The Software-Defined Enterprise With Cisco

Introduction

The pressure to digitally transform virtually every aspect of the business is disrupting companies in every industry. Strategies vary broadly, though the aim of any digital transformation initiative is to leverage technology to build new business models, processes and/or systems that bring connectivity and visibility into business operations.

To drive sustainable change, business leaders need to work closely with IT executives to develop the environment, resources and solutions needed to support a truly digital business. They also need to make smart choices when it comes to which technologies are deployed.

One way that organizations are modernizing their digital enterprises is by moving away from traditional network technology to software-defined infrastructure. This includes:

Software-Defined Wide Area Networks (SD-WAN): Pivoting from Wide Area Networks (WAN) that are rooted in providing access to centralized data centers to modern, cloud-based network technologies designed to provide increased bandwidth at lower costs, enhanced security and other benefits.

Software-Defined Data Center (SDDC): Moving to "choose your cloud" data centers where all infrastructure is virtualized and delivered as a service.

Problem statement

Software-defined technologies are emerging as not just "nice to have," but as an enabler of the modern digital business. In fact, a previous Gartner survey showed that more than one-third of organizations see cloud investments as a top-three investing priority.[1] This whitepaper examines how software-defined access and technologies can address key challenges that organizations face as they move forward with digital transformation and help enterprises run far more efficient IT environments.

Background

A host of challenges

1. IT infrastructure complexity: This is on the rise, largely due to the proliferation of multicloud environments. Organizations oftentimes deploy multiple tools and applications to manage a growing number of platforms and components, which of course adds complexity and demands on IT staff. This is especially true for global enterprises with multinational operations.

2. Operational risk and downtime: No company can afford a lengthy period of downtime for critical business systems. Even a data center or network outage lasting a brief period can lead to negative results such as high costs, especially for businesses with revenue models depending heavily on the data center for customer service delivery.

3. Decreased productivity: Downtime can also result in a large decrease in employee productivity because workers don't have access to the resources they need; disruption to the business that can lead to customer dissatisfaction and loss of loyalty, and loss of revenue from the inability to conduct transactions with clients.

4. Degraded service: Even if systems and networks are not fully down, companies might have to deal with degraded service. This can result in slow response times for customer inquiries, the erratic performance of applications and websites, and other issues. The upshot can be irritated customers who end up taking their business elsewhere.

5. Speed of business: Companies today also have to deal with the challenge of keeping up with the fast pace of business. Whether it's delivering new products or services, addressing customer feedback, creating new applications, getting the right data to the right end users or some other factor, speed is vital in today's business environment.

6. Lack of visibility into networks, workloads and applications: Along with rising complexity in IT infrastructures comes the difficulty of having enough visibility to identify risks such as unauthorized access or data misuse. The rise of mobile devices and apps, as well as the growth of the Internet of Things (IoT) and edge computing, have made visibility all the more necessary and challenging. A report from 451 Research shows that the number of IoT connected devices (excluding PCs, smart TVs, and game consoles) will reach nearly 14 billion in 2024, for a Compound Annual Growth Rate (CAGR) of 12%.[2]

7. Navigating regulatory compliance: New data privacy regulations have been passed, including the final components of General Data Protection Regulation (GDPR) in 2020 and the California Consumer Privacy Act of 2018 (CCPA) that went into effect on January 1, 2020, with modifications made throughout 2020. Additionally, there is consumer privacy protection state legislation on the horizon. These laws put increasing pressure on organizations to safeguard data such as customer records, but this becomes more difficult when information is stored in multiple locations and cloud services.

These are just a handful of the challenges that organizations face when it comes to digital transformation. Also, data centers and networks today must be able to function without errors or downtime, to support constant service delivery to end users, business partners and customers. The proliferation of multicloud models requires new approaches to security and regulatory compliance. Workloads run and data flows everywhere: in the cloud, on-premises, on mobile devices, at the edge, etc. And in many cases, workloads and data are ineffectively governed by inconsistent policies.

Solutions

For years, organizations have been relying on traditional fixes to these and other challenges. But, for a variety of reasons, this approach may present many challenges for digital businesses.

Fortunately, there is a modern solution: software-defined access. Software-Defined Wide Area Networks (SD-WAN) and the Software-Defined Data Center (SDDC) are excellent solutions for this ever-more-complex environment — and go hand in hand when transforming IT.

The benefits of SD-WAN

Organizations are finding that in the cloud era, it's a much better approach to move to SD-WAN, which has emerged as the most effective way to securely connect all users and devices within a multicloud environment to a single fabric. The move to SD-WAN also represents a major shift in network strategy for companies. For years, organizations have been relying on traditional WAN to connect users within particular geographical areas. But for a variety of reasons, this approach may present a number of challenges for digital businesses.

As cloud initiatives continue to crop up at many organizations, CIOs and other IT executives are under pressure to reevaluate their WAN requirements. Research firm IDC says the SD-WAN market will grow at a 30.8% CAGR through 2023 to reach $5.25 billion.[3] The adoption of cloud services, growing volumes of cloud data and use of virtualization across traditional WAN architectures has led to performance bottlenecks, which impair user productivity when connecting to cloud applications from branch or remote office locations.

More traffic, more users, more devices, more data and a greater level of complexity now exists with and on corporate networks. With so much more traffic on the network, organizations are more likely to lose visibility of exactly who or what is on the network. This presents huge security risks. The surface area for attack is growing significantly and with so many new devices becoming connected via IoT, there'll be even more potential attack points. IoT, as a model, also generates more data that needs to be accounted for.

How SD-WAN addresses the shortcomings of WAN technologies

By enhancing or replacing legacy branch routers with virtualization appliances that can control application-level policies and provide a network overlay, less costly internet links can act more like a dedicated circuit. This makes it easier to set up connections for branch offices and other remote personnel.

SD-WAN solutions can be physical or virtual appliances and can be installed in small remote and branch offices, large headquarter facilities or data centers. They're also available via cloud platforms.

With SD-WAN, a centralized controller is used to set policies such as bandwidth priority and restrictions. The technology takes into account the policies and the availability of network bandwidth to route traffic, which helps ensure that application performance meets service-level agreements.

Policies can be configured once from a central location and then pushed out to a multitude of devices. With an SD-WAN fabric, companies can connect campuses, branch offices, mobile users, devices and across multiple clouds.

Strong security is among the biggest benefits of SD-WAN, which can provide secure communications over any transport. Via a Virtual Private Network (VPN) overlay, data plane traffic is encrypted, and multitenancy options are available to segment sensitive traffic. Cloud security features can operate on a much larger scale than a typical on-premises WAN.

This technology simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism.

Other concerns with traditional WAN infrastructure involve complexity, inefficiency and security:

A lack of centralized management

Time-consuming troubleshooting with each WAN site in its own silo

A lack of secure and reliable WAN transport other than MPLS, and even with MPLS, there's no inherent data plane encryption

No visibility and control of who or what is consuming bandwidth on the WAN

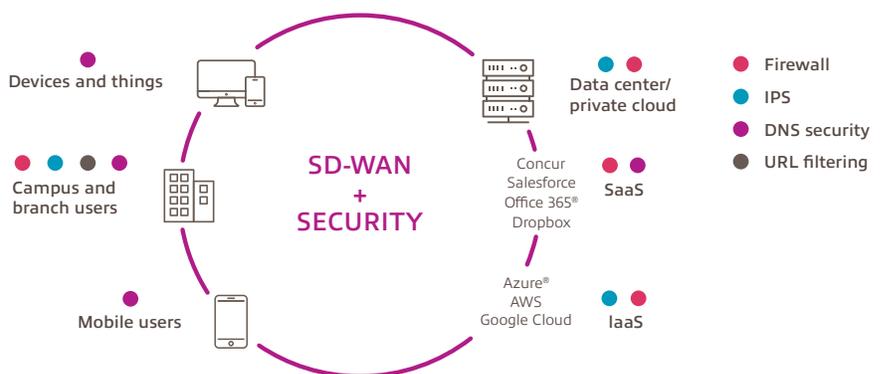Manual configuration of the WAN device at each remote location when policy changes are required

Cisco and SD-WAN

The Cisco® SD-WAN solution is an enterprise-grade WAN architecture overlay that enables digital and cloud transformation for enterprises. It fully integrates routing, security, centralized policy and orchestration into large-scale networks.

Cisco SD-WAN is highly automated, secure, scalable and application-aware with rich analytics. Cisco SD-WAN addresses the problems and challenges of common WAN architectures and provides the flexible deployment models needed to meet the vast compliance regulations found across all verticals.

Cisco SD-WAN offers:

- Centralized management and policy management, as well as operational simplicity, resulting in reduced change control and deployment times
- A mix of MPLS and low-cost broadband or any combination of transports in an active/active fashion, optimizing capacity and reducing bandwidth costs
- A transport-independent overlay that extends to the data center, branch or cloud
- Deployment flexibility: Due to the separation of the control plane and data plane, controllers can be deployed on-premises or in the cloud, or a combination of either. Cisco vEdge® router deployment can be physical or virtual and can be deployed anywhere in the network.
- Robust and comprehensive security, which includes strong encryption of data, end-to-end network segmentation, router and controller certificate identity with a Zero Trust security model, control plane protection, application firewall and insertion of Cisco Umbrella®, firewalls and other network services
- Seamless connectivity to the public cloud and movement of the WAN edge to the branch
- Application visibility, and recognition and application-aware policies, with real-time Service-Level Agreement (SLA) enforcement
- Dynamic optimization of Software as a Service (SaaS) applications, resulting in improved application performance for users
- Rich analytics with visibility into applications and infrastructure, which enables rapid troubleshooting and assists in forecasting and analysis for effective resource planning[4]

Devices and things

Campus and branch users

Mobile users

SD-WAN + SECURITY

Data center/ private cloud

Concur Salesforce Office 365® Dropbox — SaaS

Azure® AWS Google Cloud — IaaS

Firewall

IPS

DNS security

URL filtering

Source: Cisco. (October 2018). CVD — SD-WAN Design Guide.
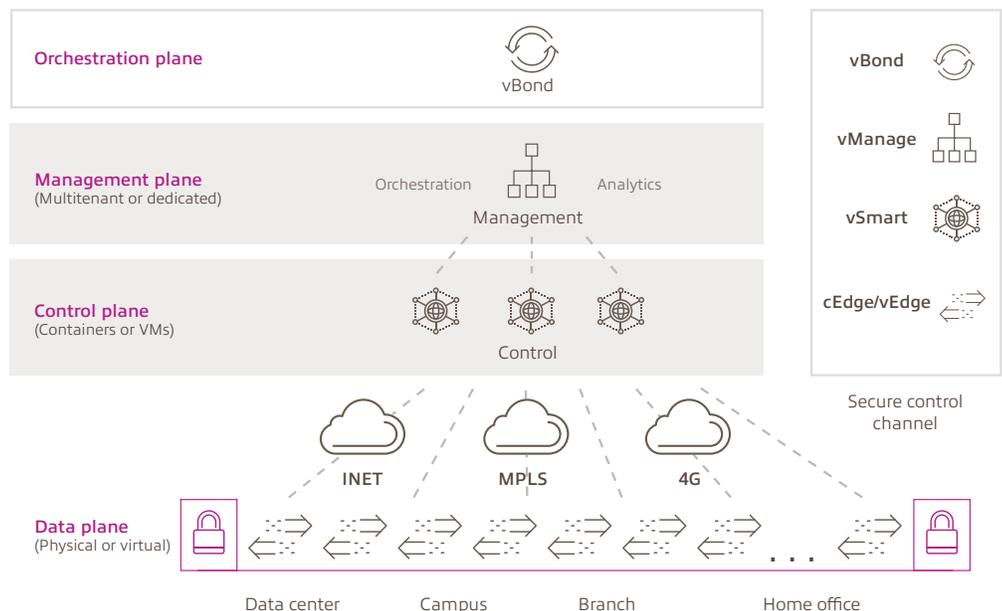
1.800.INSIGHT • insight.com

How does Cisco SD-WAN work?

Through the Cisco SD-WAN vManage console, you can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, colocation facilities and clouds to improve network speed, security and efficiency. After setting your preferred templates and policies, Cisco SD-WAN identifies connectivity and contextual issues to determine optimal paths for users to get to their destination, regardless of the connectivity they're using.

Whether hosted in the cloud or on-premises, Cisco vBond® and vSmart® orchestration and controller platforms authenticate and provision network infrastructure, making certain that the devices connecting to your SD-WAN are authorized. Once connected, the SD-WAN platforms find the best path to bring users closer to the applications they need, managing overlay routing efficiency, adjusting in real time to reflect policy updates and handling key exchanges in Cisco's full-mesh, encrypted delivery.

Cisco SD-WAN supports third-party API integration, allowing for even greater simplicity, customization and automation in day-to-day operations. Additionally, Cisco SD-WAN includes the common routing protocols that are critical for all enterprise SD-WAN deployments, such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP) and IPv6.

The Cisco SD-WAN fabric

Source: Cisco. (November 2018). Cisco SD-WAN Solution Overview. Doc #US43881619.

1.800.INSIGHT • insight.com

Cisco's cloud-first architecture
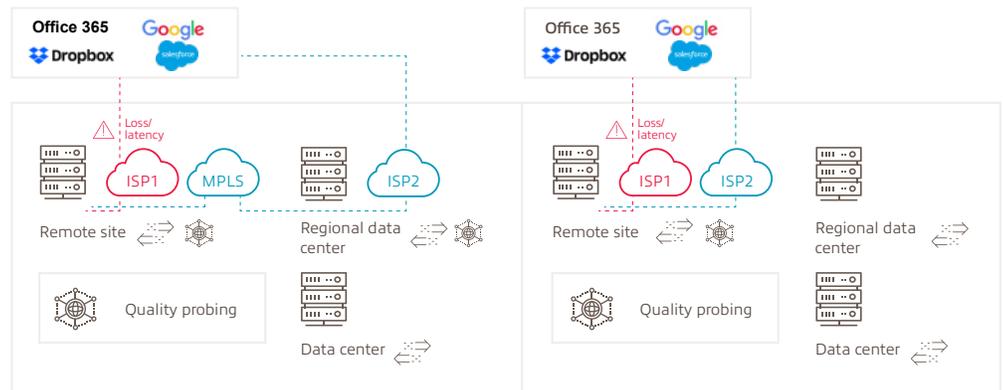
Source: Cisco. (November 2018). Cisco SD-WAN Solution Overview. Doc #US43881619.

Cisco® SD-WAN gives users the ability to not only manage connectivity across their WAN from a single dashboard, but to connect to cloud platforms with greater speed, reliability and efficiency.

Cisco SD-WAN OnRamp gives you enhanced, automated connectivity to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud environments without forcing you into existing multitenant gateways or a time-consuming manual process. Cisco SD-WAN gives instant visibility into cloud traffic, control over deployment and the convenience of automated management. Cisco SD-WAN OnRamp can also optimize the SaaS applications used in day-to-day operations.

1.800.INSIGHT • insight.com

The benefits of SDDC

A Software-Defined Data Center (SDDC), also referred to as a virtual data center, extends the concept of virtualization by abstracting, pooling and automating all resources and services within a data center. It enables the delivery of IT as a Service (ITaaS), much like the cloud enables the provision of SaaS or IaaS.

In an SDDC environment, management of the data center is fully automated by software and maintained through intelligent software systems. The use of open standard programming languages allows organizations to leverage third-party automation applications to streamline data center operations.

Within an SDDC, all elements of the infrastructure, including networking, storage, monitoring and management, are virtualized. The core components of the SDDC include Software-Defined Networking (SD networking or SDN);

Software-Defined Storage (SD storage or SDS); and software for management, monitoring, automation and orchestration.

SDN is an approach to network management that allows dynamic, programmatically efficient network configuration, leading to improved network performance and monitoring. This makes corporate network management more like cloud services than traditional network management.

SDN enables networks to be more flexible and easier to maintain, in part by centralizing network intelligence in a single component and disassociating the forwarding process of network packets from the routing process.

SDS is storage software for policy-based provisioning and management of data storage that's independent of the underlying hardware. It typically includes a form of storage virtualization to separate the hardware from the software that manages it. SDS software might also provide policy management for features such as data deduplication, replication, thin provisioning and backup.

Management, monitoring, automation and orchestration software enable administrators to provision, control and manage all of the SDDC components.

Organizations can see a number of benefits by deploying an SDDC. One is a reduction in manual processes and the time savings that can result from this. Because the SDDC enables organizations to configure, monitor and maintain data center components from a centralized interface, they do not need to physically update hardware as in the past.

Manual tasks are replaced by automation, and managers don't need to spend nearly as much time on such tasks, freeing them up to take on other responsibilities.

Another benefit is reduced management overhead. Because the SDDC allows enterprises to pool data center resources and provision and deploy them as needed, they can realize lower operating costs and refocus IT staff on more strategic priorities.

With an SDDC, companies can consume network resources as services, much as they do with the cloud. There's greater efficiency and agility, which helps organizations become the digital businesses they need to be in a fast-paced environment that thrives on speed. The flexibility and elasticity of resources across on-premises and cloud-based data centers enables easier workload migration across the environment.

Another advantage of the SDDC is that it provides consistent visibility, security and control across platforms, as well as common policy, governance and abstraction across heterogeneous environments. This is extremely important for global enterprises that have diverse and complex IT infrastructures.

Finally, the SDDC supports business continuity and disaster recovery strategies. These capabilities can be provided as cloud-based services within the SDDC, enabling companies to protect and recover applications and data without the need for a dedicated secondary site.

Through these benefits and capabilities, SDDC technology enables organizations to address the many challenges they face, including the rise in IT infrastructure complexity; operational risk and downtime; keeping up with the fast pace of business; having insufficient visibility into networks, workloads and applications; increasing regulatory compliance requirements and audits; and the need for data centers to function without errors or downtime.

1.800.INSIGHT • insight.com

Cisco and SDDC

SDDC offerings from companies such as Insight can help organizations make their digital transformation a reality. Insight's SDDC service offerings include assessment and application dependency mapping, solution positioning, proof of concept, pilot/limited production deployment and full production deployment.

We partner with leading SDDC vendors such as Cisco and VMware to create comprehensive solutions. For example, Insight helps organizations deploy and implement Cisco® Application Centric Infrastructure (ACI) and Cisco Tetration®. ACI is an SDN platform that delivers a network policy automation model. It enables software control of the network and how it operates so that software can automate and change the network based on current conditions.

ACI uses the concept of endpoints and policies, with endpoints being the virtual machines or traditional servers. Policies can be defined around which endpoint groups can communicate with whom. The platform uses a centralized controller called the Application Policy Infrastructure Controller (APIC), which creates application policies for the data center infrastructure.

Cisco Tetration is a hybrid cloud workload protection platform designed to secure compute instances in both on-premises data centers and the public cloud. Compute instances might be virtual machines, bare-metal servers or containers. The platform uses machine learning, behavior analysis and algorithmic approaches to offer a holistic workload protection strategy. It enables organizations to gain complete visibility into application components, communications and dependencies in the data center.

Insight also helps organizations deploy and implement VMware® NSX®, a network virtualization platform for the SDDC that delivers an operational model of a virtual machine for entire networks. With the platform, network functions including switching, routing and firewalls are built into a hypervisor and distributed across the environment. This creates a network hypervisor that acts as a platform for virtual networks and services. Virtual networks are programmatically provisioned and managed independently of any underlying hardware. NSX reproduces an entire network model in software, allowing organizations to create and provision any network topology within seconds.

Other benefits:

More predictable costs and reduced CapEx

Increased visibility with consistent policies throughout the environment

Faster provisioning and migration using automation

Fewer network incidents and greater network stability

Let Insight help.

More than ever before, your organization needs a reliable and secure network infrastructure that can scale and flex to support dynamic business requirements. From cloud solutions to centralized data centers, Insight and Cisco provide a variety of architectures and a comprehensive solution portfolio.

We offer:

Extensive architecture and network practice expertise

Software lifecycle management and SaaS solutions

Integrated service solutions for complex initiatives

A proprietary contract management portal

Insight OneCall™ Support Services

Insight is the optimal partner to support you with Cisco® initiatives. We've been a Gold partner since 1999 and today stand as Cisco's 4th largest national partner. Our more than 300 Cisco engineers hold over 1,000 Cisco certifications. With five Master Specializations, clients can trust that they are working with a leading Cisco partner.

CISCO
Partner

Gold Certified

Master Specialized in Collaboration

Master Specialized in
Data Center and Hybrid Cloud

Master Specialized in Networking

Master Specialized in Security

Master Specialized in
Service Provider Technology

Cloud and Managed Service
Provider Program

Conclusion

As noted, organizations are facing significant challenges when it comes to digital transformation. The SDDC and SD-WAN are crucial to creating a modern data environment: one that works in harmony with cloud services to deliver the kind of speed, flexibility, scalability and security organizations need to be truly digital businesses.

By first conducting a thorough assessment of their current IT environment, then determining how to deploy the right software-defined solutions, enterprises can enjoy an optimal transformation and excel in this emerging digital marketplace.

Rely on Insight's expert team and proven Cisco solutions to enhance your organization's access and data centers — for today and whatever the future may bring.

References

[1] Gartner Press Release, "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019," 2 April 2019. https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g
[2] 451 Research. (August 2019). IoT Market Monitor Report.
[3] IDC. (July 2019). Worldwide SD-WAN Infrastructure Forecast, 2019-2023. Doc #US43881619.
[4] Cisco. (October 2018). CVD — SD-WAN Design Guide.

1.800.INSIGHT • insight.com