By leveraging the secure, application-aware capabilities of an SD-WAN solution, the district would be able to migrate remote-site connectivity from slower MPLS-based circuits to faster (200Mbps), more inexpensive broadband Internet connectivity. The monthly savings from switching to broadband would also afford each remote site dual broadband connections, as opposed to the single MPLS circuit they each use today, which would bring a 3900% increase in bandwidth per site.

This level of redundancy was becoming more critical as unreliable connectivity can affect student online testing, causing financial loss, delayed testing, student anxiety, and upset parents. For a second broadband circuit to be used at each remote site, it was required that it use a more physically diverse path than the first path. Even though a second broadband connection that used a diverse path (when compared to the first) would cost roughly six times more than a single broadband connection, the cost savings for deploying an SD-WAN solution were still more than enough that it could pay for itself.

<table>
<thead>
<tr>
<th>Circuit type</th>
<th>Total annual circuit costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Mbps MPLS</td>
<td>$840,000</td>
</tr>
<tr>
<td>200Mbps Broadband</td>
<td>- $67,200</td>
</tr>
<tr>
<td>200Mbps Broadband – 2nd Diverse Path</td>
<td>- $436,800</td>
</tr>
<tr>
<td><strong>Total Annual Savings</strong></td>
<td><strong>= $336,000</strong></td>
</tr>
</tbody>
</table>

SD-WAN outcomes: 60% annual cost reduction & 3900% bandwidth increase
The Benefits of analytics with SD-WAN

IT operators continue to demand better application and network visibility. Traditionally, the WAN has been a blind spot for public sector operations teams, when it comes to application performance degradation. These challenges are multi-fold, both around gathering real-time information and the behavior of applications traversing the WAN. There are also challenges around gathering the necessary data to offer accurate capacity planning for bandwidth, application usage, and spending accurately on expensive WAN links.

To counter this challenge, Cisco SD-WAN offers a SaaS-based analytics solution that addresses all these challenges, gathering millions of records, isolated per customer. Consider a US federal agency that’s introducing more IoT devices (badge readers, security cameras, agency-specific mission sensors) into remote branches. The agency is also moving the collection and processing of applications to public cloud locations. This introduces an entirely new set of application behavior, usage, and bandwidth requirements.

Having this data will expose new stress points within the WAN design, particularly to those WAN exit points, and where applicable, to the TIC access-provided exit points. SD-WAN analytics provides continuous gathering of precise analytics that can help organizations understand different stress points on the WAN, such as application behavior, per site availability, as well as per carrier performance. This lets the agency tightly monitor offered SLAs with the carrier.

This level of application and network related visibility can assist in selecting more accurate bandwidth increases, top applications utilized, insights on current policies, and whether the carrier’s SLAs are being met within contract. Details on bandwidth usage alone allow pinpoint accuracy for link increase/decrease, which saves huge monthly circuit cost for the agency. Furthermore, the data gathered can be analyzed with a network-wide view, allowing capacity planners end-to-end visibility, including “what if” simulated scenarios, as opposed to cost spending based on inaccurate data.

The service is tightly coupled to the SD-WAN management offering operational consistency. And for those customers wanting additional network telemetry captures, the SD-WAN routers allow IP Flow Information Export (IPFIX) for internal and/or third-party tool usage.
Summary

The demand for higher bandwidth, cloud-based services, and a better end user experience at branch locations has not only driven the need for additional capacity, but has changed the way we deliver and measure the services we provide. As a result, having the capability to easily encrypt data, effortlessly add new locations, automatically route traffic based on application behavior, reduce costs, and actively monitor the health of the WAN is paramount in today’s digital world.

Related resources


Find out more about Cisco solutions for the US public sector:

- Education
- Federal Government
- State and Local Government
- Department of Defense