DoyleResearch

Key Aspects of Security and Multicloud in the SD-WAN Transformation

By: Lee Doyle, Principal Analyst at Doyle Research

Sponsored by Cisco

Executive Summary

The most significant IT transformation of this century is the rapid adoption of cloud-based applications. Most organizations are now dependent on a number of SaaS and IaaS platforms to deliver customer satisfaction and empower employee productivity. IT teams are responsible for delivering a high-quality user experience for cloud applications while they struggle to manage a secure environment with advanced persistent threats.

SD-WAN technology is now the primary solution for distributed users at branch locations to connect to cloud-based applications. To meet the challenges of this multicloud world, SD-WAN technology is evolving to deliver secure, reliable connectivity across a multitude of cloud platforms. As all IT environments are unique, SD-WAN must enable a flexible approach with options for direct internet access, regional hosting and cloud-based routing, policy and security.

SD-WAN technology is now the primary solution for distributed users at branch locations...

As the center of IT operations moves to the IaaS cloud, IT teams need to think differently about how they secure and manage cloud resources. The goal is to combine the simplicity and agility of IaaS resources with the security, visibility and control of the traditional data center. SD-WAN platforms can extend their fabric to the cloud which enables IT to centrally administer and monitor remote user to cloud traffic.

Advances in software virtualization and the migration of intelligence to the cloud are driving the convergence of networking and security functionality at the edge of the network. Different types of users/devices connecting to the cloud (via the Internet) means security policies must be enforced at branch, data center and in the cloud. This convergence favors solutions with a broad range of network and security functionality – well integrated and flexible in its deployment models (i.e. on premise and cloud).

As organizations transition to a cloud-first security model, they will continue to deploy a range of security assets on-premise (and in the cloud) to protect against internal and external threats. Security capabilities, including firewall, intrusion detection, anti-malware and phishing and URL filtering, should be integral to the SD-WAN solution. IT organizations need to have flexibility in deploying SD-WAN and security instances at the branch, colocation facility or IaaS platform.

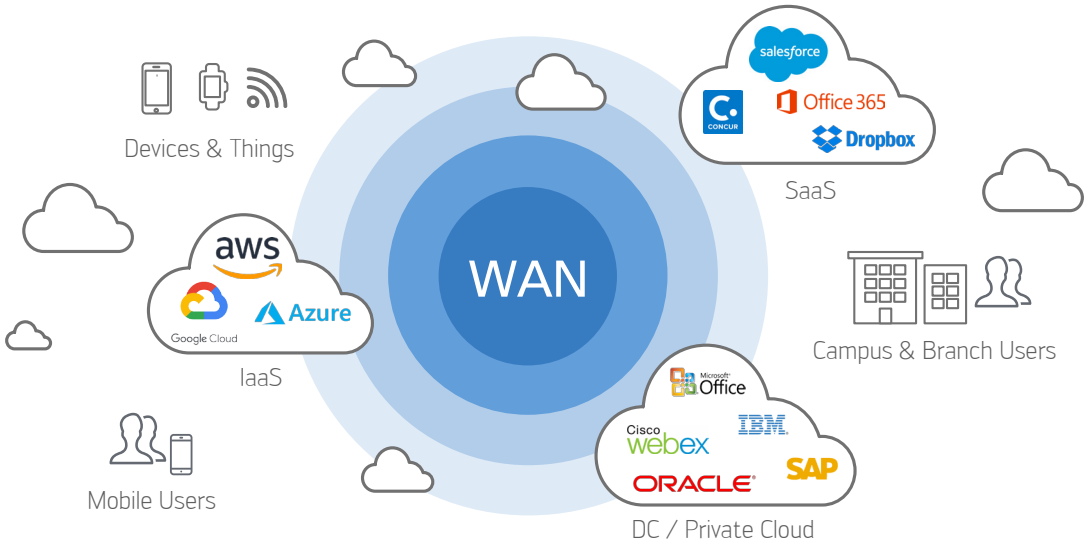
Advent of the Multicloud World

New cloud-based technologies make it easy for organizations to deploy/use applications across a mix of data centers, SaaS and IaaS platforms. As applications decentralize, the typical organization is also becoming more distributed as it “works” from branch locations, home offices and mobile locations. Multicloud enables IT to leverage an assortment of on premise (data center) and cloud-based (IaaS, PaaS and SaaS) resources to enable their agile IT operations.

Cloud and SaaS applications traffic flows from the branch to the cloud via direct Internet access. IoT (and other edge computing) applications require intelligence and low latency. The lack of a security perimeter means that network security intelligence needs to be deployed at the edge and leverage cloud-based intelligence to meet the evolving threat environment. Most IT organizations will deploy a defense in depth strategy with multiple (network) security elements at various points in their architecture (i.e. data center, branch and cloud). See Figure 1.

Figure 1

It's a Multicloud world



Multicloud Impact on Network Requirements

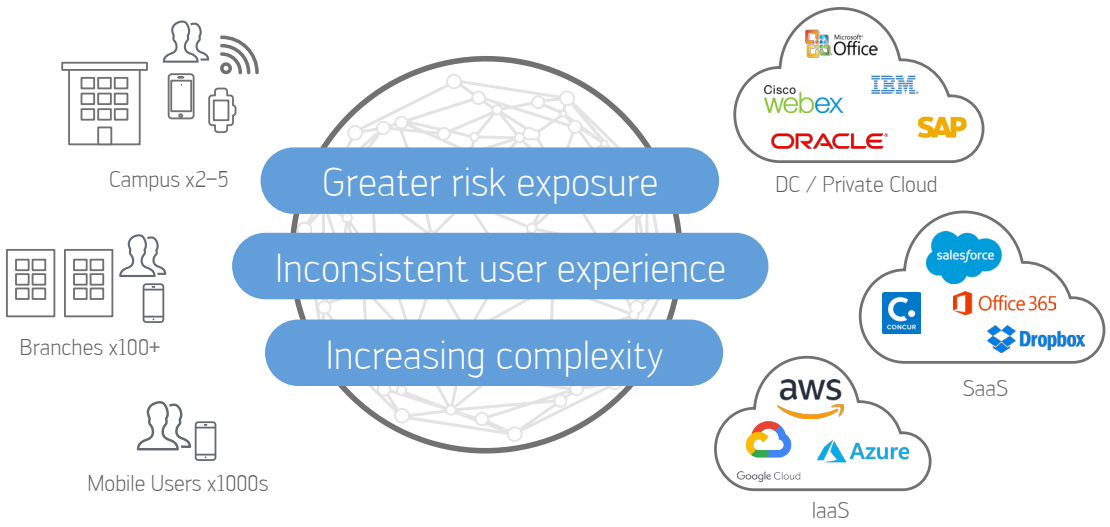
IT organizations are managing a range of private cloud, public cloud and SaaS platforms to provide their users (and developers) the flexibility to run applications on the most appropriate platform regardless of location. This results in a fragmented environment with different user requirements, multiple platform interfaces and ever-present security threats. In a multicloud environment, the WAN platform must deliver a consistent user experience and support secure application delivery anywhere it is required.

The complexity of multicloud IT environments creates a number of challenges for IT/Security teams.

The complexity of multicloud IT environments creates a number of challenges for IT/ Security teams. Each new cloud platform has a unique management/operational interface to be managed by IT personnel. IT needs to monitor multiple WAN routes to various cloud platforms and deliver quality of user experience for each environment (e.g. across AWS, Azure, Office 365 and Salesforce). The use of Internet links to connect to a variety of IaaS and SaaS platforms exposes the organization to increased security risks. See Figure 2.

Figure 2

Multicloud impact on network requirement



Flexible SD-WAN Multicloud Architectures

SD-WAN platforms are the onramp for cloud-based traffic. SD-WAN technology needs to identify the type and destination of traffic, understand its defined business and security policy and proactively route the traffic with appropriate prioritization. For example, organizations need to be able to apply different business and security policies to mission critical SaaS/IaaS applications, real time voice and video traffic, Office 365 usage, bulk file transfers and IoT traffic.

Organizations need the flexibility to architect their WAN to fit their unique business and application requirements.

Organizations need the flexibility to architect their WAN to fit their unique business and application requirements. In order to ensure quality of user experience for end-users, SD-WAN software must offer multiple paths and control points for Internet-based applications, including Direct Internet Access (DIA), Co-location at regional hubs and cloud-based gateways and make dynamic routing decisions across them in real time. Each access/control method has its role in the multicloud WAN architecture:

- **Direct Internet Access** – using one or more Internet links at remote sites to permit traffic from designated cloud-based applications to directly access the Internet.
- **Co-location Regional Hubs** – Host SD-WAN/security software at regional hubs (e.g. Equinix sites) can consolidate and secure branch traffic. This helps to simplify security operations.
- **Cloud-based SD-WAN** – Virtual SD-WAN instances can be spun up at IaaS partners (e.g. AWS and Azure) to control, prioritize and secure cloud-based traffic.

IT needs the tools that allow them to control, troubleshoot and centrally manage the IaaS cloud. SD-WAN provides the orchestration and intelligence to normalized operations across multiple IaaS environments. For example, it can help enable the underlays to connect to multiple edge cloud locations – which is otherwise a time consuming manual process.

The benefits of extending SD-WAN features to multicloud environments include:

- Normalized cloud user-experience for all kinds of applications
- Consistency for peering, security and QoS
- End-to-end observability which including analytics to solve packet loss and other slowdowns
- Automation capabilities to reduce manual provisioning of multicloud networking and security settings

SD-WAN and Multicloud Security Requirements

IT and Security teams need to consider a variety of threats to their remote branch locations.

The rise of cloud-based applications (and associated traffic pattern changes) requires a fundamental change in network security architectures. Direct internet access to a multitude of cloud-application applications exposes the organization to increased security risks. IT and security teams need the ability to securely connect any user to any application on any network. This requires a unified security architecture for remote users, at the branch, WAN and cloud.

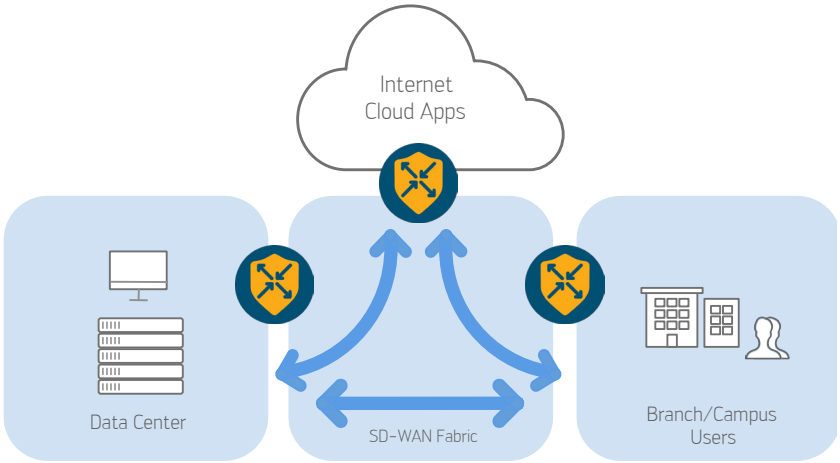
IT and Security teams need to consider a variety of threats to their remote branch locations. External threats include increased exposure to malware and phishing attacks via direct Internet and cloud access with its increased potential for sensitive data loss. Internal threats relate to untrusted access via malicious insiders, breach propagation and compliance concerns. Combating these external and internal security concerns requires a comprehensive, integrated security architecture.

Advances in cloud-based intelligence have enabled new network security solutions which are easy deploy, scalable, flexible and simple to manage. New network security capabilities enable IT to deploy a flexible balance of on-premise and cloud-based security which includes segmentation, encryption and end point authentication. On-premise security will continue to mitigate internal and external threat and cloud-based security adds the intelligence to combat external threats at scale.

Security architectures should enable security at the branch, co-location site and the cloud with the ability to centrally manage user policy end-to-end (from the user to the cloud). SD-WAN security provides traffic visibility to provide centralized network/security teams to "see" what applications are being accessed, what ports active and understand what data is in motion – even if encrypted. See Figure 3.

Figure 3

Security required on premise and in the cloud



Cisco SD-WAN Solutions for Multicloud Environments

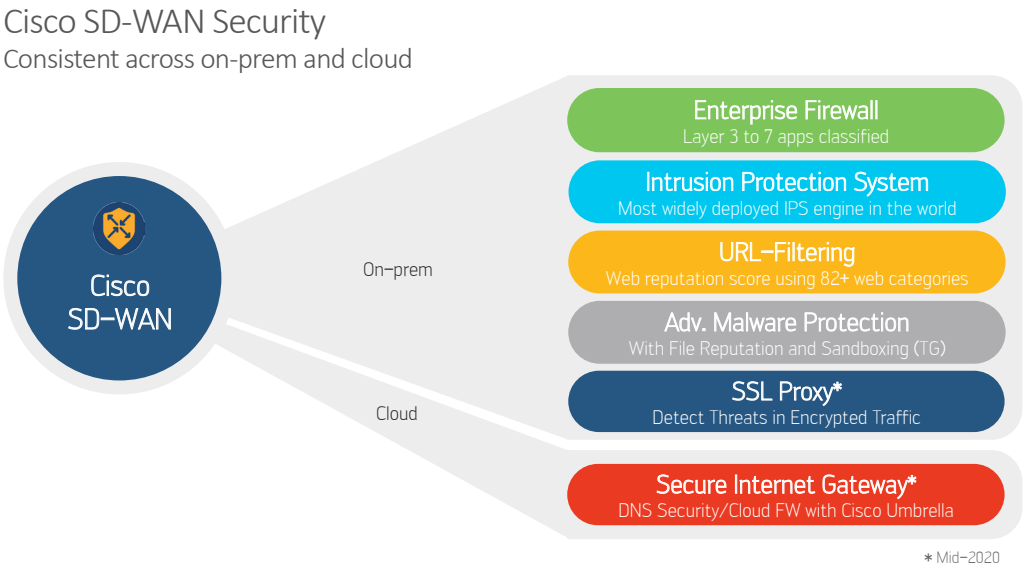
Cisco is the leading enterprise network supplier and provides a wide range of network solutions for branch, campus and data center connectivity. Cisco's SD-WAN solution makes it easier for IT to deploy new cloud-based applications, while maintaining a high level of security and optimizing the user experience. SD-WAN is part of Cisco's broader Intent-based networking strategy and comes integrated with security and cloud solutions. Cisco SD-WAN offers a centralized, cloud-managed fabric which offers consistent policy enforcement from the branch to the cloud.

Cisco SD-WAN security capabilities include:

- Enterprise firewall with application aware access control, intrusion prevention, and stateful inspection
- Advanced malware protection, DNS-layer enforcement, and URL filtering
- End-to-end segmentation to eliminate broad propagation
- Zero-trust authentication and encryption
- Secure Internet Gateway protecting data sent to and from the cloud

Cisco provides a full suite of network security capabilities integrated with the SD-WAN management framework. See Figure 4.

Figure 4



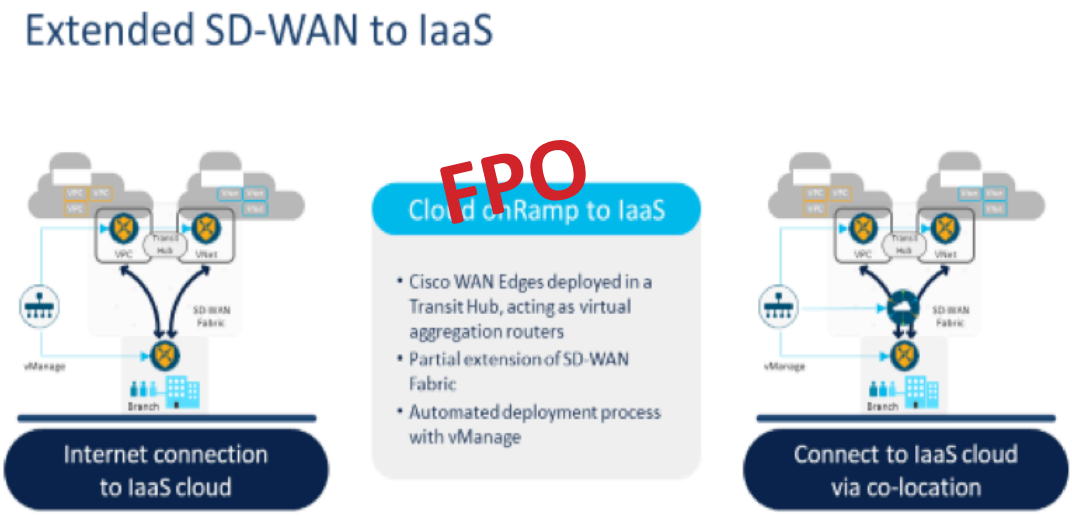
Cisco SD-WAN provides automated, high performance connections to leading cloud (IaaS) platform. Its cloud connectivity capabilities include:

- Integrated and automated connections with AWS and Azure
- Virtual deployment of SD-WAN at the cloud edge
- Network traffic visibility and telemetry across branch, edge and cloud
- Network segmentation and security policy application end-to-end

In addition, Cisco has a partnership with Equinix for co-location of the Cisco SD-WAN fabric which enables customers to dynamically add bandwidth with low-latency, private, virtual connections to the cloud. Cisco offers a unified management dashboard for branch, co-location, cloud and security policy. See Figure 5.

Figure 5

Cisco SD-WAN to IaaS Connectivity



Conclusions and Recommendations for Enterprise Customers

SD-WAN manages the on ramp to cloud-based applications. IT organizations needs tools to control and troubleshoot applications/data resident in IaaS environments. As each IaaS cloud has implemented its own networking and security protocols, IT can benefit from an architecture which abstracts the unique complicity of the cloud. SD-WAN technology can provide increased automation of manual IaaS application deployment, provide visibility and control over data in motion and a consistency operations environment regardless of the number of IaaS providers.

In a multicloud environment, the SD-WAN platform is essential to provide secure, reliable, low-latency access to data and applications. Unified security and policy management must be applied from the branch to the edge of the cloud. Many organizations will benefit from a hybrid model with both on premise and cloud-based security. These security capabilities should include data loss prevention (identification of user, device and location accessing specific data), and the ability inspect encrypted traffic.

Organizations require a flexible WAN architecture with the ability to apply network and security intelligence at the branch, a co-location facility, their data centers and directly at the cloud. Network security, including advanced firewalls, encryption, advanced threat mitigation and segmentation, should be integral to the WAN solution. Both WAN and network security must be managed centrally and be designed for operational simplicity.

Meet the Author

Lee Doyle is Principal Analyst at Doyle Research, *providing client focused targeted analysis on the Evolution of Intelligent Networks. He has over 25 years' experience analyzing the IT, network, and telecom markets. Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies, and IT-Telecom convergence. Before founding Doyle Research, Lee was Group VP for Network, Telecom, and Security research at IDC. Lee contributes to such industry periodicals as Network World, Fierce, and Tech Target. Lee holds a B.A. in Economics from Williams College.*