MPLS, SD-WAN, Internet, and Cloud Network

Understanding the Trade-offs for Your Next Generation WAN

CATO NETWORKS

Executive Summary

The Wide Area Network (WAN) is the backbone of the business. It ties together the remote locations, headquarters and data centers into an integrated network. Yet, the role of the WAN has evolved in recent years. Beyond physical locations, we now need to provide optimized and secure access to cloud-based resources for a global and mobile workforce. The existing WAN optimization and security solutions, designed for physical locations and point-to-point architectures, are stretched to support this transformation.

This paper discusses the different connectivity, optimization and security options for the 'Next Generation WAN' (NG-WAN). The NG-WAN calls for a new architecture to extend the WAN to incorporate the dynamics of cloud and mobility, where the traditional network perimeter is all but gone.

The Wide Area Network (WAN) connects all business locations into a single operating network. Traditionally, WAN design had to consider the secure connectivity of remote offices to a headquarters or a data center which hosted the enterprise applications and databases.

Let's look at evolution of the WAN.

First Generation: **Legacy WAN Connectivity**

Currently, there are 2 WAN connectivity options which offer a basic trade off between cost, availability and latency:

Option 1: **MPLS**

SLA-backed Service at Premium Price

With MPLS, a telecommunication provider provisions two or more business locations with a managed connection and routes traffic between these locations over their private backbone. In theory, since the traffic does not traverse the internet, encryption is optional. Because the connection is managed by the telco, end to end, it can commit to availability and latency SLAs. This commitment is expensive and is priced by bandwidth. Enterprises choose MPLS if they need to support applications with stringent up-time requirements and minimal quality of service (such as Voice over IP (VOIP).

To maximize the usage of MPLS links, WAN optimization equipment is deployed at each end of the line, to prioritize and reduce different types of application traffic. The effectiveness of such optimizations is protocol and application specific (for example, compressed streams benefit less from WAN optimization).

Latency	Availability	Price
👍 Low	👍 High	👎 High

Option 2: **Internet**

Best Effort Service at a Discounted Price

Internet connection procured from the ISP, typically offers nearly unlimited last mile capacity for a low monthly price. An unmanaged internet connection doesn't have the high availability and low-latency benefits of MPLS but it is inexpensive and quick to deploy. IT establishes an encrypted VPN tunnel between the branch office firewall and the headquarters/data center firewall. The connection itself is going through the internet, with no guarantee of service levels because it is not possible to control the number of carriers or the number of hops a packet has to cross. This can cause unpredictable application behavior due to increased latency and packet loss.

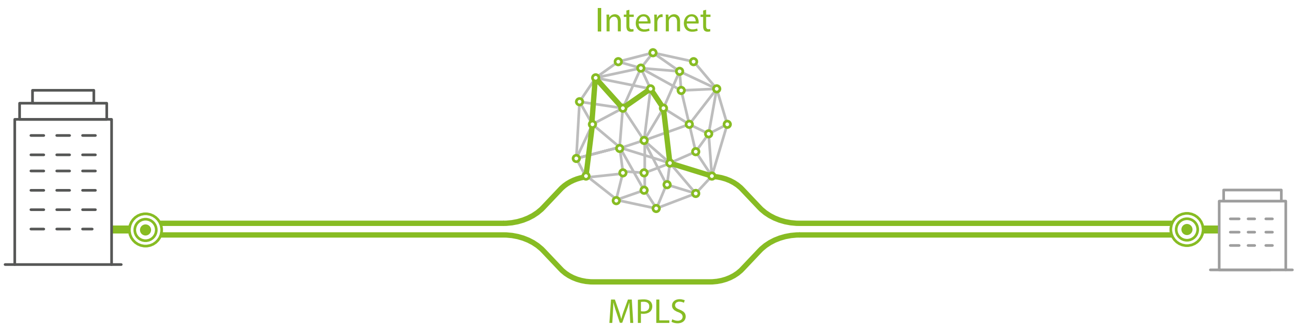
Internet-based connectivity forces customers to deploy and manage branch office security equipment.

Latency	Availability	Price
👎 Unknown	👎 Low	👍 Low

Second Generation: **Appliance-based SD-WAN**

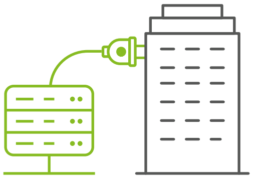
The cost/performance trade off between internet and MPLS, gave rise to SD-WAN. SD-WAN is using both MPLS and internet links to handle WAN traffic. Latency sensitive apps are using the MPLS links, while the rest of the traffic is using the internet link. The challenge customers face is to dynamically assign application traffic to the appropriate link.

SD-WAN: **Augmenting MPLS with Internet Links**



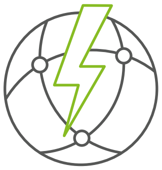
SD-WAN solutions offer the management capabilities to direct the relevant traffic according to its required class of service, offloading MPLS links and delaying the need to upgrade capacity. SD-WAN solutions, however, are limited in a few key aspects:

Footprint



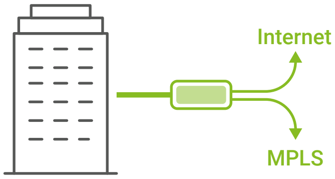
Similar to WAN optimization equipment, SD-WAN solutions must have a box deployed at each side of the link.

Connectivity



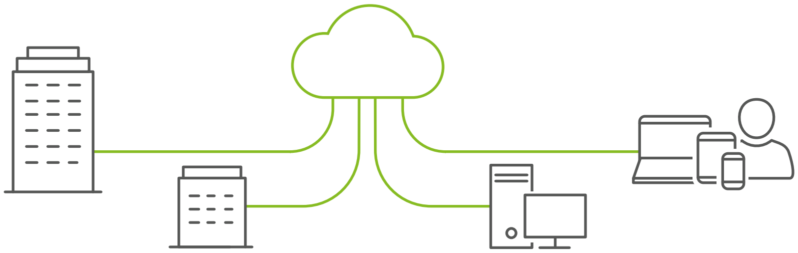
SD-WAN can’t replace the MPLS link because its internet “leg” is exposed to the unpredictable nature of an unmanaged internet connection (namely, its unpredictable latency, packet drops and availability).

Deployment



SD-WAN, like the other WAN connectivity options, is agnostic to the increased role of internet, cloud and mobility within the enterprise network. It focuses, for the most part on optimizing the legacy, physical WAN.

Third Generation: **A Cloud-based, Secure SD-WAN**



With the rapid migration to cloud applications (e.g., Office 365), cloud infrastructure (e.g. Amazon AWS) and a mobile workforce, the classic WAN architecture is severely challenged. It is no longer sufficient to think in terms of physical locations being the heart of the business. Here is why:

Limited end to end link control for the cloud

With public cloud applications outside the control of IT, organizations can't rely on optimizations that require a box at both ends of each link. In addition, cloud infrastructure (servers and storage), introduces a new production environment that has its own connectivity and security requirements. Existing WAN and Security solutions don't naturally extend to the new cloud-based environments.

Limited service and control to mobile users

Securely accessing corporate resources requires, mobile users to connect to a branch or HQ firewall VPN which could be very far from their location. This causes user experience issues, and encourages compliance violations (for example, direct access to cloud services that bypasses corporate security policy). Ultimately, the mobile workforce is not effectively covered by the WAN.

The cloud-based, Secure SD-WAN is aiming to address these challenges. It is based on the following principles:

The perimeter moves to the cloud

The notorious dissolving perimeter is re-established in the cloud. The cloud delivers a managed WAN backbone with reduced latency and optimal routing. This ensures the required quality of service for both internal and cloud-based applications.

The cloud-based WAN is "democratic" and all-inclusive

All network elements plug into the cloud WAN with secure tunnels including physical locations, cloud resources and mobile users. This ensures all business elements are integral part of the network instead of being bolted on top of a legacy architecture.

Security is integrated into the network

Beyond securing the backbone itself, it is possible to directly secure all traffic (WAN and internet) that crosses the perimeter - without deploying distributed firewalls.

WAN Connectivity and Security Use Cases: **Options and Tradeoffs**

A: **Branch to HQ Connectivity**

MPLS

PROS

- ✓ Guaranteed SLA (latency, uptime)
- ✓ No need for a branch FW (if internet access isn't required)

CONS

- × High cost per Mbps
- × Long time to provision (weeks to months)
- × Limited global coverage (requires multiple carriers)
- × Performance impact with backhaul for internet access ("Trombone Effect")

Internet Link

PROS

- ✓ Low cost (vs. MPLS)
- ✓ Ad-hoc provisioning
- ✓ Ability to create Any site-to-any site mesh

CONS

- × No SLA for internet routing
- × Susceptible to unpredictable latency/packet loss
- × Requires branch Firewall (Capex, management/ support overhead)
- × Requires local ISP/connection contract

Appliance-based SD-WAN

PROS

- ✓ Dynamic link selection (MPLS or IPVPN)
- ✓ Reduce need to increase expensive MPLS capacity
- ✓ Redundancy/availability

CONS

- × MPLS is still a costly requirement because IPVPN link subject to unpredictable internet latency/line quality
- × Requires local ISP/connection contract
- × Requires branch Firewall or cloud-based Secure Web Gateway
- × Limited optimization for branch-to-cloud access

Cloud-based, Secure SD-WAN

PROS

- ✓ MPLS-like SLA-backed latency
- ✓ Multi-ISP/LTE support for last mile redundancy
- ✓ Automated secure office mesh
- ✓ No need to backhaul
- ✓ No need for branch Firewall

CONS

- × Require local ISP connection/contract (two for resiliency)

B: **Secure and Optimized Branch Access to the Internet/Cloud**

MPLS

PROS	CONS
✓ Direct connection to cloud service providers	✗ Expensive transport for internet traffic ✗ Slow time-to-upgrade ✗ Limited security access control to the internet/cloud (requires 3rd party point solutions)

Internet Link

PROS	CONS
✓ Secure direct access to the internet with branch Firewalls	✗ Requires to deploy and maintain branch Firewalls ✗ Limited security access control to the internet/cloud, often requiring a Cloud Access Security Broker (CASB)

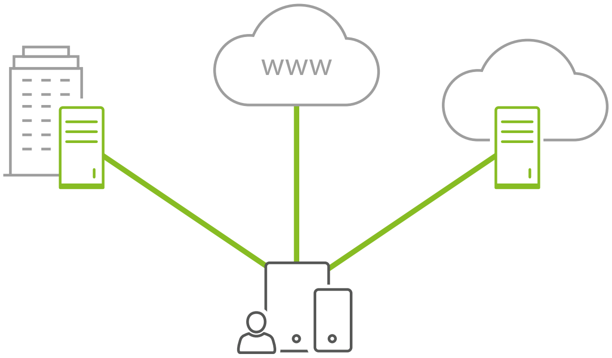
Appliance-based SD-WAN

PROS	CONS
✓ Secure and optimize cloud access with 3rd party partnerships	✗ Designed mostly for WAN connectivity and not as a cloud-focused optimization and security solution

Cloud-based, Secure SD-WAN

PROS	CONS
✓ No need for a branch Firewall ✓ Integrated Branch-to-cloud optimization, cloud access control ✓ One solution to handle both WAN, internet and cloud traffic	✗ Depends on a cloud security service availability

C: Secure and Optimized Mobile Access to WAN, Cloud and Internet



MPLS

PROS	CONS
Not Applicable	✗ Expensive transport for internet traffic ✗ Requires capacity upgrades

Internet Link

PROS	CONS
✓ Firewall/VPN-based access control	✗ User experience and productivity is impacted by the distance between user and Firewall/VPN ✗ Performance issues encourages compliance violations and direct access to the cloud

Appliance-based SD-WAN

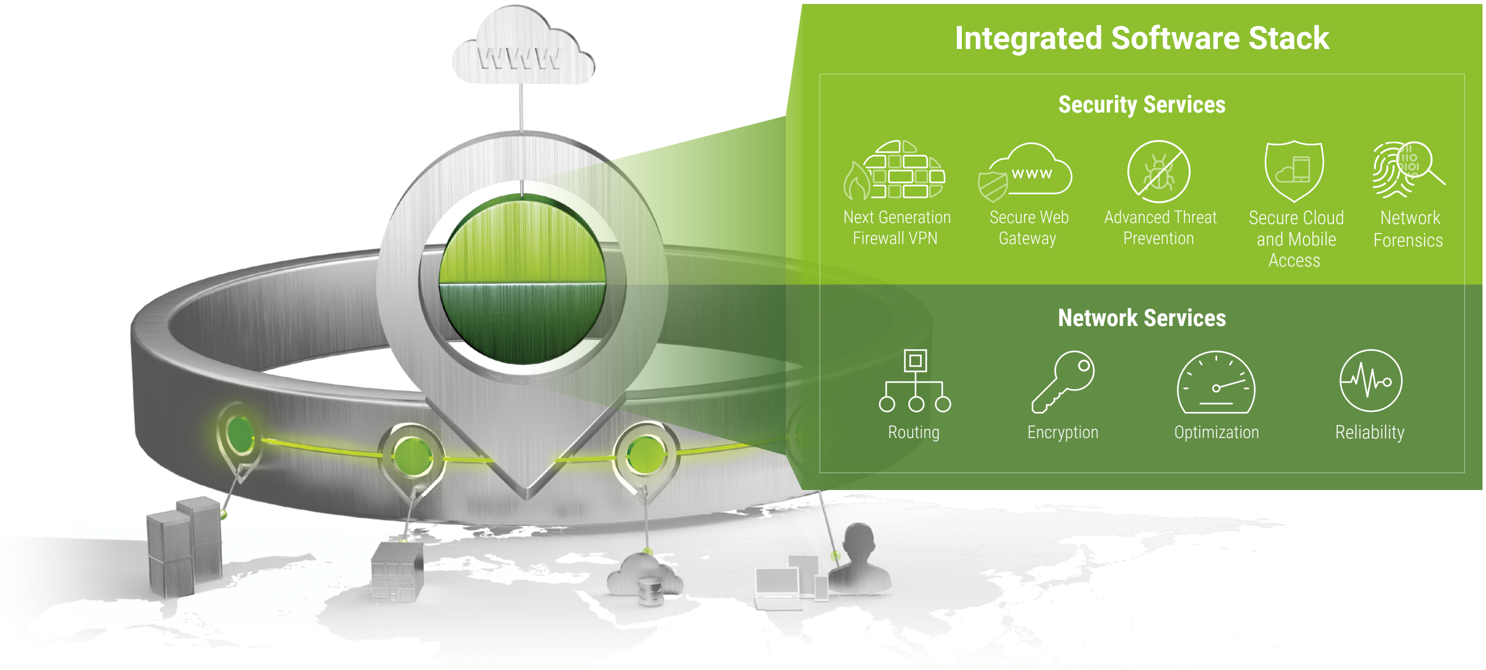
PROS	CONS
Not Applicable	✗ Mobile users are not covered from connectivity and security standpoints

Cloud-based, Secure SD-WAN

PROS	CONS
✓ Integrates mobile users to the enterprise WAN ✓ Provides optimized transport for end users to both WAN and cloud destinations ✓ Integrated security policy regardless of location or device	✗ Depends on cloud security service availability for enforcement

About Cato Networks

Cato Networks provides organizations with a software-defined and cloud-based secure enterprise network. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people and data. The Cato Cloud reduces MPLS connectivity costs, eliminates branch appliances, provides direct, secure internet access everywhere, and seamlessly integrates mobile users and cloud infrastructures to the enterprise network. Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, who previously cofounded Check Point Software Technologies and Imperva, and Gur Shatz, who previously cofounded Incapsula.



Cato Cloud Network

A global, encrypted and optimized network of PoPs interconnected with tier-1 carrier links with multi-gigabit capacity. Unlike unmanaged internet connections, this backbone provides an MPLS-like SLA-backed latency but at an affordable cost.

Cato Security Services

A full suite of enterprise-grade, agile and elastic network security services delivered from the cloud. The services have no capacity constraints and can seamlessly scale and upgrade in the background to introduce new capabilities and adapt to new threats in near real time.

For more information, visit **www.CatoNetworks.com** and Twitter: **@CatoNetworks.**