SDN: POWERING THE NEXT GENERATION OF GOVERNMENT NETWORKS

Networks are undergoing a transformation, thanks in large part to next-generation technologies and services that necessitate new and different infrastructures. The proprietary hardware of yesterday is being replaced by open technologies that are not only less expensive, but also customizable to meet multiple needs and support new applications and services. Software-defined networking (SDN) is helping make this possible.

The Open Networking Foundation (ONF), a technology organization dedicated to furthering the adoption of software-defined networking, defines SDN as "... an emerging architecture that is dynamic, manageable, cost-effective and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services."[1] Programmability, agility and vendor-neutrality are just some of the benefits of SDN.

Organizations of all types and sizes are adopting SDN to meet the needs of increasingly bandwidth-intensive and cloud-based applications for both their employees and their customers. Government agencies, too, are realizing the benefits of using SDN to build software-defined wide-area networks (SD-WAN) at lower cost.

According to Allied Market Research, the world SDN market is expected to reach $132.9 billion by 2022, growing at a compound annual growth rate of 47 percent between 2016 and 2022. Network complexities, cost and time efficiency, and flexibility in network infrastructure are some of the drivers of SDN adoption, according to the analyst firm.

BENEFITS OF SOFTWARE-DEFINED NETWORKING

Software-defined networking is fundamentally changing the way networks are built. Its benefits are many, ranging from agility and cost savings to efficiency and security. In particular, SDN offers four benefits of interest to government agencies:

Standardization: Governments lag behind enterprises in their network infrastructure. Siloed IT systems and infrastructures in government agencies have led to an incomplete view of data, which hampers service delivery and employee productivity, and increases dissatisfaction among constituents. Agencies and facilities need to upgrade their networks to meet the needs of modern government, modern citizens and the modern military. An SDN overlay on existing networks can bring together what previously could not be integrated, providing accessibility for all systems and all data regardless of where it resides.

Cost Savings: SDN does not require proprietary hardware to run. Its architecture decouples the network intelligence from the hardware and creates "dumb switches" that are managed from a central controller. As such, these switches can be industry-standard servers or even existing hardware controlled via SDN controllers. This can equate to huge cost savings for organizations looking to harness the power of SDN; they can experience SDN's value proposition in an economic, cost-effective manner, while gradually migrating to an SDN environment.

Streamline Operations: SDN centralizes controls for better management of the entire network. Because the intelligence of the network is located in a separate SDN controller rather than at each point in the network, provisioning and management becomes a more centralized and holistic endeavor. Organizations can manage both physical and virtual switches, as well as other network devices, from one central controller. This equates to less downtime and more stable networks, as there is less room for error in provisioning new equipment.

SDN AND AUTOMATION TOGETHER SUPPORT THE GOAL OF RAPIDLY RESPONDING TO CHANGING THREAT ENVIRONMENTS— WHICH IS AN ESPECIALLY CRITICAL GOAL FOR THE MILITARY.

Security: SDN not only centralizes the management of the network in one controller, it also centralizes security. The SDN controller can distribute security and policy information consistently throughout the organization, ensuring all points on the network are secure. What's more, SDN can make it easier to collect network usage information, which could help organizations better detect anomalous behavior that could point to a security breach or outright attack.

SDN and automation together support the goal of rapidly responding to changing threat environments—which is an especially critical goal for the military. Real-time information can help organizations understand and respond to attacks faster and with more precision.

SD-WAN: A MORE INTELLIGENT NETWORK

Much of the growth of SDN adoption will include SD-WAN, a next-generation solution designed to simplify complex networks, increase control and visibility, reduce costs, and deliver consistent network and application performance across a distributed government agency environment. SD-WAN utilizes open-source technologies and provides a level of intelligence to the network that doesn't exist in traditional WANs, enabling smarter, more efficient routing of traffic.

The application-aware nature of SD-WAN enables IT administrators to determine the most intelligent path for their applications, and to push, manage and update policies for optimal application and network performance to conduct the business of government. What's more, SD-WAN is centrally managed, so all provisioning and changes to the network and applications are done from one location, reducing the amount of time and manpower necessary to manage the network.

The ability for a government organization to apply SD-WAN technologies across an existing network, and grow that network's bandwidth and capability with high-speed broadband, could be a game-changer. SD-WAN has the potential to unburden agencies from their legacy connections and unleash new possibilities from a virtualized network environment.

SD-WAN is being adopted at a nice clip. Research firm Gartner predicts that by the end of 2019, 30 percent of enterprises will have deployed SD-WAN technology in their branches,[2] while IDC predicts the SD-WAN market will reach $6 billion in annual revenues by 2020, thanks to the need for faster, more cost-effective and more efficient networks.[3]

EXAMPLES OF SDN USE IN GOVERNMENT AGENCIES

SDN is proving its value in a number of vertical markets, and the government space is no exception. The U.S. Army, the National Security Agency and the Social Security Administration, to name a few, are adopting software-defined network technologies to address a range of issues, including support for more cloud-based applications, better network control, tighter security, and enhanced communications across numerous locations.

The U.S. Army, for example, is incorporating SDN in its plans for its network of the future. In a publication titled "Shaping the Army Network: 2025-2040,"the military branch outlined its long term strategic network efforts. By 2040, the Army expects every chain of command will be able to access its network from any location, and it is looking to SDN to help it achieve that goal. In addition, the Army is looking for its future network to be more intelligent and automated – another benefit of SDN.[4]

SD-WAN HAS THE POTENTIAL TO UNBURDEN AGENCIES FROM THEIR LEGACY CONNECTIONS AND UNLEASH NEW POSSIBILITIES FROM A VIRTUALIZED NETWORK ENVIRONMENT.

Because SD-WANs don't rely on expensive MPLS networks to extend the WAN and centralize the management of the network, the Army and other military organizations are able to save money and increase the security of the data, while enjoying full visibility and control of the network.

The **National Security Agency**, meanwhile, is using SDN technology to replace its current network, an effort that will ultimately meet bandwidth needs and give administrators better control over the network while remaining secure. With SDN, network administrators are able to adjust network traffic flow for a dynamic environment, while also gaining a comprehensive view of the network. Plus, SDN offers administrators more control over network security—a must for an agency that deals primarily with classified information.[5]

The **Social Security Administration** also hopes to realize the benefits of SDN. The agency has planned a $300 million IT overhaul that includes virtualization, cloud and SDN technology. Its current infrastructure currently runs on legacy equipment with extremely slow upload speeds, resulting in frequent equipment breakdowns and loss of productivity by SSA employees. Under its IT modernization plan, the agency would achieve agility, flexibility, and increased productivity, in addition to annual cost savings.[6]

SDN IN GOVERNMENT: THE NETWORK IS KEY

Software-defined networking holds the promise of greater efficiencies at lower operating costs. However, as with any other technology, the network is critical. Government agencies need highly reliable, secure and flexible networks that can help them achieve their missions. SDN and SD-WAN technologies can be simply added to an existing network to immediately deliver unprecedented network visibility and centralized control, in order to optimize network and application performance across all locations. The ability to combine SDN with high-speed broadband delivers a new, cost-effective business model for adding broadband, as well as creates intelligent SD-WAN connections to accommodate the growing need for bandwidth.

Comprehensive and uncompromised connectivity is key to ensuring agencies can reap the benefits of SDN. Next-generation technologies such as cloud computing, social media, big data analytics, mobility and the IoT can drive business transformation for all organizations, including government. Therefore, a solid and flexible network foundation is imperative.

However, delivering uncompromised connectivity can be costly and complex for many agencies. That's why agencies should work with a network service provider that can deliver both the SD-WAN and high-speed broadband connections that are essential to meet evolving mission requirements.

CONCLUSION

The growing popularity of next-generation technologies and services such as IoT and cloud computing necessitate the transformation of legacy networks to support them. For organizations of all sizes, software-defined networks hold the promise of lower cost, greater flexibility, and easier management. Government agencies already are adopting SDN technology to support the high-bandwidth, dynamic nature of applications today and in the future, as well as to streamline their operations and realize cost savings for their constituents. Key to SDN is a network robust enough to provide the platform for a digital transformation.

1 "Software-Defined Networking (SDN) Definition," Open Networking Foundation https://www.opennetworking.org/sdn-resources/sdn-definition

2 Andrew Lerner, "Predicing SD-WAN Adoption," Gartner blog, Dec. 15, 2015 http://blogs.gartner.com/andrew-lerner/2015/12/15/predicting-sd-wan-adoption/

3 "IDC Forecasts Strong Growth for Software-Defined WAN As Enterprises Seek to Optimize Their Cloud Strategies," press release, IDC, March 24, 2016 https://www.idc.com/getdoc.jsp?containerId=prUS41139716

4 Phil Goldstein, "The Army's Network of the Future Will Be Software-Defined," NextGov FedTech, April 14, 2016, http://www.nextgov.com/next-gov-sponsored/fed-tech/2016/04/armys-network-future-will-be-software-defined/127475/

5 "NSA's SDN Push," NextGov FedTech, March 21, 2016, http://www.nextgov.com/nextgov-sponsored/fed-tech/2016/03/nsas-sdn-push/126832/

6 Kayla Nick-Kearney, "Social Security Planning $300M IT Overhaul," FedScoop, July 14, 2016, https://www.fedscoop.com/social-security-will-use-aws-to-build-new-300-million-software/