GCN

SPECIAL REPORT

TAKE THE SOFTWARE-FIRST APPROACH TO APP DELIVERY:

SOFTWARE-DEFINED NETWORKING IS THE KEY TO IMPROVED NETWORK MANAGEMENT

SPONSORED BY:

CITRIX® Public Sector

MOBILITY AND CLOUD STRAIN LEGACY NETWORKS

Increased demands on agency networks are forcing them to rethink current strategy.

Federal agencies are clearly deep in the throes of change. Those changes are driven by mandates to increase mobility and embrace the cloud. The change involves not only where employees can work—in remote offices, at home or on the road—but how they work. Ensuring fast, secure, reliable access to applications and agency resources wherever they are stored, and wherever and whenever employees need them, continues to become a greater challenge.

In many cases, existing network infrastructure simply can't keep up with these growing demands. Accessing large multimedia files, for example, typically requires significant bandwidth. Older networks are often slowed to an unacceptable speed. Traditional wide area networks (WAN) lack the performance and high availability to meet growing demands. Most WANs also use connectivity protocols like MPLS, ATM or SONET, none of which work well with cloud-based applications.

These challenges are causing many agencies to rethink their existing network strategy. According to a report from consulting group Ashton, Metzler & Associates, organizations are rethinking their approach to WAN design for the following reasons:

- support real-time applications like voice and/or video
- increase security
- improve application performance
- provide access to public cloud computing services
- reduce cost

Other critical factors include increasing network speed, improving the ability to run remote applications, and enhancing network access for branch and remote workers.

The First Steps

For many organizations, the first step is optimizing the existing WAN. WAN optimization usually involves adding functions to better use existing bandwidth through processes like compression, deduplication, caching and reduced latency. This is an important step in making the best use of the networking technology already in place. It also goes a long way toward improving application acceleration.

For today's wide area networks, however, that's often insufficient. To efficiently and effectively handle modern applications and other resources accessed by remote users requires further optimization through a software-defined WAN (SD-WAN). In many cases, an SD-WAN, where software controls most aspects of the network, can provide the scalability, performance boosts and improved security agency networks need. The SD-WAN also can reduce network complexity and simplify management.

An SD-WAN helps network managers monitor, manage and troubleshoot all parts of the network from a central console, even those in far-flung branch offices. The technology also standardizes and boosts security by embedding security policies into the network and enforcing data segmentation. Speed and reliability improve due to continuous monitoring of network links and the ability to route applications on the fastest links based on their level of importance to the organization.

During a panel at 2016's Enterprise Connect conference, experts agreed SD-WANs should have these attributes:

- Centralized administration: The network's control plane is separate from the data plane and abstracted into a software layer.
- Automated provisioning: Everything is done via software without manual intervention, so it's easy for agencies to send fully configured and remotely managed network devices to branch offices.
- Orchestration capabilities: As panel leader Zeus Kerravala says, network modifications should be only orchestrated as part of the application behavior. In other words, the application should direct the network to create a dedicated path between the two points for the duration of the session and then remove the path when the session ends.
- Application communication through APIs: This is the most effective way to perform network orchestration. It also helps agencies adopt true policy-based networks and enable policies to drive application and network changes.
- Big data and analytics: An SD-WAN should be able to effectively collect and analyze relevant data. This information is critical for helping agencies fine-tune the network to optimize application performance.

APPLICATION MANAGEMENT: A NEW PARADIGM

New methods of delivering apps are evolving to keep pace with how they're being used.

A decade ago, most government applications were built on client/server environments and housed in agency data centers. Today, most applications are developed and managed in many different ways. They're often developed collaboratively in the cloud, using innovative approaches like DevOps and agile software development.

And instead of consuming applications on PCs connected to data center servers, employees can now access applications on mobile devices, through an app service or the cloud. All of this requires changing the way applications are secured, delivered and monitored. Today's applications must be able to work across different types of networks and be accessible by any device, located anywhere in the world. That means they must be fully available and secure at all times.

Agency networks generally use Application Delivery Controllers (ADC), network appliances that balance application workloads as needed. This helps ensure applications are always available, secure and performing optimally. Besides continuous load balancing and distribution, ADCs monitor server health and accelerate applications when needed with compression, caching and TCP optimization. More specifically, ADCs provide:

Layer 3, 4 and 7 load balancing and distribution: Layer 3 provides switching and routing technologies, while Layer 4 is the transport layer, responsible for transporting data between hosts. Layer 7 is the application layer, and routing is determined based on characteristics of the HTTP header, data type and contents.

Application acceleration: Different systems achieve this by different methods; including caching, TCP optimization, compression, and bandwidth optimization.

SSL offloading: This transfers terminating SSL sessions from the application server to the ADC.

DDoS protection: Protecting against Distributed Denial of Service attacks is more important than ever. ADCs pitch in by handling troublesome traffic instead of passing it on to application servers. They can also protect DNS servers via a DNS Application Firewall.

Web Application Firewall: This filters out bad HTTP traffic between a client and web application.

Most agency networks are already using ADCs, and the vast majority of them are hardware appliances. While they provide great value for traditional applications, they often can't function as well in networks that have become more virtualized, cloud-enabled and software-based. They're also running applications born in the cloud. They may have trouble scaling to accommodate large amounts of traffic. The devices must be patched and upgraded regularly, and they require on-site expertise for installation, configuring and troubleshooting.

> Today's applications must be able to work across different types of networks and be accessible by any device, located anywhere in the world.

In contrast, a virtual ADC (vADC)—a software-based system that manages applications in a virtual machine instead of a physical appliance—is more flexible, scalable and customizable. Because it is designed for virtualized and cloud environments, it works very well with applications developed and run in the cloud. Gartner's latest Magic Quadrant for ADCs notes software-based ADCs are becoming more popular for these and other reasons.

Because they are controlled by software, vADCs can quickly scale as needed. This not only provides better performance and reliability, but helps agencies pay for more capacity only when required. The software architecture also makes it easier to add additional features and capabilities like application-level firewalls, authentication and authorization, and SSL processing when needed. Finally, advanced vADCs also support multi-tenancy. This essentially provides the ability to partition into multiple virtual ADCs.

CREATE A TRULY SECURE NETWORK

Security remains a critical factor, even as security tactics evolve to meet new threats.

Large organizations across all sectors face real challenges in keeping their networks secure, and government agencies are no exception. In fact, a 2016 report from SecurityScorecard[1] found government organizations had the lowest security scores of any sector.

It tracked 35 major data breaches among government organizations between April 2015 and April 2016. Along with malware infections and software patching cadence, government struggles most with maintaining network security.

One of the reasons government agencies are having such a difficult time securing networks might be because they have been using the same technologies and techniques for years. According to a report from 451 Research[2], relying too heavily on network and endpoint security technologies simply doesn't cut it anymore, especially in fighting multi-stage attacks. While still useful, these technologies can't handle the threats posed by the multitude of devices, WiFi, cellular and satellite communications. They also have problems protecting data stored in the public cloud—something 84 percent of federal respondents say they plan to do within the next 12 months.

Fully protecting federal networks requires a more comprehensive approach. And that approach must involve securing remote access for mobile and third-party users, securing data at rest, implementing network and host segmentation, and employing multilayer security to improve availability.

Requiring secure remote access is critical to network security, especially in today's business environment. Users expect to be able to access applications, data and other resources from their own devices on their own time. It's difficult to ensure all employee devices are fully secure. It's equally difficult to detect employees who use insecure mobile devices.

A Ponemon Institute study[3] found even if an organization uses controls, more than half of employees circumvent or disable required security settings. To ensure secure remote access, agencies must automate and enforce policies, require multifactor authentication, and configure remote access authentication methods and encryption levels. It's also helpful to secure traffic between a remote access server and remote users via signing, encryption or tunneling (encapsulating and transmitting data).

Securing data at rest (stored data, as opposed to data currently traversing the network) is also critical. While most of the security risks apply to data in use, data at rest is still vulnerable if the network is compromised. Encryption at the file or folder level protects data not only on premise, but in the cloud. It's also useful to employ application-level encryption, which helps secure data as it is created. Virtual machine encryption is another critical component.

Segmenting the network improves network security by limiting access to critical applications and data. Network segmentation typically involves configuring firewalls, virtual LANs and gateways, which lets agencies split the network into multiple zones. This way, each zone can have its own security policies, and data can be segmented based on its sensitivity or use.

Agencies that have adopted software-defined networking (SDN) can more easily achieve micro-segmentation. This helps facilitate a more advanced and flexible segmentation approach. Micro-segmentation uses virtualization and software-defined network technologies to segment data and workloads down to the individual user level if needed.

Finally, one of the best ways to thwart multi-layer DDoS attacks is by adopting a multilayer approach to network security. That means that in addition to on-premises protection at the network perimeter, it's important to protect cloud-based resources. That includes defense at Layers 3, 4, and 7, network-based encryption, and packet shaping for specific data and applications traversing the network.

[1] https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Govt_Cybersecurity_Report.pdf?t=1467846772274

[2] https://451research.com/images/summit_assets/Presentations/9.05._Datacentre_Efficiency_Keynote._Lawrence.pdf

[3] http://www.ponemon.org/local/upload/file/AT%26T%20Mobility%20Report%20FINAL%202.pdf

DATA CENTER CONSOLIDATION: IT'S THE NETWORK'S TURN

After consolidating servers and storage, agencies must now include the network.

Since 2010, federal agencies have worked hard to consolidate data centers in compliance with several mandates, including the Federal Data Center Consolidation Initiative (FDCCI), the Federal Information Technology Acquisition Reform Act (FITARA), and most recently, the Data Center Optimization Initiative (DCOI). Thousands have already been shuttered or consolidated. And OMB expects that number to increase further by 2018.

In many cases, agencies have focused on server and storage reduction and virtualization. The network remains a distant third. In many ways, consolidating servers and storage has been the "low-hanging fruit" in data centers. That's partly because networking has traditionally been more difficult to downsize and modernize. Yet it's a crucial part of effective data center consolidation. What's more, with modern technologies and tools, it's no longer as difficult.

Network virtualization is the perfect stepping-stone for moving to cloud services.

The traditional networking model in data centers is inefficient, fragmented, difficult to scale, expensive and hard to manage. A more virtualized, software-based networking model addresses these challenges.

So virtualizing the network is the first step. This removes most of the hardware from the equation, and replaces it with software. The software deploys and manages network servers and resources. While some physical networking devices remain, their job is to forward packets. This infrastructure helps network managers program, deploy and manage virtual networks on demand; scaling and deploying them wherever and whenever required.

Network virtualization typically requires two technologies—software-defined networking (SDN) and network function virtualization (NFV). SDN separates network control and data flow, combines multiple physical devices into one logical network, and helps IT staff centrally manage and program network services. SDN improves security by centralizing security policy and configuration management information, blocking malicious traffic from endpoints, and automating network security remediation. It also provides more visibility throughout the network.

NFV separates network functions like intrusion detection, routers, application delivery controllers (ADC), load balancers and firewalls from the hardware devices upon which they run. It replaces the hardware with software. NFV and SDN usually are employed together to create a virtualized network infrastructure.

The next layer of network virtualization extends software-defined network capabilities to wide area networks that connect remote users and branch offices. The SD-WAN (software-defined wide area network) combines multiple physical networks into one virtual network. This helps network managers continuously balance the load and route packets correctly and efficiently. It also simplifies network management, configuration and upgrading while ensuring high availability, visibility, performance and scalability.

Cloud-enabling the data center is the next logical step. With the federal government's cloud-first mandate, it's on the minds of every agency IT leader. While some have made greater forays into the cloud than others, all are looking for more opportunities.

Network virtualization is the perfect stepping-stone for moving to cloud services because the network is now centrally managed, and operating with full visibility. Once the network is virtualized, it's much easier to manage not only physical workloads, but virtual and container-based workloads that originate in the cloud.

By cloud-enabling the data center, it's also simpler to provide compute resources to employees on demand. Agencies can also provide entire networks on demand, configured for specific use cases, geographies, workloads or employees.

MODERN APP DELIVERY

A software-first networking approach focuses on improving mission agility.

The current approach to building networks and data centers is outdated. Today's world is filled with heightened mission demands that place an increased burden on agency's IT departments to adapt without an increase in budget.

Key trends driving an increase in mission demands are:

Mobility—With an increasingly mobile workforce, agencies are being forced to evaluate device, network and security stacks to provide secure access of applications to the mobile endpoint.

Cloud—The rapid adoption of cloud-based applications such as Office365 is challenging the concept of the traditional network security perimeter to ensure government data is protected when accessed from a cloud.

Security—Breaches are on the rise at a network, application, data and user level like never before.

Infrastructure-as-a-Service—Agencies are adopting IaaS to provide flexibility and cost savings for developing and deploying new applications.

Dev Ops app methodologies—This is increasing the speed of application innovation at agencies while also drastically changing networks patterns to E-W traffic.

"Since these traditional network architecture approaches tend to be hardware and device centric, agencies have typically seen slow application deployments, as well as reduced responsiveness for workers and developers while being costly to manage, upgrade and maintain—resulting in overall lack of agility for the network administrator," says Faisal Iqbal, senior director of Networking at Citrix Public Sector.

Many organizations respond to these changing dynamics by buying more tools and hardware. While this strategy can work in the short term, it will inevitably lead to more hardware purchases, increasing costs and complexity.

The way forward is to move to an open architecture that supports your legacy datacenter and apps of today, but also allows for the adoption of cloud and hybrid approaches in the future.

Instead of cobbling together multiple solutions across hardware, software and cloud to solve this application delivery challenge, consider a holistic platform-agnostic approach to App Delivery—an approach that is "software-first" by abstracting your apps and workloads from a specific physical network devices, hypervisor, cloud or container.

The software-first approach goes even further by providing visibility for all applications in your environment regardless of location or platform. "This type of network visibility can help agencies make smarter decisions in regards to when applications are deployed, where capacity is needed and where there are security breaches." Iqbal says, "all while providing investment protection to ensure you can get the longest life out of your hardware."

A software-first approach to networking also generates efficiencies by consolidating duplicative hardware appliances. Instead of managing multiple network appliances for individual siloed functions—Load Balancing, GSLB, VPN, App Firewall, DDOS protection, Web Proxy, and Auth Gateway—a software-first approach can virtualize and consolidate these functions while retaining the performance benefits of hardware, thus ensuring administrators retain control.

The software-first approach can reduce or even eliminate another challenge with traditional networks—managing spikes in network traffic. Whether caused by an unexpected event like a national disaster or security breach, traditional networks have difficulty handling these spikes because they are statically programmed. Software-based networks, which have on-demand capacity, allow networks to ramp up when necessary, much like cloud-based architectures.

A traditional hardware-centric approach to networking is too limited to address today's mission requirements, which require more speed, scalability, agility and visibility. Only a software-first approach to application delivery can provide:

- a flexible approach that allows faster scaling and the ability to deploy new services/applications on demand
- a secure utility based consumption model that allows the business to use the best technology, whether in house or externally to meet their business strategy
- easy scaling up or scaling down of IT services to meet changing business demands
- significantly consolidated network devices and drive out operating costs
- the best security and IT control without hindering the business or user productivity

Visit the Citrix Government Briefing Center at **www.citrixgbc.com** to learn more about how you can take advantage of a software-first approach to networking to meet your mission-critical government objectives.