White Paper
U.S. Public Sector Federal

Cloud-Ready Networks

Ensure Your Agency's Missions are Enabled in a Cloud Smart, Zero Trust World

Trademarks

Every effort has been made to identify trademark information in the accompanying text. However, this information may unintentionally have been omitted in referencing particular products. Product names that are not so noted may also be trademarks of their respective manufacturers.

Table of Contents

Introduction

As the U.S. Government increasingly embraces as-a-service (aaS) consumption models, adoption of cloud technologies continues to accelerate. Government agencies are turning to the cloud for many of the same reasons as nongovernmental organizations.

- Cloud Smart technologies and architectures offer agencies the potential to:
- Enable more agile achievement of agency missions
- Address technical debt and gain access to ongoing commercial innovation
- Unlock additional IT value by integrating IT efforts and investments to deliver needed mission-impacting capabilities
- Handle and analyze growing volumes of data to support data-driven policies and operationalization of data.

When dealing with cloud applications, the leading metric for success and productivity is user experience. So it's not surprising that while 30 percent of IT Departments say they have hit roadblocks with their cloud efforts in delivering business and mission value, even more are concerned about delivering a quality cloud user experience. Now, more than ever, your agency's network is critical to your organizational and mission success. This means delivering an exceptional overall user experience, including for the users consuming applications that reside in the cloud.

Agency networks must also be able to support the growing number of hyper-distributed applications provisioned across virtual machines (VM), containers, and bare-metal hardware throughout data centers and clouds. Applications, Internet of Things (IoT) sensors, and Artificial Intelligence/Machine Learning (AI/ML) engines generate hyper-distributed data that needs to be processed in the cloud, on the premises, and at the edge. Basically, wherever it's necessary to meet the agency's mission needs. So agencies are leveraging multicloud deployment models (private, public, community, and hybrid) to deliver best-fit services for their users and help drive application rationalization for their organizations.

To help Federal agencies accelerate their adoption of cloud-based solutions, and do so successfully, the Cloud Smart program was created. Cloud Smart's practical implementation strategy is designed to help provide Federal agencies with pragmatic guidance around three key pillars of successful cloud adoption: security, procurement, and workforce. These elements embody the same interdisciplinary approach driving Federal IT modernization.

A key prerequisite for enabling successful Cloud Smart adoption is a network's readiness to support architectural shifts, driven by cloud and other disruptive technology vectors (including IoT, AI/ML, and big data). As the June 24, 2019 Federal Cloud Computing Strategy states, "agencies should assess their requirements and seek the environments and solutions, cloud or otherwise, that best enable them to achieve their mission goals while being good stewards of taxpayer resources." This means that cloud-ready networks must effectively provide access to agency workloads, applications, and data wherever they are.

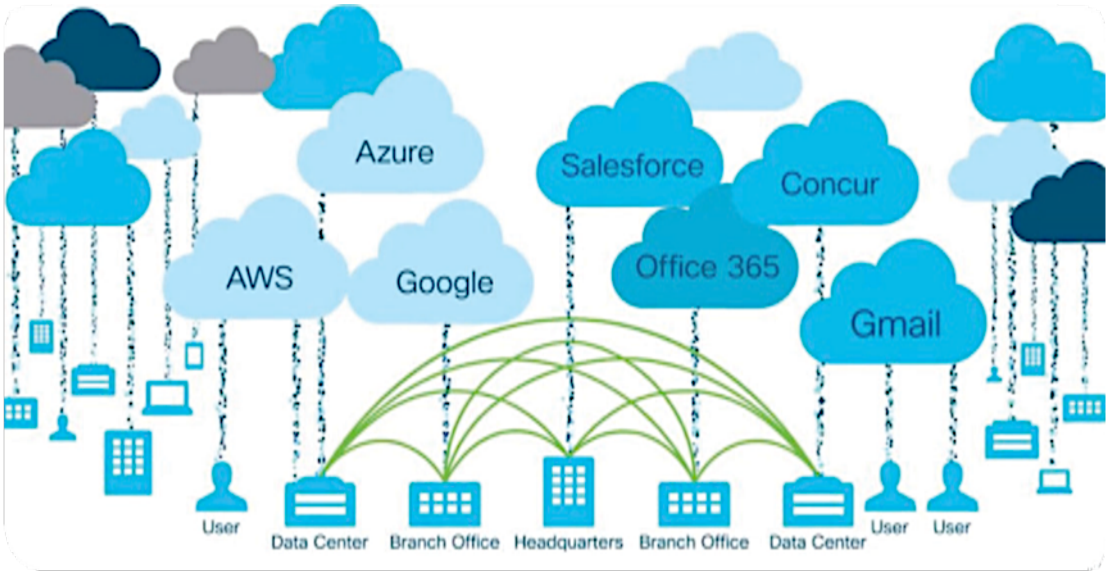
An integrated, cross-domain, cloud-ready network can help Zero Trust access across an agency's campus, wide-area network, and data centers. Federal civilian agencies seeking to step into the future are now asking the crucial question: are our networks cloud-ready?

Shifting Architectural Requirements

Today's network requirements are experiencing a fundamental shift as the traditional model of accessing highly centralized resources is coupled with the need for a distributed, decentralized architecture. This shift is driven by two key factors:

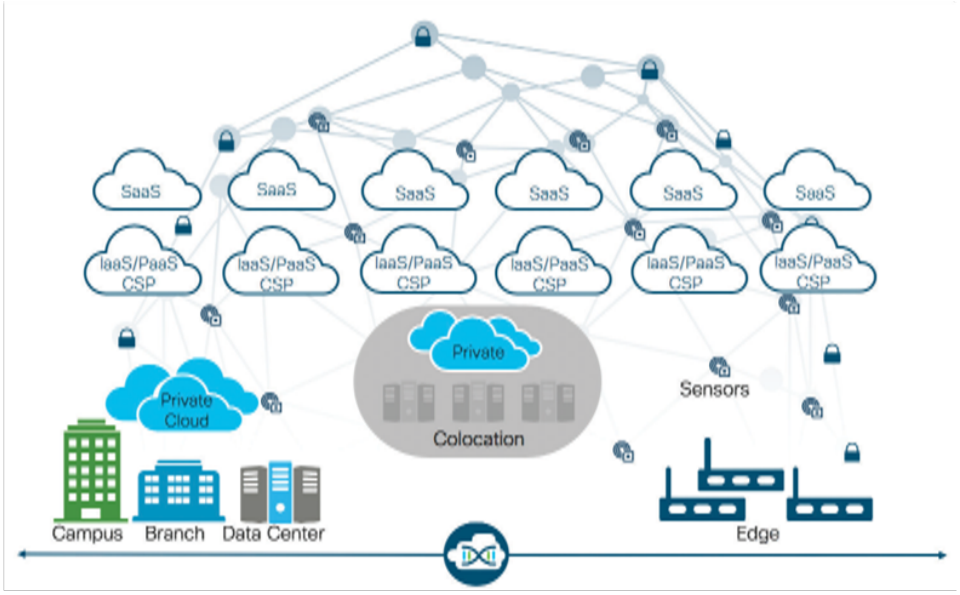
1. Centralized cloud computing models where IaaS, PaaS, SaaS, and other Cloud Solution Provider (CSP) hosted services are consumed from public and community clouds (Figure 1).

Figure 1 Centralized Cloud Computing Models



2. The rapid growth of edge devices and the distributed architectures that enable them to process data locally as well as communicate and share resources with other edge devices (Figure 2).

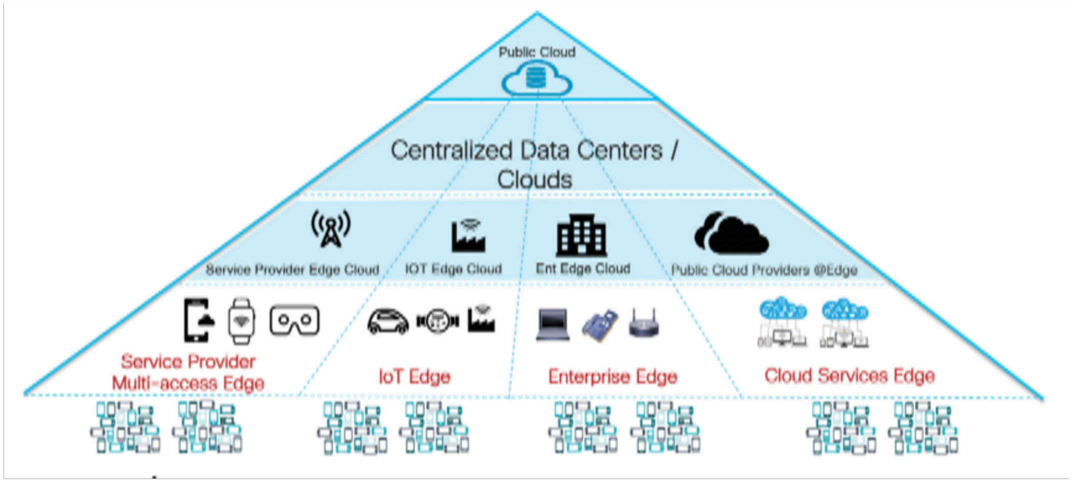
Figure 2 Edge Devices



The upsurge of edge devices and the distributed architecture to support them has given rise to a distributed architecture that brings the core building blocks of cloud (computing, storage, and networking) closer to the edge. Where latency and bandwidth constraints exist, agencies will leverage edge computing. In some cases, they leverage both an edge computing model (for real-time data processing) and a centralized cloud computing model (for heavy processing).

For example, ML models can be trained in a public cloud and then deployed at the edge to enable near-real-time predictions. Plus, agencies can leverage on-premises private clouds or hybrid cloud deployment models to make core cloud capabilities available at the edge (Figure 3).

Figure 3 Distributed Architecture


Public Cloud
Centralized Data Centers / Clouds
Service Provider Edge Cloud
IOT Edge Cloud
Ent Edge Cloud
Public Cloud Providers @Edge
Service Provider Multi-access Edge
IoT Edge
Enterprise Edge
Cloud Services Edge

To facilitate their cloud journey and reduce risks, Federal agencies will need a cloud-ready network able to support both centralized cloud and distributed architectures that comprise private, community, public, and hybrid clouds.

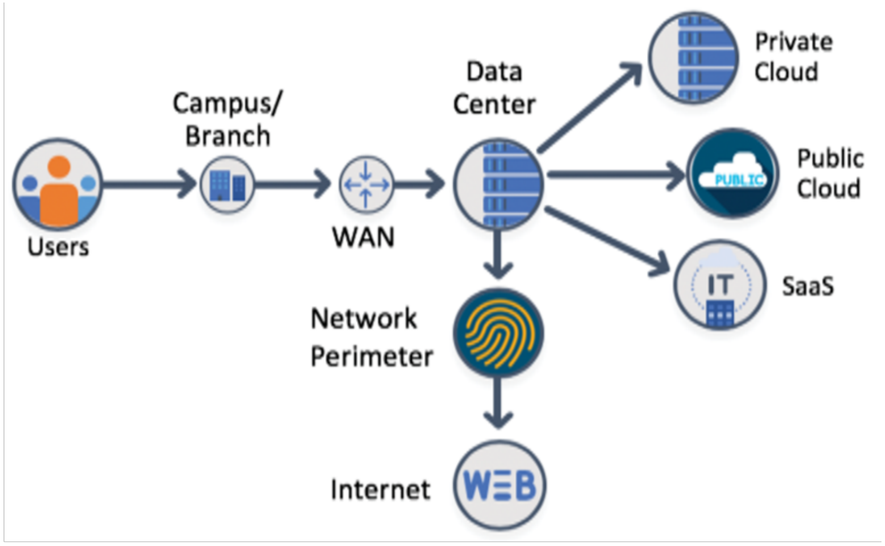
This cloud-ready network must ensure access to the cloud across an agency's existing campus, Local Area Networks (LAN), Wide Area Networks (WAN), and data centers as well as over broadband and 4G/5G environments.

Securing Optimized Connectivity to Cloud Services

Traditional hub-and-spoke network architectures are designed to support applications and services hosted at centralized "Demilitarized Zones" (DMZs) and data centers. This layout forces the backhaul of internet traffic through the DMZ, creating inefficient traffic routes that increase the distance between the end user and application. Today, most agencies still rely on this approach, backhauling traffic destined for off-premises IaaS, PaaS, and SaaS services through a trusted, central connection point.

But the reality of today's landscape, with an ever-growing influx of data and devices, is pushing the limits of hub-and-spoke networks. Traditional network designs are increasingly unable to support the edge-to-cloud shift of internet traffic, making it nearly impossible for networks to keep up (Figure 4).

Figure 4 Hub-and-Spoke Network Architecture



Today’s agency branch office users collaborate more online through the use of SaaS applications like Webex and Office 365, or other cloud services. Branch-based end users are also consuming more and more bandwidth-intensive cloud-hosted applications. In this scenario, two common approaches are available to address IaaS, PaaS, and SaaS performance challenges:

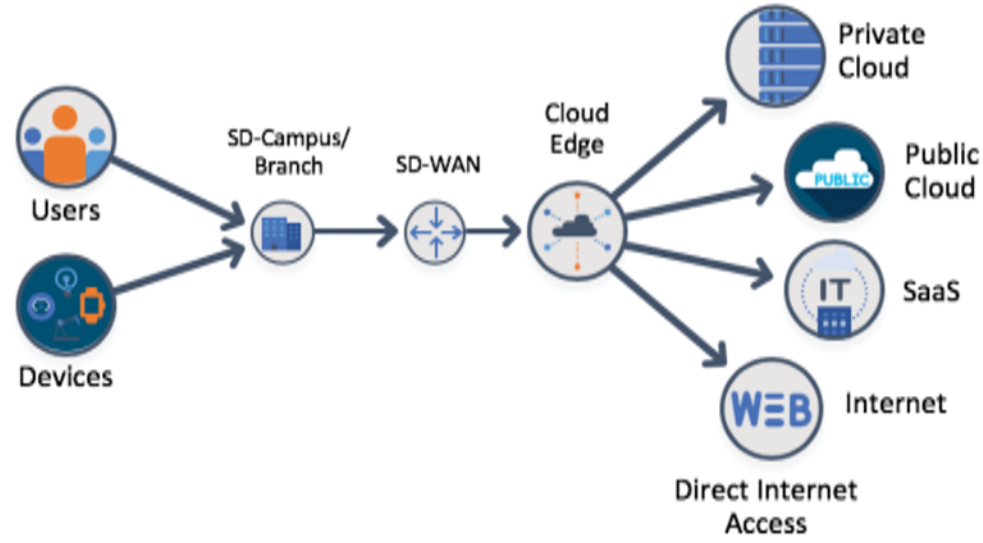
1. Decentralize and deploy multiple internet exits
2. Provide high bandwidth connectivity directly from the branch sites.

However, the combination of security, complexity, and cost arising from the rigidity of traditional WAN technologies make these solutions impractical to implement on a large scale.

By providing an architecture that integrates routing, security, centralized policy, and orchestration, Software-Defined Wide-Area Networks (SD-WANs) enable agency branch offices and remote users operating government-furnished equipment to securely connect to applications by leveraging any combination of internet transport services (MPLS, cellular, or broadband).

SD-WAN technology addresses the bandwidth and performance issues related to cloud-hosted applications, so agencies can extend their secure footprint anywhere (Figure 5).

Figure 5 Cloud-Hosted Applications



SD-WAN provides agencies the following advantages:

- Predictable application experience using multiple hybrid links with real-time steering based on Service Level Agreement (SLA) policies
- Zero Trust network security and segmentation

- Integrated security composed of enterprise firewall, intrusion prevention, advanced malware protection, DNS-layer enforcement, URL filtering, and antivirus
- Seamless public-cloud expansion and SaaS optimization
- Centralized management, zero-touch provisioning, and a high degree of automation
- Rich analytics for visibility, troubleshooting, and planning
- Highly scalable solution able to scale to 10,000+ locations.

With SD-WAN, civilian agencies can build a scalable, carrier-neutral WAN infrastructure while also reducing WAN transport costs and network operational expenses. The technology ensures a predictable end-user experience for cloud-hosted applications and supports a seamless, multicloud architecture with simplified operational experience, integrated security, and rich analytics.

Improving SaaS Performance with SD-WAN

Poor end-user experience is one of the top complaints when an agency adopts SaaS. This is often due to unpredictable SaaS performance when confronting the many dynamic changes in internet gateways. SD-WAN solves these problems and enables an optimal SaaS user experience across all agency branches. It does this by creating multiple internet exit points and dynamically steering around bandwidth and latency issues in real time.

This also involves the SD-WAN fabric continuously measuring the performance of designated SaaS applications through all permissible paths leading from a branch. For each path, the fabric computes a quality-of-experience (QoE) score that gives network administrators visibility into application performance. SD-WAN technology also makes real-time decisions about the best-performing path between the end users at a remote branch and the cloud SaaS application.

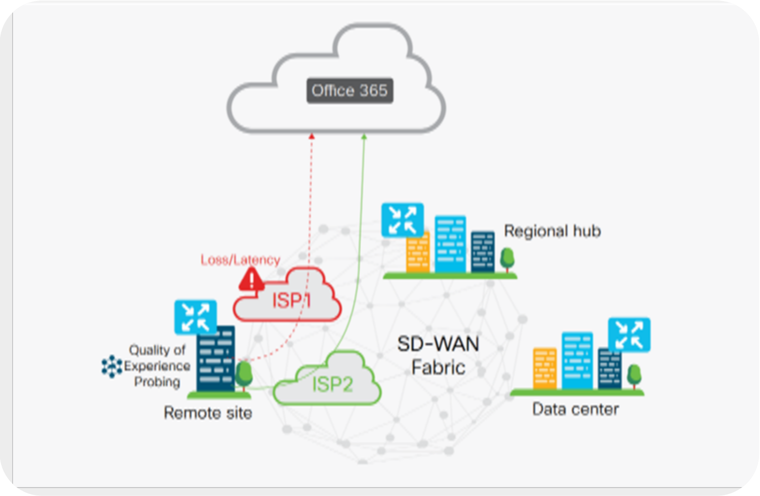
In the quest for higher availability and a better end-user experience, agencies have the flexibility to deploy this capability in multiple ways based on their mission needs and security requirements.

Option 1: Direct Cloud Access from a Remote Branch

Agencies using single or multiple inexpensive broadband internet circuits at remote sites, can direct select traffic destined to a designated SaaS to break out directly to the Internet. Only trusted and critical traffic to the designated SaaS will be allowed through a secure local breakout, while all other Internet-bound traffic will follow its usual path.

For example, an agency can specify a policy that permits the most performance-demanding and trusted Office 365 applications, such as Exchange Online and SharePoint Online, to take advantage of a local and direct internet connection, while the remaining user network communication outside of the customer network will be routed through the customer data center (Figure 6).

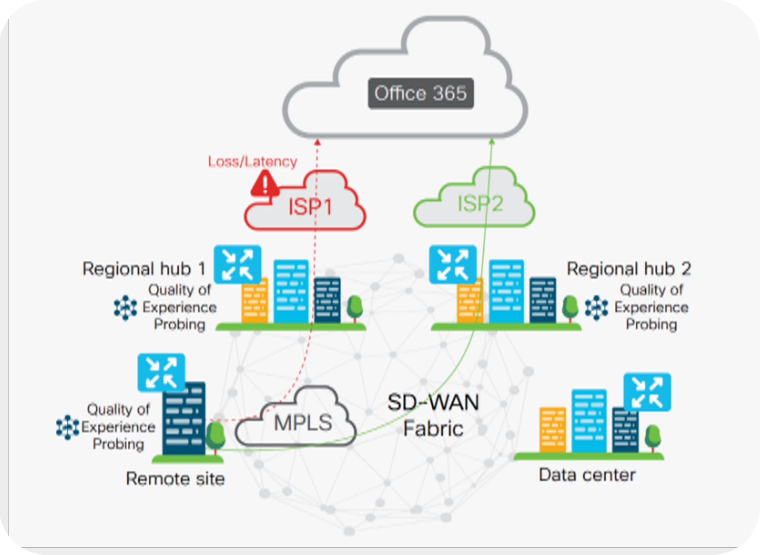
Figure 6 Direct Cloud Access from Remote Branch



Option 2: Cloud access through the most Optimal Regional Hub or Carrier-Neutral Facility

For agencies that want their SaaS to employ a regional hub egress architecture, SD-WAN can help ensure the best possible path through the available regional hub infrastructure. For example, SD-WAN capabilities can be deployed to dynamically choose the optimal regional gateway for the agency's Office 365 application traffic (Figure 7).

Figure 7 Regional Hub Infrastructure

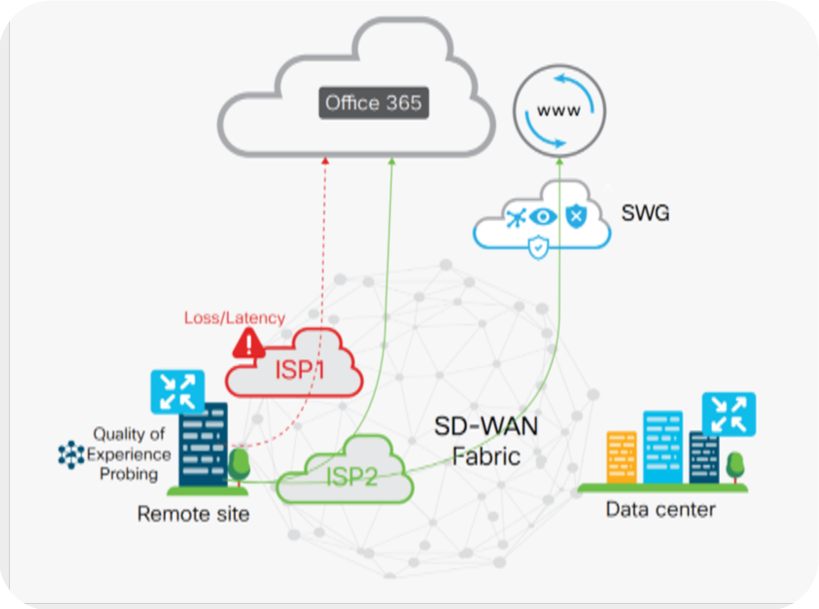


Option 3: Local Internet Access through Secure Web Gateways

Agencies can connect remote branches to the SD-WAN fabric using inexpensive broadband internet circuits and can apply differentiated security policies depending on the types of services to which users are connecting. Instead of sending all branch traffic to a Secure Web Gateway (SWG) or Cloud Access Security Broker (CASB), an organization may wish to enforce its IT security policies in a targeted manner by routing regular internet traffic through a SWG, while allowing performance-optimal direct connectivity for a limited set of sanctioned SaaS applications.

For example, the agency can leverage SD-WAN capabilities to dynamically choose the optimal path among multiple Internet Service Providers (ISPs). This can be for Office 365 applications permitted to travel directly and for applications that are routable through the SWG per-agency policy (Figure 8).

Figure 8 Local Internet Access through Secure Web Gateways



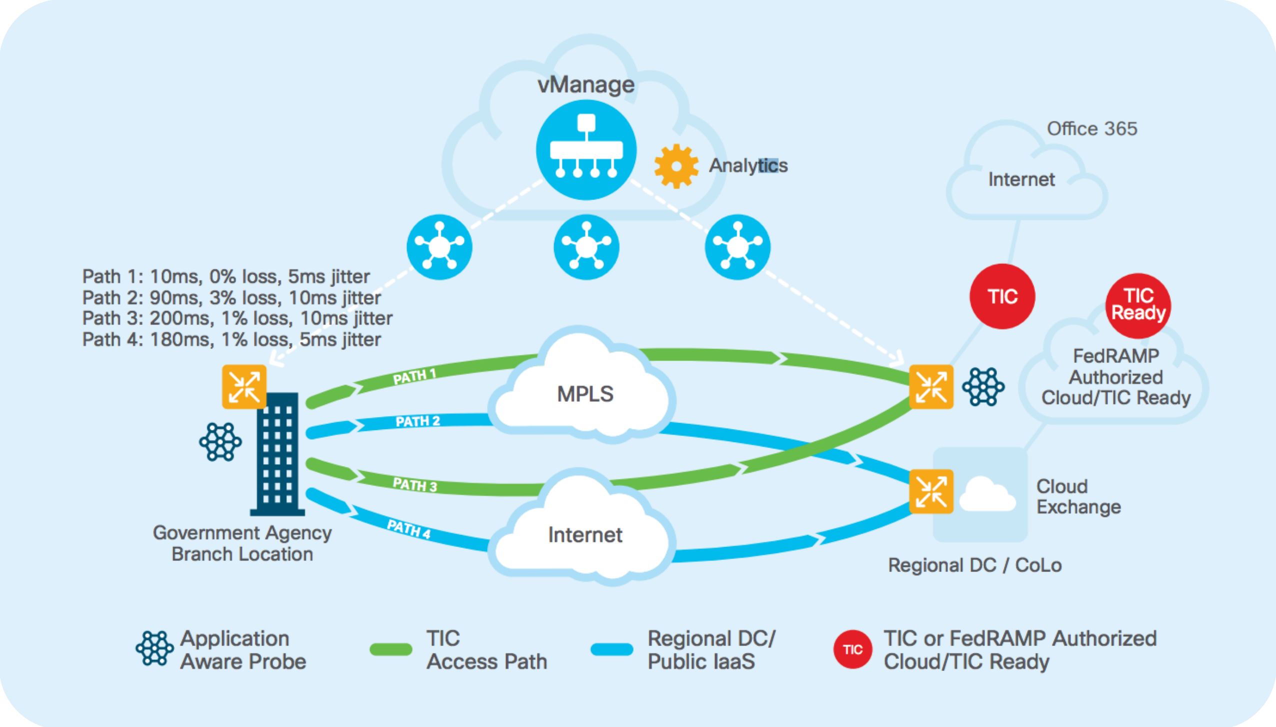
Leveraging SD-WAN with Federally Mandated Trusted Internet Connection (TIC)

SD-WAN offers the capability to inject intelligence in the path selection based on applications, but more importantly, based on how well the application is performing over a given path in the WAN. As agencies host more applications in public cloud environments and increase their SaaS consumption, they face an added level of complexity regarding the trusted internet connection (TIC).

The Office of Management and Budget (OMB) mandates standardization and optimization to secure individual network connections, specifically for connections to or through the Internet. This has a direct impact on traffic patterns and WAN designs, since 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.

As shown in Figure 9, a Federal agency can leverage multiple benefits of SD-WAN as agency applications continue to shift to SaaS. This can help assure requirements are met for TIC transit.

Figure 9 Leveraging SD-WAN with TIC


vManage
Analytics
Office 365
Internet
Path 1: 10ms, 0% loss, 5ms jitter
Path 2: 90ms, 3% loss, 10ms jitter
Path 3: 200ms, 1% loss, 10ms jitter
Path 4: 180ms, 1% loss, 5ms jitter
TIC
TIC Ready
FedRAMP Authorized Cloud/TIC Ready
PATH 1
PATH 2
PATH 3
PATH 4
MPLS
Internet
Government Agency Branch Location
Cloud Exchange
Regional DC / CoLo
Application Aware Probe
TIC Access Path
Regional DC/ Public IaaS
TIC
TIC or FedRAMP Authorized Cloud/TIC Ready

Maximizing SD-WAN brings several key benefits, including:

- Multiple WAN transport paths, including cost effective Internet paths, to the regional data center
- With SaaS application intelligence 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, and others), 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 colocation such as Equinix).

The application awareness that SD-WAN 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.).

Learn more about Cisco's SD-WAN Solution Use Cases in the Public Sector, SD-WAN, Secure Internet Gateway (Cisco Umbrella), and Cloud Access Security Broker (Cisco CloudLock) solutions.

Ensuring Application Performance

Applications are more dynamic and complicated than ever, with many parsed into services and microservices, often deployed across on-premises and off-premises cloud environments. Delivering an exceptional digital experience in a blended workload environment requires application and IT infrastructure teams to focus on what matters most: making certain that applications always perform, whether they're deployed in traditional data centers or in complex multicloud environments.

Dynamic Workload Optimization

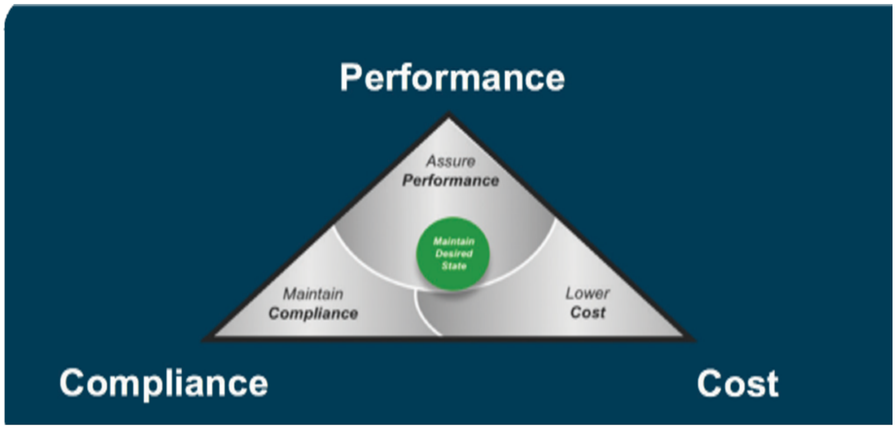
Agencies must be able to develop and deploy applications on the infrastructure that makes sense for their programmers, their users, and their budget. Agentless workload optimization management technologies can detect elements in an agency's environment, from applications to individual components, and deliver a topological map of that environment and its interdependent relationships. This can empower agencies to quickly model "what-if" scenarios based on the real-time environment in order to forecast capacity needs accurately and make the right deployment decisions.

Workload optimization management technologies can also automate the scaling of workloads, storage, and databases based on the level of comfort among IT personnel:

- Recommend (view only)
- Manual (select and apply)
- Automated (executed in real time by software).

Automated workload optimization can eliminate human error and free IT staff to focus on higher-value initiatives (Figure 10).

Figure 10 Workload Optimization Management



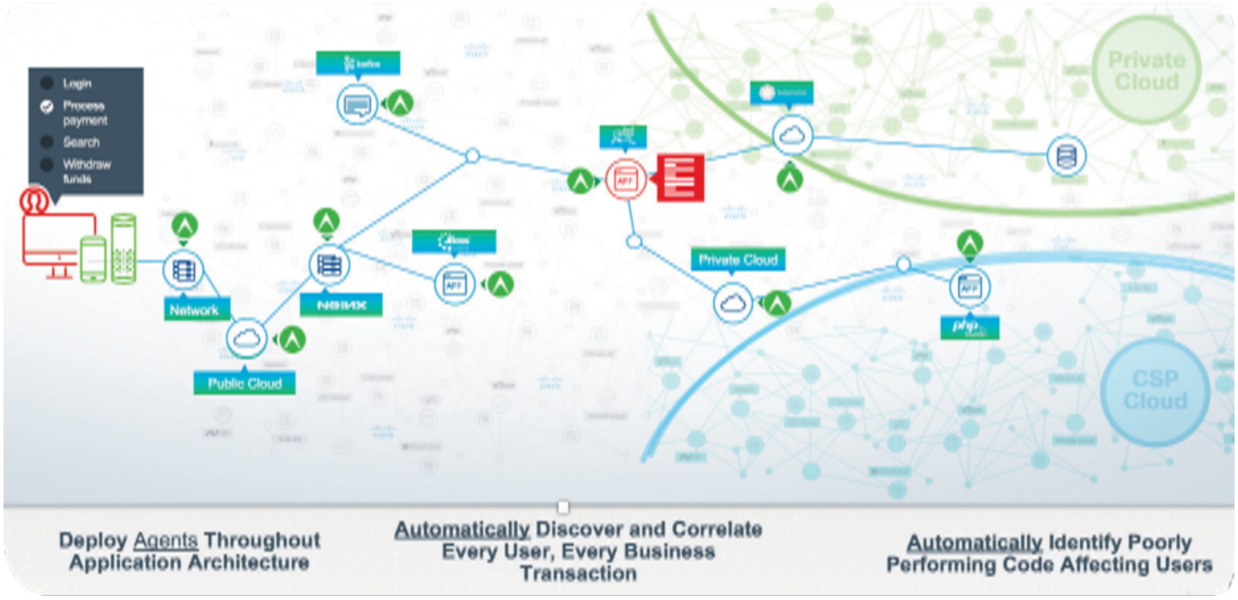
Learn more about Cisco’s Workload Optimization Manager Solution.

Application Performance Visibility

In order to deliver consistently positive digital experiences, agencies will need to connect end-user experience and application performance to mission outcomes. A solution that can monitor, correlate, analyze, and act on application and mission performance data in real time, regardless of where the application is hosted (on-premises private, hybrid cloud, or off-premises CSP cloud), can enable developers, IT operations, and mission owners to gain the insights needed to make mission-critical and strategic improvements.

Application performance monitoring solutions that leverage AI and ML to enable AI operations and cognitive operations can offer automated insights that allow agencies to avoid mission-impacting performance issues before they occur. In addition, they can perform automated root-cause analysis that expedites Mean Time to Repair (MTTR) (Figure 11).

Figure 11 Application Performance Monitoring Solutions


Login
Process payment
Search
Withdraw funds
kafka
Network
NGINX
Public Cloud
APP
Private Cloud
php
Private Cloud
CSP Cloud
Deploy Agents Throughout Application Architecture
Automatically Discover and Correlate Every User, Every Business Transaction
Automatically Identify Poorly Performing Code Affecting Users

Learn about Cisco's AppDynamics [Application Performance Monitoring](), [Business IQ](), and [AIOps Solutions]().

By leveraging workload optimization and application performance visibility solutions, agencies can replace sizing guesswork with real-time analytics and modeling, so they know how much infrastructure is needed for applications to keep pace with mission demand. Gaining insights through these solutions will allow agencies to adopt a proactive approach to IT operations and stay focused on end-user experience and mission impact.

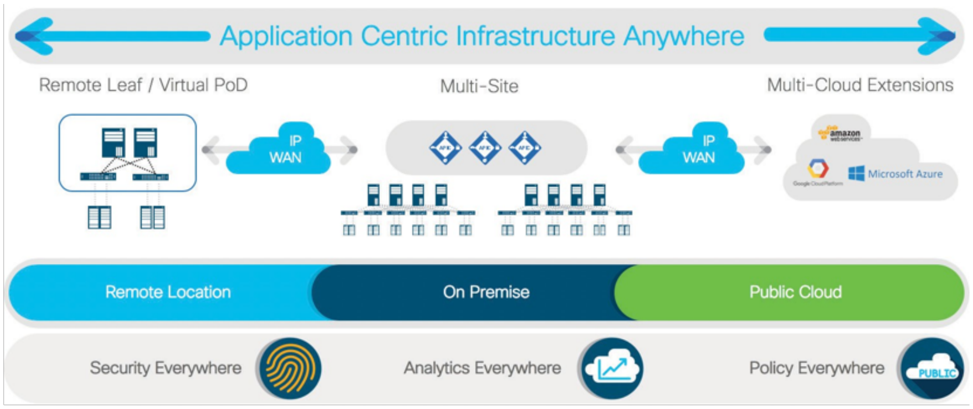
Enabling Architectural Shifts That Support Cloud Adoption

Application-Centric Infrastructure

Software-defined networking can facilitate the application agility and data center automation required to accelerate cloud adoption. An application-centric infrastructure enables simplified operations, automated network connectivity, consistent policy management, and visibility for multiple on-premises data centers and for public clouds or multicloud environments. This infrastructure also offers agencies the flexibility to move applications seamlessly to any location or cloud while maintaining security and high availability (Figure 12).

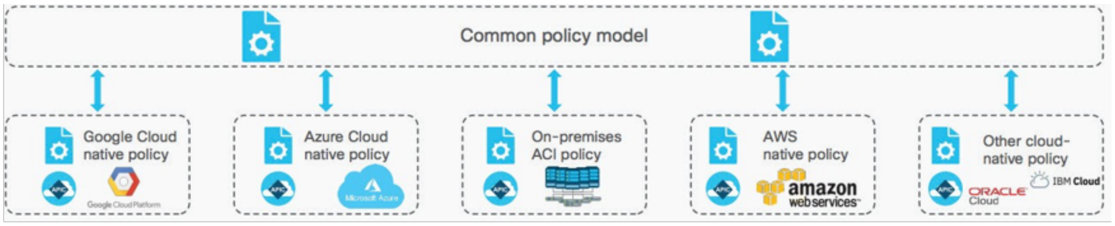
Figure 12 Application-Centric Infrastructure Anywhere

Any workload, any location, any cloud



Furthermore, an application-centric infrastructure captures mission and user intents and translates them into native policy constructs for applications deployed across various cloud environments. Using a holistic approach, it ordains availability and segmentation for bare-metal, virtualized, containerized, or microservices-based applications deployed across multicloud domains. The common policy and operating model can drastically reduce both cost and complexity associated with managing multicloud deployments (Figure 13).

Figure 13 Common Policy and Operating Model



Learn more about Cisco’s software-defined networking and Cisco Application Centric Infrastructure solutions.

DevSecOps and Containers

There is now a drive toward shorter and more iterative development cycles, with a focus on delivering mission needs. This is leading agencies to adopt Development, Security, and Operations (DevSecOps) methodologies that enable development, security, and IT teams to work more closely and collaboratively. In parallel with DevSecOps models, containers and microservices are being adopted as the building blocks of today’s software development. This is the preferred path for both new application development and application modernization projects.

Containers, which encompass the operating system, libraries, and anything else that the application needs, offer a lightweight, portable way to bundle applications. This isolation brings portability, standardization, and flexibility to development environments; applications are decoupled from the platform, so containers can move from platform-to-platform or from cloud-to-cloud without modification to the application. With containers, developers can spend less time debugging and assessing differences between environments and more time on development.

The benefits of cloud increase exponentially when organizations bring together containers and DevSecOps (a lightweight means of virtualizing applications with a methodology to join siloed IT teams). For organizations making this transition, one of the biggest challenges is maintaining common and consistent environments throughout an application’s lifecycle, from development through deployment.

To address this challenge, agencies will need hybrid-cloud architectures that deploy applications across on-premises and cloud environments in a secure, consistent manner. The supporting hybrid architectures must be tested and validated, as well as deliver consistent container clusters both on-premises and in the cloud, leveraging the best attributes of each.

Agencies that can extend on-premises capabilities and resources to the cloud, and that can also utilize services and resources from the cloud on-premises, will reduce the burden on their IT teams with respect to people, processes, and skill sets. This can then accelerate the application deployment cycle, resulting in faster innovation and increased agility.

Learn about Cisco’s integrated system for Azure Stack, Cisco’s hybrid solution for Kubernetes on AWS, Cisco’s hybrid solution for Kubernetes on Google Cloud Platform, and Cisco’s validated solutions with Docker.

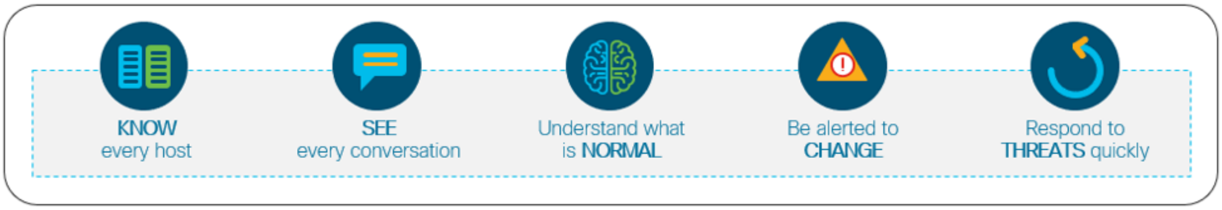
Zero Trust Architecture

To better protect government's networks, infrastructure, and data from growing digital threats, agencies are moving toward a Zero Trust network architecture based on a "verify and never trust" approach. Tenacious attackers and malicious insiders can penetrate perimeter-centric defenses, so the Zero Trust model is centered around one guiding principle: security must extend throughout the network, not just at the external perimeter.

Effective security depends on total visibility of your agency's network environment. To enable this, Zero Trust focuses on five key elements.

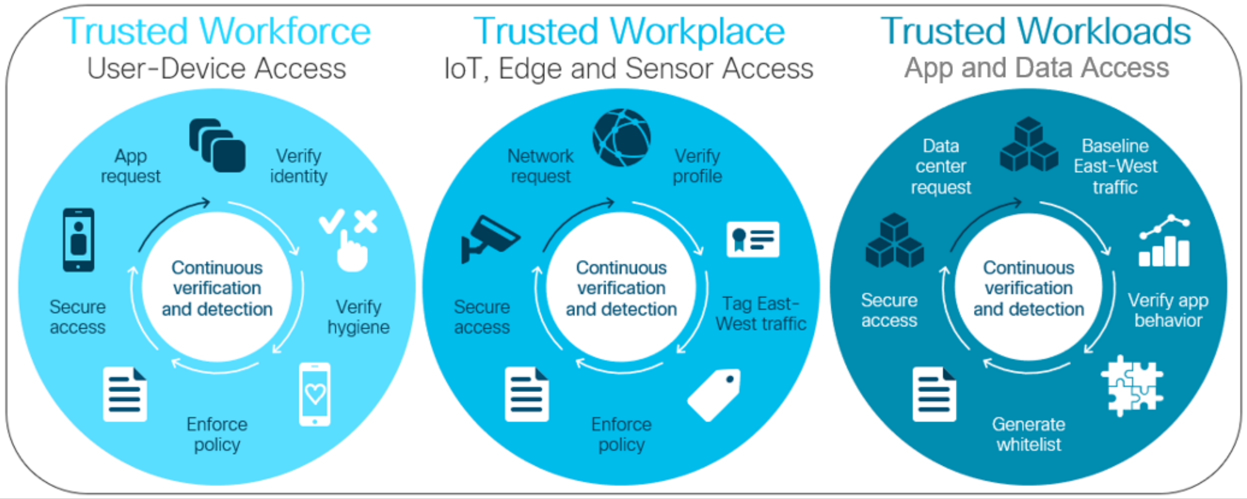
1. Eliminating unauthorized network trust: Assume all traffic, regardless of location, is a potential threat until it is verified (inspected, authorized and secured).
2. Segmenting network access: Adopt a least-privileged strategy and strictly enforced, granular controls so users have access only to the resources needed to perform their job.
3. Gaining visibility and analytics: Continuously inspect and log all traffic both internally and externally, using real-time protection capabilities, to monitor for malicious activity.
4. Acting, ideally in real time, when anomalous activity is detected in order to limit threat impact and optimally manage risk (Figure 14).

Figure 14 Key Trust Network Architecture Elements



Network segmentation and visibility remain critical, yet users also access workloads hosted outside of an agency's network. As a result, agencies must take a holistic approach and extend their Zero Trust approach to their workforce, workloads, and entire workplace (Figure 15).

Figure 15 Zero Trust Workforce, Workplace, and Workloads



- Zero Trust Work Force

  Users and devices must be authenticated. Plus, access and privileges must be continuously monitored and governed. Users must be protected as they interact with the internet.

- Zero Trust Workplace

  Access must be controlled across the entire workplace, including the cloud and edge. This is critically important as greater use of IoT and machine-to-machine sensors are becoming increasingly critical to successful agency mission and business outcomes.

- Zero Trust Workloads

  Granular access control must be enforced across the entire application stack, including connections between containers or hypervisors in the cloud as well as traditional agency data centers.

In addition to your Cisco networking infrastructure, learn about Cisco's security capabilities that can be leveraged to help your Agency achieve Zero Trust, including: Identity Services Solution (Cisco ISE), unified access solution (Cisco Duo), malware protection solution (Cisco AMP), workload protection platform (Cisco Tetration) and visibility and threat detection solution (Cisco Stealthwatch).

Summary

As the Federal civilian government pushes forward with its digital transformation, cloud-ready networks are essential to enabling the best possible user experience. And they can help agencies achieve successful organizational and mission outcomes.

Cloud-ready networks build on new network architectures that provide simplicity, adaptability, automation, security, and application-awareness. These capabilities are key to supporting the new world of Federal IT, where applications reside in many locations.

Building on a solid Cisco architecture that leverages the Federal government's broad existing investments, can help your agency optimize user experience, speed, innovation, and security. All while meeting business and mission objectives in a Zero Trust world.