WHITE PAPER

The Security Edge: Why Choose Secure SD-WAN Over VPN?
In order to curb costs, enterprises have long relied on traditional VPNs for connecting remote locations and for turning up new applications. However, as enterprise requirements continue to evolve, VPN technology is becoming less appealing. The adoption of mobility, big data, social media, cloud and the Internet of Things is extending traditional enterprise perimeters, making them complex to secure and vulnerable to threats. Ironically, as new applications are added to distributed enterprise locations, the cost and complexity of adding more VPNs to secure them have escalated.

Data centers are evolving to protect their assets by embracing innovative, multi-layered security solutions. Meanwhile, the remote sites of distributed enterprises are left without the same security protections, rendering them the weak links in the enterprise security chain. Businesses are left to grapple with the tough question of how to extend data center-grade security to remote sites with limited IT staff and tight budgets.

Secure SD-WAN is purpose built to address these challenges by combining security and simplicity into an integrated solution. The power of secure SD-WAN lies in taking a defense-in-depth approach while simultaneously reducing the enterprise attack surface by logically segmenting the network on a per application basis. Moreover, this multi-layered security approach is delivered with the architectural simplicity, scalability, reliability and dramatic cost savings of a virtual overlay network.

Let's examine how traditional VPNs are failing to meet the challenges of distributed enterprises and why secure SD-WAN solutions are gaining broad market adoption.

Top 4 Challenges of Traditional Distributed Enterprise Connectivity

1. **Too Complex.** Connecting new locations and new applications is difficult. Each location may have multiple devices, different device configurations and various security requirements. Turning up a new location on a VPN requires knowledgeable IT staff to deploy, manage, troubleshoot and support.

2. **Too Inflexible.** Traditional infrastructures are rigid and require labor intensive efforts to support changing network conditions, especially when it comes to remote locations. For example, adapting to changing network needs, turning up new applications, or responding to new security threats (such as POS malware) must be executed quickly to ensure business continuity. Traditional networks are often too bulky to adapt in a timely manner.

3. **Too Insecure.** Multiple touch points for manual security configurations leave networks prone to misconfigurations or inconsistent configurations, opening them up to security risks. Traditional security approaches are falling short of the needs of today’s enterprise.

4. **Too Expensive.** Supporting the various point product solutions typically required for VPNs is costly. The capital expenditure for various point solution hardware, public IP addresses, and software continues to rise. Also the costs of qualified IT staff management required for supporting remote sites are growing.
Secure SD-WAN Addresses These Challenges without Disrupting Your Existing Network

As more and more applications are deployed to help run your business, a simple solution to securely connect them with minimal effort is needed. Secure Software Defined WAN (SD-WAN) is particularly well suited for this cause.

Cybera’s secure SD-WAN solutions greatly simplify enterprise networks and dramatically reduce both the capex and opex costs of managing enterprise WANs. They easily extend the multi-layered security defenses used in data centers to branch locations. Most importantly, secure SD-WAN allows mission-critical applications like payments and loyalty to co-exist with public applications like Wi-Fi on a single network while providing application-specific security and end-to-end network segmentation. These applications are segmented into their own dedicated logical networks, preventing them from intermingling with other application traffic on the network.

With Cybera’s secure SD-WAN solutions, these applications are connected in a cost-effective, scalable way without compromising security. This is a distinct benefit over VPNs, which gives an either/or scenario: either all traffic intermingles on one VPN, which is lower cost but very insecure; or all traffic can be segmented on separate VPNs, which requires more cost and complexity to maintain security.

Overview of Secure SD-WAN

Secure SD-WAN virtualizes the WAN so that all network intelligence is handled in software. For example, remote locations can be defined simultaneously and then kept perfectly in sync using centralized cloud-based policy administration inherent in SD-WAN connectivity models. This revolutionary architecture helps reduce expenses and complexity while increasing network flexibility. Best of all, it can be piloted in your network incrementally on a branch-by-branch basis, mitigating concerns about network disruption, and giving you a quick way to determine the return on your investment. Additional values of secure SD-WAN are provided below.
Benefits of Secure SD-WAN

**Reduced Complexity**
Distributed enterprises can be operationalized in minutes instead of months. Secure SD-WAN simplifies network setup with automatic provisioning and configuration from a central controller. The remote location will also receive network updates and changes automatically.

**Increased Agility**
Secure SD-WAN functionality allows for zero touch deployment, resulting in the rollout of network services “on demand”, supporting the needs of an agile business. For example, new cloud applications, such as POS and loyalty, can be rolled out quickly.

**Increased Security**
Logical network segmentation allows security policies to be enforced on a per application basis. By applying complete end-to-end segmentation of each application, exposure from any potential breach is limited to that single application. Just as importantly, the centralized virtual overlay approach of secure SD-WAN configurations eliminates the multiple manual configurations that open your network up to security risks. With secure SD-WAN, you can easily extend the multi-layered security approach used in data centers out to the edge of your network without highly skilled IT professionals at the branch.

**Proven Scalability**
Secure SD-WAN is designed with scalability in mind and provides the level of security and performance on demand network services need in large distributed enterprises. Policy changes, software updates, and new branch deployment are made simple and expedient without compromising network performance. It is precisely because of all these benefits at dramatically lower costs that multi-unit retailers and restaurants such as Blimpie, Cold Stone Creamery, Rocky Mountain Chocolate Factory, Shell and Kirkland’s have incorporated secure SD-WAN into their networks.

**Decreased Costs**
With secure SD-WAN virtualization, the cost of WAN infrastructure hardware, software, and support can be reduced by up to 79%1. The technology eliminates the need for multiple, dedicated premise devices by integrating functionality, such as Wi-Fi, wireless back-up, firewall and intrusion detection/prevention in one solution.

Get Started Connecting Your Distributed Enterprise in a Simple Way

- Develop a data connectivity and security program for your remote locations
  - Be proactive about protecting your environment
  - Engage key stakeholders to ensure a holistic approach
- Pilot a secure SD-WAN solution
  - Roll-out incrementally on a branch-by-branch basis
  - Avoid disrupting your existing architecture and minimize risk
Cybera can help.

Contact us at www.cybera.net/company/contact
Or visit www.cybera.net to learn more.

Sources:
1 http://www.cybera.net/resources/whitepapers.html - Replacing Complex Internet VPN Networks